HALVES OF POINTS OF AN ODD DEGREE HYPERELLIPTIC CURVE IN ITS JACOBIAN

YURI G. ZARHIN

ABSTRACT. Let $f(x)$ be a degree $(2g+1)$ monic polynomial with coefficients in an algebraically closed field K with $\mathrm{char}(K) \neq 2$ and without repeated roots. Let $\mathfrak{R} \subset K$ be the $(2g+1)$-element set of roots of $f(x)$. Let $\mathcal{C}: y^2 = f(x)$ be an odd degree genus g hyperelliptic curve over K. Let J be the jacobian of $\mathcal{C}$ and $J[2] \subset J(K)$ the (sub)group of points of order dividing 2. We identify $\mathcal{C}$ with the image of its canonical embedding into J (the infinite point of $\mathcal{C}$ goes to the identity element of J). Let $P = (a, b) \in \mathcal{C}(K) \subset J(K)$ and

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

which is $J[2]$-torsor. In a previous work we established an explicit bijection between the sets $M_{1/2,P}$ and

$$\mathfrak{R}_{1/2,P} := \{\mathfrak{r} : \mathfrak{R} \to K \mid \mathfrak{r}(\alpha)^2 = a - \alpha \ \forall \alpha \in \mathfrak{R};\ \prod_{\alpha \in \mathfrak{R}} \mathfrak{r}(\alpha) = -b\}.$$

The aim of this paper is to describe the induced action of $J[2]$ on $\mathfrak{R}_{1/2,P}$ (i.e., how signs of square roots $r(\alpha) = \sqrt{a - \alpha}$ should change).

1. Introduction

Let K be an algebraically closed field of characteristic different from 2, g a positive integer, $\mathfrak{R} \subset K$ a $(2g+1)$-element set,

$$f(x) = f_{\mathfrak{R}}(x) := \prod_{\alpha \in \mathfrak{R}} (x - \alpha)$$

a degree $(2g+1)$ polynomial with coefficients in K and without repeated roots, $\mathcal{C} : y^2 = f(x)$ the corresponding genus g hyperelliptic curve over K, and J the jacobian of $\mathcal{C}$. We identify $\mathcal{C}$ with the image of its canonical embedding

$$\mathcal{C} \hookrightarrow J,\ P \mapsto \mathrm{cl}((P) - (\infty))$$

into J (the infinite point ∞ of $\mathcal{C}$ goes to the identity element of J). Let $J[2] \subset J(K)$ be the kernel of multiplication by 2 in $J(K)$, which is a $2g$-dimensional $\mathbb{F}_2$-vector space. All the $(2g+1)$ points

$$\mathfrak{W}_\alpha := (\alpha, 0) \in \mathcal{C}(K) \subset J(K)\ (\alpha \in \mathfrak{R})$$

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

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

Partially supported by Simons Foundation Collaboration grant # 585711.

This paper was started during my stay in May-July 2018 at the Max-Planck-Institut für Mathematik (Bonn, Germany), whose hospitality and support are gratefully acknowledged.

lie in $J[2]$ and generate it as the $2g$-dimensional $\mathbb{F}_2$-vector space; they satisfy the only relation

$$\sum_{\alpha\in\mathfrak{R}} \mathfrak{W}_\alpha = 0 \in J[2] \subset J(K).$$

This leads to a well known canonical isomorphism [4] between $\mathbb{F}_2$-vector spaces $J[2]$ and

$$({\mathbb{F}_2}^{\mathfrak{R}})^0 = \{\phi : \mathfrak{R} \to \mathbb{F}_2 \mid \sum_{\alpha\in\mathfrak{R}} \phi(\alpha) = 0\}.$$

Namely, each function $\phi \in ({\mathbb{F}_2}^{\mathfrak{R}})^0$ corresponds to

$$\sum_{\alpha\in\mathfrak{R}} \phi(\alpha)\mathfrak{W}_\alpha \in J[2].$$

For example, for each $\beta \in \mathfrak{R}$ the point $\mathfrak{W}_\beta = \sum_{\alpha\neq\beta} \mathfrak{W}_\alpha$ corresponds to the function $\psi_\beta : \mathfrak{R} \to \mathbb{F}_2$ that sends β to 0 and all other elements of $\mathfrak{R}$ to 1.

If $\mathfrak{b} \in J(K)$ then the finite set

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

consists of 2^{2g} elements and carries the natural structure of a $J[2]$-torsor.

Let

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

Let us consider, the set

$$\mathfrak{R}_{1/2,P} := \{\mathfrak{r} : \mathfrak{R} \to K \mid \mathfrak{r}(\alpha)^2 = a - \alpha \ \forall\alpha \in \mathfrak{R};\ \prod_{\alpha\in\mathfrak{R}} \mathfrak{r}(\alpha) = -b\}.$$

Changes of signs in the (even number of) square roots provide $\mathfrak{R}_{1/2,P}$ with the natural structure of a $({\mathbb{F}_2}^{\mathfrak{R}})^0$-torsor. Namely, let

$$\chi : \mathbb{F}_2 \to K^*$$

be the **additive character** such that

$$\chi(0) = 1, \chi(1) = -1.$$

Then the result of the action of a function $\phi : \mathfrak{R} \to \mathbb{F}_2$ from $({\mathbb{F}_2}^{\mathfrak{R}})^0$ on $\mathfrak{r} : \mathfrak{R} \to K$ from $\mathfrak{R}_{1/2,P}$ is just the product

$$\chi(\phi)\mathfrak{r} : \mathfrak{R} \to K,\ \alpha \mapsto \chi(\phi(\alpha))\mathfrak{r}(\alpha).$$

On the other hand, I constructed in [9] an explicit *bijection* of finite sets

$$\mathfrak{R}_{1/2,P} \cong M_{1/2,P},\ \mathfrak{r} \mapsto \mathfrak{a}_\mathfrak{r} \in M_{1/2,P} \subset J(K).$$

Identifying (as above) $J[2]$ and $({\mathbb{F}_2}^{\mathfrak{R}})^0$, we obtain a second structure of a $({\mathbb{F}_2}^{\mathfrak{R}})^0$-torsor on $\mathfrak{R}_{1/2,P}$. Our main result asserts that these two structures actually coincide. In down-to-earth terms this means the following.

Theorem 1.1. *Let* $\mathfrak{r} \in \mathfrak{R}_{1/2,P}$ *and* $\beta \in \mathfrak{R}$. *Let us define* $\mathfrak{r}^\beta \in \mathfrak{R}_{1/2,P}$ *as follows.*

$$\mathfrak{r}^\beta(\beta) = \mathfrak{r}(\beta),\ \mathfrak{r}^\beta(\alpha) = -\mathfrak{r}(\alpha)\ \forall\alpha \in \mathfrak{R} \setminus \{\beta\}.$$

Then

$$\mathfrak{a}_{\mathfrak{r}^\beta} = \mathfrak{a}_\mathfrak{r} + \mathfrak{W}_\beta = \mathfrak{a}_\mathfrak{r} + \left(\sum_{\alpha\neq\beta} \mathfrak{W}_\alpha\right).$$

Remark 1.2. In the case of elliptic curves (i.e., when $g = 1$) the assertion of Theorem 1.1 was proven in [2, Th. 2.3(iv)].

Example 1.3. If $P = \mathfrak{W}_\beta = (\beta, 0)$ then

$$\mathfrak{a}_\mathfrak{r} + \mathfrak{W}_\beta = \mathfrak{a}_\mathfrak{r} - \mathfrak{W}_\beta = \mathfrak{a}_\mathfrak{r} - 2\mathfrak{a}_\mathfrak{r} = -\mathfrak{a}_\mathfrak{r}$$

while

$$-\mathfrak{a}_\mathfrak{r} = \mathfrak{a}_{-\mathfrak{r}}$$

(see [9, Remark 3.5]). On the other hand, $\mathfrak{r}(\beta) = \sqrt{\beta - \beta} = 0$ for all $\mathfrak{r}$ and

$$\mathfrak{r}^\beta = -\mathfrak{r} : \alpha \mapsto -\mathfrak{r}(\alpha)\ \forall \alpha \in \mathfrak{R}.$$

This implies that

$$\mathfrak{a}_{\mathfrak{r}^\beta} = \mathfrak{a}_{-\mathfrak{r}} = \mathfrak{a}_\mathfrak{r} + \mathfrak{W}_\beta.$$

This proves Theorem 1.1 in the special case $P = \mathfrak{W}_\beta$.

The paper is organized as follows. In Section 2 we recall basic facts about Mumford representations of points of $J(K)$ and review results of [9], including an explicit description of the bijection between $\mathfrak{R}_{1/2,P}$ and $M_{1/2,P}$. In Section 3 we give explicit formulas for the Mumford representation of $\mathfrak{a} + \mathfrak{W}_\beta$ when $\mathfrak{a}$ lies neither on the theta divisor of J nor on its translation by $\mathfrak{W}_\beta$, assuming that we know the Mumford representation of $\mathfrak{a}$. In Section 4 we prove Theorem 1.1, using auxiliary results from commutative algebra that are proven in Section 5.

2. Halves and square roots

Let $\mathcal{C}$ be the smooth projective model of the smooth affine plane K-curve

$$y^2 = f(x) = \prod_{\alpha \in \mathfrak{R}} (x - \alpha)$$

where $\mathfrak{R}$ is a $(2g+1)$-element subset of K. In particular, $f(x)$ is a monic degree $(2g+1)$ polynomial without repeated roots. It is well known that $\mathcal{C}$ is a genus g hyperelliptic curve over K with precisely one *infinite* point, which we denote by ∞. In other words,

$$\mathcal{C}(K) = \{(a,b) \in K^2 \mid b^2 = \prod_{\alpha \in \mathfrak{R}} (a - \alpha_i)\} \bigsqcup \{\infty\}.$$

Clearly, x and y are nonconstant rational functions on $\mathcal{C}$, whose only pole is ∞. More precisely, the polar divisor of x is $2(\infty)$ and the polar divisor of y is $(2g+1)(\infty)$. The zero divisor of y is $\sum_{\alpha \in \mathfrak{R}} (\mathfrak{W}_\alpha)$. In particular, y is a *local parameter* at (every) $\mathfrak{W}_\alpha$.

We write ι for the hyperelliptic involution

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

The set of fixed points of ι consists of ∞ and all $\mathfrak{W}_\alpha$ ($\alpha \in \mathfrak{R}$). It is well known that for each $P \in \mathcal{C}(K)$ the divisor $(P) + \iota(P) - 2(\infty)$ is principal. More precisely, if $P = (a,b) \in \mathcal{C}(K)$ then $(P) + \iota(P) - 2(\infty)$ is the divisor of the rational function $x - a$ on C. In particular, if $P = \mathfrak{W}_\alpha = (\alpha, 0)$ then

$$2(\mathfrak{W}_\alpha) - 2(\infty) = \operatorname{div}(x - \alpha).$$

In particular, $x - \alpha$ has a double zero at $\mathfrak{W}_\alpha$ (and no other zeros). If D is a divisor on $\mathcal{C}$ then we write $\operatorname{supp}(D)$ for its *support*, which is a finite subset of $\mathcal{C}(K)$.

Recall that the jacobian J of $\mathcal{C}$ is a g-dimensional abelian variety over K. If D is a degree zero divisor on $\mathcal{C}$ then we write $\mathrm{cl}(D)$ for its linear equivalence class, which is viewed as an element of $J(K)$. Elements of $J(K)$ may be described in terms of so called **Mumford representations** (see [4, Sect. 3.12], [8, Sect. 13.2] and Subsection 2.3 below).

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

2.1. Since K is algebraically closed, the commutative group $J(K)$ is divisible. It is well known that for each $\mathfrak{b} \in J(K)$ there are exactly 2^{2g} elements $\mathfrak{a} \in J(K)$ such that $2\mathfrak{a} = \mathfrak{b}$. In [9] we established explicitly the following bijection $\mathfrak{r} \mapsto \mathfrak{a}_\mathfrak{r}$ between the 2^{2g}-element sets $\mathfrak{R}_{1/2,P}$ and $M_{1/2,P}$.

If $\mathfrak{r} \in \mathfrak{R}_{1/2,P}$ then for each positive integer $i \le 2g+1$ let us consider $\mathbf{s}_i(\mathfrak{r}) \in K$ defined as the value of ith basic symmetric function at $(2g+1)$ elements $\{\mathfrak{r}(\alpha) \mid \alpha \in \mathfrak{R}\}$ (notice that all $\mathfrak{r}(\alpha)$ are distinct, since their squares $\mathfrak{r}(\alpha)^2 = a - \alpha$ are distinct). Let us consider the degree g monic polynomial

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

and the polynomial

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

whose degree is *strictly less* than g. Let $\{c_1, \dots, c_g\} \subset K$ be the collection of all g roots of $U_\mathfrak{r}(x)$, i.e.,

$$U_\mathfrak{r}(x) = \prod_{j=1}^{g} (x - c_j) \in K[x].$$

Let us put

$$d_j = V_\mathfrak{r}(c_j) \ \forall j = 1, \dots, g.$$

It is proven in [9, Th. 3.2] that $Q_j = (c_j, d_j)$ lies in $\mathcal{C}(K)$ for all j and

$$\mathfrak{a}_\mathfrak{r} := \mathrm{cl}\left(\left(\sum_{j=1}^{g} (Q_j)\right) - g(\infty)\right) \in J(K)$$

satisfies $2\mathfrak{a}_\mathfrak{r} = P$, i.e., $\mathfrak{a}_\mathfrak{r} \in M_{1/2,P}$. In addition, **none of Q_j coincides with any** $\mathfrak{W}_\alpha$, i.e.,

$$U_\mathfrak{r}(\alpha) \ne 0, \ c_j \ne \alpha, \ d_j \ne 0.$$

The main result of [9] asserts that the map

$$\mathfrak{R}_{1/2,P} \to M_{1/2,P}, \ \mathfrak{r} \mapsto \mathfrak{a}_\mathfrak{r}$$

is a **bijection**.

Remark 2.2. Notice that one may express explicitly $\mathfrak{r}$ in terms of $U_{\mathfrak{r}}(x)$ and $V_{\mathfrak{r}}(x)$. Namely [9, Th. 3.2], *none* of $\alpha \in \mathfrak{R}$ is a root of $U_{\mathfrak{r}}(x)$ and

$$\mathfrak{r}(\alpha) = \mathbf{s}_1(\mathfrak{r}) + (-1)^g \frac{V_{\mathfrak{r}}(\alpha)}{U_{\mathfrak{r}}(\alpha)} \text{ for all } \alpha \in \mathfrak{R}. \tag{1}$$

In order to determine $\mathbf{s}_1(\mathfrak{r})$, let us fix two *distinct* roots $\beta, \gamma \in \mathfrak{R}$. Then [9, Cor. 3.4]

$$\frac{V_{\mathfrak{r}}(\gamma)}{U_{\mathfrak{r}}(\gamma)} \neq \frac{V_{\mathfrak{r}}(\beta)}{U_{\mathfrak{r}}(\beta)}$$

and

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

2.3. Mumford representations (see [4, Sect. 3.12], [8, Sect. 13.2, pp. 411–415, especially, Prop. 13.4, Th. 13.5 and Th. 13.7]). Recall [8, Sect. 13.2, p. 411] that if D is an effective divisor on $\mathcal{C}$ of (nonnegative) degree m, whose support does *not* contain ∞, then the degree zero divisor $D - m(\infty)$ is called *semi-reduced* if it enjoys the following properties.

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

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

It is known ([4, Ch. 3a], [8, Sect. 13.2, Prop. 3.6 on p. 413]) that for each $\mathfrak{a} \in J(K)$ there exist *exactly one* nonnegative m and (effective) degree m divisor D such that the degree zero divisor $D - m(\infty)$ is *reduced* and $\operatorname{cl}(D - m(\infty)) = \mathfrak{a}$. If

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

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

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

The *Mumford representation* of $\mathfrak{a} \in J(K)$ is the pair $(U(x), V(x))$ of polynomials $U(x), V(x) \in K[x]$ such that

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

is a degree m monic polynomial while $V(x)$ has degree $< m = \deg(U)$, the polynomial $V(x)^2 - f(x)$ is divisible by $U(x)$, and

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

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

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

2.4. In the notation of Subsect. 2.1, let us consider the effective degree g divisor

$$D_{\mathfrak{r}} := \sum_{j=1} (Q_j)$$

on $\mathcal{C}$. Then $\mathrm{supp}(D_{\mathfrak{r}})$ (obviously) does contain *neither* ∞ *nor* any of $\mathfrak{W}_\alpha$'s. It is proven in [9, Th. 3.2] that the divisor $D_{\mathfrak{r}} - g(\infty)$ is *reduced* and the pair $(U_{\mathfrak{r}}(x), V_{\mathfrak{r}}(x))$ is the Mumford representation of

$$\mathfrak{a}_{\mathfrak{r}} := \mathrm{cl}(D_{\mathfrak{r}} - g(\infty)).$$

In particular, if $Q \in C(K)$ lies in $\mathrm{supp}(D)$ (i.e., is one of Q_j's) then $\iota(Q)$ does *not*.

Lemma 2.5. *Let D be an effective divisor on $\mathcal{C}$ of degree $m > 0$ such that $m \le 2g+1$ and* $\mathrm{supp}(D)$ *does not contain ∞. Assume that the divisor $D - m(\infty)$ is principal.*

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

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

Proof. All the assertions except (2)(iii) are already proven in [9, Lemma 2.2]. In order to prove the remaining one, let us split the polynomial $v(x)$ into a product $v(x) = (x - \alpha)^d v_1(x)$ where d is a nonnegative integer and $v_1(x) \in K[x]$ satisfies $v_1(\alpha) \neq 0$. Then $\mathfrak{W}_\alpha$ appears in $D - m(\infty)$ with multiplicy $2d$, because $(x - \alpha)$ has a double zero at $\mathfrak{W}_\alpha$. (See also [5].) □

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

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

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

Theorem 2.6 (See Th. 2.5 of [9])**.** *Suppose that $g > 1$ and let*

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

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

3. Adding Weierstrass points

In this section we discuss how to compute a sum $\mathfrak{a}+\mathfrak{W}_\beta$ in $J(K)$ when $\mathfrak{a}\in J(K)$ lies neither on Θ nor on its translation $\Theta+\mathfrak{W}_\beta$. Let $D-g(\infty)$ be the reduced divisor on $\mathcal{C}$, whose class represents $\mathfrak{a}$. Here

$$D=\sum_{j=1}^{g}(Q_j) \text{ where } Q_j=(a_j,b_j)\in\mathcal{C}(K)\setminus\{\infty\}$$

is a degree g effective divisor. Let $(U(x),V(x))$ be the Mumford representation of $\mathrm{cl}(D-g(\infty))$. We have

$$\deg(U)=g>\deg(V)$$

,

$$U(x)=\prod_{j=1}^{g}(x-a_j),\ b_j=V(a_j)\ \forall j$$

and $f(x)-V(x)^2$ is divisible by $U(x)$.

Example 3.1. Assume additionally that *none* of Q_j coincides with $\mathfrak{W}_\beta=(\beta,0)$, i.e.,

$$U(\beta)\neq 0.$$

Let us find explicitly the Mumford representation $(U^{[\beta]}(x),V^{[\beta]}(x))$ of the sum

$$\mathfrak{a}+\mathfrak{W}_\beta=\mathrm{cl}(D-m(\infty))+\mathrm{cl}((\mathfrak{W}_\beta)-(\infty))=\mathrm{cl}((D+(\mathfrak{W}_\beta))-(g+1)(\infty))=\mathrm{cl}(D_1-(g+1)(\infty)).$$

where

$$D_1:=D+(\mathfrak{W}_\beta)=\left(\sum_{j=1}^{g}(Q_j)\right)+(\mathfrak{W}_\beta)$$

is a degree $(g+1)$ effective divisor on $\mathcal{C}$. (We will see that $\deg(\tilde{U}^{[\beta]})=g$.) Clearly, $D_1-(g+1)(\infty)$ is *semi-reduced* but *not* reduced.

Let us consider the polynomials

$$U_1(x)=(x-\beta)U(x),\ V_1(x)=V(x)-\frac{V(\beta)}{U(\beta)}U(x)\in K[x].$$

Then U_1 is a degree $(g+1)$ monic polynomial, $\deg(V_1)\leq g$,

$$V_1(\beta)=0,\ V_1(a_j)=V(a_j)=b_j\ \forall j$$

and $f(x)-V_1(x)^2$ is divisible by $U_1(x)$. (The last assertion follows from the divisibility of both $f(x)$ and $V_1(x)$ by $x-\beta$ combined with the divisibility of $f(x)-V(x)^2$ by $U(x)$.) If we put

$$a_{g+1}=\beta,\ b_{g+1}=0,\ Q_{g+1}=\mathfrak{W}_\beta=(\beta,0)$$

then

$$U_1(x)=\prod_{j=1}^{g+1}(x-a_j),\ D_1=\sum_{j=1}^{g+1}(Q_j) \text{ where } Q_j=(a_j,b_j)\in\mathcal{C}(K),\ b_j=V_1(a_j)\forall j$$

and $f(x)-V_1(x)^2$ is divisible by $U_1(x)$. In particular, $(U_1(x),V_1(x))$ is the pair of polynomials that corresponds to semi-reduced $D_1-(g+1)(\infty)$ as described in [8, Prop. 13.4 and Th. 3.5]. In order to find the Mumford representation of

$\mathrm{cl}(D_1 - (g+1)(\infty))$, we use an algorithm described in [8, Th. 13.9]. Namely, let us put

$$\tilde{U}(x) = \frac{f(x) - V_1(x)^2}{U_1(x)} \in K[x].$$

Since $\deg(V_1(x)) \le g$ and $\deg(f) = 2g+1$, we have

$$\deg\left(V_1(x)^2\right) \le 2g,\ \deg\left(f(x) - V_1(x)^2\right) = 2g+1, \deg\left(\tilde{U}(x)\right) = g.$$

Since $f(x)$ is monic, $f(x) - V_1(x)^2$ is also monic and therefore $\tilde{U}(x)$ is also monic, because $U_1(x)$ is monic. By [8, Th. 13.9], $U^{[\beta]}(x) = \tilde{U}(x)$ (since the latter is monic and has degree $g \le g$) and $V^{[\beta]}(x)$ is the *remainder* of $-V_1(x)$ with respect to division by $\tilde{U}(x)$. Let us find this remainder. We have

$$-V_1(x) = -\left(V(x) - \frac{V(\beta)}{U(\beta)}U(x)\right) = -V(x) + \frac{V(\beta)}{U(\beta)}U(x).$$

Recall that

$$\deg(V) < g = \deg(U) = \deg(\tilde{U}).$$

This implies that the coefficient of $-V_1$ at x^g equals $V(\beta)/U(\beta)$ and therefore

$$V^{[\beta]}(x) = \left(-V(x) + \frac{V(\beta)}{U(\beta)}U(x)\right) - \frac{V(\beta)}{U(\beta)}\tilde{U}(x) = -V(x) + \frac{V(\beta)}{U(\beta)}\left(U(x) - \tilde{U}(x)\right).$$

Using formulas above for $U_1, V_1, \tilde{U}$, we obtain that

$$U^{[\beta]}(x) = \frac{f(x) - \left(V(x) - \frac{V(\beta)}{U(\beta)}U(x)\right)^2}{(x-\beta)U(x)}, \tag{3}$$

$$V^{[\beta]}(x) = -V(x) + \frac{V(\beta)}{U(\beta)}\left(U(x) - \frac{f(x) - \left(V(x) - \frac{V(\beta)}{U(\beta)}U(x)\right)^2}{(x-\beta)U(x)}\right). \tag{4}$$

Remark 3.2. There is an algorithm of David Cantor [8, Sect. 13.3] that explains how to compute the Mumford representation of a sum of arbitrary divisor classes (elements of $J(K)$) when their Mumford representations are given.

Remark 3.3. Suppose that $\mathfrak{a} \in J(K)$ and $P = 2\mathfrak{a}$ lies in $\mathcal{C}(K)$ but is not the zero of the group law. Then $\mathfrak{a}$ does not lie on the theta divisor (Theorem 2.6) and satisfies the conditions of Example 3.1 for all $\beta \in \mathfrak{R}$ (see Subsect. 2.1).

4. Proof of Main Theorem

Let us choose an order on $\mathfrak{R}$. This allows us to identify $\mathfrak{R}$ with $\{1, \dots, 2g, 2g+1\}$ and list elements of $\mathfrak{R}$ as $\{\alpha_1, \dots, \alpha_{2g}, \alpha_{2g+1}\}$. Then

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

and the affine equation for $\mathcal{C} \setminus \{\infty\}$ is

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

Slightly abusing notation, we denote $\mathfrak{W}_{\alpha_i}$ by $\mathfrak{W}_i$.

Let us consider the closed affine K-subset $\tilde{\mathcal{C}}$ in the affine K-space $\mathbb{A}^{2g+1}$ with coordinate functions $z_1, \dots, z_{2g}, z_{2g+1}$ that is cut out by the system of quadratic equations

$$z_1^2 + \alpha_1 = z_2^2 + \alpha_2 = \cdots = z_{2g+1}^2 + \alpha_{2g+1}.$$

We write x for the regular function $z_i^2 + \alpha_i$ on $\tilde{\mathcal{C}}$, which does *not* depend on a choice of i. By Hilbert's Nullstellensatz, the K-algebra $K[\tilde{\mathcal{C}}]$ of regular functions on $\tilde{\mathcal{C}}$ is canonically isomorphic to the following K-algebra. First, we need to consider the quotient A of the polynomial $K[x]$-algebra $K[x][T_1, \dots, T_{2g+1}]$ by the ideal generated by all quadratic polynomials $T_i^2 - (x - \alpha_i)$. Next, $K[\tilde{\mathcal{C}}]$ is canonically isomorphic to the quotient $A/\mathcal{N}(A)$ where $\mathcal{N}(A)$ is the nilradical of A. In the next section (Example 5.4) we will prove that A has no zero divisors (in particular, $\mathcal{N}(A) = \{0\}$) and therefore $\tilde{\mathcal{C}}$ is *irreducible*. (See also [3].) We write y for the regular function

$$y = -\prod_{i=1}^{2g} z_i \in K[\tilde{\mathcal{C}}].$$

Clearly, $y^2 = \prod_{i=1}^{2g}(x - \alpha_i)$ in $K[\tilde{\mathcal{C}}]$. The pair (x, y) gives rise to the finite regular map of affine K-varieties (actually, curves)

$$\text{(5)} \qquad \mathfrak{h} : \tilde{\mathcal{C}} \to \mathcal{C} \setminus \{\infty\}, \ (r_1, \dots, r_{2g}, r_{2g+1}) \mapsto (a, b) = \left(r_1^2 + \alpha_1, -\prod_{i=1}^{2g+1} r_i\right)$$

of degree 2^{2g}. For each

$$P = (a, b) \in K^2 = \mathbb{A}^2(K) \text{ with } b^2 = \prod_{i=1}^{2g+1}(a - \alpha_i)$$

the fiber $\mathfrak{h}^{-1}(P) = \mathfrak{R}_{1/2,P}$ consists of (familiar) collections of square roots

$$\mathfrak{r} = \{r_i = \sqrt{a - \alpha_i} \mid 1 \le i \le 2g + 1\}$$

with $\prod_{i=1}^{2g+1} r_i = -b$. Each such $\mathfrak{r}$ gives rise to $\mathfrak{a}_{\mathfrak{r}} \in J(K)$ such that

$$2\mathfrak{a}_{\mathfrak{r}} = P \in \mathcal{C}(K) \subset J(K)$$

(see [9, Th. 3.2]). On the other hand, for each $\mathfrak{W}_l = (\alpha_l, 0)$ (with $1 \le l \le 2g + 1$) the sum $\mathfrak{a}_{\mathfrak{r}} + \mathfrak{W}_l$ is also a half of P and therefore corresponds to a certain collection of square roots. Which one? The answer is given by Theorem 1.1. We repeat its statement, using the new notation.

Theorem 4.1. *Let $P = (a, b)$ be a K-point on $\mathcal{C}$ and $\mathfrak{r} = (r_1, \dots, r_{2g}, r_{2g+1})$ be a collection of square roots $r_i = \sqrt{a - \alpha_i} \in K$ such that $\prod_{i=1}^{2g+1} r_i = -b$. Let l be an integer that satisfies $1 \le l \le 2g + 1$ and let*

$$\text{(6)} \qquad \mathfrak{r}^{[l]} = \left(r_1^{[l]}, \dots, r_{2g}^{[l]}, r_{2g+1}^{[l]}\right) \in \mathfrak{h}^{-1}(P) \subset \tilde{\mathcal{C}}(K)$$

be the collection of square roots $r_i^{[l]} = \sqrt{a - \alpha_i}$ such that

$$\text{(7)} \qquad r_l^{[l]} = r_l, \ r_i^{[l]} = -r_i \ \forall \ i \ne l.$$

Then

$$\mathfrak{a}_{\mathfrak{r}} + \mathfrak{W}_l = \mathfrak{a}_{\mathfrak{r}^{[l]}}.$$

Example 4.2. Let us take as P the point $\mathfrak{W}_l = (\alpha_l, 0)$. Then

$$r_l = \sqrt{\alpha_l - \alpha_l} = 0 \ \forall \ \mathfrak{r} = (r_1, \dots, r_{2g}, r_{2g+1}) \in \mathfrak{h}^{-1}(\mathfrak{W}_l)$$

and therefore

$$\mathfrak{r}^{[l]} = (-r_1, \dots, -r_{2g}, -r_{2g+1}) = -\mathfrak{r}.$$

It follows from Example 1.3 (if we take $\beta = \alpha_l$) that

$$\mathfrak{a}_{\mathfrak{r}} + \mathfrak{W}_l = \mathfrak{a}_{\mathfrak{r}} - \mathfrak{W}_l = \mathfrak{a}_{\mathfrak{r}} - 2\mathfrak{a}_{\mathfrak{r}} = -\mathfrak{a}_{\mathfrak{r}} = \mathfrak{a}_{\mathfrak{r}^{[l]}}.$$

This proves Theorem 4.1 in the case of $P = \mathfrak{W}_l$. We are going to deduce the general case from this special one.

4.3. Before starting the proof of Theorem 4.1, let us define for each collections of signs

$$\varepsilon = \{\epsilon_i = \pm 1 \mid 1 \le i \le 2g+1, \prod_{i=1}^{2g+1} \epsilon_i = 1\}$$

the biregular automorphism

$$T_\varepsilon : \tilde{\mathcal{C}} \to \tilde{\mathcal{C}}, \ z_i \mapsto \epsilon_i z_i \ \forall i.$$

Clearly, all T_ε constitute a finite automorphism group of $\tilde{\mathcal{C}}$ that leaves invariant every K-fiber of $\mathfrak{h} : \tilde{\mathcal{C}} \to \mathcal{C} \setminus \{\infty\}$, acting on it **transitively**. Notice that if T_ε leaves invariant all the points of a certain fiber $\mathfrak{h}^{-1}(P)$ with $P \in \mathcal{C}(K)$ then all the $\epsilon_i = 1$, i.e., T_ε is the identity map.

Proof of Theorem 4.1. Let us put

$$\beta := \alpha_l.$$

Then we have

$$\mathfrak{W}_l = (\alpha_l, 0) = (\beta, 0).$$

Let us consider the automorphism (involution)

$$\mathfrak{s}^{[l]} : \tilde{\mathcal{C}} \to \tilde{\mathcal{C}}, \ \mathfrak{r} \mapsto \mathfrak{r}^{[l]}$$

of $\tilde{\mathcal{C}}$ defined by (6) and (7). We need to define another (actually, it will turn out to be the same) involution (and therefore an automorphism)

$$\mathfrak{t}^{[l]} : \tilde{\mathcal{C}} \to \tilde{\mathcal{C}}$$

that is defined by

$$\mathfrak{a}_{\mathfrak{t}^{[l]}(\mathfrak{r})} = \mathfrak{a}_{\mathfrak{r}} + \mathfrak{W}_l$$

as a composition of the following **regular** maps. First, $\mathfrak{r} \in \tilde{\mathcal{C}}(K)$ goes to the pair of polynomials $(U_{\mathfrak{r}}(x), V_{\mathfrak{r}}(x))$ as in Remark 2.2, which is the Mumford representation of $\mathfrak{a}_{\mathfrak{r}}$ (see Subsect. 2.4). Second, $(U_{\mathfrak{r}}(x), V_{\mathfrak{r}}(x))$ goes to the pair of polynomials $(U^{[\beta]}(x), V^{[\beta]}(x))$ defined by formulas (3) and (3) in Section 3, which is the Mumford representation of $\mathfrak{a}_{\mathfrak{r}} + \mathfrak{W}_l$. Third, applying formulas (1) and (2) in Remark 2.2 to $(U^{[\beta]}(x), V^{[\beta]}](x))$ (instead of $(U(x), V(x))$), we get at last $\mathfrak{t}^{[l]}(\mathfrak{r}) \in \tilde{\mathcal{C}}(K)$ such that

$$\mathfrak{a}_{\mathfrak{t}^{[l]}(\mathfrak{r})} = \mathfrak{a}_{\mathfrak{r}} + \mathfrak{W}_l.$$

Clearly, $\mathfrak{t}^{[l]}$ is a regular selfmap of $\tilde{\mathcal{C}}$ that is an involution, which implies that $\mathfrak{t}^{[l]}$ is a biregular automorphism of $\tilde{\mathcal{C}}$. It is also clear that both $\mathfrak{s}^{[l]}$ and $\mathfrak{t}^{[l]}$ leave invariant every fiber of $\mathfrak{h} : \tilde{\mathcal{C}} \to \mathcal{C} \setminus \{\infty\}$ and coincide on $\mathfrak{h}^{-1}(\mathfrak{W}_l)$, thanks to Example 4.2. This implies that $\mathfrak{u} := \left(\mathfrak{s}^{[l]}\right)^{-1} \mathfrak{t}^{[l]}$ is a biregular automorphism of $\tilde{\mathcal{C}}$ that leaves invariant every fiber of $\mathfrak{h} : \tilde{\mathcal{C}} \to \mathcal{C} \setminus \{\infty\}$ and acts as the identity map on $\mathfrak{h}^{-1}(\mathfrak{W}_l)$. The invariance of each fiber of $\mathfrak{h}$ implies that $\tilde{\mathcal{C}}(K)$ coincides with the finite union of its closed subsets $\tilde{\mathcal{C}}_\varepsilon$ defined by the condition

$$\tilde{\mathcal{C}}_\varepsilon := \{Q \in \tilde{\mathcal{C}}(K) \mid \mathfrak{u}(Q) = T_\varepsilon(Q)\}.$$

Since $\tilde{\mathcal{C}}$ is irreducible, the whole $\tilde{\mathcal{C}}(K)$ coincides with one of $\tilde{\mathcal{C}}_\varepsilon$. In particular, the fiber

$$\mathfrak{h}^{-1}(\mathfrak{W}_l) \subset \tilde{\mathcal{C}}_\varepsilon$$

and therefore T_ε acts identically on all points of $\mathfrak{h}^{-1}(\mathfrak{W}_l)$. In light of arguments of Subsect. 4.3, T_ε is the *identity map* and therefore $\mathfrak{u}$ acts identically on the whole $\tilde{\mathcal{C}}(K)$. This means that $\mathfrak{s}^{[l]} = \mathfrak{t}^{[l]}$, i.e.,

$$\mathfrak{a}_{\mathfrak{r}} + \mathfrak{W}_l = \mathfrak{a}_{\mathfrak{r}^{[l]}}.$$

□

4.4. Let $\phi : \mathfrak{R} \to \mathbb{F}_2$ be a function that satisfies $\sum_{\alpha\in\mathfrak{R}} \phi(\alpha) = 0$, i.e. $\phi \in (\mathbb{F}_2^{\mathfrak{R}})^0$. Then the finite subset

$$\text{supp}(\phi) = \{\alpha \in \mathfrak{R} \mid \phi(\alpha) \neq 0\} \subset \mathfrak{R}$$

has *even* cardinality and the corresponding point of $J[2]$ is

$$\mathfrak{T}_\phi = \sum_{\alpha\in\mathfrak{R}} \phi(\alpha)\mathfrak{W}_\alpha = \sum_{\alpha\in\text{supp}(\phi)} \mathfrak{W}_\alpha = \sum_{\gamma\notin\text{supp}(\phi)} \mathfrak{W}_\gamma.$$

Theorem 4.5. *Let $\mathfrak{r} \in \mathfrak{R}_{1/2,P}$. Let us define $\mathfrak{r}^{(\phi)} \in \mathfrak{R}_{1/2,P}$ as follows.*

$$\mathfrak{r}^{(\phi)}(\alpha) = -\mathfrak{r}(\alpha)\ \forall \alpha \in \text{supp}(\phi);\ \ \mathfrak{r}^{(\phi)}(\gamma) = \mathfrak{r}(\gamma)\ \forall \gamma \notin \text{supp}(\phi).$$

Then

$$\mathfrak{a}_{\mathfrak{r}} + \mathfrak{T}_\phi = \mathfrak{a}_{\mathfrak{r}^{(\phi)}}.$$

Remark 4.6. If ϕ is identically zero then

$$\mathfrak{T}_\phi = 0 \in J[2],\ \ \mathfrak{r}^{(\phi)} = \mathfrak{r}$$

and the assertion of Theorem 4.5 is obviously true. If $\alpha_l \in \mathfrak{R}$ and $\phi = \psi_{\alpha_l}$, i.e. $\text{supp}(\phi) = \mathfrak{R} \setminus \{\alpha_l\}$ then

$$\mathfrak{T}_\phi = \mathfrak{W}_l \in J[2],\ \ \mathfrak{r}^{(\phi)} = \mathfrak{r}^{[l]}$$

and the assertion of Theorem 4.5 follows from Theorem 4.1.

Proof of Theorem 4.5. We may assume that ϕ is *not* identically zero. We need to apply Theorem 4.1 d times where d is the (even) cardinality of $\text{supp}(\phi)$ in order to get $\mathfrak{r}' \in \mathfrak{R}_{1/2,P}$ such that

$$\mathfrak{a}_{\mathfrak{r}} + \sum_{\alpha\in\text{supp}(\phi)} \mathfrak{W}_\alpha = \mathfrak{a}_{\mathfrak{r}'}.$$

Let us check how many times do we need to change the sign of each $\mathfrak{r}(\beta)$. First, if $\beta \notin \text{supp}(\phi)$ then we need to change to sign of $\mathfrak{r}(\beta)$ at every step, i.e., we do it exactly d times. Since d is even, the sign of $\mathfrak{r}(\beta)$ remains the same, i.e.,

$$\mathfrak{r}'(\beta) = \mathfrak{r}(\beta)\ \forall \beta \notin \text{supp}(\phi).$$

Now if $\beta \in \text{supp}(\phi)$ then we need to change the sign of $\mathfrak{r}(\beta)$ every time when we add W_α with $\alpha \neq \beta$ and it occurs exactly $(d-1)$ times. On the other hand, when we add $\mathfrak{W}_\beta$, we don't change the sign of $\mathfrak{r}(\beta)$. So, we change the sign of $\mathfrak{r}(\beta)$ exactly $(d-1)$ times, which implies that

$$\mathfrak{r}'(\beta) = -\mathfrak{r}(\beta)\ \forall \beta \in \text{supp}(\phi).$$

Combining the last two displayed formula, we obtained that

$$\mathfrak{r}' = \mathfrak{r}^{(\phi)}.$$

□

5. Useful Lemma

As usual, we define the Kronecker delta δ_{ik} as 1 if $i = k$ and 0 if $i \neq k$.

The following result is probably well known but I did not find a suitable reference. (However, see [3, Lemma 5.10] and [1, pp. 425–427].)

Lemma 5.1. *Let n be a positive integer, E a field provided with n distinct discrete valuation maps*

$$\nu_i : E^* \twoheadrightarrow \mathbb{Z},\ (i = 1, \dots, n).$$

For each i let $O_{\nu_i} \subset E$ the discrete valuation ring attached to ν_i and $\pi_i \in O_{\nu_i}$ its uniformizer, i.e., a generator of the maximal ideal in O_{ν_i}. Suppose that for each i we are given a prime number p_i such that the characteristic of the residue field O_{ν_i}/π_i is different from p_k for all $k \neq i$. Let us assume also that

$$\nu_i(\pi_k) = \delta_{ik}\ \forall i, k = 1, \dots n,$$

i.e, each π_i is a ν_k-adic unit if $i \neq k$.

Then the the quotient $B = E[T_1, \dots, T_n]/(T_1^{p_1} - \pi_1, \dots, T_n^{p_n} - \pi_n)$ of the polynomial E-algebra $E[T_1, \dots T_n]$ by the ideal generated by all $T_i^{p_i} - \pi_i$ is a field that is an algebraic extension of E of degree $\prod_{i=1}^n p_i$. In addition, the set of monomials

$$S = \{\prod_{i=1}^n T_i^{e_i} \mid 0 \le e_i \le p_i - 1\} \subset E[T_1, \dots T_n]$$

maps injectively into B and its image is a basis of the E-vector space B.

Remark 5.2. By definition of a uniformizer, $\nu_i(\pi_i) = 1$ for all i.

Proof of Lemma 5.1. First, the cardinality of S is $\prod_{i=1}^n p_i$ and the image of S generates B as the E-vector space. This implies that if the E-dimension of B is $\prod_{i=1}^n p_i$ then the image of S is a basis of the E-vector space B. Second, notice that for each i the polynomial $T^{p_i} - \pi_i$ is irreducible over E, thanks to the Eisenstein criterion applied to ν_i and therefore $E[T_i]/(T^{p_i} - \pi_i)$ is a *field* that is an algebraic degree p_i extension of E. In particular, the E-dimension of $E[T_i]/(T^{p_i} - \pi_i)$ is p_i. This proves Lemma for $n = 1$.

Induction by n. Suppose that $n > 1$ and consider the finite degree p_i field extension $E_n = E[T_n]/(T^{p_n} - \pi_n)$ of E.

Clearly, the E-algebra B is isomorphic to the quotient $E_n[T_1, \dots T_{n-1}]/(T_1^{p_1} - \pi_1, \dots, T_{n-1}^{p_{n-1}} - \pi_{n-1})$ of the polynomial ring $E_n[T_1, \dots T_{n-1}]$ by the ideal generated by all polynomials $T_i^{p_i} - \pi_i$ with $i < n$. Our goal is to apply the induction assumption to E_n instead of E. In order to do that, let us consider for each $i < n$ the integral closure $\tilde{O}_i$ of O_{ν_i} in E_n. It is well known that $\tilde{O}_i$ is a Dedekind ring. Our conditions imply that E_n/E is *unramified* at all ν_i for all $i < n$. This means that if $\mathcal{P}_i$ is a maximal ideal of $\tilde{O}_i$ that contains $\pi_i\tilde{O}_i$ (such an ideal always exists) and

$$\mathrm{ord}_{\mathcal{P}_i} : E_n^* \twoheadrightarrow \mathbb{Z}$$

is the discrete valuation map attached to $\mathcal{P}_i$ then the restriction of $\mathrm{ord}_{\mathcal{P}_i}$ to E^* coincides with ν_i. This implies that for all positive integers $i, k \le n-1$

$$\mathrm{ord}_{\mathcal{P}_i}(\pi_k) = \nu_i(\pi_k) = \delta_{ik}.$$

In particular,

$$\mathrm{ord}_{\mathcal{P}_i}(\pi_i) = \nu_i(\pi_i) = 1,$$

i.e, π_i is a uniformizer in the corresponding discrete valuation (sub)ring $O_{\mathrm{ord}_{\mathcal{P}_i}}$ of E_n attached to $\mathrm{ord}_{\mathcal{P}_i}$. Now the induction assumption applied to E_n and its $(n-1)$ discrete valuation maps $\mathrm{ord}_{\mathcal{P}_i}$ $(1 \le i \le n-1)$ implies that B/E_n is a field extension of degree $\prod_{i=1}^{n-1} p_i$. This implies that the degree

$$[B : E] = [B : E_n][E_n : E] = \left(\prod_{i=1}^{n-1} p_i\right) p_n = \prod_{i=1}^{n} p_i.$$

This means that the E-dimension of B is $\prod_{i=1}^{n} p_i$ and therefore the image of S is a basis of the E-vector space B. □

Corollary 5.3. *We keep the notation and assumptions of Lemma 5.1. Let R be a subring of E that contains 1 and all π_i $(1 \le i \le n)$. Then the quotient $B_R = R[T_1, \dots, T_n]/(T_1^{p_1} - \pi_1, \dots, T_n^{p_n} - \pi_n)$ of the polynomial R-algebra $R[T_1, \dots, T_n]$ by the ideal generated by all $T_i^{p_i} - \pi_i$ has no zero divisors.*

Proof. There are the natural homomorphisms of R-algebras

$$R[T_1, \dots T_n] \twoheadrightarrow B_R \to B$$

such that the first homomorphism is surjective and the *injective* image of

$$S \subset R[T_1, \dots T_n] \subset E[T_1, \dots T_n]$$

in B is a basis of the E-vector space B. On the other hand, the image of S generates B_R as R-module. It suffices to prove that $B_R \to B$ is injective, since B is a field by Lemma 5.1.

Suppose that $u \in B_R$ goes to 0 in B. Clearly, u is a linear combination of (the images of) elements of S with coefficients in R. Since the image of u in B is 0, all these coefficients are zeros, i.e., $u = 0$ in B_R. □

Example 5.4. We use the notation of Section 4. Let us put $n = 2g+1, R = K[x], E = K(x), \pi_i = x - \alpha_i, p_i = 2$ and let

$$\nu_i : E^* = K(x)^* \twoheadrightarrow \mathbb{Z}$$

be the discrete valuation map of the field of rational functions $K(x)$ attached to α_i. Then $K[\tilde{\mathcal{C}}] = B_R/\mathcal{N}(B_R)$ where $\mathcal{N}(B_R)$ is the nilradical of B_R. It follows from Corollary 5.3 that $\mathcal{N}(B_R) = \{0\}$ and $K[\tilde{\mathcal{C}}]$ has no zero divisors, i.e., $\tilde{\mathcal{C}}$ is irreducible.

References

[1] T. Bandman, S. Garion, F. Grunewald, *On the surjectivity of Engel words on* PSL$(2, q)$. Groups Geom. Dyn. **6** (2012), 409–439.

[2] B.M. Bekker, Yu.G. Zarhin, *The divisibility by 2 of rational points on elliptic curves.* Algebra i Analiz **29:4** (2017), 196–239; St. Petersburg Math. J. **29** (2018), 683–713.

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

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

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

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

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

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

[9] Yu. G. Zarhin, *Division by 2 on odd degree hyperelliptic curves and their jacobians.* Izvestiya RAN **83:3** (2019), 93–112; Izvestiya Mathematics **83:3** (2019), 501–520.

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

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