ANNALES

DE

L'INSTITUT FOURIER

Jordi GUÀRDIA

Jacobian Nullwerte, periods and symmetric equations for hyperelliptic curves

Tome 57, n° 4 (2007), p. 1253-1283.

<http://aif.cedram.org/item?id=AIF_2007__57_4_1253_0>

Ann. Inst. Fourier, Grenoble
57, 4 (2007) 1253-1283

JACOBIAN NULLWERTE, PERIODS AND SYMMETRIC EQUATIONS FOR HYPERELLIPTIC CURVES

by Jordi GUÀRDIA (*)

Abstract. — We propose a solution to the hyperelliptic Schottky problem, based on the use of Jacobian Nullwerte and symmetric models for hyperelliptic curves. Both ingredients are interesting on its own, since the first provide period matrices which can be geometrically described, and the second have remarkable arithmetic properties.

Résumé. — Nous proposons une solution au problème de Schottky hyperelliptique. Celle-ci est basée sur l'utilisation de matrices jacobiennes de fonctions thêta et de modèles symétriques pour les courbes hyperelliptiques. Ces ingrédients sont intéressants en eux-mêmes : le premier fournit des matrices de périodes qui peuvent être décrites géométriquement et le second possède de remarquables propriétés arithmétiques.

Introduction

The problem of determining a complex abelian variety from its period lattice is very-well understood from the theoretical viewpoint. The situation is slightly different when the problem is considered with a computational insight. Efficient numerical algorithms to find equations of an elliptic curve from its period lattice were available many years ago, and there are large tables of elliptic curves both in printed and electronic form ([3], [5], [18]). Concerning higher-dimensional abelian varieties, last years have seen a significant progress which has led to the elaboration of tables of hyperelliptic curves whose jacobian variety has a given period lattice ([27], [31], [10], [9]). There are two main directions in the proposed solutions.

Keywords: Hyperelliptic curves, periods, Jacobian Nullwerte.
Math. classification: 11G30, 14H42.
(*) Partially supported by MCYT BFM2003-06768-C02-02.

The first solution is essentially due to Mestre [20], who considered the case of abelian surfaces. Weber [29] generalized his work to Jacobian varieties of hyperelliptic curves of any genus. The general outline of Mestre's method is the following: given a normalized period matrix in the Siegel upper half space corresponding to an abelian variety, one calculates, by means of *Thetanullwerte*, certain algebraic invariants of a curve whose Jacobian variety is isomorphic to the desired abelian variety. One deduces from these invariants the field of moduli of the curve and finds an equation of the curve over its field of definition. The computations require a certain degree of accuracy, tend to produce huge intermediate results, and yield final equations with large coefficients, which must be reduced by some additional method. Apart from computational issues, this method has a second drawback: its geometric nature overpasses the arithmetic of the problem: the initial abelian variety and the Jacobian of the found curve may be only isomorphic over the algebraic closure of its field of definition.

We proposed a second solution for genus two curves inspired in the use of Jacobian Nullwerte. The ideas in [10] drove us to an algorithm which, given the period lattice of a basis of algebraic differential forms of an abelian surface, finds the equation of a genus two hyperelliptic curve defined over the same field as the differential forms. With our method the arithmetic is preserved, but it requires a better knowledge of the abelian variety. It has been applied satisfactorily to build a table of 2-dimensional factors of certain modular Jacobian varieties [9] and provide examples of abelian surfaces with several polarizations [7]. Unfortunately, the algorithm cannot be applied when we only know a normalized period matrix in the Siegel upper half plane, since in general these periods do not correspond to algebraic differential forms.

Our initial motivation for the present work was to overcome this difficulty controlling the arithmetic of the problem. Classical ideas already found in [30] explain a method to determine a basis of algebraic differential forms from a normalized period matrix. Jacobian Nullwerte are the key tool for making this construction explicit. The combination of this ideas with our original algorithm for abelian surfaces led us to a particular kind of equation for hyperelliptic curves, which we have called *symmetric models*. We studied symmetric equations for elliptic curves and its applications in class field theory in [12]. We present here the geometric study of symmetric models for hyperelliptic curves of any genus. We describe their arithmetic properties, as well as its interest in relation with the problem mentioned above.

After a very short summary of basic facts on hyperelliptic curves and their Jacobians, we develop the study of symmetric equations in section 2. The next section is devoted to recall the main results concerning Jacobian Nullwerte for hyperelliptic curves. In section 4 we recall classical formulas of Thomae relating Thetanullwerte and Jacobian Nullwerte to Weierstrass points of hyperelliptic curves. Some remarks on the theoretical implications of these results are collected in sections 5 and 6. We explain the construction of algebraic differential forms from normalized period matrices in section 7. We then give in section 8 a general method to find a symmetric equation for a general hyperelliptic curve given a normalized period matrix for it. In the last two sections we particularize the results of the paper for hyperelliptic curves of genus 2 and 3, in which some improvements can be obtained.

1. Preliminaries on hyperelliptic curves and their Jacobians

We introduce here the notation which will be used along the paper. Consider a hyperelliptic curve in Weierstrass form:

$$C : Y^2 = f(X) = (X - \alpha_1) \cdots (X - \alpha_{2g+2}),$$

so that $W_1 = (\alpha_1, 0), \ldots, W_{2g+2} = (\alpha_{2g+2}, 0)$ are its Weierstrass points. We denote by $\{\omega_j = x^j dx/y\}_{j=0,\ldots,g-1}$ the usual basis of $H^0(C, \Omega_1)$, and by (Ω_1, Ω_2) a period matrix for this basis with respect to some symplectic basis of $H_1(C, \mathbb{Z})$, so that $Z := \Omega_1^{-1}\Omega_2 \in \mathbb{H}_g$. The Jacobian variety of C can be described as the complex torus $J(C) := \mathbb{C}^g/(1_g|Z)$. We will denote by Π the normalized degree $g-1$ Abel-Jacobi map, $\Pi : C_{g-1} \longrightarrow J(C)$, whose image $\Pi(C_{g-1})$ is precisely the divisor on $J(C)$ cut out by the Riemann theta function $\theta(Z; z)$.

The choice of the basis $\omega_1, \ldots, \omega_g$ of the space of holomorphic differential forms on C provides a *canonical map* from C to $\mathbb{P}^{g-1} = \mathbb{P}H^0(C, \Omega^1)^*$, given by:

$$\begin{array}{rcl} \phi : C & \to & \mathbb{P}^{g-1} \\ P & \to & \phi(P) = (\omega_1(P), \ldots, \omega_g(P)). \end{array}$$

Note that if the the differential forms $\omega_1, \ldots, \omega_g$ are defined over the same number field K as the curve, then the canonical map is also defined over K. The following result (which in fact is valid for a general curve) relates the canonical images of certain divisors with their images through the Abel-Jacobi map (*cf.* [10]):

PROPOSITION 1.1. — *Let $P_1, \dots, P_{g-1} \in C(\bar{K})$ such that the divisor $D = P_1 + \cdots + P_{g-1}$ satisfies $l(D) = 1$. The equation:*

$$H_D(X_1, \dots, X_g) := \left(\frac{\partial\theta}{\partial z_1}(\Pi(D)), \dots, \frac{\partial\theta}{\partial z_g}(\Pi(D)) \right) \Omega_1^{-1} \begin{pmatrix} X_1 \\ \vdots \\ X_g \end{pmatrix} = 0$$

determines a hyperplane H_D of $\mathbb{P}^{g-1}$, which contains the divisor $\phi(D)$ on the curve $\phi(C)$.

2. Symmetric normal forms for hyperelliptic curves

The normalization of the roots of the polynomial $f(X)$ defining an hyperelliptic curve $Y^2 = f(X)$ has been traditionally done following Rosenhain: one sends three of the roots of $f(X)$ to 0, 1 and ∞. This normalization has a number of advantages, but it could be not the most natural one. We introduce here a new normal model for hyperelliptic curves; the symmetries of this model allow the simplification of some common tasks related to hyperelliptic curves, as we will see later.

2.1. Symmetric equations

We assume that we are working over a field K of characteristic different from 2, and denote by $\mu_{4g}(\bar{K}) = \{\zeta_1, \dots, \zeta_R\}$ the $4g$-th roots of unity in $\bar{K}$.

DEFINITION 2.1. — *Let $C : Y^2 = f(X) = (X - \alpha_1) \cdots (X - \alpha_{2g+2})$ be an hyperelliptic curve of genus g, defined over a field K with* $\operatorname{char} K \neq 2$. *For $i \neq j \in \{1, 2, \dots, 2g+2\}$ and $t \in \{1, \dots, R\}$ we define the following* symmetric invariants*:*

a) *The* symmetric ratios *of C:*

$$p_{ijt} := \zeta_t \sqrt[2g]{\prod_{k \neq i,j} \frac{\alpha_j - \alpha_k}{\alpha_i - \alpha_k}} = \zeta_t \sqrt[2g]{-\frac{f'(\alpha_j)}{f'(\alpha_i)}} \in \bar{K}.$$

b) *The* symmetric roots *of C:*

$$\ell_{ijtk} := p_{ijt} \frac{\alpha_i - \alpha_k}{\alpha_j - \alpha_k}, \quad k \in \{1, 2, \dots, 2g+2\},\ k \neq i, j.$$

c) *The* symmetric normal models *for C:*

$$\mathcal{M}_{ijt} : Y^2 = \mathcal{F}_{ijt}(X) := X \prod_{k\neq i,j} (X - \ell_{ijtk}) = X^{2g+1} + G_{ijt,1}X^{2g} + \ldots + G_{ijt,2g-1}X^2 \pm X.$$

(The coefficients $G_{ijt,k}$ will be called symmetric coefficients.*)*

d) *The* symmetric discriminants *of C:*

$$\mathcal{D}_{ijt} = \prod_{r<s} (\ell_{ijtr} - \ell_{ijts})^2 = \pm \frac{(\alpha_i - \alpha_j)^{2g(2g+1)} \Delta(f)}{f'(\alpha_i)^{2g+1} f'(\alpha_j)^{2g+1}}. \tag{2.1}$$

Remarks 2.2.

a) The word *symmetric* refers to the relative position of the non-zero roots of $X(X^{2g} + G_1X^{2g-1} + \ldots + G_{2g-1}X \pm 1)$ with respect to 0 and ∞.

b) In the case that the polynomial $f(X)$ defining the curve C has degree $2g+1$, *i.e.*, that one of its roots is $\alpha_i = \infty$, we can compute all the symmetric invariants with the same formulas, just substituting any factor $\alpha_i - \alpha_r$ by a 1.

c) Since for fixed i, j, t the symmetric roots ℓ_{ijtk} are obtained from $\alpha_1, \ldots, \alpha_{2g+2}$ by means of a common Möbius transformation, it is clear that $\mathcal{M}_{ijt}$ is a model of the curve C.

d) The roots of unity involved in the definition of the symmetric invariants are necessary to cover all the Galois conjugates of a given invariant. In order to simplify the notation, we will not write them explicitly anymore: we will denote the symmetric roots simply by ℓ_{ijk}, assuming that a common root of unity has been chosen for fixed i, j. Hence, any equality involving the symmetric invariants should be understood, unless explicitly stated, modulo these $4g$-th roots of unity. For instance, when we write

$$\ell_{ijk} = \ell_{jik}^{-1}$$

it should be understood that for a proper choice of $\zeta_t, \zeta_{t'}$ we have $\ell_{ijtk} = \ell_{jit'k}^{-1}$ for every value of k.

LEMMA 2.3. — *The symmetric roots satisfy the following relations:*

a) $\ell_{jik} = \ell_{ijk}^{-1}$;

b) $\ell_{ijk}\ell_{jki}\ell_{kij} = -1$;

c) $\ell_{irj} = \ell_{ijr} \prod_{k\neq i,j,r} (\ell_{ijk} - \ell_{ijr})$;

d) $\ell_{ijr} = \dfrac{\ell_{sji} - \ell_{sjr}}{\ell_{sij}}$;

As a consequence of part a), we see that when the symmetric model $\mathcal{M}_{ij}$ is

$$\mathcal{M}_{ij} : Y^2 = X^{2g+1} + G_1 X^{2g} + \cdots + G_{2g-1} X^2 + X,$$

the symmetric model $\mathcal{M}_{ji}$ is

$$\mathcal{M}_{ji} : Y^2 = X^{2g+1} + G_{2g-1} X^{2g} + \cdots + G_1 X^2 + X.$$

There are also quite simple relations between the symmetric discriminants:

LEMMA 2.4.

a) $\mathcal{D}_{ij} = \mathcal{D}_{ji}$.

b) $\mathcal{D}_{ij} = \ell_{jki}^{2g(2g+1)} \mathcal{D}_{ik}$.

c) $\mathcal{D}_{ij} = \ell_{irs}^{2g(2g+1)} \ell_{jsi}^{2g(2g+1)} \mathcal{D}_{rs}$.

The symmetric normal model $\mathcal{M}_{ij}$ is determined by the choice of the roots α_i, α_j, which can be done in $(2g+2)(2g+1)$ different ways, and the choice of a $4g$-th root of unity, so that we have up to $4g(2g+2)(2g+1)$ symmetric models for a generic hyperelliptic curve. For arithmetic applications, it is worth noting that they may be not defined over the field of definition of the curve.

Example 2.5. — We have studied the symmetric models of elliptic curves in [12]. For an elliptic curve $E : Y^2 = (X - e_1)(X - e_2)(X - e_3)$, the symmetric roots take the aspect:

$$\ell_{ijr} = \sqrt{\pm \frac{e_i - e_r}{e_j - e_r}},$$

and hence they are essentially the well-known *moduli* for E, which are the roots of the equation

$$256(k^4 - k^2 + 1)^3 - k^4 (k^2 - 1)^2 j_E = 0,$$

where j_E is the absolute invariant of the elliptic curve E.

This fact generalizes to hyperelliptic curves of any genus g: their symmetric roots are absolute invariants of the curve with certain level structure:

THEOREM 2.6. — *If two hyperelliptic curves defined over a field of odd characteristic are isomorphic, then their sets of symmetric roots are equal (after a proper labelling of the roots).*

Proof. — Suppose that we are given two isomorphic curves over a field K

$$C : Y^2 = \prod_i (X - \alpha_i), \quad C' : Y^2 = \prod_i (X - \alpha'_i),$$

with an isomorphism between them realized by a fractional linear transformation $\gamma(X) = \frac{AX+B}{CX+D}$ with $A, B, C, D \in \bar{K}$ such that $\gamma(\alpha_j) = \alpha'_j$. We have:

$$\frac{\alpha'_i - \alpha'_k}{\alpha'_j - \alpha'_k} = \frac{C\alpha_j + D}{C\alpha_i + D} \cdot \frac{\alpha_i - \alpha_k}{\alpha_j - \alpha_k},$$

and hence the symmetric roots ℓ_{ijk} of C and the symmetric roots ℓ'_{ijk} of C' will coincide. □

The symmetric roots ℓ_{ijk} being invariants of the curve C, any rational expression in them will produce new invariants. Particularly interesting will be the symmetric discriminants $\mathcal{D}_{ij}$.

2.2. Reduction properties of symmetric models

We shall work now on a discrete valuation ring A, with field of fractions K of characteristic different of 2. An integral model for a hyperelliptic curve C over K can be given by an equation of the form $Y^2 = f(X)$ with $f(X) \in A[X]$. Such a model can be reduced modulo $\mathfrak{p}$ (the prime ideal in A), yielding a new curve $\tilde{C}$ over the residual field $k = A/\mathfrak{p}$. This curve is non-singular if and only if $\mathfrak{p} \nmid 2\Delta(f)$, where $\Delta(f)$ denotes the discriminant of the polynomial $f(X)$; in this case it is said that the curve C has good reduction; otherwise it is said that the curve has bad reduction. A minimal model for C is an integral model such that $\Delta(f)$ has minimal valuation with respect to $\mathfrak{p}$. A curve C with bad reduction may have a model over an extension A' of A with good reduction at the prime $\mathfrak{p}'$ of A' lying over $\mathfrak{p}$; in this case it is said that C has potentially good reduction over $\mathfrak{p}$.

The following results illustrate the interest of symmetric models concerning the reduction of curves:

THEOREM 2.7. — *Let $C : Y^2 = f(X)$ be an hyperelliptic curve over A, with potentially good reduction. Let $A' := A[G_{ij,1}, \ldots, G_{ij,2g-1}]$ be the ring of definition of the symmetric model $\mathcal{M}_{ij}$ of C, and let $\mathfrak{p}'$ be the prime in A' lying over $\mathfrak{p}$.*

a) *The symmetric coefficients G_{ij} are $\mathfrak{p}'$-integral.*
b) *The symmetric equation $\mathcal{M}_{ij}$ has good reduction at $\mathfrak{p}'$.*

Proof. — Let $\alpha_1, \dots, \alpha_{2g+2}$ be the roots of $f(X)$ in $\bar{K}$. Since

$$\ell_{ijk}^{2g} = \pm \frac{(\alpha_i - \alpha_k)^{2g-1}}{(\alpha_j - \alpha_k)^{2g-1}} \prod_{r \neq i,j,k} \frac{\alpha_j - \alpha_r}{\alpha_i - \alpha_r},$$

it is clear that the symmetric roots ℓ_{ijt} are integral over the ring $A[\frac{1}{\Delta(f)}]$, since the denominators appearing in the last expression divide $\Delta(f)$. Thus the symmetric coefficients $G_{ij,k}$ are also integral over this ring. Let $Y^2 = f_1(X) = \prod_i (X - \beta_i)$ be a model of C over a finite extension A_1 of A, with good reduction at the prime $\mathfrak{p}_1 \in \operatorname{Spec}(A_1)$ above $\mathfrak{p}$. The discriminant $\Delta(f_1)$ must be a unit in A_1. We may now compute the symmetric models from this new model, since they are invariants of the curve C by theorem 2.6. We see thus that the coefficients $G_{ij,k}$ are integral over the ring $A_1[\frac{1}{\Delta(f_1)}] = A_1 \supseteq A'$, and hence they are finally $\mathfrak{p}'$-integral.

The discriminant $\mathcal{D}_{ij}$ of the symmetric model $\mathcal{M}_{ij}$ is given by

$$\begin{aligned}\mathcal{D}_{ij,t} &= p_{ij\,t}^{2g(2g-1)} (\beta_i - \beta_j)^{2g(2g-1)} \prod_{\substack{r<s \\ r,s \neq i,j}} \frac{(\beta_r - \beta_s)^2}{(\beta_j - \beta_r)^2 (\beta_j - \beta_r)^2} \\ &\qquad (\beta_i - \beta_j)^{2g(2g-1)} \prod_{\substack{r \neq s \\ r,s \neq i,j}} (\beta_r - \beta_s) \\ &= \frac{}{\prod_{r \neq i,j} (\beta_i - \beta_r)^{2g-1} (\beta_j - \beta_r)^{2g-1}} \in A_1[\frac{1}{\Delta(f_1)}] = A_1,\end{aligned}$$

so that it does not belong to $\mathfrak{p}_1$, and hence the symmetric model $\mathcal{M}_{ij}$ has good reduction at $\mathfrak{p}'$. □

Corollary 2.8. — *If $v_{\mathfrak{p}}(\mathcal{D}_{ij}) \leqslant 0$ for some i, j then C cannot have potentially good reduction at $\mathfrak{p}$.*

This corollary can be understood as a generalization of the well-known criterion for an elliptic curve having potentially good reduction (*cf.* [24, p. 181]). It leads to the following definition:

Definition 2.9. — *The odd geometric locus of bad reduction of an hyperelliptic curve $C : Y^2 = f(X)$ defined over a domain A is*

$$\mathrm{BR}(C)^{\mathrm{odd}} = \big\{ \mathfrak{p} \cap A \mid \exists i, j \text{ such that } \mathfrak{p} \in \operatorname{Spec} A[\mathcal{D}_{ij}] \text{ and } v_{\mathfrak{p}}(\mathcal{D}_{ij}) < 0 \big\}.$$

For the primes in $\mathrm{BR}(C)^{\mathrm{odd}}$, symmetric models have also good properties:

Theorem 2.10. — *Let C be a hyperelliptic curve over discrete valuation ring A, and suppose that C has not potentially good reduction at the unique prime $\mathfrak{p}$ in* Spec *A. If the symmetric coefficients $G_{ij,2}, \dots, G_{ij,2g-1}$*

are integral over A, then the symmetric model $\mathcal{M}_{ij}$ is a minimal model for C over the ring $A' = A[G_{ij,2}, \dots, G_{ij,2g-1}]$.

Proof. — Let $B = A'[\{\ell_{ij,r}\}_r]$, and let $\mathcal{P}$ the prime of B above $\mathfrak{p}$. By [17, lemma 2.3], it is enough to see that the roots of the polynomial $X\prod_{r\neq i,j}(X-\ell_{ijr})$ defining $\mathcal{M}_{ij}$ are not all congruent $\mod \mathcal{P}$. This is clear, since $\prod_{r\neq i,j}\ell_{ijr} = \pm 1$, so that these roots cannot be $0 \pmod{\mathcal{P}}$. □

The minimality of symmetric models suggest that their coefficients G_k should be small in some sense. The following example illustrates this behavior:

Example. — Weng ([31]) computed the equation of a genus 3 hyperelliptic curve C whose jacobian has complex multiplication by the field $K = \mathbb{Q}(w,i)$, where $w^3 - w^2 - 10w + 8 = 0, i^2 = -1$. She found

$$C : Y^2 = f(X) := X^7 + 961X^5 - 3694084X^3 + 1832265664X.$$

The discriminant of the polynomial $f(X)$ is $\Delta(f) = -2^{44}31^{35}$. A symmetric model for this equation is:

$$Y^2 = g(X) := X^7 + \frac{\sqrt[3]{31}}{4}X^5 - \frac{\sqrt[3]{31^2}}{4}X^3 + X,$$

which has only bad reduction at the primes dividing 2 in $\mathbb{Q}(\sqrt[3]{31})$, since $\Delta(g) = -2^{14}$.

2.3. The μ-invariants

We shall explain now a particular construction of the symmetric roots of a hyperelliptic curve, useful when we have not an explicit set of Weierstrass points, but certain intermediate invariants. This construction will be necessary in section 8.

DEFINITION 2.11. — *For $i,j,r,s, \in \{1,\dots,2g+2\}$*

$$\mu_{ijrs} := \frac{(\alpha_i - \alpha_r)(\alpha_j - \alpha_s)}{(\alpha_i - \alpha_s)(\alpha_j - \alpha_r)}.$$

LEMMA 2.12.

a) $\mu_{ijrs} = \mu_{rsij} = \mu_{jisr} = \mu_{jirs}^{-1} = \mu_{ijsr}^{-1}$.

b) $\dfrac{\ell_{ijr}}{\ell_{ijs}} = \mu_{ijrs}$.

c) $\ell_{ijk}^{4g} = \prod_{r\neq i,j,k}\mu_{ijkr}^2$.

Proof. — Parts a) and b) are immediate. Part b) follows from:

$$\ell_{ijk}^{4g} = \left(\frac{\alpha_i - \alpha_k}{\alpha_j - \alpha_k}\right)^{4g} \prod_{r\neq i,j,k} \left(\frac{\alpha_j - \alpha_r}{\alpha_i - \alpha_r}\right)^2$$
$$= \prod_{r\neq i,j,k} \left(\frac{(\alpha_i - \alpha_k)(\alpha_j - \alpha_s)}{(\alpha_i - \alpha_s)(\alpha_j - \alpha_k)}\right)^2 = \prod_{r\neq i,j,k} \mu_{ijkr}^2.$$

□

Later on we will see how to compute the μ_{ijrs} by means of Jacobian Nullwerte. We see now how to obtain a symmetric equation from them.

PROPOSITION 2.13. — *A symmetric equation for an hyperelliptic curve can be deduced from a family* $\{\mu_{ijrs}\}_{r,s}$.

Proof. — We can compute the symmetric roots $\{\ell_{ijr}\}_r$ up to a $4g$-th root of unity by means of the third formula of the lemma. This root of unity must be determined coherently for all the symmetric roots, but this can be done using the second part of the lemma. □

3. Preliminaries on Thetanullwerte and Jacobian Nullwerte

3.1. Theta-functions and theta-characteristics

For $z \in \mathbb{C}^g, Z \in \mathbb{H}_g$, the Riemann theta function on $\mathbb{C}^g$ is defined by:

$$\theta(z, Z) := \sum_{n\in\mathbb{Z}^g} \exp(\pi i^t n.Z.n + 2\pi i^t n.z).$$

When the matrix Z is fixed and we consider $\theta(z, Z)$ as a function of the first variable z, we will write it as $\theta(z)$. A vector $m = {}^t(m', m'')$, with $m', m'' \in \mathbb{R}^g$, defines a translate of θ as follows:

$$\theta[m](z, Z) := e^{\pi i^t m'.Z.m' + 2\pi i^t m'.(z+m'')}\theta(z + Zm' + m'')$$
$$= \sum_{n\in\mathbb{Z}^g} e^{\pi i^t (n+m').Z.(n+m') + 2\pi i^t (n+m').(z+m'')}.$$

It is called theta function with characteristic m. If $m', m'' \in \frac{1}{2}\mathbb{Z}^g$ we call m a *theta-characteristic*. For a theta-characteristic m, the corresponding theta function $\theta[m](z, Z)$ is an even or odd function of z according to the parity of m, which is defined to be the parity of the sign $e(m) := (-1)^{4^t m'.m''}$.

For a fixed matrix $Z \in \mathbb{H}_g$, theta-characteristics are in bijection with two torsion points on the complex torus $T_Z := \mathbb{C}^g/(1_g|Z)$:

$$m = \begin{pmatrix} m' \\ m'' \end{pmatrix} \in \{0, 1/2\}^{2g} \longleftrightarrow w := Z.m' + m'' \in T_Z[2].$$

Along the paper, we shall use the symbols $m, m_k, \ldots$ for theta-characteristics, and the symbols $w, w_k, \ldots$ for the corresponding 2-torsion points on T_Z, the relation between them being implicitly assumed. For instance, we define the parity of $w \in T_Z[2]$ to be the parity of m.

The values $\theta[m](0, Z)$ are usually called *Thetanullwerte*, and denoted shortly by $\theta[m](Z)$ or $\theta[w](Z)$ (even by $\theta[m] = \theta[w]$ when the matrix Z is fixed). It is also usual to look at the Thetanullwerte $\theta[m](0, Z)$ as a functions of Z, *i.e.,* defined on the Siegel upper half space $\mathbb{H}_g$. The $\mathbb{C}$-algebra spanned by them is called *ring of Thetanullwerte*, and it is denoted by $\mathbb{C}[\theta]$. It has theoretical significance in relation to certain rings of Siegel modular forms.

3.2. Jacobian Nullwerte

If we fix an odd characteristic m, then the Thetanullwerte $\theta[m](Z)$ vanishes for every Z. For a sequence $M = \{m_1, \ldots, m_g\}$ of odd characteristics one considers the matrix:

$$J[M](Z) := J[m_1, \ldots, m_g](Z) := \begin{pmatrix} \dfrac{\partial\theta[m_1]}{\partial z_1}(0; Z) & \cdots & \dfrac{\partial\theta[m_1]}{\partial z_g}(0; Z) \\ \vdots & & \vdots \\ \dfrac{\partial\theta[m_g]}{\partial z_1}(0; Z) & \cdots & \dfrac{\partial\theta[m_g]}{\partial z_g}(0; Z) \end{pmatrix}$$

and its determinant:

$$[m_1, \ldots, m_g](Z) := \pi^g D(M)(Z) := \det J[m_1, \ldots, m_g](Z),$$

which is usually called *Jacobian Nullwert*. If the matrix Z is fixed, we shall denote $J[m_1, \ldots, m_g](Z)$ and its determinant by $J[w_1, \ldots, w_g]$ and $[w_1, \ldots, w_g]$ respectively.

3.3. Fundamental systems

Given three theta characteristics m_1, m_2, m_3, define $e(m_1, m_2, m_3) := e(m_1)e(m_2)e(m_3)e(m_1+m_2+m_3)$. A triplet $\{m_1, m_2, m_3\}$ is called *azygetic*

if $e(m_1,m_2,m_3)=-1$, and syzygetic otherwise. A sequence $\{m_1,\dots,m_r\}$ is azygetic if every triplet contained in it is azygetic.

A *fundamental system* is an azygetic sequence $S=\{m_1,\dots,m_{2g+2}\}$ of $2g+2$ theta characteristics. A *special fundamental system* is a fundamental system with the first g odd terms and the remaining $g+2$ even terms. The same concepts for two-torsion points on an abelian variety are defined analogously.

Fundamental systems play a basic role in the generalizations of Jacobi's derivative formula obtained by Igusa. For low dimension we have

THEOREM 3.1 ([13]). — *Assume $g\leqslant 5$. Let $m_1,\dots,m_g$ be odd analytic theta characteristics such that the function $[m_1,\dots,m_g](Z)$ is not identically zero and is contained in the ring of Thetanullwerte $\mathbb{C}[\theta]$. Then $m_1,\dots,m_g$ can be completed to form a fundamental system, and:*

$$[m_1,\dots,m_g](Z)=\pi^g \sum_{\{m_{g+1},\dots,m_{2g+2}\}\in\mathcal{S}} \pm \prod_{i=g+1}^{2g+2}\theta[m_i](0;Z),$$

where $\mathcal{S}$ is the set of all $(g+2)$-tuples $\{m_{g+1},\dots,m_{2g+2}\}$ of even theta characteristics such that $\{m_1,\dots,m_g,\ m_{g+1},\dots,m_{2g+2}\}$ form a fundamental system. If Z is the period matrix of a hyperelliptic curve, there is exactly one non-zero term in the sum of the right hand side of the equality.

For higher dimensions $g>5$, Igusa provides a broader version of the formula above, relating a sum of Jacobian Nullwerte with a certain sum of products of Thetanullwerte ([15], [16]).

Particular cases of Igusa's theorem are:

THEOREM 3.2 (Rosenhain's Formula, [22], [10]). — *For any $Z\in\mathbb{H}_2$ and any pair of odd characteristics m_1,m_2*

$$[m_1,m_2]=\pm\pi^2 \prod_{\substack{m \text{ odd},\\ m\neq m_1,m_2}} \theta[m_1+m_2-m], \tag{3.1}$$

where the sign does not depend on Z.

THEOREM 3.3 (Frobenius, [6], [10]). — *Let C be a hyperelliptic curve of genus 3, with Weierstrass points $W_1,\dots,W_8$. Let $w_{ij}:=\Pi(W_i+W_j)$, $w_{ijkr}:=\Pi(W_i+W_j+W_k-W_r)$. The following equality holds for every triplet W_i,W_j,W_k:*

$$[w_{ik},w_{ij},w_{jk}]=\pm\pi^3 \prod_{r\neq i,j,k}\theta[w_{ijkr}],$$

where the sign does not depend on Z.

3.4. A fundamental system for Jacobians of hyperelliptic curves

The following construction will be useful later:

PROPOSITION 3.4 ([10]). — *Let $W_1, \dots, W_g$ be g different Weierstrass points on a hyperelliptic curve C, and denote $W_{g+1}, \dots, W_{2g+2}$ the remaining Weierstrass points. Consider the divisors*

$$\begin{aligned} D &= \textstyle\sum_{i=1}^{g} W_i, \\ D_i &= D - W_i, && i = 1, \dots, g, \\ D_i &= D + W_i - 2W_{2g+2}, && i = g+1, \dots, 2g+2; \end{aligned}$$

The images $w_1 = \Pi(D_1), \dots, w_{2g+2} = \Pi(D_{2g+2})$ of these divisors through the Abel-Jacobi map form a fundamental system of 2-torsion points in $J(C)$.

4. Jacobian Thomae's formula

After propositions 1.1 and 3.4, if we fix g Weierstrass points $W_1 = (\alpha_1, 0), \dots, W_g = (\alpha_g, 0)$ on C and define $w_1 = \Pi(\sum_{i \neq 1} W_i), \dots, w_g = \Pi(\sum_{i \neq g} W_i)$, the Jacobian Nullwerte $[w_1, \dots, w_g]$ has a clear geometric interpretation: the rows of this determinant are the equations of the g hyperplanes spanned by $g-1$ of the fixed Weierstrass points. It is then natural to ask if there is some Jacobian version of Thomae's formula, connecting $[w_1, \dots, w_g]$ with the discriminant of the polynomial $(X-\alpha_1)\cdots(X-\alpha_g)$. It was a beautiful surprise to find what seems to be a forgotten result in last page of Thomae's original paper, which provides this connection:

THEOREM 4.1 (Thomae, [26, p. 222]). — *Fix a partition $\{W_1, \dots, W_{g-1}\} \cup \{W_g, \dots, W_{2g+2}\}$ of the set of Weierstrass points of C, and consider the odd two-torsion point $w_0 = \Pi(W_1 + \cdots + W_{g-1})$. Define $F_{w_0,1}(X) = \prod_{i=1}^{g-1}(X - \alpha_i)$, $F_{w_0,2}(X) = f(X)/F_{w_0,1}(X)$. The following relation holds*[(1)]*:*

$$2(2\pi)^{g/2} \operatorname{grad}\theta[w_0](Z) = (\Delta(F_{w_0,1})\Delta(F_{w_0,2}))^{1/8} \cdot \sqrt{\det \Omega_1}\, S(\alpha_1, \dots, \alpha_{g-1}) \cdot \Omega_1,$$

where $S(\alpha_1, \dots, \alpha_{g-1}) = ((-1)^{g-1}\prod \alpha_i, \dots, -\sum \alpha_i, 1)$ is the row-vector formed by the coefficients of the polynomial $F_{w_0}(X)$.

We also recall the *standard* Thomae's formula ([26], [21]):

(1) Note that the term $\sqrt{\det \Omega_1}$ is misplaced in Thomae's paper.

THEOREM 4.2. — *Fix a partition* $\{W_1,\dots,W_{g+1}\}\cup\{W'_1,\dots,W'_{g+1}\}$ *of the set of Weierstrass points on* C*, and consider the even two-torsion point* $w_e=\Pi(W_1+\cdots+W_{g+1}-2W)$ *on* $J(C)$*. Define* $G_{w_e,1}(X)=\prod_{i=1}^{g+1}(X-\alpha_i)$, $G_{w_e,2}(X)=f(X)/G_{w_e,1}(X)$*. The following relation holds:*

$$\theta[w_e](Z)=(2\pi)^{-g/2}\sqrt{\det\Omega_1}\sqrt[8]{\Delta(G_{w_e,1})\Delta(G_{w_e,2})}.$$

The combination of both Thomae formulas yields the following nice results:

PROPOSITION 4.3. — *Let* $w_0=\Pi(W_1+\cdots+W_{g-1})$ *and* $w_e=\Pi(W'_1+\cdots+W'_{g+1})$ *. Then*

$$\frac{2}{\theta[w_e](Z)}\operatorname{grad}\theta[w_0](Z)=\sqrt[8]{\frac{\Delta(F_{w_0,1})\Delta(F_{w_0,2})}{\Delta(G_{w_e,1})\Delta(G_{w_e,2})}}S(\alpha_1,\dots,\alpha_{g-1})\cdot\Omega_1.$$

THEOREM 4.4. — *Write* $W_g=(\gamma_1,0),W_{g+1}=(\gamma_2,0)$*, and denote by* $W_k=(\alpha_k,0),k\neq 0$ *the remaining Weierstrass points on* C*. Define* $w_e=\Pi(W_1+\cdots+W_{g+1}-2W_t)$*,* $G_{w_e,2}(X)=(X-\alpha_{g+2})\cdots(X-\alpha_{2g+2})$*. Then*

$$\frac{2}{\theta[w_e](Z)}\operatorname{grad}\theta[w_0](Z)=\left(\frac{G_{w_e,2}(\gamma_1)G_{w_e,2}(\gamma_2)}{F_{w_0,1}(\gamma_1)F_{w_0,1}(\gamma_2)}\right)^{1/4}S(\alpha_1,\dots,\alpha_{g-1})\cdot\Omega_1.$$

Proof. — We need only to simplify the expression inside the eighth root appearing in proposition 4.3. We note that $G_{w_e,1}(X)=(X-\gamma_1)(X-\gamma_2)F_{w_0,1}(X)$ and $F_{w_0,2}(X)=(X-\gamma_1)(X-\gamma_2)G_{w_e,2}(X)$. Hence

$$\frac{\Delta(F_{w_0,1})\Delta(F_{w_0,2})}{\Delta(G_{w_e,1})\Delta(G_{w_e,2})}=\frac{\Delta(F_{w_0,1})\Delta(G_{w_e,2})(\gamma_1-\gamma_2)^2G_{w_e,2}(\gamma_1)^2G_{w_e,2}(\gamma_2)^2}{\Delta(F_{w_0,1})(\gamma_1-\gamma_2)^2F_{w_0,1}(\gamma_1)^2F_{w_0,1}(\gamma_2)^2\Delta(G_{w_e,2})}.$$

□

5. A remark on Igusa's theorem 3.1

Let us consider theorem 3.1 for hyperelliptic period matrices Z. Fix a Jacobian Nullwerte $[w_1,\dots,w_g](Z)$ with no identically zero row. Igusa's theorem asserts that it can be represented as a product of $g+2$ Thetanullwerte $\theta[w'_1](Z)\cdots\theta[w'_{g+2}]$, whenever $[w_1,\dots,w_g]$ is contained in the ring of Thetanullwerte $\mathbb{C}[\theta]$. Igusa states a non-representability result in [14, p. 93]. The results in previous section provide a simple way to generate new results in this direction. After theorem 4.1, we know that

$$[w_1,\dots,w_g](Z)=2^{-g}(2\pi)^{-g^2/2}\Delta(\{w_r\}_r)\begin{pmatrix}S(\{\alpha_r^1\}_r)\\ \vdots\\ S(\{\alpha_r^g\}_r)\end{pmatrix}\cdot\Omega_1$$

where the term $\Delta(\{w_r\}_r)$ denotes a product of differences of the x-coordinates α_j^i of the Weierstrass points involved in the w_i. If this expression equals a product of even Thetanullwerte, the standard Thomae's formula 4.2 implies that the determinant $\det(\big(S(\{\alpha_r^i\}_r)\big)_i)$ must factor as a product of factors $(\alpha_j - \alpha_k)$. A formal computation may check this condition quite easily.

6. Jacobi's formula revisited

The Jacobi triple product identity is usually written as

$$\theta_1(\tau)' = \pi\theta_2(\tau)\theta_3(\tau)\theta_4(\tau),$$

where $\theta_r(\tau)$ is the usual notation for the Thetanullwerte in dimension 1. A proper rearrangement of the formula drives to interesting remarks. Consider the elliptic curve E_τ associated to the complex torus $\mathbb{C}/\langle 1, \tau\rangle$:

$$E_\tau : Y^2 = X^3 - g_2(\tau)X - g_3(\tau) = (X - e_1(\tau))(X - e_2(\tau))(X - e_3(\tau)),$$

where $g_2(\tau), g_3(\tau)$ are given by the classical Eisenstein series, and $e_j(\tau) = \dfrac{\pi^2}{3}(\theta_r[\tau] \pm \theta_s[\tau])$ (*cf.* [19, p. 133]). We have seen in [11] that the differential form $(r, s \neq 1)$

$$\frac{\theta_1(\tau)'}{\theta_t(\tau)}dz = \pi\theta_r(\tau)\theta_s(\tau)dz$$

is defined over a finite extension of $\mathbb{Q}(j(\tau))$, and it is well-known (*cf.* [19, p. 132]) that

$$\pi\theta_r(\tau)\theta_s(\tau) = \sqrt[4]{(e_i(\tau) - e_j(\tau))(e_i(\tau) - e_k(\tau))}.$$

Hence, we can re-write Jacobi formula as

$$\frac{\theta_1(\tau)'}{\pi\theta_r(\tau)} = \sqrt[4]{(e_i(\tau) - e_j(\tau))(e_i(\tau) - e_k(\tau))} \in \overline{\mathbb{Q}(j(\tau))}.$$

For a general elliptic curve $E : Y^2 = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)$, we obtain

$$\frac{\theta_1(\tau)'}{\pi\theta_r(\tau)} = \omega_1 \sqrt[4]{(\alpha_i - \alpha_j)(\alpha_i - \alpha_k)},$$

where ω_1 is a proper period of E.

In this way, Jacobi formula can be thought as a result in the area of algebraic values of transcendental functions. In this direction, proposition 4.3 provides a general version of it:

THEOREM 6.1. — *Let $C : Y^2 = (X-\alpha_1)\cdots(X-\alpha_{2g+2})$ be a genus g hyperelliptic curve, and let $(\Omega_1|\Omega_2)$ a period matrix of C with respect to a symplectic basis of $H_1(C,\mathbb{Z})$, so that $Z := \Omega_1^{-1}\Omega_2 \in \mathbb{H}_g$. For any choice of g odd two torsion points $w_1,\ldots,w_g \in J(C)$ and g even two torsion points $w_1',\ldots,w_g' \in J(C)$:*

$$\left(\frac{1}{\pi^g \det \Omega_1}\ \frac{[w_1,\ldots,w_g]}{\theta[w_1']\cdots\theta[w_g']}\right)^8 \in \mathbb{Q}(\alpha_1,\ldots,\alpha_{2g+2}),$$

7. Algebraic differential forms and periods

7.1. Algebraic differential forms for abelian varieties

Given a principally polarized abelian variety A of dimension g, defined over a field $k \subset \mathbb{C}$, and a basis $\omega_1,\ldots,\omega_g \in H^0(A,\Omega^1_{/k})$, we form the period matrix $(\Omega_1|\Omega_2)$ of these differential forms with respect to any symplectic basis of $H_1(A,\mathbb{Z})$. We may identify $A(\mathbb{C})$ with the complex torus $\mathbb{C}^g/(\Omega_1|\Omega_2)$. It is well-known that the 4^g theta-functions $\theta[m](z)$ with half integer characteristic provide a map

$$\begin{array}{ccc} A(\mathbb{C}) & \longrightarrow & \mathbb{P}^{4^g-1}(\mathbb{C}) \\ z & \longrightarrow & \big(\theta[m](\Omega_1^{-1}\cdot 2z)\big)_m, \end{array}$$

whose image is isomorphic to A over a certain field K which is a finite extension of k. We now take an even theta function $\theta_0(z)$ such that $\theta_0(0) \neq 0$, and an odd one $\theta_1(z)$, and form the quotient $\theta_1(z)/\theta_0(z)$; it can be seen as an element of $K(A)$, the field of K-rational functions on A. Hence, its differential at the point $z=0$ must be a K-linear combination of the original differential forms $\omega_1,\ldots,\omega_g$:

$$d(\theta_1(z)/\theta_0(z))\big|_{z=0} = \theta_0(0)^{-1} d\theta_1(z)\big|_{z=0} = \sum_{k=1}^{g} c_k\omega_k.$$

We observe that it is always possible to choose g odd theta functions $\theta_1(z),\ldots,\theta_g(z)$ such that $d\theta_1(z),\ldots,d\theta_g(z)$ are linearly independent differential forms on the torus $\mathbb{C}^g/(\Omega_1|\Omega_2)$ (*cf.* [23], p. 192). These differential forms will be defined over K, but not necessarily over k. We will use the term **algebraic differential form** to describe a differential form on a variety defined over a finite extension of its field of moduli.

It is a frequent setting that the only available data of a complex abelian variety A is a normalized period matrix $Z \in \mathbb{H}_g$. In this situation, in order to build a period lattice for A coming from and algebraic basis of differential

forms, we look for a set of theta-functions $\theta_0(z), \theta_1(z), \ldots, \theta_g(z)$ as before. Equivalently, we look for 2-torsion points $w_0, w_1, \ldots, w_g$ such that

$$\Omega_1(w_1, \ldots, w_g; w_0; Z) := \frac{1}{2\pi i \theta[w_0]} J[w_1, \ldots, w_g](Z)$$

is a non-singular matrix. By the remarks above, then

$$(\widetilde{\omega}_1, \ldots, \widetilde{\omega}_g) = (dz_1, \ldots, dz_g)\Omega_1(w_1, \ldots, w_g; w_0; Z) \tag{7.1}$$

are algebraic differential forms and yield a basis of $H^0(A, \Omega^1_{/\bar{K}})$, with periods $\Omega_1(w_1, \ldots, w_g; w_0; Z)(1_g \mid Z)$.

7.2. Algebraic differential forms for hyperelliptic curves

We assume now that A is the jacobian variety $J(C)$ of a hyperelliptic curve $C : Y^2 = f(X)$ of genus g, defined over a field $k \subseteq \mathbb{C}$. We have studied how to find a good algebraic equation for an elliptic curve from its normalized period lattice in [11], so that from now on we will assume that we are working with a hyperelliptic curve of genus $g \geqslant 2$.

Our initial data will be a normalized period matrix $Z \in \mathbb{H}_g$ for the curve C, coming from a model $Y^2 = (X - \alpha_1) \cdots (X - \alpha_{2g+2})$ of the curve C. The procedure described above provides a basis $(\widetilde{\omega}_1, \ldots, \widetilde{\omega}_g) = \Pi^* \left((dz_1, \ldots, dz_g)\Omega_1(w_1, \ldots, w_g; w_0; Z)\right)$ of algebraic differential forms in $H^0(C, \Omega^1_{/\bar{K}})$ derived from a set of g odd two-torsion points $w_1, \ldots, w_g \in J(C)$, which are only subject to the condition $[w_1, \ldots, w_g](Z) \neq 0$.

We can easily describe now a geometric method to build a basis $\widetilde{\omega}_1, \ldots, \widetilde{\omega}_g$ of algebraic holomorphic differentials from a normalized period matrix for C. We take g Weierstrass points $W_1 = (\alpha_1, 0), \ldots, W_g = (\alpha_g, 0)$ on C, and form the divisors $D_i = \sum_{j \neq i} W_j$, and their images $w_i = \Pi(D_i)$ in $J(C)$ through the Abel-Jacobi map. By 1.1, the rows of the matrix $J[w_1, \ldots, w_g]$ are linearly independent, and thus for every even theta-characteristic $\theta[w_0] \not\equiv 0$

$$(\widetilde{\omega}_1, \ldots, \widetilde{\omega}_g) = \Pi^*\big((dz_1, \ldots, dz_g)\Omega_1(w_1, \ldots, w_g; w_0; Z)\big)$$

is a basis of $H^0(C, \Omega^1_{/\bar{K}})$. The point is that this construction can be done working only with the two torsion points of $J(C)$, without explicit knowledge of the Weierstrass points of C. In this situation, theorem 4.3 will determine the field of definition of these differential forms.

8. Jacobian Nullwerte and symmetric equations

We now describe a method to build a symmetric equation of C by means of Jacobian Nullwerte. The fundamentals of the method are certain relations between quotients of Jacobian Nullwerte and the μ-invariants. Although these relations can be deduced directly from theorem 4.1 or theorem 4.3, we provide some geometric intuition to derive these formulas.

We assume that the period matrix Z comes from a certain model $Y^2 = (X-\alpha_1)\cdots(X-\alpha_{2g+2})$ of the curve C.

The procedure described in section 7 provides a basis $(\widetilde{\omega}_1,\dots,\widetilde{\omega}_g) = \Pi^*\left((dz_1,\dots,dz_g)\Omega_1(w_1,\dots,w_g;w_0;Z)\right)$ of algebraic differential forms in $H^0(C,\Omega^1_{\overline{K}})$ coming from certain odd two-torsion points $w_1,\dots,w_g \in J(C)$, which are only subject to the condition $[w_1,\dots,w_g](Z) \neq 0$. By the Riemann singularity theorem, we know that $w_i = \Pi(D_i)$ for certain geometric theta-characteristic D_i on C with $l(D_i) = 1$. This theta-characteristic D_i must be the sum of $g-1$ Weierstrass points (*cf.* [1, p. 288]).

Proposition 8.1. — *Let W be a Weierstrass point on C. The image of W through the canonical map ϕ_G given by $\widetilde{\omega}_1,\dots,\widetilde{\omega}_g$ is*

$$\phi_G(W) = \left([w_1,w_2',\dots,w_g'] : [w_2,w_2',\dots,w_g'] : \cdots : [w_g,w_2',\dots,w_g']\right),$$

where $w_j' = \Pi(W + \sum_{r=2}^{g-1} W_{jr})$ are any $g-1$ odd 2-torsion points on $J(C)$ whose associated divisors contain the point W and which do not coincide with the w_i.

Proof. — Let us write $\Omega_1 = \Omega_1(w_1,\dots,w_g,w_0;Z)$. By [10, proposition 3.1], the solution of the linear system

$$\begin{pmatrix} \dfrac{\partial\theta}{\partial z_1}(w_2',Z) & \cdots & \dfrac{\partial\theta}{\partial z_g}(w_2',Z) \\ \vdots & & \vdots \\ \dfrac{\partial\theta}{\partial z_1}(w_g',Z) & \cdots & \dfrac{\partial\theta}{\partial z_g}(w_g',Z) \end{pmatrix} \Omega_1^{-1} \begin{pmatrix} X_1 \\ X_2 \\ \vdots \\ X_g \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

is the canonical image $\phi_G(W)$ of the point $W = W_1'$. Let $(Y_1,\dots,Y_g) = (X_1,\dots,X_g)^t({\Omega_1}^t)^{-1}$, and call A the first matrix in the equality above. The solutions of the system

$$A \begin{pmatrix} Y_1 \\ \vdots \\ Y_g \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

are:

$$(Y_1 : Y_2 : \cdots : Y_g) = (A_1 : -A_2 : \cdots : (-1)^{g+1}A_g),$$

where A_j is the determinant of the matrix obtained by deleting the i-th column of A. Now:

$$\begin{pmatrix} X_1 \\ \vdots \\ X_g \end{pmatrix} = \begin{pmatrix} \dfrac{\partial\theta}{\partial z_1}(w_1, Z) & \cdots & \dfrac{\partial\theta}{\partial z_g}(w_1, Z) \\ \vdots & & \vdots \\ \dfrac{\partial\theta}{\partial z_1}(w_g, Z) & \cdots & \dfrac{\partial\theta}{\partial z_g}(w_g, Z) \end{pmatrix} \begin{pmatrix} A_1 \\ \vdots \\ (-1)^{g+1} A_g \end{pmatrix},$$

and the result follows immediately. □

This result is specially significant when the original theta-characteristics $D_1, \ldots, D_g$ are well-posed:

PROPOSITION 8.2. — *Suppose that the 2-torsion points $w_1, \ldots, w_g$ related to the basis $\widetilde{\omega}_1, \ldots, \widetilde{\omega}_g$ of $H^0(C, \Omega^1_{\bar{K}})$ are the images of certain divisors $D_i = \sum_{j \neq i} W_j$. Let $\phi_G(W_r) = (u_1, \ldots, u_g), \phi_G(W_s) = (v_1, \ldots, v_g)$, with $r, s > g$. Then*

$$\frac{u_m v_n}{u_n v_m} = \mu_{mnrs}.$$

Proof. — Let us denote by $\phi_S : C \to \mathbb{P}^{g-1}$ the canonical map given by the standard basis $\{\frac{x^r dx}{y}\}_r$ of $H^0(C, \Omega^1)$. We know that $\phi_S(W_n) = (1, \alpha_n, \ldots \alpha_n^{g-1})$, and proposition 1.1 shows that $\phi_G = P^{-1} \circ \phi_S$, where P is the linear map given by the Vandermonde matrix:

$$V(\alpha_1, \ldots \alpha_g) := \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_g \\ \alpha_1^2 & \alpha_2^2 & & \alpha_g^2 \\ \vdots & \vdots & & \vdots \\ \alpha_1^{g-1} & \alpha_2^{g-1} & \cdots & \alpha_g^{g-1} \end{pmatrix}.$$

Let $F(X) = (X - \alpha_1) \cdots (X - \alpha_g)$, and consider the polynomials $H_i(X) = \frac{1}{F'(\alpha_i)} \frac{F(X)}{(X - \alpha_i)} = \sum_{j=0}^{g-1} a_{i,j+1} X^j$, whose coefficients are the entries of the matrix $IV(\alpha_1, \ldots \alpha_g) := V(\alpha_1, \ldots, \alpha_g)^{-1} = (a_{i,j})_{i,j=1\ldots,g}$, since $H_i(\alpha_j) = \delta_{ij}$. The map P^{-1} is then given by a matrix $\mathrm{diag}(\lambda_1, \ldots, \lambda_g) IV(\alpha_1, \ldots \alpha_g)$, where the λ_i are certain numbers which we don't need to determine. Hence

the coordinates of $\phi_G(W_r)$ are:

$$\phi_G(W_r) = \begin{pmatrix} \dfrac{\lambda_1 F(\alpha_r)}{(\alpha_r-\alpha_1)F'(\alpha_1)} \\ \vdots \\ \vdots \\ \dfrac{\lambda_g F(\alpha_r)}{(\alpha_r-\alpha_g)F'(\alpha_g)} \end{pmatrix},$$

and the result follows immediately. □

We can combine this two results in order to find nice formulas for double ratios of Jacobian Nullwerte. An easy example is the following:

COROLLARY 8.3. — *Let $W_1,\dots,W_g,W_r,W_s$ be $g+2$ different Weierstrass points on C, and form the divisors:*

$$\begin{aligned} D &= \textstyle\sum_{i=1}^{g} W_i, \\ D' &= \textstyle\sum_{i>g, i\neq r,s} W_i, \\ D_i &= D - W_i, && i=1,\dots,g, \\ D_i' &= D_i + W_r - W_1, && i=2,\dots,g, \\ D_i'' &= D_i + W_s - W_1, && i=2,\dots,g. \end{aligned}$$

a) *Let $w_i=\Pi(D_i)$, $w_i'=\Pi(D_i')$, $w_i''=\Pi(D_i'')$. The following equalities hold:*

$$\frac{[w_m,w_2',\dots,w_g'][w_n,w_2'',\dots,w_g'']}{[w_m,w_2'',\dots,w_g''][w_n,w_2',\dots,w_g']} = \mu_{mnrs}. \tag{8.1}$$

b) *Let $w_{mr}=\Pi(D'+W_m+W_r)$, $w_{ms}=\Pi(D'+W_m+W_s)$, $w_{nr}=\Pi(D'+W_n+W_r)$, $w_{mr}=\Pi(D'+W_n+W_s)$. We have:*

$$\frac{[w_m,w_2',\dots,w_g'][w_n,w_2'',\dots,w_g'']}{[w_m,w_2'',\dots,w_g''][w_n,w_2',\dots,w_g']} = \pm\left(\frac{\theta[w_{mr}]\theta[w_{ns}]}{\theta[w_{ms}]\theta[w_{nr}]}\right)^2.$$

Proof. — The first equality follows from propositions 8.1 and 8.2. The second relation is derived from the first one and Thomae's formula 4.2. □

As a by-product of this corollary we obtain a relation between some double ratios of Jacobian Nullwerte:

COROLLARY 8.4. — *Consider a second family $W_1''',\dots,W_g'''$ of g Weierstrass points different from $W_{g+1},\dots,W_{g+2}$, and form the divisors $D_i'''=\sum_{j\neq i} W_j'''$. Let $w_i'''=\Pi(D_i''')$. We have:*

$$\frac{[w_m,w_2',\dots,w_g'][w_n,w_2'',\dots,w_g'']}{[w_m,w_2'',\dots,w_g''][w_n,w_2',\dots,w_g']} = \frac{[w_m''',w_2',\dots,w_g'][w_n''',w_2'',\dots,w_g'']}{[w_m''',w_2'',\dots,w_g''][w_n''',w_2',\dots,w_g']}.$$

All the formulas above concerning Jacobian Nullwerte have been obtained by geometric means, but they could have been obtained directly from theorem 4.1, which is a source for lots of such relations.

An important consequence of corollary 8.3 and proposition 2.13 is the fact that *Jacobian Nullwerte provide an effective solution to the hyperelliptic Schottky problem in every genus*. In the next two sections we shall explicit this construction for genus 2 and genus 3 hyperelliptic curves. These are the cases which are usually considered for applications (for instance, in cryptography) and which are at the reach of present standard computational power.

9. Genus 2 curves

We shall now consider the results in previous sections for the particular case of genus 2 curves, where a number of refinements can be obtained, both in the algebraic and the analytic sides. We will explain how to find a symmetric equation for a hyperelliptic curve given its Igusa-Clebsch invariants or a normalized period matrix. Both methods are simple and efficient.

9.1. Symmetric invariants for genus 2 curves

Given a symmetric equation $Y^2 = X(X^4 + G_1X^3 + G_2X^2 + G_3X + 1)$, it is a simple matter the determination of its Igusa-Clebsch invariants:

$$
\begin{aligned}
(9.1)\qquad I_2 =& 2\left(20 + 3\,G_2^2 - 8\,G_1\,G_3\right),\\
I_4 =& -4\left(20 + 3\,G_1^2\,G_2 - 9\,G_2^2 - G_1\,G_3 - G_1^2\,G_3^2 + 3\,G_2\,G_3^2\right),\\
I_6 =& -2\left(160 + 18\,G_1^4 - 13\,G_1^2\,G_2 - 88\,G_2^2 + 12\,G_1^2\,G_2^3 - 36\,G_2^4\right.\\
&- 32\,G_1\,G_3 - 38\,G_1^3\,G_2\,G_3 + 119\,G_1\,G_2^2\,G_3 - 14\,G_1^2\,G_3^2\\
&- 13\,G_2\,G_3^2 - 4\,G_1^2\,G_2^2\,G_3^2 + 12\,G_2^3\,G_3^2 + 12\,G_1^3\,G_3^3\\
&\left.-38\,G_1\,G_2\,G_3^3 + 18\,G_3^4\right),\\
I_{10} =& -27\,G_1^4 + 144\,G_1^2\,G_2 - 128\,G_2^2 - 4\,G_1^2\,G_2^3 + 16\,G_2^4\\
&- 192\,G_1\,G_3 + 18\,G_1^3\,G_2\,G_3 - 80\,G_1\,G_2^2\,G_3 - 6\,G_1^2\,G_3^2\\
&+ 144\,G_2\,G_3^2 + G_1^2\,G_2^2\,G_3^2 - 4\,G_2^3\,G_3^2 - 4\,G_1^3\,G_3^3\\
&+ 18\,G_1\,G_2\,G_3^3 - 27\,G_3^4 + 256.
\end{aligned}
$$

On the other hand, the determination of an hyperelliptic curve with prescribed invariants $I_2 = \mathcal{I}_2, I_4 = \mathcal{I}_4, I_6 = \mathcal{I}_6, I_{10} = \mathcal{I}_{10}$ is a non-trivial problem, solved by [20] and [4]. We will explain here an elementary method to find a symmetric equation with prescribed invariants, which takes profit of the simplicity of the expressions above. Since the Igusa-Clebsch invariants are homogeneous invariants and the symmetric coefficients are absolute invariants, we need to introduce a proportionality constant, and solve the equations above for $I_{2k} = r^k \mathcal{I}_{2k}$.

First of all, we note that the formulas above are symmetric polynomials in G_1, G_3, so that we can express them in terms of

$$S_1 = G_1 + G_3, \qquad S_2 = G_1 G_3. \tag{9.2}$$

We obtain:

$$\begin{aligned}
r\mathcal{I}_2 =& 2\left(20 + 3\,G_2^2 - 8\,S_2\right),\\
r^2\mathcal{I}_4 =& 4\left(-20 + 9\,G_2^2 - 3\,G_2\,S_1^2 + S_2 + 6\,G_2\,S_2 + S_2^2\right),\\
r^3\mathcal{I}_6 =& 2\left(-160 + 88\,G_2^2 + 36\,G_2^4 + 13\,G_2\,S_1^2 - 12\,G_2^3\,S_1^2 - 18\,S_1^4\right.\\
&+ 32\,S_2 - 26\,G_2\,S_2 - 119\,G_2^2\,S_2 + 24\,G_2^3\,S_2 + 72\,S_1^2\,S_2\\
&\left.+ 38\,G_2\,S_1^2\,S_2 - 22\,S_2^2 - 76\,G_2\,S_2^2 + 4\,G_2^2\,S_2^2 - 12\,S_2^3\right),\\
r^5\mathcal{I}_{10} =& -128\,G_2^2 + 16\,G_2^4 + 144\,G_2\,S_1^2 - 4\,G_2^3\,S_1^2 - 27\,S_1^4 - 192\,S_2\\
&- 288\,G_2\,S_2 - 80\,G_2^2\,S_2 + 8\,G_2^3\,S_2 + 108\,S_1^2\,S_2 + 18\,G_2\,S_1^2\,S_2\\
&- 60\,S_2^2 - 36\,G_2\,S_2^2 + G_2^2\,S_2^2 - 4\,S_2^3 + 256.
\end{aligned}$$

From the first equality we have:

$$S_2 = (6G_2^2 + 40 - r\mathcal{I}_2)/16, \tag{9.3}$$

and we replace this relation in the remaining equations:

$$\begin{aligned}
2^6\mathcal{I}_4 =& 36\,G_2^4 + 576\,G_2^3 - 12\,(r\mathcal{I}_2 - 240)\,G_2^2 - 96\left(8\,S_1^2 + r\mathcal{I}_2 - 40\right)G_2\\
&+ (r\mathcal{I}_2 - 120)\,(r\mathcal{I}_2 + 24),\\
2^9\mathcal{I}_6 =& -72\,G_2^6 - 1728\,G_2^5 + 12\,(11\,\mathcal{I}_2\,r - 1440)\,G_2^4\\
&+ 192\left(12\,S_1^2 + 11\,\mathcal{I}_2\,r - 492\right)G_2^3\\
&- 2\left(-13824\,S_1^2 + 19\,{\mathcal{I}_2}^2\,r^2 - 5856\,\mathcal{I}_2\,r + 152640\right)G_2^2\\
&- 16\,(19\,\mathcal{I}_2\,r - 864)\left(8\,S_1^2 + \mathcal{I}_2\,r - 40\right)G_2\\
&- 18432\,S_1^4 - 4608\,(+\mathcal{I}_2\,r - 40)\,S_1^2 + 3\,\mathcal{I}_2^3\,r^3\\
&- 448\,\mathcal{I}_2^2\,r^2 + 19392\,\mathcal{I}_2\,r - 414720,
\end{aligned}$$

$$\begin{aligned}2^{10}\mathcal{I}_{10} = &-72\,G_2^6 - 2112\,G_2^5 + 4\,(15\,\mathcal{I}_2\,r - 6344)\,G_2^4\\ &+ 64\,\left(44\,S_1^2 + 19\,\mathcal{I}_2\,r - 2488\right)\,G_2^3\\ &- 2\,\left(-20736\,S_1^2 + 7\,{\mathcal{I}_2}^2\,r^2 - 4560\,\mathcal{I}_2\,r + 273600\right)\,G_2^2\\ &- 144\,(\mathcal{I}_2\,r - 168)\,\left(8\,S_1^2 + \mathcal{I}_2\,r - 40\right)\,G_2\\ &- 27648\,S_1^4 - 6912\,(+\mathcal{I}_2\,r - 40)\,S_1^2\\ &+ {\mathcal{I}_2}^3\,r^3 - 360\,{\mathcal{I}_2}^2\,r^2 + 36288\,\mathcal{I}_2\,r - 677376.\end{aligned}$$

The first equality yields:

(9.4)

$$S_1^2 = \frac{36\,G_2^4+576\,G_2^3-12\,(r\,\mathcal{I}_2-240)\,G_2^2-96\,(r\,\mathcal{I}_2-40)\,G_2+r^2\,\mathcal{I}_2^2-96\,\mathcal{I}_2-64\,r^2\,\mathcal{I}_4-2880}{768G_2}.$$

We now substitute this value in the equations for $\mathcal{I}_6, \mathcal{I}_{10}$:

(9.5)

$$\begin{aligned}&432\,G_2^8-864\,G_2^6\,(48+r\,\mathcal{I}_2)+72\,G_2^4\left(18240+672\,r\,\mathcal{I}_2+5\,r^2\,\mathcal{I}_2^2+64\,r^2\,\mathcal{I}_4\right)\\ &\quad-8\,G_2^2\left(1797120+81216\,r\,\mathcal{I}_2+432\,r^2\,\mathcal{I}_2^2+7\,r^3\,\mathcal{I}_2^3+27648\,r^2\,\mathcal{I}_4+1856\,r^3\,\mathcal{I}_2\,\mathcal{I}_4-6144\,r^3\,\mathcal{I}_6\right)\\ &\quad+2^{12}3^45\,r\,\mathcal{I}_2-576\,r^3\,\mathcal{I}_2\left(\mathcal{I}_2^2-64\,\mathcal{I}_4\right)+3\,r^4\left(\mathcal{I}_2^2-64\,\mathcal{I}_4\right)^2\\ &\quad+3456\,r^2\left(3\,\mathcal{I}_2^2+320\,\mathcal{I}_4\right)+2^{12}3^55^2=0,\end{aligned}$$

$$\begin{aligned}&144\,G_2^8-96\,G_2^6\,(176+5\,r\,\mathcal{I}_2)+8\,G_2^4\left(89280+4704\,r\,\mathcal{I}_2+59\,r^2\,\mathcal{I}_2^2+448\,r^2\,\mathcal{I}_4\right)\\ &\quad+24\,G_2^2\left(-525312-36288\,r\,\mathcal{I}_2-720\,r^2\,\mathcal{I}_2^2-5\,r^3\,\mathcal{I}_2^3-9216\,r^2\,\mathcal{I}_4-192\,r^3\,\mathcal{I}_2\,\mathcal{I}_4+8192\,r^5\,\mathcal{I}_{10}\right)\\ &\quad+2^{12}3^55\,r\,\mathcal{I}_2-1728\,r^3\,\mathcal{I}_2\left(\mathcal{I}_2^2-64\,\mathcal{I}_4\right)+9\,r^4\left(\mathcal{I}_2^2-64\,\mathcal{I}_4\right)^2\\ &\quad+10368\,r^2\left(3\,\mathcal{I}_2^2+320\,\mathcal{I}_4\right)+2^{12}3^65^2=0.\end{aligned}$$

We can solve these equations by a resultant elimination. It turns out that the elimination of G_2 produces a much simpler result:

(9.6)

$$\begin{aligned}&2^83^6\,r^{15}\,\mathcal{I}_{10}^4+2^63^6\;r^{13}\,\mathcal{I}_{10}^3(\mathcal{I}_2\,\mathcal{I}_4-4\,\mathcal{I}_6)-2^63^5\,r^{12}\,\mathcal{I}_{10}^3\left(\mathcal{I}_2^2-16\,\mathcal{I}_4\right)\\ &+108\,r^{11}\,\mathcal{I}_{10}^2\left(19\,\mathcal{I}_2^2\,\mathcal{I}_4^2+8\,\mathcal{I}_4^3-168\,\mathcal{I}_2\,\mathcal{I}_4\,\mathcal{I}_6+360\,\mathcal{I}_6^2+5616\,\mathcal{I}_2\,\mathcal{I}_{10}\right)\\ &-216\,r^{10}\,\mathcal{I}_{10}^2\left(11\,\mathcal{I}_2^3\,\mathcal{I}_4+16\,\mathcal{I}_2\,\mathcal{I}_4^2-36\,\mathcal{I}_2^2\,\mathcal{I}_6-192\,\mathcal{I}_4\,\mathcal{I}_6-105408\,\mathcal{I}_{10}\right)\\ &+2\,r^9\,\mathcal{I}_{10}\,(\mathcal{I}_2^5\,\mathcal{I}_4^2+25\,\mathcal{I}_2^3\,\mathcal{I}_4^3-26\,\mathcal{I}_2\,\mathcal{I}_4^4-6\,\mathcal{I}_2^4\,\mathcal{I}_4\,\mathcal{I}_6-324\,\mathcal{I}_2^2\,\mathcal{I}_4^2\,\mathcal{I}_6+168\,\mathcal{I}_4^3\,\mathcal{I}_6+9\,\mathcal{I}_2^3\,\mathcal{I}_6^2\\ &\qquad+1242\,\mathcal{I}_2\,\mathcal{I}_4\,\mathcal{I}_6^2-1512\,\mathcal{I}_6^3-270\,\mathcal{I}_2^4\,\mathcal{I}_{10}-11556\,\mathcal{I}_2^2\,\mathcal{I}_4\,\mathcal{I}_{10}+92016\,\mathcal{I}_4^2\,\mathcal{I}_{10}+37584\,\mathcal{I}_2\,\mathcal{I}_6\,\mathcal{I}_{10})\\ &+36\,r^8\,\mathcal{I}_{10}\,(\mathcal{I}_2^4\,\mathcal{I}_4^2-17\,\mathcal{I}_2^2\,\mathcal{I}_4^3+16\,\mathcal{I}_4^4-6\,\mathcal{I}_2^3\,\mathcal{I}_4\,\mathcal{I}_6+96\,\mathcal{I}_2\,\mathcal{I}_4^2\,\mathcal{I}_6+9\,\mathcal{I}_2^2\,\mathcal{I}_6^2-144\,\mathcal{I}_4\,\mathcal{I}_6^2\\ &\qquad-1350\,\mathcal{I}_2^3\,\mathcal{I}_{10}+23544\,\mathcal{I}_2\,\mathcal{I}_4\,\mathcal{I}_{10}-54432\,\mathcal{I}_6\,\mathcal{I}_{10})\end{aligned}$$

$$+r^7\,(\mathcal{I}_2^4\,\mathcal{I}_4^4-2\,\mathcal{I}_2^2\,\mathcal{I}_4^5+\mathcal{I}_4^6-12\,\mathcal{I}_2^3\,\mathcal{I}_4^3\,\mathcal{I}_6+12\,\mathcal{I}_2\,\mathcal{I}_4^4\,\mathcal{I}_6+54\,\mathcal{I}_2^2\,\mathcal{I}_4^2\,\mathcal{I}_6^2-18\,\mathcal{I}_4^3\,\mathcal{I}_6^2-108\,\mathcal{I}_2\,\mathcal{I}_4\,\mathcal{I}_6^3$$
$$+81\,\mathcal{I}_6^4+30\,\mathcal{I}_2^5\,\mathcal{I}_4\,\mathcal{I}_{10}+156\,\mathcal{I}_2^3\,\mathcal{I}_4^2\,\mathcal{I}_{10}+1272\,\mathcal{I}_2\,\mathcal{I}_4^3\,\mathcal{I}_{10}-72\,\mathcal{I}_2^4\,\mathcal{I}_6\,\mathcal{I}_{10}-3672\,\mathcal{I}_2^2\,\mathcal{I}_4\,\mathcal{I}_6\,\mathcal{I}_{10}$$
$$+2448\,\mathcal{I}_4^2\,\mathcal{I}_6\,\mathcal{I}_{10}+7236\,\mathcal{I}_2\,\mathcal{I}_6^2\,\mathcal{I}_{10}-1202364\,\mathcal{I}_2^2\,\mathcal{I}_{10}^2+4167936\,\mathcal{I}_4\,\mathcal{I}_{10}^2)$$
$$-4\,r^6\,\mathcal{I}_{10}\,(\mathcal{I}_2^6-218\,\mathcal{I}_2^4\,\mathcal{I}_4-512\,\mathcal{I}_2^2\,\mathcal{I}_4^2-5832\,\mathcal{I}_4^3+312\,\mathcal{I}_2^3\,\mathcal{I}_6+18480\,\mathcal{I}_2\,\mathcal{I}_4\,\mathcal{I}_6-28152\,\mathcal{I}_6^2$$
$$+2^4 3^7 67\,\mathcal{I}_2\,\mathcal{I}_{10})$$
$$-3\,r^5\,(-5\,\mathcal{I}_2^4\,\mathcal{I}_4^3+19\,\mathcal{I}_2^2\,\mathcal{I}_4^4-14\,\mathcal{I}_4^5+42\,\mathcal{I}_2^3\,\mathcal{I}_4^2\,\mathcal{I}_6-96\,\mathcal{I}_2\,\mathcal{I}_4^3\,\mathcal{I}_6-117\,\mathcal{I}_2^2\,\mathcal{I}_4\,\mathcal{I}_6^2+126\,\mathcal{I}_4^2\,\mathcal{I}_6^2$$
$$+108\,\mathcal{I}_2\,\mathcal{I}_6^3+48\,\mathcal{I}_2^5\,\mathcal{I}_{10}-906\,\mathcal{I}_2^3\,\mathcal{I}_4\,\mathcal{I}_{10}+372\,\mathcal{I}_2\,\mathcal{I}_4^2\,\mathcal{I}_{10}-6120\,\mathcal{I}_2^2\,\mathcal{I}_6\,\mathcal{I}_{10}+85824\,\mathcal{I}_4\,\mathcal{I}_6\,\mathcal{I}_{10}$$
$$+7589376\,\mathcal{I}_{10}^2)$$
$$-2\,r^4\,(\mathcal{I}_2^5\,\mathcal{I}_4^2-110\,\mathcal{I}_2^3\,\mathcal{I}_4^3+109\,\mathcal{I}_2\,\mathcal{I}_4^4-6\,\mathcal{I}_2^4\,\mathcal{I}_4\,\mathcal{I}_6+810\,\mathcal{I}_2^2\,\mathcal{I}_4^2\,\mathcal{I}_6-156\,\mathcal{I}_4^3\,\mathcal{I}_6+9\,\mathcal{I}_2^3\,\mathcal{I}_6^2$$
$$-1917\,\mathcal{I}_2\,\mathcal{I}_4\,\mathcal{I}_6^2+1404\,\mathcal{I}_6^3+594\,\mathcal{I}_2^4\,\mathcal{I}_{10}+24678\,\mathcal{I}_2^2\,\mathcal{I}_4\,\mathcal{I}_{10}+27216\,\mathcal{I}_4^2\,\mathcal{I}_{10}-140616\,\mathcal{I}_2\,\mathcal{I}_6\,\mathcal{I}_{10})$$
$$-9\,r^3\,(4\,\mathcal{I}_2^4\,\mathcal{I}_4^2-116\,\mathcal{I}_2^2\,\mathcal{I}_4^3+31\,\mathcal{I}_4^4-24\,\mathcal{I}_2^3\,\mathcal{I}_4\,\mathcal{I}_6+672\,\mathcal{I}_2\,\mathcal{I}_4^2\,\mathcal{I}_6+36\,\mathcal{I}_2^2\,\mathcal{I}_6^2-1008\,\mathcal{I}_4\,\mathcal{I}_6^2-24\,\mathcal{I}_2^3\,\mathcal{I}_{10}$$
$$+36960\,\mathcal{I}_2\,\mathcal{I}_4\,\mathcal{I}_{10}-94464\,\mathcal{I}_6\,\mathcal{I}_{10})$$
$$-54\,r^2\left(4\,\mathcal{I}_2^3\,\mathcal{I}_4^2-31\,\mathcal{I}_2\,\mathcal{I}_4^3-24\,\mathcal{I}_2^2\,\mathcal{I}_4\,\mathcal{I}_6+108\,\mathcal{I}_4^2\,\mathcal{I}_6+36\,\mathcal{I}_2\,\mathcal{I}_6^2-504\,\mathcal{I}_2^2\,\mathcal{I}_{10}+9792\,\mathcal{I}_4\,\mathcal{I}_{10}\right)$$
$$-432\,r\left(\mathcal{I}_2^2\,\mathcal{I}_4^2-\mathcal{I}_4^3-6\,\mathcal{I}_2\,\mathcal{I}_4\,\mathcal{I}_6+9\,\mathcal{I}_6^2-54\,\mathcal{I}_2\,\mathcal{I}_{10}\right)-2^8 3^6\,\mathcal{I}_{10}=0.$$

Note that the coefficient of r^n in this expression is an homogeneous weighted polynomial of degree $2n+10$ in the invariants $\mathcal{I}_2, \mathcal{I}_4, \mathcal{I}_6, \mathcal{I}_8$.

9.2. Jacobian nullwerte and symmetric equations in genus two

We now proceed to specialize the results in sections 7 and 8 for hyperelliptic genus two curves. Our starting point now is the normalized period matrix for the Jacobian of a hyperelliptic curve defined over a number field, and our goal is the determination of a symmetric model for the curve. The procedure described in section 7 provides a basis of algebraic differential forms for the curve, and then proposition 8.1 gives formulas for the canonical image of the Weierstrass points of the curve with respect to this basis. We obtain the following simple formulas:

THEOREM 9.1. — *Let C be a genus 2 curve, with field of moduli $K \subset \mathbb{C}$. Let $Z \in \mathbb{H}_2$ be a normalized period matrix for C. Given two odd 2-torsion points $w_1, w_2 \in J(C)[2]$.*

a) *For every even 2-torsion point $w_0 \in J(C)[2]$, the non-singular matrix $\Omega_1(w_1, w_2, w_0; Z) := \frac{1}{2\pi i \theta[w_0]} J[w_1, w_2]$ is a period matrix of a basis of differential forms on C defined over a finite extension L of K.*

b) *Let w be a third odd 2-torsion point on $J(C)$. The point cut by the hyperplane*

$$\left(\frac{\partial\theta}{\partial z_1}(w),\ \frac{\partial\theta}{\partial z_2}(w)\right)\Omega_1(w_1,w_2,w_0;Z)^{-1}\begin{pmatrix}X_1\\X_2\end{pmatrix}=0,$$

in $\mathbb{P}^1(\mathbb{C})$ has projective coordinates $([w_1,w]:[w_2,w]|)$ and it is independent of w_0.

c) *Let $J(C)[2]^{\mathrm{odd}}=\{w_1,w_2,w_3,w_4,w_5,w_6\}$. The ratios*

$$\ell_{12j}:=\frac{[w_1,w_j]}{[w_2,w_j]}\in\mathbb{C}\cup\{\infty\},\quad j=1,\dots,6, \tag{9.7}$$

are algebraic over K.

d) *The curve C admits the symmetric model*

$$\mathcal{C}_{12}\colon Y^2=X(X-\ell_{123})(X-\ell_{124})(X-\ell_{125})(X-\ell_{126}) \tag{9.8}$$

over a finite extension of K.

e) *The symmetric discriminant $\mathcal{D}_{12}$ of the symmetric model $\mathcal{C}_{12}$ is given by:*

$$\mathcal{D}_{12}=\frac{[w_1,w_2]^{16}}{([w_1,w_3][w_1,w_4][w_1,w_5][w_1,w_6])^4}.$$

Proof.

a) The discussion in section 7 shows that $\Omega_1(w_1,w_2,w_0;Z)$ is a period matrix for certain basis η_1,η_2 of $H^0(J(C),\Omega^1_{/\bar{K}})$ defined over a finite extension of K. Since the Abel-Jacobi map $\Pi: C\to J(C)$ is defined over a finite extension of K, the forms $\omega_1=\Pi^*\eta_1,\omega_2=\Pi^*\eta_2$ are defined over a finite extension L of K, and $\Omega_1(w_1,w_2,w_0;Z)$ is a period matrix for them.

b) From the equality

$$\Omega_1(w_1,w_2,w_0;Z)^{-1}=\lambda\begin{pmatrix}\dfrac{\partial\theta[w_2]}{\partial z_2}(0) & -\dfrac{\partial\theta[w_1]}{\partial z_2}(0)\\ -\dfrac{\partial\theta[w_2]}{\partial z_1}(0) & \dfrac{\partial\theta[w_1]}{\partial z_1}(0)\end{pmatrix},$$

with $\lambda\in\mathbb{C}^*$, a simple matrix calculation shows that

$$\left(\frac{\partial\theta}{\partial z_1}(w),\ \frac{\partial\theta}{\partial z_2}(w)\right)\Omega_1(w_1,w_2,w_0;Z)^{-1}=\lambda\,h(w)\,([w,w_2],[w_1,w]),$$

with $h(w)\neq 0$, and the assertion follows.

c) The ratios of Jacobian Nullwerte can be reduced to ratios of differences of x-coordinates of the Weierstrass points of any algebraic model $Y^2=f(X)$ of C, by theorem 4.1, and hence they are algebraic themselves.

d) By [8, p. 399], there exists two functions $x,y\in\bar{K}(C)$ such that $\omega_1=dx/y$, $\omega_2=x\,dx/y$, providing a model $y^2=f(x)$ for C, defined over L. For

this model we know by 1.1 that their Weierstrass points have the ratios ℓ_{12j} as x-coordinates. Using theorem 4.1 is easy to see that $\prod_{j=3}^{6} \ell_{12j} = \pm 1$, and hence $\mathcal{C}_{12}$ is a symmetric model for C.

d) The expression for $\mathcal{D}_{12}$ follows from the equality:

$$\ell_{12i} - \ell_{12j} = \frac{[w_1, w_2][w_i, w_j]}{[w_i, w_2][w_j, w_2]}.$$

□

After theorem 9.1, we have a complete and effective solution to the hyperelliptic Torelli problem in genus 2. We have applied this result in three different situations, to present irreducible abelian surfaces with extra multiplications as Jacobians of curves ([9], [7], [2]).

Theorem 9.1 also has a number of theoretical consequences: we can rephrase the properties of the symmetric roots in terms of the corresponding expressions with the Jacobian Nullwerte, thus providing elementary proofs for relations between them. For instance:

PROPOSITION 9.2. — *Let* $J(C)[2]^{\text{odd}} = \{w_1, w_2, w_3, w_4, w_5, w_6\}$. *We have*

$$[w_1, w_3][w_1, w_4][w_1, w_5][w_1, w_6] = \pm [w_2, w_3][w_2, w_4][w_2, w_5][w_2, w_6].$$

This result could be proved by means of the Rosenhain formula, but the interpretation of the quotients $[w_1, w_i]/[w_2, w_i]$ as symmetric roots gives it immediately.

9.3. Thetanullwerte and symmetric equations in genus two

We now combine the expression (9.7) of the symmetric roots in terms of Jacobian Nullwerte with Rosenhain formula (3.2), obtaining expressions for the symmetric roots as quotients of Thetanullwerte:

PROPOSITION 9.3. — *Let* $J(C)[2]^{\text{odd}} = \{w_i, w_j, w_k, w_a, w_b, w_c\}$. *We have:*

$$\begin{aligned}
\ell_{ijk} &= \pm \prod_{\substack{r=1,\dots,6 \\ r \neq i,j,k}} \frac{\theta[w_i + w_k - w_r]}{\theta[w_j + w_k - w_r]} \\
&= \pm \frac{\theta[w_i + w_k - w_a]\theta[w_i + w_k - w_b]\theta[w_i + w_k - w_c]}{\theta[w_j + w_k - w_a]\theta[w_j + w_k - w_b]\theta[w_j + w_k - w_c]} \\
&= \pm \frac{\theta[w_i + w_k - w_a]\theta[w_i + w_k - w_b]\theta[w_i + w_k - w_c]}{\theta[w_i + w_a - w_b]\theta[w_i + w_a - w_c]\theta[w_i + w_b - w_c]};
\end{aligned}$$

(The sign depends only on w_i, w_j, w_k and can be explicitly determined.)

$$\mathcal{D}_{ij}=\frac{(\theta[w_i+w_j+w_k]\theta[w_i+w_j+w_a]\theta[w_i+w_j+w_b]\theta[w_i+w_j+w_c])^{12}}{(\theta[w_i+w_k+w_a]\theta[w_i+w_k+w_b]\theta[w_i+w_k+w_c]\theta[w_i+w_a+w_b]\theta[w_i+w_a+w_c]\theta[w_i+w_b+w_c])^{8}}.$$

Weber [29] and Takase [25] have given expressions for the roots of a Rosenhain model for C in terms of even Thetanullwerte. Takase's formulas are simpler, since they are quotients of Thetanullwerte. One can recover these formulas from the proposition above, just by deriving a Rosenhain model from our symmetric model.

The simple expressions in the proposition (or Takase's formulas) worth attention for practical applications. In case we want to compute a (symmetric) equation for C from its period matrix, it happens that actually only six different Thetanullwerte are involved in the computation of a set of symmetric roots of C. In particular, the computation of the Igusa invariants of C by means of these formulas requires only six numerical evaluations of the Theta function. This represents a gain of 40% with respect to the methods applied in ([29], [31], [28]). Moreover, the minimality properties of the symmetric models (theorem 2.10) suggest that their coefficients should be relatively small. In case we have some extra information about the arithmetic of the curve (for instance, if we know that its Jacobian variety has complex multiplication and we know over which primes its reduction is not irreducible), we will be able to bound the denominators appearing on the symmetric equations, a crucial point to be sure that numerical results have enough precision to be correct.

10. Genus 3 curves

We shall now describe an effective solution to the Torelli problem for hyperelliptic genus 3 curves, based on the combination of Jacobian Nullwerte and symmetric roots.

We are given a normalized period matrix $Z \in \mathbb{H}_3$, corresponding to a genus 3 hyperelliptic curve C, and we are asked for an equation of the curve.

We may suppose that the period matrix Z comes from a model $Y^2 = (X-\alpha_1)\cdots(X-\alpha_8)$ of C. The Weierstrass points of this model are then $W_i := (\alpha_i, 0)$. There are twenty-eight odd two torsion points in $J(C)$, and they are given by the degree 2 divisors of the form $W_i + W_j$. We shall write $w_{rs} = \Pi(W_r + W_s)$. Note that $w_{rs} + w_{st} = w_{rt}$.

The following result is a particular case of corollary 8.3 for genus 3 hyperelliptic curves:

LEMMA 10.1. — *Let $m,n,r,s,t \in \{1,2,\dots,8\}$. We have:*

$$\mu_{mnrs} = \frac{[w_{mt}, w_{ts}, w_{sn}][w_{nt}, w_{tr}, w_{rn}]}{[w_{mt}, w_{tr}, w_{rn}][w_{nt}, w_{ts}, w_{sn}]}.$$

The first step in the computation of a symmetric model for C is the proper identification of the elements of $J(C)[2]^{\mathrm{odd}}$ with the divisors $W_i + W_j$. We proceed as follows: we take an arbitrary pair $w_1, w_2 \in J(C)[2]^{\mathrm{odd}}$ such that $w_3 := w_1 + w_2$ is also odd. This assures that these points come from three divisors geometrically well posed in the sense of proposition 3.4:

$$w_1 := w_{23} = \Pi(W_2 + W_3), \quad w_2 = w_{13} = \Pi(W_1 + W_3), \qquad w_3 = w_{12} = \Pi(W_1 + W_2),$$

(a formal re-labelling of the α_i may be necessary). We now look for the remaining five points $w \in J(C)[2]^{\mathrm{odd}}$ such that $w_2 + w, w_3 + w$ are simultaneously odd; they must came from divisors $W_1 + W$. We can write them as

$$w_{14} = \Pi(W_1 + W_4), \quad w_{15} = \Pi(W_1 + W_5), \dots, w_{18} = \Pi(W_1 + W_8).$$

Since $w_{jk} = w_{1j} + w_{1k}$, we are already in position to apply the lemma above to compute all the μ_{12rs}:

$$\mu_{12rs} = \frac{[w_{1t}, w_{ts}, w_{s2}][w_{2t}, w_{tr}, w_{r2}]}{[w_{1t}, w_{tr}, w_{r2}][w_{2t}, w_{ts}, w_{s2}]}. \tag{10.1}$$

There are eighteen 2-torsion points involved in this computation, so that, in principle, we will have to compute 54 theta-derivatives (but these calculations are highly parallelizable).

Finally, we compute a set of symmetric roots for C. After lemma 2.12 we have

$$\ell_{123} = \sqrt[6]{\prod_{k \neq 1,2,3} \mu_{123k}}$$

(no matter which root we take), and then

$$\ell_{12k} = \mu_{123k}^{-1} \ell_{123}, \qquad k = 4, \dots, 8.$$

We have obtained:

THEOREM 10.2. — *Let us denote by* $[ab, cd, ef]$ *the Jacobian Nullwerte* $[w_{a,b}, w_{b,c}, w_{c,d}](Z)$. *A set of symmetric roots for* C *is:*

$$\ell_{123} = \sqrt[6]{\frac{[14,48,28]\,[18,48,24]\,[18,58,25]\,[18,68,26]\,[18,78,27]\,[24,34,23]\,[28,38,23]^4}{[14,34,23]\,[18,38,23]^4\,[24,48,28]\,[28,48,24]\,[28,58,25]\,[28,68,26]\,[28,78,27]}}$$

$$\ell_{124} = \sqrt[6]{\frac{[14,48,28]\,[18,38,23]^2\,[18,58,25]\,[18,68,26]\,[18,78,27]\,[24,34,23]\,[28,48,24]^5}{[14,34,23]\,[18,48,24]^5\,[24,48,28]\,[28,38,23]^2\,[28,58,25]\,[28,68,26]\,[28,78,27]}}$$

$$\ell_{125} = \sqrt[6]{\frac{[14,48,28]\,[18,38,23]^2\,[18,48,24]\,[18,68,26]\,[18,78,27]\,[24,34,23]\,[28,58,25]^5}{[14,34,23]\,[18,58,25]^5\,[24,48,28]\,[28,38,23]^2\,[28,48,24]\,[28,68,26]\,[28,78,27]}}$$

$$\ell_{126} = \sqrt[6]{\frac{[14,48,28]\,[18,38,23]^2\,[18,48,24]\,[18,58,25]\,[18,78,27]\,[24,34,23]\,[28,68,26]^5}{[14,34,23]\,[18,68,26]^5\,[24,48,28]\,[28,38,23]^2\,[28,48,24]\,[28,58,25]\,[28,78,27]}}$$

$$\ell_{127} = \sqrt[6]{\frac{[14,48,28]\,[18,38,23]^2\,[18,48,24]\,[18,58,25]\,[18,68,26]\,[24,34,23]\,[28,78,27]^5}{[14,34,23]\,[18,78,27]^5\,[24,48,28]\,[28,38,23]^2\,[28,48,24]\,[28,58,25]\,[28,68,26]}}$$

$$\ell_{128} = \sqrt[6]{\frac{[14,34,23]^5\,[18,48,24]\,[18,58,25]\,[18,68,26]\,[18,78,27]\,[24,48,28]^5\,[28,38,23]^4}{[14,48,28]^5\,[18,38,23]^4\,[24,3423]^5\,[28,48,24]\,[28,58,25]\,[28,68,26]\,[28,78,27]}}.$$

These expressions are not unique, since they depend on the value of t chosen in (10.1) to determine μ_{123k}. In any case, the chance to pick two different t for the same k gives a lot of equalities between quotients of Jacobian Nullwerte. We give just one example:

PROPOSITION 10.3. — *For every hyperelliptic period matrix* $Z \in \mathbb{H}_3$

$$\frac{[w_{15}, w_{45}, w_{24}](Z)\,[w_{25}, w_{35}, w_{23}](Z)}{[w_{15}, w_{35}, w_{23}](Z)\,[w_{25}, w_{45}, w_{24}](Z)} = \frac{[w_{16}, w_{46}, w_{24}](Z)\,[w_{26}, w_{36}, w_{23}](Z)}{[w_{16}, w_{36,}w_{23}](Z)\,[w_{26}, w_{46}, w_{24}](Z)}$$

We finally remark that one can also express the symmetric roots ℓ_{12k} as quotients of Thetanullwerte, using Frobenius formula (3.3). For instance:

$$\ell_{123} = \sqrt[6]{\frac{\theta[1345]^3\theta[1346]\theta[1367]\theta[1368]\theta[1456]^3\theta[1478]^5}{\theta[1356]^5\theta[1378]^3\theta[1457]\theta[1458]\theta[1578]\theta[1678]^3}},$$

where the Thetanullwerte $\theta[\Pi(W_a + W_b + W_c + W_d)]$ has been written $\theta[abcd]$. An important remark for computational purposes is that the whole set of formulas for the symmetric roots involve only twelve even Thetanullwerte.

BIBLIOGRAPHY

[1] E. Arbarello, M. Cornalba, P. A. Griffiths & J. Harris, *Geometry of algebraic curves. Vol. I*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 267, Springer-Verlag, New York, 1985.

[2] P. Bayer & J. Guàrdia, "Hyperbolic uniformization of the Fermat curves", *Ramanjujan J.* **12** (2006), p. 207-223.

[3] B. J. Birch & W. Kuyk (eds.), *Modular functions of one variable. IV*, Springer-Verlag, Berlin, 1975, Lecture Notes in Mathematics, Vol. 476.

[4] G. Cardona & J. Quer, "Field of moduli and field of definition for curves of genus 2", in *Computational aspects of algebraic curves*, Lecture Notes Ser. Comput., vol. 13, World Sci. Publ., Hackensack, NJ, 2005, p. 71-83.

[5] J. E. Cremona, *Algorithms for modular elliptic curves*, Cambridge University Press, Cambridge, 1992.

[6] F. G. Frobenius, "Über die constanten Factoren der Thetareihen", *J. reine angew. Math.* **98** (1885), p. 241-260.

[7] J. González, J. Guàrdia & V. Rotger, "Abelian surfaces of GL_2-type as Jacobians of curves", *Acta Arith.* **116** (2005), no. 3, p. 263-287.

[8] E. González-Jiménez & J. González, "Modular curves of genus 2", *Math. Comp.* **72** (2003), no. 241, p. 397-418 (electronic).

[9] E. González-Jiménez, J. González & J. Guàrdia, "Computations on modular Jacobian surfaces", in *Algorithmic number theory (Sydney, 2002)*, Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, p. 189-197.

[10] J. Guàrdia, "Jacobian nullwerte and algebraic equations", *J. Algebra* **253** (2002), no. 1, p. 112-132.

[11] ———, "Jacobi Thetanullwerte, periods of elliptic curves and minimal equations", *Math. Res. Lett.* **11** (2004), no. 1, p. 115-123.

[12] J. Guàrdia, E. Torres & M. Vela, "Stable models of elliptic curves, ring class fields, and complex multiplication", in *Algorithmic number theory*, Lecture Notes in Comput. Sci., vol. 3076, Springer, Berlin, 2004, p. 250-262.

[13] J.-i. Igusa, "On Jacobi's derivative formula and its generalizations", *Amer. J. Math.* **102** (1980), no. 2, p. 409-446.

[14] ———, "On the nullwerte of Jacobians of odd theta functions", in *Symposia Mathematica, Vol. XXIV (Sympos., INDAM, Rome, 1979)*, Academic Press, London, 1981, p. 83-95.

[15] ———, "Problems on abelian functions at the time of Poincaré and some at present", *Bull. Amer. Math. Soc. (N.S.)* **6** (1982), no. 2, p. 161-174.

[16] ———, "Multiplicity one theorem and problems related to Jacobi's formula", *Amer. J. Math.* **105** (1983), no. 1, p. 157-187.

[17] P. Lockhart, "On the discriminant of a hyperelliptic curve", *Trans. Amer. Math. Soc.* **342** (1994), no. 2, p. 729-752.

[18] MAGMA, "http://magma.math.usyd.edu.au/magma/", University of Sydney, 2004.

[19] H. McKean & V. Moll, *Elliptic curves*, Cambridge University Press, Cambridge, 1997, Function theory, geometry, arithmetic.

[20] J.-F. Mestre, "Construction de courbes de genre 2 à partir de leurs modules", in *Effective methods in algebraic geometry (Castiglioncello, 1990)*, Progr. Math., vol. 94, Birkhäuser Boston, Boston, MA, 1991, p. 313-334.

[21] D. Mumford, *Tata lectures on theta. II*, Progress in Mathematics, vol. 43, Birkhäuser Boston Inc., Boston, MA, 1984, Jacobian theta functions and differential equations, With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura.

[22] G. Rosenhain, "Mémoire sur les fonctions de deux variables et à quatre périodes qui sont les inverses des intégrales ultra-elliptiques de la première classe", *Mémoires des savants étrangers* **XI** (1851), p. 362-468.

[23] G. Shimura, *Abelian varieties with complex multiplication and modular functions*, Princeton Mathematical Series, vol. 46, Princeton University Press, Princeton, NJ, 1998.

[24] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1992, Corrected reprint of the 1986 original.

[25] K. Takase, "A generalization of Rosenhain's normal form for hyperelliptic curves with an application", *Proc. Japan Acad. Ser. A Math. Sci.* **72** (1996), no. 7, p. 162-165.

[26] J. Thomae, "Beitrag zur Bestimmung von $\theta(0,0,...,0)$ durch die Klassenmoduln algebraischer Funktionen", *J. reine angew. Math.* **71** (1870), p. 201-222.

[27] P. van Wamelen, "Examples of genus two CM curves defined over the rationals", *Math. Comp.* **68** (1999), no. 225, p. 307-320.

[28] X. D. Wang, "2-dimensional simple factors of $J_0(N)$", *Manuscripta Math.* **87** (1995), no. 2, p. 179-197.

[29] H.-J. Weber, "Hyperelliptic simple factors of $J_0(N)$ with dimension at least 3", *Experiment. Math.* **6** (1997), no. 4, p. 273-287.

[30] A. Weil, "Sur les périodes des intégrales abéliennes", *Comm. Pure Appl. Math.* **29** (1976), no. 6, p. 813-819.

[31] A. Weng, "A class of hyperelliptic CM-curves of genus three", *J. Ramanujan Math. Soc.* **16** (2001), no. 4, p. 339-372.

Manuscrit reçu le 11 mai 2006,
accepté le 15 septembre 2006.

Jordi GUÀRDIA
Escola Politècnica Superior d'Enginyeria
de Vilanova i la Geltrú
Departament de Matemàtica Aplicada IV
Avinguda Víctor Balaguer s/n
08800 Vilanova i la Geltrú (Spain)
guardia@ma4.upc.es