DIVISION BY 2 ON HYPERELLPTIC CURVES AND JACOBIANS

YURI G. ZARHIN

1. Introduction

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

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

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

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 genus $g$ hyperelliptic curve over $K$ with precisely one infinite point, which we denote by $\infty$. In other words,

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

Clearly, $x$ and $y$ are nonconstant rational functions on $C$, 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 $\sum_{i=1}^{2g+1} (2\mathcal{W}_i)$ where

$$\mathcal{W}_i = (\alpha_i, 0) \in C(K) \; \forall i = 1, \ldots , 2g + 1.$$

We write $\iota$ for the hyperelliptic involution

$$\iota : C \to C, \; (x, y) \mapsto (x, -y), \; \infty \mapsto \infty.$$

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

We write $J$ for the jacobian of $C$, which is a $g$-dimensional abelian variety over $K$. If $D$ is a degree zero divisor on $C$ then we write $\text{cl}(D)$ for its linear equivalence class, which is viewed as an element of $J(K)$. We will identify $C$ with its image in $J$ with respect to the canonical regular map $C \hookrightarrow J$ under which $\infty$ goes to the zero of group law on $J$. In other words, a point $P \in C(K)$ is identified with $\text{cl}((P) - (\infty)) \in J(K)$. Then the action of $\iota$ on $C(K) \subset J(K)$ coincides with
multiplication by $-1$ on $J(K)$. In particular, the list of points of order $2$ on $C$ consists of all $\mathfrak{M}_i$.

Recall [21, Sect. 13.2, p. 411] that if $D$ is an effective divisor of (nonnegative) degree $m$, whose support does not contain $\infty$, then the degree zero divisor $D - m(\infty)$ is called semi-reduced if it enjoys the following properties.

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

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

It is known ([9, Ch. 3a], [21, Sect. 13.2, Prop. 3.6 on p. 413]) that for each $a \in J(K)$ there exist exactly one nonnegative $m$ and (effective) degree $m$ divisor $D$ such that the degree zero divisor $D - m(\infty)$ is reduced and $\text{cl}(D - m(\infty)) = a$. (E.g., the zero divisor with $m = 0$ corresponds to $a = 0$.) If $m \geq 1$, $D = \sum_{j=1}^{m} (Q_j)$ where $Q_j = (b_j, c_j) \in C(K) \forall j = 1, \ldots, m$ (here $Q_j$ do not have to be distinct) then the corresponding

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

The Mumford’s representation ([9, Sect. 3.12], [21, Sect. 13.2, pp. 411–415, especially, Prop. 13.4, Th. 13.5 and Th. 13.7] of $a \in J(K)$ is is the pair $(U(x), V(x))$ of polynomials $U(x), V(x) \in K[x]$ such that

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

is a degree $r$ monic polynomial while $V(x)$ has degree $m < \deg(U)$, the polynomial $V(x)^2 - f(x)$ is divisible by $U(x)$, and $D - m(\infty)$ coincides with the gcd (i.e., with the minimum) of the divisors of rational functions $U(x)$ and $y - V(x)$ on $C$. This implies that each $Q_j$ is a zero of $y - V(x)$, i.e.,

$$b_j = V(a_j), \ Q_j = (a_j, V(a_j)) \in C(K) \forall j = 1, \ldots, m.$$  

Such a pair always exists, it is unique, and (as we’ve just seen) uniquely determines not only $a$ but also divisors $D$ and $D - m(\infty)$. (The case $\alpha = 0$ corresponds to $m = 0, D = 0$ and the pair $(U(x) = 1, V(x) = 0)$.)

Conversely, if $U(x)$ is a monic polynomial of degree $m \leq g$ 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 $a = \text{cl}(D - m(\infty))$ where $D - m(\infty)$ is a reduced divisor such that $(U(x), V(x))$ is the Mumford’s representation of $\text{cl}(D - m(\infty))$.

Let $P = (a, b)$ be a $K$-point on $C$, i.e.,

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

The aim of this note is to divide explicitly $P$ by 2 in $J(K)$, i.e., to give explicit formulas for the Mumford’s representation of all $2^{2g}$ divisor classes $\text{cl}(D - g(\infty))$ such that $2D + \iota(P)$ is linearly equivalent to $(2g + 1)\infty$, i.e.,

$$2\text{cl}(D - g(\infty)) = P \in C(K) \subset J(K).$$
(It turns out that each such $D$ has degree $g$ and its support does not contain any of $\mathcal{G}_1$.)

The paper is organized as follows. In Section 2 we obtain auxiliary results about divisors on hyperelliptic curves. In particular, we prove (Theorem 2.4) that if $g > 1$ then the only point of $\mathcal{C}(K)$ that is divisible by two in $\mathcal{C}(K)$ (rather than in $J(K)$) is $\infty$ (of course, if $g > 1$). We also prove that $\mathcal{C}(K)$ does not contain points of order $n$ if $2 < n \leq 2g$. In Section 3 we describe explicitly for a given $P = (a, b) \in \mathcal{C}(K)$ the Mumford’s representation of $2^g$ divisor classes $\text{cl}(D - g(\infty))$ such that $D$ is an effective degree $g$ reduced divisor on $\mathcal{C}$ and

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

The description is given in terms of square roots $\sqrt{a - \alpha_i}$’s ($1 \leq i \leq 2g + 1$), whose product is $-b$. (There are exactly $2^{2g}$ choices of such square roots.) In Section 4 we discuss the rationality questions, i.e., the case when $f(x), \mathcal{C}, J$ and $P$ are defined over a subfield $K_0$ of $K$ and ask when dividing $P$ by 2 we get a point of $J(K_0)$.

Sections 5 and 6 deal with torsion points on certain naturally arised subvarieties of $J$ containing $\mathcal{C}$. In particular, we discuss the case of a generic hyperelliptic curve in characteristic zero, using as a starting point results of B. Poonen - M. Stoll [11] and of J. Yelton [22]. Our approach is based on ideas of J.-P. Serre [17] and F. Bogomolov [4].

This paper is a follow up of [24, 3] where the (more elementary) case of elliptic curves is discussed.

Acknowledgements. I am deeply grateful to Bjorn Poonen for helpful stimulating discussions. This work was partially supported by a grant from the Simons Foundation (#246625 to Yuri Zarkhin). I’ve started to write this paper during my stay in May-June 2016 at the Max-Planck-Institut für Mathematik (Bonn, Germany), whose hospitality and support are gratefully acknowledged.

2. Divisors on hyperelliptic curves

Lemma 2.1 (Key Lemma). Let $D$ be an effective divisor on $\mathcal{C}$ of degree $m > 0$ such that $m \leq 2g + 1$ and supp$(D)$ does not contain $\infty$. 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$(v) \leq g$.
   (ii) If $\mathcal{G}_1$ lies in supp$(D)$ then it appears in $D$ with multiplicity 1.
   (iii) If $b$ is a nonzero element of $K$ and a $K$-point $P = (a, b) \in \mathcal{C}(K)$ lies in supp$(D)$ then $v(P) = (a, -b)$ does not lie in 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 $v(x)$ coincides with $D - m(\infty)$. In particular, every point $Q \in \mathcal{C}(K)$ appears in $D - m(\infty)$ with the same multiplicity as $v(Q)$.

Proof. Let $h$ be a rational function on $\mathcal{C}$, whose divisor coincides with $D - m(\infty)$. Since $\infty$ is the only pole of $h$, the function $h$ is a polynomial in $x, y$ and therefore may be presented as

$$h = s(x)y - v(x), \text{ with } u, v \in K[x].$$
If $s = 0$ then $h$ has at $\infty$ the pole of even order $2\deg(v)$ and therefore $m = 2\deg(v)$.

Suppose that $s \neq 0$. Clearly, $s(x)y$ has at $\infty$ the pole of odd order $2\deg(s) + (2g+1) \geq (2g+1)$. 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 $\max(2\deg(s) + (2g+1), 2\deg(v)) \geq 2g + 1$. This implies that $m = 2g + 1$; in particular, $m$ is even. It follows that $m$ is even if and only if $s(x) = 0$, i.e., $h = -v(x)$; in addition, $\deg(v) \leq (2g+1)/2$, i.e., $\deg(v) \leq g$. 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 $m \leq 2g + 1$, 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 $\deg(v) \leq g$. 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 (i). (The uniqueness of $v$ is obvious.) The assertion (ii) is contained in Proposition 13.2(b) on pp. 409-10 of [21]. In order to prove (iii), we just follow arguments on p. 410 of [21] (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, $b \neq 0$, $v(a) = b \neq 0$ and $y - v(x)$ takes on at $i(P) = (a, -b)$ the value $-b - v(a) = -2b \neq 0$. This implies that $i(P)$ is not a zero of $y - v(x)$, i.e., $i(P)$ does not lie in $\text{supp}(D)$. \qed

Remark 2.2. Lemma 2.1(1)(ii,iii) asserts that if $m$ is odd the divisor $D - m(\infty)$ is semi-reduced. See [21, the penultimate paragraph on p. 411].

Corollary 2.3. Let $P = (a, b)$ be a $K$-point on $C$ and $D$ an effective divisor on $C$ such that $m = \deg(D) \leq g$ and $\text{supp}(D)$ does not contain $\infty$. 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 $\deg(v) \leq g$ and the divisor of $y - v_D(x)$ coincides with $2D + \iota(P) -(2g + 1)(\infty)$. In particular, $-b = v(a)$.

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

1. none of $\mathfrak{W}_i$ lies in $\text{supp}(D)$;
2. $D - g(\infty)$ is reduced.

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

Proof. One has only to apply Lemma 2.1 to the divisor $2D + \iota(P)$ of odd degree $2m+1 \leq 2g+1$ and notice that $\iota(P) = (a, -b)$ is a zero of $y - v(x)$ while $\iota(\mathfrak{W}_i) = \mathfrak{W}_i$ for all $i = 1, \ldots, 2g + 1$. \qed

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

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

It is well known that $\Theta_d$ is a closed $d$-dimensional subvariety of $J$ that coincides with $C$ for $d = 1$ and with $J$ if $d \geq g$; in addition, $\Theta_d \subset \Theta_{d+1}$ for all $d$. 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 2.4. Suppose that \( g > 1 \) and let
\[
C_{1/2} := 2^{-1}C \subset J
\]
be the preimage of \( C \) with respect to multiplication by 2 in \( J \). Then the intersection of \( C_{1/2}(K) \) and \( \Theta \) consists of points of order dividing 2 on \( J \). In particular, the intersection of \( C \) and \( C_{1/2} \) consists of \( \infty \) and all \( \mathcal{M}_i \)'s.

Proof. Suppose that \( m \leq g - 1 \) is a positive integer and we have \( m \) (not necessarily distinct) points \( Q_1, \ldots, Q_m \) of \( C(K) \) and a point \( P \in C(K) \) 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 \( \infty \) (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 \( C \). The equality in \( J \) means that the divisors \( 2[D - m(\infty)] \) and \( (P) - (\infty) \) on \( C \) are linearly equivalent. This means that the divisor \( 2D + (\iota(P)) - (2m + 1)(\infty) \) is principal. Now Corollary 2.3 tells us that \( m = g \), which is not the case. The obtained contradiction proves that the intersection of \( C_{1/2} \) and \( \Theta \) consists of points of order 2 and 1.

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

Remark 2.5. It is known [16, Ch. VI, last paragraph of Sect. 11, p. 122] that the curve \( C_{1/2} \) is irreducible. (Its projectiveness and smoothness follow readily from the projectiveness and smoothness of \( C \) and the ´etaleness of multiplication by 2 in \( J \).) See [7] for an explicit description of equations that cut out \( C_{1/2} \) in a projective space.

Corollary 2.6. Suppose that \( g > 1 \). Let \( n \) an integer such that \( 3 \leq n \leq 2g \). Then \( C(K) \) does not contain a point of order \( n \) in \( J(K) \). In particular, \( C(K) \) does not contain points of order 3 or 4.

Proof. Suppose that such a point say, \( P \) exists. Clearly, \( P \) is neither \( \infty \) nor one of \( \mathcal{M}_i \), i.e., \( P \neq \iota(P) \).

Suppose that \( n \) is odd. Then we have \( n = 2m + 1 \) with \( 1 \leq m < g \). This implies that \( mP \in \Theta \) and
\[
2(mP) = 2mP = -P = \iota(P) \in C(K).
\]
It follows from Theorem 2.4 that either \( mP = 0 \) in \( J(K) \) or \( (2m)P = (2mP) = 0 \) in \( J(K) \). However, the order of \( P \) in \( J(K) \) is \( n = 2m + 1 > m \geq 1 \) and we get a desired contradiction.

Assume now that \( n \) is even. Then we have \( n = 2m \) with \( 1 \leq m \leq g \). Then \( mP \) has order 2 in \( J(K) \). It follows that
\[
mP = -mP = m(-P) = m \iota(P).
\]
This means that the degree zero divisors \( mP - m(\infty) \) and \( m(\iota(P)) - m(\infty) \) belong to the same linear equivalence class. Since both divisors are reduced, they must...
coincide (see [21, Ch. 13, Prop. 13.6 on p. 413]). This implies that \( P = \iota(P) \), which is not the case and we get a desired contradiction. \( \square \)

**Remark 2.7.** If \( \text{char}(K) = 0 \) 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 [12]. Using a \( p \)-adic approach, B. Poonen [10] developed and implemented an algorithm that finds all complex torsion points on genus 2 hyperelliptic curves \( C : y^2 = f(x) \) such that \( f(x) \) has rational coefficients. (See also [11].)

**Theorem 2.8.** Suppose that \( g > 1 \) and let \( N > 1 \) be a positive integer. Suppose that \( N \leq 2g - 1 \) and let us put

\[
d(N) = \left\lceil \frac{2g}{N + 1} \right\rceil.
\]

Let \( K_0 \) be a subfield of \( K \) such that \( f(x) \in K_0[x] \). Let \( a \) be a \( K \)-point on \( \Theta_{d(N)} \). Suppose that there is a field automorphism \( \sigma \in \text{Aut}(K/K_0) \) such that \( \sigma(a) = N\overline{a} \) or \( -N\overline{a} \). Then \( a \) has order 1 or 2 in \( J(K) \).

**Proof.** Clearly, \( (N + 1) \cdot d(N) < 2g + 1 \). Let us assume that \( 2a \neq 0 \) in \( J(K) \). We need to arrive to a contradiction. Then there is a positive integer \( r \leq d(N) \) and a sequence of points \( P_1, \ldots, P_r \) of \( C(K) \setminus \infty \) such that \( \tilde{D} := \sum_{j=1}^r (P_j) - r(\infty) \) is the Mumford’s representation of \( a \) while (say) \( P_1 \) does not coincide with any of \( W_i \) (here we use the assumption that \( 2a \neq 0 \)); we may also assume that \( P_1 \) has the largest multiplicity say, \( M \) among \( \{P_1, \ldots, P_r\} \). (In particular, none of \( P_j \)’s coincides with \( \iota(P_1) \).) Then \( \sigma(\tilde{D}) = \sum_{j=1}^r (\sigma(P_j)) - r(\infty) \) is the Mumford’s representation of \( \sigma a \). In particular, the multiplicity of each \( \sigma(P_j) \) in \( \sigma(\tilde{D}) \) does not exceed \( M \); similarly, the multiplicity of each \( \iota\sigma(P_j) \) in \( \iota\sigma(\tilde{D}) \) does not exceed \( M \).

Suppose that \( \sigma(a) = N\overline{a} \).

\[
N\tilde{D} + \iota\sigma(\tilde{D}) = N \left\lceil \sum_{j=1}^r (P_j) \right\rceil + \left\lceil \sum_{j=1}^r (\iota\sigma(P_j)) \right\rceil - r(N + 1)(\infty)
\]

is a principal divisor on \( C \). Since \( m := r(N + 1) \leq (N + 1) \cdot d(N) < 2g + 1 \), we are in position to apply Lemma 2.1, 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 \( N\tilde{D} + \iota\sigma(\tilde{D}) \). This implies that a point \( Q \in C(K) \) appears in \( N\tilde{D} + \iota\sigma(\tilde{D}) \) with the same multiplicity as \( uQ \). It follows that \( \iota P_1 \) is (at least) one of \( \iota\sigma(P_j) \)’s. Clearly, the multiplicity of \( P_1 \) in \( N\tilde{D} + \iota\sigma(\tilde{D}) \) is, at least, \( NM \) while the multiplicity of \( \iota(P_1) \) is, at most, \( M \). This implies that \( NM \leq M \). Taking into account that \( N > 1 \), we obtain the desired contradiction.

If \( \sigma(a) = -N\overline{a} \) then literally the same arguments applied to to the principal divisor

\[
N\tilde{D} + \sigma(\tilde{D}) = N \left\lceil \sum_{j=1}^r (P_j) \right\rceil + \left\lceil \sum_{j=1}^r (\sigma(P_j)) \right\rceil - r(N + 1)(\infty)
\]

also lead to the contradiction. \( \square \)
3. Division by 2

Suppose we are given a point 

\[ P = (a, b) \in C(K) \subseteq J(K). \]

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

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

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

\[ D = D(a) \]  

of positive degree \( m \) on \( C \) such that \( \text{supp}(D) \) does not contain \( \infty \), 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, thanks to Corollary 2.3, \( m = g \) and \( \text{supp}(D) \) does not contain \( W_i \). (In addition, \( D - g(\infty) \) is reduced.) Then the degree \( g \) effective divisor 

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

with \( Q_i = (c_j, d_j) \in C(K) \). Since none of \( Q_j \) coincides with any of \( W_i \),

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

By Corollary 2.3, 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 \( y - v_D(x) \),

\[ b = -v_D(a), \quad d_j = v_D(c_j) \quad \forall j = 1, \ldots, g. \]

It follows from Proposition 13.2 on pp. 409–410 of [21] 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, \( f(x) - v_D(x)^2 \) is divisible by

\[ u_D(x) := \prod_{j=1}^{g} (x - c_j). \]  

**Remark 3.1.** Summing up:

\[ D = D(a) = \sum_{j=1}^{g} (Q_j), \quad Q_j = (c_j, v_D(c_j)) \quad \forall j = 1, \ldots, g \]

and the degree monic polynomial \( u_D(x) = \prod_{j=1}^{g} (x - c_j) \) divides \( f(x) - v_D(x)^2 \).

By Prop. 13.4 on p. 412 of [21], this implies that reduced \( D - g(\infty) \) coincides with the gcd of the divisors of \( u_D(x) \) and \( y - v_D(x) \). Therefore the pair \( (u_D, v_D) \) is the Mumford’s 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, if we replace \( v_D(x) \) by its remainder with respect to the division by \( u_D(x) \) then we get the Mumford’s representation of \( a \) (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.,

\[
v_D(\alpha_i)^2 = (a - \alpha_i) \left( \prod_{j=1}^{g} (c_j - \alpha_i) \right)^2 \quad \forall \ i = 1, \ldots, 2g + 1.
\]

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

\[
r_i = r_{i,D} := \frac{v_D(\alpha_i)}{\prod_{j=1}^{g} (c_j - \alpha_i)} \quad (5)
\]

with

\[
r_i^2 = a - \alpha_i \quad \forall \ i = 1, \ldots, 2g + 1 \quad (6)
\]

and

\[
\alpha_i = a - r_i^2, \quad c_j - \alpha_i = r_i^2 - a + c_j \quad \forall \ i = 1, \ldots, 2g + 1; \ j = 1, \ldots, g.
\]

Clearly, all \( r_i \)'s 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

\[
\prod_{i=1}^{2g+1} r_i = \pm b, \quad (7)
\]
because

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

Now we get

\[
r_i = \frac{v_D(a - r_i^2)}{\prod_{j=1}^{g} (r_i^2 - a + c_j)}
\]
i.e.,

\[
r_i \prod_{j=1}^{g} (r_i^2 - a + c_j) - v_D(a - r_i^2) = 0 \quad \forall \ i = 1, \ldots, 2g + 1.
\]

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

\[
h_r(t) := t \prod_{j=1}^{g} (t^2 - a + c_j) - v(a - t^2)
\]
has \((2g + 1)\) distinct roots \( r_1, \ldots, r_{2g+1} \). This means that

\[
h_r(t) = \prod_{i=1}^{2g+1} (t - r_i).
\]
Clearly, \( t \prod_{j=1}^{2g+1} (t^2 - a + c_j) \) coincides with the odd part of \( h_r(t) \) while \( -v_D(a - t^2) \) coincides with the even part of \( h_r(t) \). 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.,

\[
\prod_{i=1}^{2g+1} r_i = -b. \quad (9)
\]

Let us define

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

Since

\[ s_i(r) = s_i(r_1, \ldots, r_{2g+1}) \]

is the \( i \)th basic symmetric function in \( r_1, \ldots, r_{2g+1} \),

\[ h_r(t) = t^{2g+1} + \sum_{i=1}^{2g+1} (-1)^i s_i(r) t^{2g+1-i} = \left[ t^{2g+1} + \sum_{i=1}^{2g} (-1)^i s_i(r) t^{2g+1-i} \right] + b. \]

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

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

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

This implies that

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

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

\[ U_r(t) := u_D(t) = \prod_{j=1}^{g} (t - c_j) \]

then

\[
U_r(t) = ( -1 )^g \left[ (a - t)^g + \sum_{j=1}^{g} s_{2j}(r)(a - t)^{g-j} \right]. \quad (11)
\]

Recall that \( \deg(v_D) \leq g \) and notice that the coefficient of \( v(x) \) at \( x^g \) is \( ( -1 )^g s_1(r) \). This implies that the polynomial

\[ V_r(t) := v_D(t) - ( -1 )^g s_1(r) U_r(t) = \]
formulas (11) and (12) give us an explicit construction of \( D \) square roots.

On the other hand, in light of (6)-(8), there is exactly the same number 2 of pairs \((u, v)\) such that \( u \) corresponds to an element of \( \mathbb{J}(K) \) and \( v \) corresponds to an element of \( \mathbb{J}(K) \). Theorem 3.2.

There is a natural bijection between \( \mathcal{R}_{1/2, P} \) and \( M_{1/2, P} \) such that \( \mathcal{R}_{1/2, P} \) corresponds to \( \mathcal{M}_{1/2, P} \) with Mumford’s representation \( (U_\mathcal{R}, V_\mathcal{R}) \). More explicitly, if \( \{c_1, \ldots, c_g\} \) is the list of \( g \) roots (with multiplicities) of \( U_\mathcal{R}(x) \) then \( \mathcal{R} \) corresponds to \( \alpha_\mathcal{R} = \text{cl}(D - g(\infty)) \in J(K), \ 2\alpha_\mathcal{R} = P \)

\[
\left[ \sum_{j=1}^{g} s_{2j-1}(r)(a - t)^{g-j+1} \right] - b - s_1(r) \left[ (a - t)^g + \sum_{j=1}^{g} s_{2j}(r)(a - t)^{g-j} \right] \quad (12)
\]

has degree < \( g \), i.e.,

\[
\text{deg}(V_\mathcal{R}) < \text{deg}(U_\mathcal{R}) = g.
\]

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

\[
d_j = v_D(c_j) = V_\mathcal{R}(c_j) \forall j = 1, \ldots, g,
\]

because \( U_\mathcal{R}(x) \) divides \( v_D(x) - V_\mathcal{R}(x) \) and vanishes at all \( b_j \). Actually, \( \{b_1, \ldots, b_g\} \) is the list of all roots (with multiplicities) of \( U_\mathcal{R}(x) \). So,

\[
D = D(a) = \sum_{j=1}^{g} (Q_j), \quad Q_j = (c_j, v_D(c_j)) = (c_j, V_\mathcal{R}(c_j)) \forall j = 1, \ldots, g.
\]

This implies (again via Prop. 13.4 on p. 412 of [21]) that reduced \( D - g(\infty) \) coincides with the gcd of the divisors of \( U_\mathcal{R}(x) \) and \( y - V_\mathcal{R}(x) \). It follows that the pair \((U_\mathcal{R}(x), V_\mathcal{R}(x))\) is the Mumford’s representation of \( \text{cl}(D - g(\infty)) = a \). So, the formulas (11) and (12) give us an explicit construction of \( (D(a) \text{ and } a) \) in terms of \( r = (r_1, \ldots, r_{2g+1}) \) for each of \( 2^{2g} \) choices of \( a \) with \( 2a = P \in J(K) \). On the other hand, in light of (6)-(8), there is exactly the same number \( 2^{2g} \) of choices of square roots \( \sqrt{a - \alpha_i} \) \((1 \leq i \leq 2g)\), whose product is \( -b \). 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 \( a \in J(K) \) with \( 2a = P \) such that the corresponding \( r_i \) defined by (5) coincides with chosen \( \sqrt{a - \alpha_i} \) for all \( i = 1, \ldots, 2g + 1 \), and the Mumford’s representation \((U_\mathcal{R}(x), V_\mathcal{R}(x))\) for this \( a \) is given by explicit formulas (11)-(12). This gives us the following assertion.

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

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

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

\[
v_i = a - \alpha_i \quad \forall \ i = 1, \ldots, 2g + 1; \quad \prod_{i=1}^{2g+1} v_i = -b.
\]

Let \( s_i(r) \) be the \( i \)-th basic symmetric function in \( r_1, \ldots, r_{2g+1} \). Let us put

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

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

Then there is a natural bijection between \( \mathcal{R}_{1/2, P} \) and \( M_{1/2, P} \) such that \( \mathcal{R} \in \mathcal{R}_{1/2, P} \) corresponds to \( a_\mathcal{R} \in M_{1/2, P} \) with Mumford’s representation \( (U_\mathcal{R}, V_\mathcal{R}) \). More explicitly, if \( \{c_1, \ldots, c_g\} \) is the list of \( g \) roots (with multiplicities) of \( U_\mathcal{R}(x) \) then \( a_\mathcal{R} = \text{cl}(D - g(\infty)) \in J(K), \ 2a_\mathcal{R} = P \).
where the divisor

\[ D = D(a_r) = \sum_{j=1}^{g} (Q_j), \quad Q_j = (b_j, V_\xi(b_j)) \in \mathcal{C}(K) \ \forall \ j = 1, \ldots, g. \]

In addition, none of \( \alpha_i \) is a root of \( U_\xi(x) \) (i.e., the polynomials \( U_\xi(x) \) and \( f(x) \) are relatively prime) and

\[ \tau_i = s_1(\tau) + (-1)^g \frac{V_\xi(\alpha_i)}{U_\xi(\alpha_i)} \forall \ i = 1, \ldots, 2g + 1. \]

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

\[ \tau_i = (-1)^g \frac{v_D(a_r)(\alpha_i)}{u_D(a_r)(\alpha_i)} = (-1)^g \frac{v_D(a_r)(\alpha_i)}{U_\xi(\alpha_i)}. \]

It follows from (12) that

\[ v_D(a_r)(x) = (-1)^g s_1(\tau)U_\xi(x) + V_\xi(x). \]

This implies that

\[ \tau_i = (-1)^g \left( (-1)^g s_1(\tau)U_\xi(\alpha_i) + V_\xi(\alpha_i) \right) \frac{U_\xi(\alpha_i)}{U_\xi(\alpha_i)} = s_1(\tau) + (-1)^g \frac{V_\xi(\alpha_i)}{U_\xi(\alpha_i)}. \]

\[ \square \]

**Example 3.3.** Let us take as \( P = (a, b) \) the point \( \mathcal{M}_{2g+1} = (\alpha_{2g+1}, 0) \). Then \( b = 0 \) and \( \tau_{2g+1} = 0 \). We have 2g arbitrary independent choices of (nonzero) square roots \( \tau_j = \sqrt{\alpha_{2g+1}} - \alpha_j \) with \( 1 \leq j \leq 2g \) (and always get an element of \( \mathcal{R}_{1/2,p} \)). Now Theorem 3.2 gives us (if we put \( a = \alpha_{2j+1}, b = 0 \)) all \( 2^{2g} \) points \( \alpha_r \) of order 4 in \( J(K) \) with \( 2\alpha_r = \mathcal{M}_{2j+1} \).

4. **Rationality Questions**

Let \( K_0 \) be a subfield of \( K \) and \( K_0^{\text{sep}} \) its separable algebraic closure in \( K \). Recall that \( K_0^{\text{sep}} \) is separably closed. Clearly,

\[ \text{char}(K_0) = \text{char}(K_0^{\text{sep}}) = \text{char}(K) \neq 2. \]

Let us assume that \( f(x) \in K_0[x] \), i.e., all the coefficients of \( f(x) \) lie in \( K_0 \). However, we don’t make any additional assumptions about its roots \( \alpha_i \); still, all of them lie in \( K_0^{\text{sep}} \), because \( f(x) \) has no multiple roots. Recall that both \( \mathcal{C} \) and \( J \) are defined over \( K_0 \); the point \( \infty \in \mathcal{C}(K_0) \) and therefore the embedding \( \mathcal{C} \hookrightarrow J \) is defined over \( K_0 \); in particular, \( \mathcal{C} \) is a closed algebraic \( K_0 \)-subvariety of \( J \).

Let us assume that our \( K \)-point \( P = (a, b) \) of \( \mathcal{C} \) lies in \( \mathcal{C}(K_0^{\text{sep}}) \), i.e., \( a, b \in K_0^{\text{sep}} \) and

\[ P = (a, b) \in \mathcal{C}(K_0^{\text{sep}}) \subset J(K_0^{\text{sep}}) \subset J(K). \]

In the notation of Theorem 3.2, for each \( \tau \in M_{1/2,p} \) all its components \( \tau_i \) lie in \( K_0^{\text{sep}} \), because \( \tau_i^2 = a - \alpha_i \in K_0^{\text{sep}} \). This implies that the monic degree \( 2g + 1 \) polynomial

\[ h_\tau(t) = \prod_{i=1}^{2g+1} (t - \tau_i) = t^{2g+1} + \sum_{i=1}^{2g} (-1)^i s_i(\tau)t^{2g+1-i} \in K_0^{\text{sep}}[t], \]
i.e., all \( s_i(t) \in K_0^{\text{sep}} \). It follows immediately from the explicit formulas above that the Mumford representation \((U_\ell, V_\ell)\) of \( a_\ell = \text{cl}(D(a_\ell) - g(\infty)) \) consists of polynomials \( U_\ell \) and \( V_\ell \) with coefficients in \( K_0^{\text{sep}} \). In addition, \( a_\ell \) lies in \( J(K_0^{\text{sep}}) \), because \( 2a_\ell = P \in J(K_0^{\text{sep}}) \), the multiplication by 2 in \( J \) is an étale map and \( K_0^{\text{sep}} \) is separably closed.

**Lemma 4.1.** Suppose that either \( K_0 \) is a perfect field (e.g., \( \text{char}(K) = 0 \) or \( K_0 \) is finite) or \( \text{char}(K_0) > g \). Suppose that

\[
P = (a, b) \in \mathcal{C}(K_0^{\text{sep}}) \subset J(K_0^{\text{sep}}).
\]

Then for all \( \ell \in \mathfrak{R}_{1/2,P} \) the Mumford representation \((U_\ell, V_\ell)\) of \( a_\ell = \text{cl}(D(a_\ell) - g(\infty)) \) enjoys the following properties.

(i) The polynomial \( U_\ell(x) \) splits over \( K_0^{\text{sep}} \), i.e., all its roots \( b_j \) lie in \( K_0^{\text{sep}} \).

(ii) The divisor

\[
D = D(a_\ell) = \sum_{j=1}^{\text{deg}(U_\ell)} (Q_j)
\]

where

\[
Q_j = (c_j, V_\ell(c_j)) \in \mathcal{C}(K_0^{\text{sep}}) \quad \forall j = 1, \ldots, g.
\]

**Proof.** If \( K_0 \) is perfect then \( K_0^{\text{sep}} \) is algebraically closed and there is nothing to prove. So, we may assume that \( \text{char}(K_0^{\text{sep}}) = \text{char}(K_0) > g \). In order to prove (i), recall that \( \text{deg}(U_\ell) = g \). Every root \( c_j \) of \( U_\ell(x) \) lies in \( K \) and the algebraic field extension \( K_0^{\text{sep}}(b_j)/K_0^{\text{sep}} \) has finite degree that does not exceed

\[
\text{deg}(U_\ell) = g < \text{char}(K_0^{\text{sep}})
\]

and therefore this degree is not divisible by \( \text{char}(K_0^{\text{sep}}) \). This implies that the field extension \( K_0^{\text{sep}}(b_j)/K_0^{\text{sep}} \) is separable. Since \( K_0^{\text{sep}} \) is separably closed, the overfield \( K_0^{\text{sep}}(c_j) = K_0^{\text{sep}} \), i.e., \( c_j \) lies in \( K_0^{\text{sep}} \). This proves (i). As for (ii), since \( V_\ell(x) \in K_0^{\text{sep}} \) and all \( c_j \in K_0^{\text{sep}} \), we have \( V_\ell(c_j) \in K_0^{\text{sep}} \) and therefore \( Q_j = (c_j, V_\ell(c_j)) \in \mathcal{C}(K_0^{\text{sep}}) \). This proves (ii). \( \square \)

**Remark 4.2.** If \( g = 2 \) then the conditions of Lemma 4.1 do not impose any additional restrictions on \( K_0 \). (The case \( \text{char}(K) = 2 \) was excluded from the very beginning.)

**Remark 4.3.** If \( P = (a, b) \in \mathcal{C}(K_0) \) then for each \( \ell \in \mathfrak{R}_{1/2,P} \)

\[
s_{2g+1}(t) = (-1)^{2g+1} \prod_{i=1}^{2g+1} \frac{2g+1}{2g+1} t_i = - \prod_{i=1}^{2g+1} t_i = -(b) = b \in K_0.
\]

This observation (reminder) explains the omission of \( i = 2g + 1 \) in the following statement.

**Theorem 4.4.** Suppose that a point

\[
P = (a, b) \in \mathcal{C}(K_0) \subset J(K_0),
\]

i.e.,

\[
a, b \in K_0, \quad b^2 = f(a).
\]

If \( \ell \) is an element of \( \mathfrak{R}_{1/2,P} \) then \( a_\ell \) lies in \( J(K_0) \) if and only if \( h_\ell(t) \) lies in \( K_0[t] \), i.e.,

\[
s_i(t) \in K_0 \quad \forall i = 1, \ldots, 2g.
\]
Proof. Let \( \bar{K}_0 \) be the algebraic closure of \( K_0 \). Clearly, \( \bar{K}_0 \) is algebraically closed and

\[
K_0 \subset K_0^{\text{sep}} \subset \bar{K}_0 \subset K.
\]

In the course of the proof we may and will assume that \( K = \bar{K}_0 \).

Let \( r \) be an element of \( \mathfrak{P}_{1/2, \mathcal{P}} \). We know that \( a_r \in J(K_0^{\text{sep}}) \) and the corresponding polynomials \( U_r(x) \) and \( V_r(x) \) have coefficients in \( K_0^{\text{sep}} \). This means that there is a finite Galois field extension \( E/K_0 \) with Galois group \( \text{Gal}(E/K) \) such that

\[
K_0 \subset E \subset K_0^{\text{sep}}
\]

such that

\[
a_{rr} \in J(E); \quad U_r(x), V_r(x) \in E[x].
\]

Let \( \text{Aut}(K/K_0) \) be the group of all field automorphisms of \( K \) that leave invariant every element of \( K_0 \). Clearly, the (sub)field \( E \) is \( \text{Aut}(K/K_0) \)-stable and the natural (restriction) group homomorphism

\[
\text{Aut}(K/K_0) \to \text{Gal}(E/K_0)
\]

is surjective. Since the subfield \( E^{\text{Gal}(E/K_0)} \) of Galois invariants coincides with \( K_0 \), we conclude that the subfield of invariants \( E^{\text{Aut}(K/K_0)} \) also coincides with \( K_0 \). It follows that

\[
U_r(x), V_r(x) \in K_0[x].
\]

Taking into account that \( a, b \in K_0 \), we obtain from the formulas in Theorem 3.2 that

\[
s_i(r) \in K_0 \quad \forall \; i = 1, \ldots, 2g.
\]

Conversely, let us assume that for a certain \( r \in \mathfrak{P}_{1/2, \mathcal{P}} \)

\[
s_i(r) \in K_0 \quad \forall \; i = 1, \ldots, 2g.
\]

(We know that \( s_{2g+1}(r) \) also lies in \( K_0 \).) This implies that both \( U_r(x) \) and \( V_r(x) \) lie in \( K_0[x] \). In other words,

\[
\sigma U_r(x) = U_r(x), \quad \sigma V_r(x) = V_r(x) \quad \forall \; \sigma \in \text{Aut}(K/K_0).
\]

This means that for every \( \sigma \in \text{Aut}(K/K_0) \) both \( a_r \) and \( \sigma a_r \) have the same Mumford representation, namely, \( (U_r, V_r) \). This implies that

\[
\sigma a_r = a_r \quad \forall \; \sigma \in \text{Aut}(K/K_0),
\]

i.e.,

\[
a_r \in J(E)^{\text{Aut}(K/K_0)} = J(K_0).
\]

\( \square \)
Theorem 4.5. Suppose that a point
\[ P = (a, b) \in C(K_0) \subset J(K_0), \]
i.e.,
\[ a, b \in K_0, \quad b^2 = f(a). \]
Then the following conditions are equivalent.
(i) \( \alpha_i \in K_0 \) and \( a - \alpha_i \) is a square in \( K_0 \) for all \( i \) with \( 1 \leq i \leq 2g + 1 \).
(ii) All \( 2^{2g} \) elements \( a \in J(K) \) with \( 2a = P \) actually lie in \( J(K_0) \).

Proof. Assume (i). Then \( a = a_r \) for a certain \( r \in \mathfrak{R}_{1/2,p} \). Our assumptions imply that all \( \tau_i = \sqrt{a - \alpha_i} \) lie in \( K_0 \) and therefore
\[ s_i(t) \in K_0 \quad \forall \ i = 1, \ldots, 2g. \]
Now Theorem 4.4 tells us that \( a_r \in J(K_0) \). This proves (ii).
Assume (ii). It follows from Theorem 4.4 that \( s_i(t) \in K_0 \) for all \( r \in \mathfrak{R}_{1/2,p} \) and \( i \) with \( 1 \leq i \leq 2g + 1 \). In particular, for \( i = 1 \)
\[ \sum_{i=1}^{2g+1} r_i = s_1(t) \in K_0 \quad \forall \ r \in \mathfrak{R}_{1/2,p}. \]
Pick any \( r \in \mathfrak{R}_{1/2,p} \) and for any index \( l \) (\( 1 \leq l \leq 2j + 1 \)) consider \( r^{(l)} \in \mathfrak{R}_{1/2,p} \) such that
\[ r^{(l)} = r_i, \quad r^{(l)}_i = -r_i \quad \forall \ i \neq l. \]
We have
\[ s_1(t) \in K_0, \quad -2s_1(t) + 2r_i = s_1(t^{(l)}) \in K_0. \]
This implies that \( r_i \in K_0 \). Since \( r_i^2 = a - \alpha_i \) and \( a \in K_0 \), we conclude that \( \alpha_i \) lies in \( K_0 \) and \( a - \alpha_i \) is a square in \( K_0 \). This proves (i). \( \square \)

Remark 4.6. In the case of elliptic curves \( (i.e., \text{when } g = 1) \) Theorem 4.5 is well known, see, e.g., [5, p. 269–270].

The following assertion was inspired by results of Schaefer [14].

Theorem 4.7. Let us consider the \( (2g + 1) \)-dimensional commutative semisimple
\( K_0 \)-algebra \( L = K_0[x]/f(x)K_0[x] \).
A \( K_0 \)-point \( P = (a, b) \) on \( C \) is divisible by 2 in \( J(K_0) \) if and only if
\[ (a - x) + f(x)K_0[x] \in K_0[x]/f(x)K_0[x] = L \]
is a square in \( L \).

Proof. For each \( q(x) \in K_0[x] \) we write \( \overline{q(x)} \) for its image in \( K_0[x]/f(x)K_0[x] \).
For each \( i = 1, \ldots, 2g + 1 \) there is a homomorphism of \( K_0 \)-algebras
\[ \phi_i : L = K_0[x]/f(x)K_0[x] \rightarrow K_0^{\text{sep}}, \quad \overline{q(x)} = q(x) + f(x)K_0[x] \rightarrow q(\alpha_i); \]
the intersection of the kernels of all \( \phi_i \) is \( \{0\} \). Indeed, if \( \overline{q(x)} \in \ker(\phi_i) \) then \( q(x) \) is divisible by \( x - \alpha_i \) and therefore if \( \overline{q(x)} \) lies in \( \ker(\phi_i) \) for all \( i \) then \( q(x) \) is divisible by \( \prod_{i=1}^{2g+1} (x - \alpha_i) = f(x), \) i.e., \( 
\overline{q(x)} = 0 \) in \( K_0[x]/f(x)K_0[x] \). Clearly,
\[ \phi_i(\overline{x}) = \alpha_i, \quad \phi_i(a - x) = a - \alpha_i. \]
Since \( f(x) \) lies in \( K_0[x] \), the set of its roots \( \{\alpha_1, \ldots, \alpha_{2g+1}\} \) is a Galois-stable subset of \( K_0^{\text{sep}} \). This implies that for each \( q(x) \in K_0[x] \) and
\[ Z = \overline{q(x)} \in K_0[x]/f(x)K_0[x] \]
the product
\[ H_Z(t) = H_{q(x)}(t) := \prod_{i=1}^{2g+1} \left( t - \phi_i(q(x)) \right) = \prod_{i=1}^{2g+1} \left( t - q(\alpha_i) \right) \]
is a degree \((2g+1)\) monic polynomial with coefficients in \(K_0\). In particular, if \(q(x) = a - x\) then
\[ H_{a-x}(t) = H_{a-x}(t) = \prod_{i=1}^{2g+1} \left( t - (a - \alpha_i) \right). \]

Assume that \(P\) is divisible by \(2\) in \(J(K_0)\), i.e., there is \(a \in J(K_0)\) with \(2a = P\). It follows from Theorems 3.2 and 4.4 that there is \(r \in \mathcal{R}_{1/2 \ P}\) such that \(a_r = a\) and all \(s_i(r)\) lie in \(K_0\). This implies that both polynomials \(U_\gamma(x)\) and \(V_\gamma(x)\) have coefficients in \(K_0[x]\). Recall (Theorem 3.2) that \(f(x)\) and \(U_\gamma(x)\) are relatively prime. This means that \(\overline{U_\gamma(x)} = U_\gamma(\bar{x})\) is a unit in \(K_0[x]/f(x)K_0[x]\). Therefore we may define
\[ \mathcal{R} = s_1(x) + (-1)^g \frac{V_\gamma(\bar{x})}{U_\gamma(\bar{x})} \in K_0[x]/f(x)K_0[x]. \]
The last formula of Theorem 3.2 implies that for all \(i\) we have \(\phi_i(\mathcal{R}) = r_i\) and therefore
\[ \phi_i(\mathcal{R})^2 = r_i^2 = a - \alpha_i = \phi_i(a - \bar{x}). \]
This implies that \(\mathcal{R}^2 = a - \bar{x}\). It follows that
\[ a - \bar{x} = (a - x) + f(t)K_0[t] \in K_0[x]/f(x)K_0[x] \]
is a square in \(K_0[x]/f(x)K_0[x]\).
Conversely, assume now that there is an element \(\mathcal{R} \in L\) such that
\[ \mathcal{R}^2 = a - \bar{x} = a - \bar{x}. \]
This implies that
\[ \phi_i(\mathcal{R})^2 = \phi_i(a - \bar{x}) = a - \alpha_i, \]
i.e.,
\[ \phi_i(\mathcal{R}) = \sqrt{a - \alpha_i} \forall i = 1, \ldots, 2g + 1. \]
This implies that
\[ \prod_{i=1}^{2g+1} \phi_i(\mathcal{R}) = \sqrt{f(a)} = \pm b. \]
Since \((-1)^{2g+1} = -1\), replacing if necessary, \(\mathcal{R}\) by \(-\mathcal{R}\), we may and will assume that
\[ \prod_{i=1}^{2g+1} \phi_i(\mathcal{R}) = -b. \]
Now if we put
\[ r_i = \phi_i(\mathcal{R}) \forall i = 1, \ldots, 2g + 1: r = (r_1, \ldots, r_{2g+1}) \]
then \(r \in \mathcal{R}_{1/2 \ P}\) and
\[ h_\epsilon(t) = \prod_{i=1}^{2g+1} (t - r_i) = \prod_{i=1}^{2g+1} (t - \phi_i(\mathcal{R})) = H_\mathcal{R}(t). \]
Since $\delta_R(t)$ lies in $K_0[t]$, the polynomial $h_r(t)$ also lies in $K_0[t]$. It follows from Theorem 4.4 that $a_r \in J(K_0)$. Since $2a_r = P$, the point $P$ is divisible by 2 in $J(K_0)$.

\[\square\]

**Remark 4.8.** If one assumes additionally that $\text{char}(K_0) = 0$ and $P$ is none of $W_i$ (i.e., $a \neq \alpha_i$ for any $i$) then the assertion of Theorem 4.7 follows from [14, Th. 1.2 and the first paragraph of p. 224].

5. Torsion Points on $\Theta_d$

We keep the notation of Section 4. In particular, $K_0$ be a subfield of $K$ such that

$$f(x) \in K_0[x].$$

Notice that the involution $\iota$ is also defined over $K_0$, the absolute Galois group $\text{Gal}(K_0)$ leaves invariant $\infty$ and permutes points of $C(K_0^{\text{sep}})$; in addition, it permutes elements of $J(K_0^{\text{sep}})$, respecting the group structure on $J(K_0^{\text{sep}})$.

If $n$ is a positive integer that is not divisible by $\text{char}(K)$ then we write $J[n]$ for the kernel of multiplication by $n$ in $J(K)$. It is well known that $J[n]$ is a free $\mathbb{Z}/n\mathbb{Z}$-module of rank $2g$ that lies in $J(K_0^{\text{sep}})$; in addition, it is a $\text{Gal}(K_0)$-stable subgroup of $J(K_0^{\text{sep}})$, which gives us the (continuous) group homomorphism

$$\rho_{n,J} : \text{Gal}(K_0) \to \text{Aut}_{\mathbb{Z}/n\mathbb{Z}}(J[n])$$

that defines the Galois action on $J[n]$. We write $\bar{G}_{n,J,K_0}$ for the image

$$\rho_{n,J}(\text{Gal}(K_0)) \subset \text{Aut}_{\mathbb{Z}/n\mathbb{Z}}(J[n]).$$

Let $\text{Id}_n$ be the identity automorphism of $J[n]$. The following assertion was inspired by a work of F. Bogomolov [4] (where the $\ell$-primary part of the Manin-Mumford conjecture was proven).

**Theorem 5.1.** Suppose that $g > 1$ and $n \geq 3$ is an integer that is not divisible by $\text{char}(K)$. Let $N > 1$ be an integer that is relatively prime to $n$ and such that $N \leq 2g - 1$ and $\bar{G}_{n,J,K_0}$ contains either $N \cdot \text{Id}_n$ or $-N \cdot \text{Id}_n$. Let us put $d(N) := [2g/(N + 1)]$.

Then $\Theta_{d(N)}(K)$ does not contain nonzero points of order dividing $n$ except points of order 1 or 2. In particular, if $n$ is odd then $\Theta_{d(N)}(K)$ does not contain nonzero points of order dividing $n$.

**Proof.** Clearly, $(N + 1) \cdot d(N) < 2g + 1$. Suppose that $b$ is a nonzero point of order dividing $n$ in $\Theta_{d(N)}(K)$. We need to prove that $2b = 0$.

Indeed, $b \in J[n] \subset J(K_0^{\text{sep}})$ and therefore

$$b \in \Theta_d(K) \cap J(K_0^{\text{sep}}) = \Theta_d(K_0^{\text{sep}}).$$

By our assumption, there is $\sigma \in \text{Gal}(K)$ such that $\sigma(a) = Na$ or $-Na$ for all $a \in J[n]$. This implies that $\sigma(b) = Nb$ or $-Nb$. It follows from Theorem 2.8 that $2b = 0$ in $J(K)$.

\[\square\]

**Example 5.2.** Suppose that $K$ is the field $\mathbb{C}$ of complex numbers, $g = 2$ and $C$ is the genus 2 curve

$$y^2 = x^5 - x + 1.$$ 

Let us put $N = 2$. Then $d(N) = 2$. Let $n = \ell$ be an odd prime. Then $\mathbb{Z}/n\mathbb{Z}$ is the prime field $\mathbb{F}_\ell$. Results of L. Dieulefait [6, Th. 5.8 on pp. 509–510] and Serre's
Modularity Conjecture [18] that was proven by C. Khare and J.-P. Wintenberger [8] imply that $\tilde{G}_{\ell,J,K_0}$ is “as large as possible”; in particular, it contains all the homotheties $\mathbb{F}_\ell^* \cdot \text{Id}_\ell$. This implies that $\tilde{G}_{\ell,J,K_0}$ contains $2 \cdot \text{Id}_\ell$, since $\ell$ is odd. It follows from Corollary 5.1 that $\Theta_1 = \mathcal{C}(\mathbb{C})$ does not contain points of order $\ell$ for all odd primes $\ell$.

Actually, using his algorithm mentioned above, B. Poonen had already checked that the only torsion points on this curve are the Weierstrass points $\mathcal{W}_i$ (of order 2) and $\infty$ (of order 1) [10, Sect. 14].

Notice that the Galois group of $x^5 - x + 1$ over $\mathbb{Q}$ is the full symmetric group $S_5$. This implies that the ring of $\mathbb{C}$-endomorphisms of $J$ coincides with $\mathbb{Z}$ [23]. In particular, $J$ is an absolutely simple abelian surface.

**Theorem 5.3.** Suppose that $g > 1$, $K_0 = \mathbb{Q}$, $K = \mathbb{C}$ and $\alpha_1, \ldots, \alpha_{2g+1} \in \mathbb{C}$ are algebraically independent (transcendental) elements of $\mathbb{C}$ (i.e.,

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

is a generic hyperelliptic curve). Then:

(i) $\Theta_{[2g/3]}(\mathbb{C})$ does not contain nonzero points of odd order.

(ii) All 2-power torsion points in $\Theta_{[g/2]}(\mathbb{C})$ have order 1 or 2.

We will prove Theorems 5.3 in Section 6.

**Remark 5.4.** Let $K_0, K = \mathbb{C}$ and $\mathcal{C}$ be as in Theorem 5.3.

(i) B. Poonen and M. Stoll [11, Th. 7.1] proved that the only torsion points on this generic curve are the Weierstrass points $\mathcal{W}_i$ (of order 2) and $\infty$ (of order 1).

(ii) Let $s_1, \ldots, s_{2g+1} \in \mathbb{C}$ be the corresponding basic symmetric functions in $\alpha_1, \ldots, \alpha_{2g+1}$ and let us consider the (sub)field

$$L := \mathbb{Q}(s_1, \ldots, s_{2g+1} \subset \mathbb{Q}(\alpha_1, \ldots, \alpha_{2g+1}) = K_0.$$ 

Then $f(x)$ lies in $L[x]$ and its Galois group over $L$ is the full symmetric group $S_{2g+1}$. This implies that the ring of $\mathbb{C}$-endomorphisms of $J$ coincides with $\mathbb{Z}$ [23]. In particular, $J$ is an absolutely simple abelian variety. (Of course, this result is well known.) It follows from the generalized Manin-Mumford conjecture (also proven by M. Raynaud [13]) that the set of torsion points on $\Theta_d(\mathbb{C})$ is finite for all $d < g$.

6. **Abelian varieties with big $\ell$-adic Galoid images**

We need to recall some basic facts about fields of definition of torsion points on abelian varieties.

Recall that a positive integer $n$ is not divisible by $\text{char}(K)$ and the rank $2g$ free $\mathbb{Z}/n\mathbb{Z}$-module $J[n]$ lies in $J(K^{\text{sep}})$. Clearly, all $n$th roots of unity of $K$ lie in $K^{\text{sep}}$. We write $\mu_n$ for the order $n$ cyclic multiplicative group of $n$th roots of unity in $K^{\text{sep}}$. We write $K(\mu_n) \subset K^{\text{sep}}$ for the $n$th cyclotomic field extension of $K$ and

$$\chi_n : \text{Gal}(K) \to (\mathbb{Z}/n\mathbb{Z})^*$$

for the $n$th cyclotomic character that defines the Galois action on all $n$th roots of unity. The Galois group $\text{Gal}(K(\mu_n)/K)$ of the abelian extension $K(\mu_n)/K$ is
canonically isomorphic to the image
\[ \chi_n(\Gal(K)) \subset (\mathbb{Z}/n\mathbb{Z})^* = \Gal(\mathbb{Q}(\mu_n)/\mathbb{Q}); \]
the equality holds if and only if the degree \([K(\mu_n) : K]\) coincides with \(\phi(n)\) where \(\phi\) is the Euler function. For example, if \(K\) is the field \(\mathbb{Q}\) of rational numbers then for all \(n\)
\[ \mathbb{Q}(\zeta_n) : \mathbb{Q} = \phi(n), \quad \chi_n(\Gal(\mathbb{Q})) = (\mathbb{Z}/n\mathbb{Z})^*. \]

The Jacobian \(J\) carries the canonical principal polarization that is defined over \(K_0\) and gives rise to a nondegenerate alternating bilinear form (Weil-Riemann pairing)
\[ \bar{e}_n : J[n] \times J[n] \to \mathbb{Z}/n\mathbb{Z} \]
such that for all \(\sigma \in \Gal(K)\) and \(a_1, a_2 \in J[n]\) we have
\[ \bar{e}_n(\sigma a_1, \sigma a_2) = \chi_n(\sigma) \cdot \bar{e}_n(a_1, a_2). \]
(Such a form is defined uniquely up to multiplication by an element of \(\mathbb{Z}/n\mathbb{Z}\) and depends on a choice between of an isomorphism between \(\mu_n\) and \(\mathbb{Z}/n\mathbb{Z}\).

Let
\[ \Gp(J[n], \bar{e}_n) \subset \Aut_{\mathbb{Z}/n\mathbb{Z}}(J[n]) \]
be the group of symplectic similitudes of \(\bar{e}_n\) that consists of all automorphisms \(u\) of \(J[n]\) such that there exists a constant \(c = c(u) \in (\mathbb{Z}/n\mathbb{Z})^*\) such that
\[ \bar{e}_n(ua_1, ua_2) = c(u) \cdot \bar{e}_n(a_1, a_2) \quad \forall a_1, a_2 \in J[n]. \]
The map
\[ \mult_n : \Gp(J[n], \bar{e}_n) \to (\mathbb{Z}/n\mathbb{Z})^*, \quad u \mapsto c(u) \]
is a surjective group homomorphism, whose kernel coincides with the symplectic group
\[ \Sp(J[n], \bar{e}_n) \cong \Sp_{2g}(\mathbb{F}_l) \]
of \(\bar{e}_n\). Both \(\Sp(J[n], \bar{e}_n)\) and the group of homotheties \((\mathbb{Z}/n\mathbb{Z})\text{Id}_n\) are subgroups of \(\Gp(J[n], \bar{e}_n)\). The Galois-equivariance of the Weil-Riemann pairing implies that
\[ \tilde{G}_{n,J,K_0} \subset \Gp(J[n], \bar{e}_n) \subset \Aut_{\mathbb{Z}/n\mathbb{Z}}(J[n]). \]
It is also clear that for each \(\sigma \in \Gal(K)\)
\[ \chi_n(\sigma) = c(\rho_{n,J,K_0}(\sigma)) = \mult_n(\rho_{n,J,K_0}(\sigma)) \in (\mathbb{Z}/n\mathbb{Z})^*. \]
Since \(\Sp(J[n], \bar{e}_n) = \ker(\mult_n)\), we obtain the following useful assertion.

**Lemma 6.1.** Let us assume that \(\chi_n(\Gal(K)) = (\mathbb{Z}/n\mathbb{Z})^*\) (E.g., \(K = \mathbb{Q}\) or the field \(\mathbb{Q}(t_1, \ldots, t_d)\) of rational functions in \(d\) independent variables over \(\mathbb{Q}\).)

Suppose that \(\tilde{G}_{n,J,K_0}\) contains \(\Sp(J[n], \bar{e}_n)\). Then \(\tilde{G}_{n,J,K_0} = \Gp(J[n], \bar{e}_n)\). In particular, \(\tilde{G}_{n,J,K_0}\) contains the whole group of homotheties \((\mathbb{Z}/n\mathbb{Z})^* \cdot \text{Id}_n\).

**Example 6.2.** Let \(K_0\), \(K = \mathcal{C}\) and \(\mathcal{C}\) be as in Theorem 5.3, i.e., \(\mathcal{C}\) is a generic hyperelliptic curve.

(i) B. Poonen and M. Stoll proved [11, Proof of Th. 7.1] that if \(n\) is odd then \(\tilde{G}_{n,J,K_0}\) contains \(\Sp(J[n], \bar{e}_n)\). It follows from Lemma 6.1 that \(\tilde{G}_{n,J,K_0} = \Gp(J[n], \bar{e}_n)\) for all odd \(n\). In particular, it contains \((\mathbb{Z}/n\mathbb{Z})^* \cdot \text{Id}_n\) and therefore contains \(2 \cdot \text{Id}_n\).
Proof of Theorem 5.3. Recall that $2$ is a power of $2$. J. Yelton [22] proved that $G_{n,J,K_0}$ contains the level $2$ congruence subgroup $\Gamma(2)$ of $Sp(J[n],\bar{\epsilon}_n)$ defined by the condition

$$\Gamma(2) = \{g \in Sp(J[n],\bar{\epsilon}_n) \mid g \equiv Id_n \mod 2\} \triangleleft Sp(J[n],\bar{\epsilon}_n).$$

Let us consider the level $2$ congruence subgroup $GT(2)$ of $Gp(J[n],\bar{\epsilon}_n)$ defined by the condition

$$GT(2) = \{g \in Gp(J[n],\bar{\epsilon}_n) \mid g \equiv Id_n \mod 2\} \triangleleft Gp(J[n],\bar{\epsilon}_n).$$

Clearly, $GT(2)$ contains $3\cdot Id_n$ while the intersection of $GT(2)$ and $Sp(J[n],\bar{\epsilon}_n)$ coincides with $\Gamma(2)$. The latter means that $\Gamma(2)$ coincides with the kernel of the restriction of $\text{mult}_n$ to $GT(2)$. In addition, one may easily check that

$$\text{mult}_n(GT(2)) = (\mathbb{Z}/n\mathbb{Z})^* = \text{mult}_n(Gp(J[n],\bar{\epsilon}_n),$$

since

$$(\mathbb{Z}/n\mathbb{Z})^* = \{c \in \mathbb{Z}/n\mathbb{Z} \mid c \equiv 1 \mod 2\}.$$ 

This implies that $G_{n,J,K_0}$ contains $GT(2)$. In particular, $G_{n,J,K_0}$ contains $3\cdot Id_n$. (See also [11, Proof of Th. 7.1].)

Proof of Theorem 5.3. Recall that $d(2) = [2g/3]$. Combining Theorem 5.1 (with $N = 2$ and any odd $n$) with Example 6.2(i), we conclude that $\Theta_{[2g/3]}(\mathbb{C})$ does not contain nonzero points of odd order $n$. This proves (i).

Recall that $d(3) = [2g/4] = [g/2]$. Combining Theorem 5.1 (with $N = 3$ and $n = 2^e$) with Example 6.2(ii), we conclude that all $2$-power torsion points in $\Theta_{[g/2]}(\mathbb{C})$ are points of order $1$ or $2$. 

The rest of this paper is devoted to the proof of the following result.

**Theorem 6.3.** Let $K_0$ be the field $\mathbb{Q}$ of rational numbers, $K = \mathbb{C}$ the field of complex numbers. Suppose that $g > 1$. Let $S$ be a non-empty set of odd primes such that for all $\ell \in S$ the image $G_{\ell,J,K_0} = Gp(J[\ell],\bar{\epsilon}_\ell)$.

If $n > 1$ is a positive odd integer, all whose prime divisors lie in $S$ then $\Theta_{[2g/3]}(\mathbb{C})$ does not contain nonzero points of order dividing $n$.

Let us start with the following elementary observation on Galois properties of torsion points on $J$.

**Remark 6.4.**

(i) Let $G_n$ be the derived subgroup $[G_{n,J,K_0},G_{n,J,K_0}]$ of $G_{n,J,K_0}$. Then $G_n$ is a normal subgroup of finite index in $G_{n,J,K_0}$. Let $K_{0,n} \subset K_0^{\text{sep}}$ be the finite Galois extension of $K_0$ such that the absolute Galois (sub)group $\text{Gal}(K_{0,n}) \subset \text{Gal}(K_0)$ coincides with the preimage

$$\rho_{n,J}(G_n) \subset \rho_{n,J}(G_{n,J,K_0}) = \text{Gal}(K).$$

We have

$$G_{n,J,K_0,n} = \rho_{n,J}(\text{Gal}(K_{0,n})) = G_n = [G_{n,J,K_0},G_{n,J,K_0}] \subset [Gp(J[n],\bar{\epsilon}_n),Gp(J[n],\bar{\epsilon}_n)] \subset Sp(J[n],\bar{\epsilon}_n).$$

This implies that

$$G_{n,J,K_0,n} \subset Sp(J[n],\bar{\epsilon}_n).$$
Let \( m > 1 \) be an integer dividing \( n \). The inclusion of Galois modules \( J[m] \subset J[n] \) induces the surjective group homomorphisms
\[
\tilde{G}_{m, J, K_0} \to \tilde{G}_{m, J, K_0}, \tilde{G}_{n, J, K_0, n} \to \tilde{G}_{m, J, K_0, n} \subset \tilde{G}_{m, J, K_0};
\]
the latter homomorphism coincides with the restriction of the former one to the (derived) subgroup \( \tilde{G}_{m, J, K_0, n} \subset \tilde{G}_{n, J, K_0} \). This implies that
\[
\tilde{G}_{m, J, K_0, n} = [\tilde{G}_{m, J, K_0}, \tilde{G}_{m, J, K_0}]
\]
is the derived subgroup of \( \tilde{G}_{m, J, K_0} \). In addition,
\[
\tilde{G}_{m, J, K_0, n} = [\tilde{G}_{m, J, K_0}, \tilde{G}_{m, J, K_0}] \subset [\text{Sp}(J[m], \bar{e}_m), \text{Sp}(J[m], \bar{e}_m)] \subset \text{Sp}(J[m], \bar{e}_m).
\]

(ii) Recall that \( g \geq 2 \). Now assume that \( m = \ell \) is an odd prime dividing \( n \). Then \( \text{Sp}(J[\ell], \bar{e}_\ell) \) is perfect, i.e., coincides with its own derived subgroup. Assume also that \( \tilde{G}_{\ell, J, K_0} \) contains \( \text{Sp}(J[\ell], \bar{e}_\ell) \). Then
\[
\text{Sp}(J[\ell], \bar{e}_\ell) \supset \tilde{G}_{\ell, J, K_0, n} = \tilde{G}_{\ell, J, K_0, n} \subset [\text{Sp}(J[\ell], \bar{e}_\ell), \text{Sp}(J[\ell], \bar{e}_\ell)] = \text{Sp}(J[\ell], \bar{e}_\ell)
\]
and therefore
\[
\tilde{G}_{\ell, J, K_0, n} = \text{Sp}(J[\ell], \bar{e}_\ell).
\]

We will also need the following result about closed subgroups of symplectic groups over the ring \( \mathbb{Z}_\ell \) of \( \ell \)-adic integers ([17, pp. 52–53], [20, Th. 1.3]).

**Lemma 6.5.** Let \( g \geq 2 \) be an integer and \( \ell \) an odd prime. Let \( G \) be a closed subgroup of \( \text{Sp}(2g, \mathbb{Z}_\ell) \) such that the corresponding reduction map \( G \to \text{Sp}(2g, \mathbb{Z}/\ell\mathbb{Z}) \) is surjective. Then \( G = \text{Sp}(2g, \mathbb{Z}_\ell) \).

**Proof.** The result follows from [20, Theorem 1.3 on pp. 326–327] applied to
\[
p = q = \ell, k = F_\ell, W(k) = \mathbb{Z}_\ell, G = \text{Sp}_{2g}.
\]

**Corollary 6.6.** Let \( g \geq 2 \) be an integer and \( \ell \) an odd prime. Then for each positive integer \( i \) the group \( \text{Sp}_{2g}(\mathbb{Z}/\ell^i\mathbb{Z}) \) is perfect.

**Proof.** The case \( i = 1 \) is well known. Let \( i \geq 1 \) be an integer. It is also well known that the reduction modulo \( \ell^i \) map
\[
\text{red}_i : \text{Sp}_{2g}(\mathbb{Z}_\ell) \to \text{Sp}_{2g}(\mathbb{Z}/\ell^i\mathbb{Z})
\]
is a surjective group homomorphism. This implies that the reduction modulo \( \ell \) map
\[
\overline{\text{red}}_{i,1} : \text{Sp}_{2g}(\mathbb{Z}/\ell^i\mathbb{Z}) \to \text{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})
\]
is also a surjective group homomorphism. Clearly, \( \text{red}_i \) coincides with the composition \( \overline{\text{red}}_{i,1} \circ \text{red}_i \).

Suppose that \( \text{Sp}_{2g}(\mathbb{Z}/\ell^i\mathbb{Z}) \) is not perfect and let
\[
H := [\text{Sp}_{2g}(\mathbb{Z}/\ell^i\mathbb{Z}), \text{Sp}_{2g}(\mathbb{Z}/\ell^i\mathbb{Z})]
\]
be the derived subgroup of \( \text{Sp}_{2g}(\mathbb{Z}/\ell^i\mathbb{Z}) \). Since \( \text{Sp}(2g, \mathbb{Z}/\ell\mathbb{Z}) \) is perfect, i.e., coincides with its derived subgroup,
\[
\overline{\text{red}}_{i,1}(H) = \text{Sp}(2g, \mathbb{Z}/\ell\mathbb{Z}).
\]
Now the closed subgroup
\[ G := \text{red}_i^{-1}(H) \subset \text{Sp}_{2g}(\mathbb{Z}_\ell) \]
maps surjectively on \( \text{Sp}_{2g}(\mathbb{Z}/\ell) \) but does not coincide with \( \text{Sp}_{2g}(\mathbb{Z}_\ell) \), because \( H \) is a proper subgroup of \( \text{Sp}_{2g}(\mathbb{Z}/\ell') \) and \( \text{red}_{i,1} \) is surjective. This contradicts to Lemma 6.5, which proves the desired perfectness. \( \Box \)

The following lemma will be proven at the end of this section.

**Lemma 6.7.** Suppose that \( g > 1 \). Suppose that \( n > 1 \) is an odd integer that is not divisible by \( \text{char}(K) \). If for all primes \( \ell \) dividing \( n \) the image \( \tilde{G}_{\ell,n,K_0} \) contains \( \text{Sp}(J[n], \bar{e}_\ell) \) then \( \tilde{G}_{\ell,n,K_0,0} \) contains \( \text{Sp}(J[n], \bar{e}_n) \).

In addition, if \( K_0 \) is the field \( \mathbb{Q} \) of rational numbers then \( \tilde{G}_{\ell,n,K_0} = \text{Gp}(J[n], \bar{e}_n) \).

**Remark 6.8.** Thanks to Lemma 6.1, the second assertion of Lemma 6.7 follows from the first one.

**Proof of Theorem 6.3.** Recall that \( \text{Gp}(J[\ell], \bar{e}_\ell) \) contains \( \text{Sp}(J[\ell], \bar{e}_\ell) \). It follows from Lemma 6.7 that \( \tilde{G}_{\ell,n,K_0} = \text{Gp}(J[n], \bar{e}_n) \).

This implies that \( \tilde{G}_{\ell,n,K_0} \) contains \( 2 \cdot \text{Id}_n \), because it contains the whole \( (\mathbb{Z}/n\mathbb{Z})^* \cdot \text{Id}_n \).

It follows from Corollary 5.1 that \( \mathcal{C}(K) \) does not contain points of order \( n \). \( \Box \)

**Proof of Lemma 6.7.** First, let us do the case when \( n \) is a power of an odd prime \( \ell \).

Let \( \ell \neq \text{char}(K) \) be a prime. Let \( T_\ell(J) \) be the \( \ell \)-adic Tate module of \( J \) that is the projective limit of \( J[\ell^i] \) where the transition maps \( J[\ell^{i+1}] \to J[\ell^i] \) are multiplications by \( \ell \). It is well known that \( T_\ell(J) \) is a free \( \mathbb{Z}_\ell \)-module of rank \( 2g \), the Galois actions on \( J[\ell^i] \)'s are glued together to the continuous group homomorphism
\[ \rho_{\ell,n,K_0} : \text{Gal}(K) \to \text{Aut}_{\mathbb{Z}_\ell}(T_\ell(J)) \]
such that the canonical isomorphisms of \( \mathbb{Z}_\ell \)-modules
\[ T_\ell(J)/\ell^i T_\ell(J) = J[\ell^i] \]
become isomorphisms of Galois modules. (Recall that \( \mathbb{Z}/\ell^i \mathbb{Z} = \mathbb{Z}_\ell/\ell^i \mathbb{Z}_\ell \).) The polarization \( \lambda \) gives rise to the alternating perfect/unimodular \( \mathbb{Z}_\ell \)-bilinear form
\[ e_\ell : T_\ell(J) \times T_\ell(J) \to \mathbb{Z}_\ell \]
such that for each \( \sigma \in \text{Gal}(K) \)
\[ e_\ell(\rho_{\ell}(\sigma)(v_1), \rho_{\ell}(\sigma)(v_2)) = \chi_\ell(\sigma) \cdot e_\ell(v_1, v_2) \quad \forall \, v_1, v_2 \in T_\ell(J). \]

Here
\[ \chi_\ell : \text{Gal}(K) \to \mathbb{Z}_\ell^* \]
is the (continuous) cyclotomic character of \( \text{Gal}(K) \) characterized by the property
\[ \chi_\ell(\sigma) \mod \ell^i = \bar{\chi}_{\ell^i}(\sigma) \quad \forall \, i. \]

This implies that
\[ G_{\ell,n,K_0} = \rho_{\ell,n,K_0} \text{Gal}(K) \subset \text{Gp}(T_\ell(J), e_\ell) \]
where
\[ \text{Gp}(T_\ell(J), e_\ell) \subset \text{Aut}_{\mathbb{Z}_\ell}(T_\ell(J)) \]
is the group of symplectic similitudes of $e_\ell$. Clearly, $\text{Gp}(T_\ell(J), e_\ell)$ contains the corresponding symplectic group

$$\text{Sp}(T_\ell(J), e_\ell) \cong \text{Sp}_{2g}(\mathbb{Z}_\ell)$$

and the subgroup of homotheties/scalars $\mathbb{Z}_\ell^*$. It is also clear that the derived subgroup $[\text{Gp}(T_\ell(J), e_\ell), \text{Gp}(T_\ell(J), e_\ell)]$ lies in $\text{Sp}(T_\ell(J), e_\ell)$.

For each $n = \ell^i$ the reduction map modulo $\ell^i$ sends $\text{Gp}(T_\ell(J), e_\ell)$ onto $\text{Gp}(J[\ell^i], \bar{e}_\ell)$, $\text{Sp}(T_\ell(J), e_\ell)$ onto $\text{Sp}(J[\ell^i], \bar{e}_\ell)$ and $\mathbb{Z}_\ell^*$ onto $(\mathbb{Z}/\ell^i\mathbb{Z})^*$. In particular, if $\ell$ is odd then the scalar $2 \in \mathbb{Z}_\ell^*$ goes to

$$2 \cdot \text{Id}_{\ell^i} \in \text{Gp}(J[\ell^i], \bar{e}_\ell).$$

As for $G_{\ell,J,K_0}$, its image under the reduction map modulo $\ell^i$ coincides with $\bar{G}_{\ell,J,K_0}$. It is known [15] that $G_{\ell,J,K_0}$ is a compact $\ell$-adic Lie subgroup in $\text{Gp}(T_\ell(J), e_\ell)$ and therefore is a closed subgroup of $\text{Sp}(T_\ell(J), e_\ell)$ with respect to $\ell$-adic topology. Clearly, the intersection

$$G_\ell := G_{\ell,J,K_0} \cap \text{Sp}(T_\ell(J), e_\ell)$$

is a closed subgroup of $\text{Sp}(T_\ell(J), e_\ell)$. In addition, the derived subgroup of $G_{\ell,J,K_0}$

$$[G_{\ell,J,K_0}, G_{\ell,J,K_0}] \subset G_{\ell,J,K_0} \cap \bigcap \text{Gp}(T_\ell(J), e_\ell), \text{Gp}(T_\ell(J), e_\ell) \bigg\} \subset G_{\ell,J,K_0} \cap \bigcap \text{Sp}(T_\ell(J), e_\ell) = G_\ell,$$

i.e.,

$$[G_{\ell,J,K_0}, G_{\ell,J,K_0}] \subset G_\ell.$$

Let us assume that $\ell$ is odd and $G_{\ell,J,K_0}$ contains $\text{Sp}(J[\ell], \bar{e}_\ell)$. Then the reduction modulo $\ell$ of $[G_{\ell,J,K_0}, G_{\ell,J,K_0}]$ contains the derived subgroup $[\text{Sp}(J[\ell], \bar{e}_\ell), \text{Sp}(J[\ell], \bar{e}_\ell)]$. Since our assumptions on $g$ and $\ell$ imply that the group $\text{Sp}(J[\ell], \bar{e}_\ell)$ is perfect, i.e.,

$$[\text{Sp}(J[\ell], \bar{e}_\ell), \text{Sp}(J[\ell], \bar{e}_\ell)] = \text{Sp}(J[\ell], \bar{e}_\ell),$$

the reduction modulo $\ell$ of $[G_{\ell,J,K_0}, G_{\ell,J,K_0}]$ contains $\text{Sp}(J[\ell], \bar{e}_\ell)$. This implies that the reduction modulo $\ell$ of $G_\ell$ also contains $\text{Sp}(J[\ell], \bar{e}_\ell)$. Since $G_\ell$ is a (closed) subgroup of $\text{Sp}(T_\ell(J), e_\ell)$, its reduction modulo $\ell$ actually coincides with $\text{Sp}(J[\ell], \bar{e}_\ell)$. It follows from Lemma 6.5 that

$$G_\ell = \text{Sp}(T_\ell(J), e_\ell).$$

In particular, the reduction of $G_\ell$ modulo $\ell^i$ coincides with $\text{Sp}(J[\ell^i], \bar{e}_\ell)$ for all positive integers $i$. Since $G_{\ell,J,K_0}$ contains $G_\ell$, its reduction modulo $\ell^i$ contains $\text{Sp}(J[\ell^i], \bar{e}_\ell)$. This means that $\bar{G}_{\ell,J,K_0}$ contains $\text{Sp}(J[\ell^i], \bar{e}_\ell)$ for all positive $i$. This proves Lemma 6.7 for all $n$ that are powers of an odd prime $\ell$.

Now let us consider the general case. So, $n > 1$ is an odd integer. Let $S$ be the (finite nonempty) set of prime divisors $\ell$ of $n$ and $n = \prod_{\ell \in S} \ell^{d(\ell)}$ where all $d(\ell)$ are positive integers. Using Remark 6.4, we may replace if necessary $K_0$ by $K_{0,n}$ and assume that

$$\bar{G}_{\ell,J,K_0} = \text{Sp}(J[\ell], \bar{e}_\ell)$$

for all $\ell \in S$. The already proven case of prime powers tells us that

$$\bar{G}_{\ell^{d(\ell)}, J,K_0} = \text{Sp} \left( J \left[ \ell^{d(\ell)} \right], \bar{e}_\ell \right)$$

for all $\ell \in S$. On the other hand, we have

$$\mathbb{Z}/n\mathbb{Z} = \oplus_{\ell \in S} \mathbb{Z}/\ell^{d(\ell)}\mathbb{Z}, \quad J[n] = \oplus_{\ell \in S} J \left[ \ell^{d(\ell)} \right],$$

where
\[ \text{Gp}(J[n], \bar{e}_n) = \prod_{\ell \in S} \text{Gp}\left( J \left[ \ell^d(\ell) \right], \bar{e}_{\ell^d(\ell)} \right), \quad \text{Sp}(J[n], \bar{e}_n) = \prod_{\ell \in S} \text{Sp}\left( J \left[ \ell^d(\ell) \right], \bar{e}_{\ell^d(\ell)} \right), \]

\[ \check{G}_{n,J,K_0} \subseteq \prod_{\ell \in S} \check{G}_{\ell^d(\ell),J,K_0} = \prod_{\ell \in S} \text{Sp}(J[\ell^d(\ell)], \bar{e}_{\ell^d(\ell)}). \]

Recall that the group homomorphisms

\[ \check{G}_{n,J,K_0} \rightarrow \check{G}_{\ell^d(\ell),J,K_0} = \text{Sp}\left( J \left[ \ell^d(\ell) \right], \bar{e}_{\ell^d(\ell)} \right) \]

(induced by the inclusion of the Galois modules \( J \left[ \ell^d(\ell) \right] \subseteq J[n] \)) are surjective. We want to use Goursat’s Lemma and Ribet’s Lemma [19, Sect. 1.4], in order to prove that the subgroup

\[ \check{G}_{n,J,K_0} \subseteq \prod_{\ell \in S} \text{Sp}(J[\ell^d(\ell)], \bar{e}_{\ell^d(\ell)}) \]

coincides with the whole product. In order to do that, we need to check that simple finite groups that are quotients of \( \text{Sp}(J[\ell^d(\ell)]) \)'s are mutually nonisomorphic for different \( \ell \). Recall that

\[ \text{Sp}\left( J \left[ \ell^d(\ell) \right], \bar{e}_{\ell^d(\ell)} \right) \cong \text{Sp}_{2g} \left( \mathbb{Z}/\ell^d(\ell)\mathbb{Z} \right) \]

and therefore is perfect. Therefore, all its simple quotients are also perfect, i.e., are finite simple nonabelian groups. Clearly, the only simple nonabelian quotient of \( \text{Sp}_{2g} \left( \mathbb{Z}/\ell^d(\ell)\mathbb{Z} \right) \) is

\[ \Sigma_{\ell} := \text{Sp}_{2g} \left( \mathbb{Z}/\ell\mathbb{Z} \right)/\{\pm1\}. \]

However, the groups \( \Sigma_{\ell} \) are perfect and mutually nonisomorphic for distinct \( \ell \) [1, 2]. This ends the proof. \( \square \)

**Remark 6.9.** Remark 6.4, Lemmas 6.1 and 6.7, and their proofs remain true if one replaces the Jacobian \( J \) by any principally polarized \( g \)-dimensional abelian variety \( A \) over \( K_0 \) with \( g \geq 2 \).

**References**

[1] E. Artin, *The orders of the linear groups*. Comm. Pure Appl. Math. 8 (1955), 355–365.
[2] E. Artin, *The orders of the classical simple groups*. Comm. Pure Appl. Math. 8 (1955), 455–472.
[3] B.M. Bekker, Yu.G. Zarhin, *The divisibility by 2 of rational points on elliptic curves*. Max-Planck-Institut für Mathematik Preprint Series 2016-32, Bonn.
[4] F.A. Bogomolov, *Points of finite order on an Abelian variety*. Math. USSR-Izv., 17:1 (1981), 55–72.
[5] J.W.C. Cassels, *Diophantine equations with special reference to elliptic curves*. J. London Math. Soc. 41 (1966), 193–291.
[6] L. Dieulefait, *Explicit determination of the images of the Galois representations attached to abelian surfaces with \( \text{End}(A) = \mathbb{Z} \).* Experimental Math. 11:4 (2002/03), 503–512.
[7] N. Bruin, E.V. Flynn, *Towers of 2-covers of hyperelliptic curves*. Trans. Amer. Math. Soc. 357 (2005), no. 11, 4329–4347.
[8] C. Khare and J.-P. Wintenberger, *Serre’s modularity conjecture. I.* Invent. Math. 178 (2009), 485–586.
[9] D. Mumford, *Tata Lectures on Theta. II.* Progress in Math. 43, Birkhäuser, Boston Basel Stuttgart, 1984.
[10] B. Poonen, *Computing torsion points on curves*. Experimental Math. 10 (2001), no. 3, 449–465.
[11] B. Poonen, M. Stoll, *Most odd degree hyperelliptic curves have only one rational point*. Annals of Math. 180 (2014), Issue 3, 1137–1166.
[12] M. Raynaud, *Courbes sur une variété abélienne et points de torsion*. Invent. Math. 71 (1983), no. 1, 207–233.
[13] 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 (1983), Birkhäuser, Boston Basel Stuttgart.
[14] E. Schaefer, 2-descent on the Jacobians of hyperelliptic curves. J. Number Theory 51 (1995), no. 2, 219–232.
[15] J.-P. Serre, Abelian \( \ell \)-adic representations and elliptic curves, 2nd edition. Advanced Book Classics, Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989.
[16] J.-P. Serre, Algebraic groups and class fields. Graduate Texts in Math. 117, Springer-Verlag, New York, 1988.
[17] J.-P. Serre, Lettre à Marie-France Vignéras. Collected papers. IV:137, Springer-Verlag, New York, 2000, pp. 38–55.
[18] J.-P. Serre, Sur le repré sentations modulaires de degré 2 de \( \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \). Duke Math. J. 54 (1987), 179–230.
[19] J.-P. Serre, Finite Groups: An Introduction. International Press, Boston, 2016.
[20] A. Vasiu, Surjectivity criteria for \( p \)-adic representations. I. Manuscripta Math. 112 (2003), no. 3, 325–355.
[21] L.C. Washington, Elliptic Curves: Number Theory and Cryptography. Second edition. Chapman & Hall/CRC Press, Boca Raton London New York, 2008.
[22] J. Yelton, Images of 2-adic representations associated to hyperelliptic jacobians. J. Number Theory 151 (2015), 7–17.
[23] Yu. G. Zarhin, Hyperelliptic jacobians without complex multiplication. Math. Research Letters 7 (2000), 123–132.
[24] Yu. G. Zarhin, Division by 2 on elliptic curves. arXiv:1507.08238 [math.AG].

Pennsylvania State University, Department of Mathematics, University Park, PA 16802, USA
E-mail address: zarhin@math.psu.edu