Resolution of degree ≤ 6 algebraic equations by genus two theta constants

Angel Zhivkov*

Faculty of Mathematics and Informatics, Sofia University

5 J. Bourchier, 1164 Sofia, Bulgaria; e-mail: zhivkov@fmi.uni-sofia.bg

Abstract

We adjoin complete first kind Abelian integrals of genus two to solve the general degree six algebraic equation $a_0 z^6 + a_1 z^5 + \cdots + a_6 = 0$ by genus two theta constants. Using the same formulas, later we resolve degree five, four and three algebraic equations. We study the monodromy group, which permutes the roots of degree six polynomials.

1 Introduction

Two thousand years B.C. the Babylonians, Indians and Chinese solved some special cases of second and third degree equations; Diophantus was the first to expound the theory of the solution of quadratic equations $ax^2 + bx + c = 0$ in his book "Arithmetica" (third century A.C.). The solution of any cubic equation is nowadays known as Cardano formula and was derived in the beginning of 16^{th} century by del Ferro. In 1545 was published Ferrari's method for resolving by radicals the fourth degree equations.

During the next three hundred years, fruitless efforts were made to find solutions by radicals of the fifth and higher degrees equations, which coefficients are letters. It was finally demonstrated by Abel [1] in 1826 that such solutions do not exist. A complete answer to the question when an algebraic equation is solvable by radicals was given by Galois [6] about the year 1830.

These discoveries of Abel and Galois had been followed by the also remarkable theorems of Hermite and Kronecker: in 1858 they independently proved that we can solve the algebraic equations of degree five by using an elliptic modular function [8], [12]. The result of Hermite and Kronecker was in fact analogous to the formula

*Supported by DFG project number 436 BUL 113/86/0 and MM1003/2000 with Ministry of Education of Bulgaria.

[0]1991 Mathematics Subject Classification: 01A60, 12D10, 14D05, 14E20, 14J30, 14K25, 20H05

Key words: roots of polynomials, theta constants

$\sqrt[n]{a} = \exp\left(\frac{1}{n}\int\limits_1^a \frac{dx}{x}\right)$ but the exponent replaced by an elliptic modular function and the integral $\int \frac{dx}{x}$ by an elliptic integral. Kronecker thought that the resolution of the equation of degree five would be a special case of a more general theorem which might exist. This hypothesis was realized in few cases by F. Klein [11]; Jordan [10] showed that any algebraic equation is solvable by modular functions.

In 1984 Umemura realized the Kronecker idea in his appendix to Mumford's book [13], deducing from a formula of Thomae [16] a root of arbitrary algebraic equation by Siegel modular forms. This solution was expressed by genus $\left[\frac{n+2}{2}\right]$ theta constants related the hyperelliptic curve

$$R_n \ : \ \begin{cases} w^2 = z(z-1)P_n(z) & \text{if n is odd} \\ w^2 = z(z-1)(z-2)P_n(z) & \text{if n is even} \end{cases}$$

with, $P_n(z)$ is the n^{th} degree polynomial, whose roots have to be found. Especially if $n = 6$, R_n is a genus 4 hyperelliptic curve and its matrix of the periods depends on 10 parameters which, however, are not free: there exists a Schottky relation between them and two Schottky–type relations extracting hyperelliptic between general genus four curves.

The aims of this paper are to resolve the equation $P_6(z) = 0$ by genus two theta constants and to give both elementary and transparent proof; in particular, Thomae's formula will be avoided. We use a simple idea: if Δ denotes the Riemann theta divizor for genus two algebraic curve $R : \, w^2 = P_6(z)$ and $\mathcal{A}$ denotes Abel's map, then the Riemann theta function $f(Q) := \theta\big(\mathcal{A}(Q - \Delta)\big)$ vanishes identically for $Q \in R$; differentiating $f(Q)$ and setting $Q = (z = z_j, w = 0)$ gives explicitly the root z_j of the polynomial $P_6(z)$.

Moreover, we resolve each degree five, four or three algebraic equation, specifying correspondingly $z_6 = \infty$; $z_6 = \infty$, $z_5 = 0$; $z_6 = \infty$, $z_5 = 0$, $z_4 = 1$ to be roots of the polynomial $P_6(z)$.

In section 4 we study the monodromy group of degree six polynomials. This group turns out [14] to be the symplectic group $\mathrm{Sp}_4(\mathbb{F}_2)$. Finally we discuss the theorem of Torelli in the case of genus two Riemann surfaces.

2 Explicit roots of degree six polynomials

In this section, we will find explicit expressions for the roots of an arbitrary degree six polynomial in terms of genus two theta constants; it seems that the formulas for the roots (Theorem 2.1) could not be simplified.

Let us fix a degree six polynomial

$$P_6(z) = a_0 z^6 + a_1 z^5 + \cdots + a_6 \ , \qquad a_j \in \mathbb{C}, \quad a_0 \neq 0 \,.$$

The complex Sturm theorem [17] says that there exists an algorithm of separation the roots of the polynomial $P_6(z)$ and further we shall consider that each root z_j is located inside some circle $U_j \in \mathbb{C}$.

Choose an arbitrary order $z_1, z_2, \ldots, z_6$ of the already localized roots and fix some paths γ_{12}, γ_{34} and γ_{56} to join correspondingly U_1 with U_2, U_3 with U_4 and U_5 with U_6, see the figure (1b) below. This defines a single–valued branch of the function

$$w \;=\; \pm\sqrt{P_6(z)} \qquad \text{for all} \quad z \;\in\; \mathbb{C} - \bigcup_{j=1}^{6} U_j - \gamma_{12} - \gamma_{34} - \gamma_{56} \;;$$

when z crosses some γ_{ij}, the sign of w has to be changed. More generally, w is a well-defined meromorphic function on the genus two Riemann surface

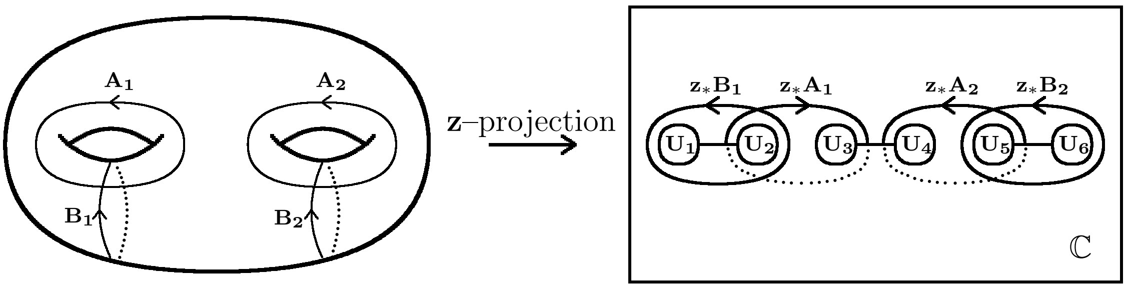
$$R \,:\; w^2 = P_6(z)\,.$$

Equip R with a canonical basis of cycles $A_1, A_2, B_1, B_2 \subset R$, such that:

(i) the intersection indexes are

$$A_k \circ A_l = B_k \circ B_l = 0\,, \qquad A_k \circ B_l = \delta_{kl} = \text{(Kronecker's symbol)},$$

(ii) the projection on the z-plane z_*B_1 surrounds U_1 and U_2, while z_*A_1 surrounds U_2 and U_3, z_*A_2 surrounds U_4 and U_5, z_*B_2 surrounds U_5 and U_6. Alternatively, chosen first the projections z_*A_k and z_*B_k, then the cycles $A_k \subset z^{-1}(z_*A_k)$ and $B_k \subset z^{-1}(z_*B_k)$.



1a: Riemann surface R.

1b: Cycles on the z–plane.

Now we can define the following first-kind-complete-abelian integrals:

$$\sigma_{11} := \oint\limits_{A_1} \frac{dz}{w}, \qquad \sigma_{12} := \oint\limits_{A_2} \frac{dz}{w}, \qquad \rho_{11} := \oint\limits_{B_1} \frac{dz}{w}, \qquad \rho_{12} := \oint\limits_{B_2} \frac{dz}{w},$$

$$\sigma_{21} := \oint\limits_{A_1} \frac{z\,dz}{w}, \qquad \sigma_{22} := \oint\limits_{A_2} \frac{z\,dz}{w}, \qquad \rho_{21} := \oint\limits_{B_1} \frac{z\,dz}{w}, \qquad \rho_{22} := \oint\limits_{B_2} \frac{z\,dz}{w}.$$

It turns out that the numbers $\sigma_{11}, \sigma_{12}, \sigma_{21}, \sigma_{22}, \rho_{11}, \rho_{12}, \rho_{21}$ and ρ_{22} contain all information we need; even arbitrary seven of them do.

Denote by $\sigma^{11}, \sigma^{12}, \sigma^{21}, \sigma^{22}$ the normalizing constants, i.e.

$$\begin{pmatrix} \sigma^{11} & \sigma^{12} \\ \sigma^{21} & \sigma^{22} \end{pmatrix} \begin{pmatrix} \sigma_{11} & \sigma_{12} & \rho_{11} & \rho_{12} \\ \sigma_{21} & \sigma_{22} & \rho_{21} & \rho_{22} \end{pmatrix} = \begin{pmatrix} 1 & 0 & \Omega_{11} & \Omega_{12} \\ 0 & 1 & \Omega_{21} & \Omega_{22} \end{pmatrix}$$

and, therefore,

$$\oint\limits_{A_k} \frac{\sigma^{s1} + \sigma^{s2} z}{w} dz = \delta_{ks}\,, \qquad \oint\limits_{B_k} \frac{\sigma^{s1} + \sigma^{s2} z}{w} dz = \Omega_{sk}\,, \qquad k, s = 1, 2.$$

It is a standard fact [7] that the matrix of the periods

$$\Omega \;:=\; \begin{pmatrix} \Omega_{11} & \Omega_{12} \\ \Omega_{21} & \Omega_{22} \end{pmatrix}$$

is a (2×2) symmetric matrix and $\operatorname{Im}\Omega > 0$; the last property enables to define correctly the Riemann theta function with characteristics $\alpha = (\alpha_1, \alpha_2) \in \mathbb{Q}^2$ and $\beta = (\beta_1, \beta_2) \in \mathbb{Q}^2$ by its Fourier expansion

$$\theta\left[\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right](u\,,\Omega) := \sum_{n \in \mathbb{Z}^2} \exp\, 2\pi i \big(\tfrac{1}{2}(n+\alpha)\Omega + u + \beta\big)\big(n+\alpha\big)^t, \quad u = (u_1, u_2) \in \mathbb{C}^2.$$

This classical function obeys the laws

$$\theta\left[\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right](u + M + N\Omega\,,\,\Omega) = \theta\left[\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right](u, \Omega)\, \exp 2\pi i\big(-\tfrac{1}{2} N\Omega N^t - uN^t + \alpha M^t - \beta N^t\big),$$

$$\theta\left[\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right](u\,,\Omega) = \theta\big(u + \left[\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right],\Omega\big)\, \exp 2\pi i \big(\tfrac{1}{2}\alpha\Omega + u + \beta\big)\alpha^t$$

for all $M, N \in \mathbb{Z}^2$, $u \in \mathbb{C}^2$, $\theta(u, \Omega) := \theta\begin{bmatrix}0\,0\\ 0\,0\end{bmatrix}(u, \Omega)$; since every $u \in \mathbb{C}^2$ can be written uniquely by its characteristics $\alpha, \beta \in \mathbb{R}^2$ as

$$u \;=\; \alpha + \beta\Omega \;:=\; \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \;=\; \begin{bmatrix} \alpha_1 & \alpha_2 \\ \beta_1 & \beta_2 \end{bmatrix},$$

we use the notation $\left[\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right]$ for the points of $\mathbb{C}^2$ if not misleading.

When α and β are half–integers, an alternative arises: if $4\alpha\beta^t \equiv 0 \bmod 2$, then $\left[\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right] \in \mathbb{C}^2$ is called even half-period and $\theta\left[\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right](u, \Omega)$ is an even function with regard to u, whereas if $4\alpha\beta^t \equiv 1 \bmod 2$, $\left[\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right]$ is called odd half-period and $\theta\left[\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right](u, \Omega)$ is an odd function.

Recall also that the two dimensional complex torus

$$J(R) := \mathbb{C}^2 \Big/ \big\{ M + N\Omega \mid M, N \in \mathbb{Z}^2 \big\}$$

is named Jacobian of R and the Abel's map is defined by

$$\begin{aligned} \mathcal{A} :\;\; R \;&\rightarrow\; J(R) \\ Q \;&\mapsto\; \mathcal{A}(Q) := \left(\int\limits_{Q_{ini}}^{Q} \frac{\sigma^{11} + \sigma^{12} z}{w} dz \;,\; \int\limits_{Q_{ini}}^{Q} \frac{\sigma^{21} + \sigma^{22} z}{w} dz \right), \end{aligned}$$

the point $Q_{ini} \in R$ is arbitrary but fixed. An easy computation shows that

$$\int\limits_{z_1}^{z_2} \frac{\sigma^{s1} + \sigma^{s2} z}{w} dz \;=\; \frac{1}{2} \int\limits_{z_* B_1} \frac{\sigma^{s1} + \sigma^{s2} z}{w} dz \;=\; \frac{1}{2}\,\Omega_{s1}\,, \qquad s = 1, 2$$

and hence if $Q_m := \big(z = z_m, w = 0\big)$ denotes the m^{th} Weierstrass point on R,

$$\mathcal{A}(Q_2) - \mathcal{A}(Q_1) = \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & 0 \end{bmatrix} \quad \text{on } J(R).$$

Analogously, the following identities are true on $J(R)$:

$$\mathcal{A}(Q_3) - \mathcal{A}(Q_2) = \begin{bmatrix} 0 & 0 \\ \frac{1}{2} & 0 \end{bmatrix}\,, \qquad \mathcal{A}(Q_4) - \mathcal{A}(Q_3) = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ 0 & 0 \end{bmatrix}\,,$$
$$\mathcal{A}(Q_5) - \mathcal{A}(Q_4) = \begin{bmatrix} 0 & 0 \\ 0 & \frac{1}{2} \end{bmatrix}\,, \qquad \mathcal{A}(Q_6) - \mathcal{A}(Q_5) = \begin{bmatrix} 0 & \frac{1}{2} \\ 0 & 0 \end{bmatrix},$$

which suggests to connect the Weierstrass points Q_j and the six odd half-periods:

$$Q_1 \leftrightarrow \big[\eta_1\big] := \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ 0 & \frac{1}{2} \end{bmatrix}\,, \qquad Q_2 \leftrightarrow \big[\eta_2\big] := \begin{bmatrix} 0 & \frac{1}{2} \\ 0 & \frac{1}{2} \end{bmatrix}\,, \qquad Q_3 \leftrightarrow \big[\eta_3\big] := \begin{bmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}\,,$$
$$Q_4 \leftrightarrow \big[\eta_4\big] := \begin{bmatrix} \frac{1}{2} & 0 \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}\,, \qquad Q_5 \leftrightarrow \big[\eta_5\big] := \begin{bmatrix} \frac{1}{2} & 0 \\ \frac{1}{2} & 0 \end{bmatrix}\,, \qquad Q_6 \leftrightarrow \big[\eta_6\big] := \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & 0 \end{bmatrix}\,,$$

whence for all $m, s = 1, 2, \ldots, 6$,

$$\mathcal{A}(Q_m - Q_s) \;:=\; \mathcal{A}(Q_m) - \mathcal{A}(Q_s) \;\overset{\text{mod}\,1}{\equiv}\; \big[\eta_m\big] - \big[\eta_s\big]\,.$$

To have got more compact expressions for the roots of $P_6(z)$, write

$$\theta_s\big[\eta_m\big] \;:=\; \frac{\partial}{\partial u_s}\theta\big[\eta_m\big]\big((u_1, u_2), \Omega\big)\Big|_{u_1 = u_2 = 0}$$

for the first partial derivatives of thetas, taken at $u = 0$.

Theorem 2.1 *The roots of the polynomial $P_6(z)$ are written by*

$$z_m \;=\; \frac{\sigma_{22}\theta_1[\eta_m] - \sigma_{21}\theta_2[\eta_m]}{\sigma_{12}\theta_1[\eta_m] - \sigma_{11}\theta_2[\eta_m]}\,, \qquad m = 1, 2, \ldots, 6\,.$$

Proof. According to Riemann's theorem on the theta divisor [7], either the section

$$f(Q) \;:=\; \theta[\eta_1]\big(\mathcal{A}(Q - Q_1)\,,\,\Omega\big)\;, \qquad Q \in R$$

vanishes identically, or $f(Q)$ has exactly two zeroes on R.[1] But for any $m \leq 6$,

$$\begin{aligned} f(Q_m) \;&=\; \theta[\eta_1]\big(\mathcal{A}(Q_m - Q_1)\,,\,\Omega\big) \\ &=\; constant_1\,.\,\theta\big([\eta_m]\,,\,\Omega\big) \\ &=\; constant_2\,.\,\theta[\eta_m](0\,,\,\Omega) \\ &=\; 0 \end{aligned}$$

[1]Integrating the logarithmic derivative $d\ln f(Q)$ taken within the Riemann surface R dissected along the cycles A_1, A_2, B_1 and B_2 verifies this assertion.

since $\theta[\eta_m](u,\Omega)$ is an odd function with regard to u subject $[\eta_m]$ be an odd half-period. These six zeroes can only happen if $f(Q)$ vanishes identically.

A chain of implications finishes the proof of the theorem: for every $m = 1,\ldots,6$,

$$
\begin{aligned}
& f(Q) = \theta[\eta_1]\big(\mathcal{A}(Q-Q_1),\Omega\big) \;\equiv\; 0 \\
\Longrightarrow\quad & \frac{d}{dw(Q)} f(Q)\Big|_{Q=Q_m} \;=\; 0 \\
\Longleftrightarrow\quad & \sum_{s=1}^{2} \theta_s[\eta_1]\big(\mathcal{A}(Q_m-Q_1),\Omega\big)\cdot \frac{d}{dw(Q)} \int\limits_{z(Q_1)}^{z(Q)} \frac{\sigma^{s1}+\sigma^{s2}z(Q)}{w(Q)} dz(Q)\Big|_{Q=Q_m} \;=\; 0 \\
\Longleftrightarrow\quad & \sum_{s=1}^{2} \theta_s[\eta_1+\eta_m-\eta_1]\cdot \frac{d}{dw(Q)} \int\limits_{w(Q_1)}^{w(Q)} \frac{\sigma^{s1}+\sigma^{s2}z(Q)}{w(Q)} \cdot \frac{2w(Q)\,dw(Q)}{P_6'\big(z(Q)\big)}\Big|_{Q=Q_m} \;=\; 0 \\
\Longleftrightarrow\quad & \sum_{s=1}^{2} \theta_s[\eta_m]\cdot \frac{\sigma^{s1}+\sigma^{s2}z(Q_m)}{P_6'\big(z(Q_m)\big)}\cdot 2 \;=\; \frac{2}{P_6'(z_m)} \sum_{s=1}^{2} \theta_s[\eta_m]\cdot(\sigma^{s1}+\sigma^{s2}z_m) \;=\; 0 \\
\Longleftrightarrow\quad & z_m \;=\; -\frac{\sigma^{11}\theta_1[\eta_m]+\sigma^{21}\theta_2[\eta_m]}{\sigma^{12}\theta_1[\eta_m]+\sigma^{22}\theta_2[\eta_m]} \\
\Longleftrightarrow\quad & z_m \;=\; \frac{\sigma_{22}\theta_1[\eta_m]-\sigma_{21}\theta_2[\eta_m]}{\sigma_{12}\theta_1[\eta_m]-\sigma_{11}\theta_2[\eta_m]}\,.
\end{aligned}
$$

We have used $w^2 = P_6(z)$ to deduce $2w\,dw = P_6'(z)\,dz$. $\square$

3 The algorithm of extracting the roots

In this short section we briefly recall the procedure for computing the roots of any fixed degree six polynomial $P_6(z)$ with complex coefficients and different roots.

Step 1. Apply the complex Sturm theorem to localize the roots $z_1, z_2, \ldots, z_6$ of $P_6(z)$.

Step 2. Fix the z–images z_*A_1, z_*A_2, z_*B_1 and z_*B_2 of the cycles A_1, A_2, B_1 and B_2 as in the above figure (1b).

Step 3. Compute the integrals

$$
\sigma_{11} = \oint\limits_{z_*A_1} \frac{dz}{w}, \qquad \sigma_{12} = \oint\limits_{z_*A_2} \frac{dz}{w}, \qquad \rho_{11} = \oint\limits_{z_*B_1} \frac{dz}{w}, \qquad \rho_{12} = \oint\limits_{z_*B_2} \frac{dz}{w},
$$
$$
\sigma_{21} = \oint\limits_{z_*A_1} \frac{z\,dz}{w}, \qquad \sigma_{22} = \oint\limits_{z_*A_2} \frac{z\,dz}{w}, \qquad \rho_{21} = \oint\limits_{z_*B_1} \frac{z\,dz}{w}, \qquad \rho_{22} = \oint\limits_{z_*B_2} \frac{z\,dz}{w}.
$$

Step 4. Compute the matrix of the periods

$$
\Omega \;:=\; \begin{pmatrix} \sigma_{11} & \sigma_{12} \\ \sigma_{21} & \sigma_{22} \end{pmatrix}^{-1} \begin{pmatrix} \rho_{11} & \rho_{12} \\ \rho_{21} & \rho_{22} \end{pmatrix} \;.
$$

Step 5. Write down the roots

$$z_m \;=\; \frac{\sigma_{22}\,\theta_1[\eta_m]-\sigma_{21}\,\theta_2[\eta_m]}{\sigma_{12}\,\theta_1[\eta_m]-\sigma_{11}\,\theta_2[\eta_m]}\;, \qquad m=1,2,\ldots,6,$$

where $\big[\eta_1\big]\,,\big[\eta_2\big]\,,\ldots,\big[\eta_6\big] \;=\; \begin{bmatrix}\frac12 & \frac12\\ 0 & \frac12\end{bmatrix},\ \begin{bmatrix}0 & \frac12\\ 0 & \frac12\end{bmatrix},\ \begin{bmatrix}0 & \frac12\\ \frac12 & \frac12\end{bmatrix},\ \begin{bmatrix}\frac12 & 0\\ \frac12 & \frac12\end{bmatrix},\ \begin{bmatrix}\frac12 & 0\\ \frac12 & 0\end{bmatrix},\ \begin{bmatrix}\frac12 & \frac12\\ \frac12 & 0\end{bmatrix},$

$$\theta_s\begin{bmatrix}\alpha_1 & \alpha_2\\ \beta_1 & \beta_2\end{bmatrix} \;=\; -2\pi\sum_{n_1,\,n_2\,\in\mathbb{Z}}(-1)^{2\beta_1 n_1+2\beta_2 n_2}(n_s+\alpha_s)\,q_{11}^{(n_1+\alpha_1)^2}\,q_{12}^{2(n_1+\alpha_1)(n_2+\alpha_2)}\,q_{22}^{(n_2+\alpha_2)^2}$$

and $q_{rs} := \exp\big(\pi i \Omega_{rs}\big)$ for $r,s=1,2$.

4 The monodromy group

The algorithm of computing the roots of a polynomial $P_6(z)$ requires to fix their order $z_1,z_2,\ldots,z_6$; whereas the (extended) monodromy group permutes the six roots. Intending to study this monodromy, we shall introduce certain groups, normal subgroups, factor-groups, exact sequences and homomorphisms:

$$\begin{array}{ccccccccccc}
1 & \to & \widehat{\mathcal{B}}_6 & \to & \mathcal{B}_6 & \to & \mathcal{S}_6 & \to & 1 & & b_i\\
 & & \updownarrow & & \updownarrow & & \updownarrow & & & & \updownarrow\\
1 & \to & \Gamma_2(\pi_1) & \to & \pi_1(\mathbb{C}^6\!-\!\mathcal{D}) & \to & \pi_1(\mathbb{C}^6\!-\!\mathcal{D})\big/\Gamma_2(\pi_1) & \to & 1 & & \nu_i\\
 & & \downarrow & & \downarrow & & \updownarrow & & & & \updownarrow\\
1 & \to & \Gamma_2(4) & \to & \mathrm{Sp}_4(\mathbb{Z}) & \to & \mathrm{Sp}_4(\mathbb{F}_2) & \to & 1\,, & & \mu_i\,.\\
 & & \downarrow & & \downarrow & & & & & & \\
 & & 1 & & 1 & & & & & &
\end{array}$$

By $\mathcal{B}_6$ we have denoted the braids group with six strings, five generators $b_1,\ldots,b_5$ and 10 relations [2], [5]:

$$(1)\qquad \begin{array}{ll} b_s b_{s+1} b_s = b_{s+1} b_s b_{s+1} & \text{for}\ \ s=1,2,3,4,\\ b_i b_s = b_s b_i & \text{for}\ \ i-s>1,\ \ i,s=1,\ldots,5\,. \end{array}$$

Each braid can be considered as a continuous map

$$f:[0,1]\;\to\;\mathbb{C}^6\!-\!\mathcal{D}\;:=\big\{(z_1,\ldots,z_6)\in\mathbb{C}^6:\ z_i\neq z_s\ \text{for}\ i\neq s\big\},\quad f(0)=f(1)$$

modulo homotopy of f, which implies the braids group $\mathcal{B}_6$ coincides with the fundamental group $\pi_1(\mathbb{C}^6-\mathcal{D})$ and the points $(z_1,\ldots,z_6)$ of the configuration space $\mathbb{C}^6-\mathcal{D}$ are the roots of $P_6(z) \;=\; a_0\prod_{i=1}^{6}(z-z_i)$. Denote by $\nu_1,\ldots,\nu_5$ the correspondent generators of $\pi_1(\mathbb{C}^6\!-\!\mathcal{D})$.

Let $\widehat{\mathcal{B}}_6$ be the group of colored braids with six strings. This group is the normalizer of the subgroup of $\mathcal{B}_6$ generated by the squares $b_1^2, \dots, b_5^2$, that is $\widehat{\mathcal{B}}_6$ is the smallest normal subgroup of $\mathcal{B}_6$, which necessarily contains $b_1^2, \dots, b_5^2$. Then the factor-group $\mathcal{B}_6 \big/ \widehat{\mathcal{B}}_6$ has generators $b_1, \dots, b_5$ related by

$$
\begin{aligned}
&b_s b_{s+1} b_s = b_{s+1} b_s b_{s+1} &&\text{for } \ s = 1, 2, 3, 4,\\
(2) \qquad &b_i b_s = b_s b_i &&\text{for } \ i - s > 1, \ \ i, s = 1, \dots, 5\,,\\
&b_i^2 = 1 &&\text{for } \ i = 1, \dots, 5\,.
\end{aligned}
$$

As $b_1, \dots, b_5$ are conjugate each other, $\widehat{\mathcal{B}}_6$ could be generate by $b_1^2 = 1$ complements relations (1), see [5].

Notice that the same relations (2) but b_s replaced by the elementary transposition $\begin{pmatrix} 1 \dots & s & s{+}1 & \dots\ 6 \\ 1 \dots & s{+}1 & s & \dots\ 6 \end{pmatrix}$ define the symmetric group $\mathcal{S}_6$ [5]. This gives rise of the isomorphism

$$\mathcal{B}_6 \big/ \widehat{\mathcal{B}}_6 \ \cong \ \mathcal{S}_6$$

as well as the exact sequence $1 \to \widehat{\mathcal{B}}_6 \to \mathcal{B}_6 \to \mathcal{S}_6 \to 1\,.$

Recall now that the symplectic group $\mathrm{Sp}_4(\mathbb{Z})$ consists of all $(4{\times}4)$ integer matrises $\mu := \begin{pmatrix} a\, b \\ c\, d \end{pmatrix}$, ($a$, b, c and d are $2{\times}2$ matrices), which change every canonical basis of cycles A_1, A_2, B_1, B_2 by the canonical basis

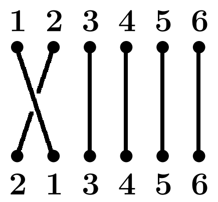
$$(\widehat{A}_1, \widehat{A}_2, \widehat{B}_1, \widehat{B}_2)^t = \mu\,.\,(A_1, A_2, B_1, B_2)^t\,,$$

preserving the intersection indexes. Algebraically,

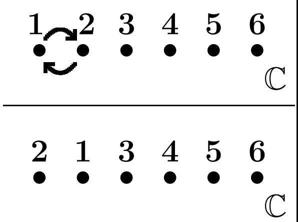
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^t \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}$$

or, equivalently, $a^t d - c^t b = I\,,\ a^t c = c^t a\,,\ b^t d = d^t b\,.$

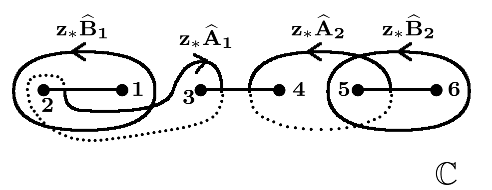
Next figures demonstrate the correspondence between the braid b_1, the monodromy ν_1 and the symplectic change μ_1:



2a: Braid b_1.



2b: Monodromy ν_1.



2c: μ_1^*–cycles on the z–plane.

As a result we calculate $\mu_1 \in \mathrm{Sp}_4(\mathbb{Z})$ and, in the same way, $\mu_2, \ldots, \mu_5$:

$$\mu_1 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \mu_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \mu_3 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

$$\mu_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix}, \quad \mu_5 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

One checks immediately that the relations (1) are fulfilled for μ_i's instead of b_i's to conclude the correspondence $b_s \leftrightarrow \mu_s$, $s = 1, \ldots, 5$, defines a homomorphism of groups $\mathcal{B}_6 \to \mathrm{Sp}_4(\mathbb{Z})$. Moreover, this is a surjective homomorphism, as μ_1, μ_3,

$$\mu_0 := \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}, \quad \mu_6 := \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 1 \end{pmatrix}, \quad \mu_7 := \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

generate $\mathrm{Sp}_4(\mathbb{Z})$, see [3], and $\mu_0 = \mu_1\mu_2\mu_1\mu_4\mu_5\mu_4$, $\mu_6 = \mu_1^{-1}\mu_3^{-1}\mu_5\mu_4\mu_3\mu_5^{-1}\mu_4^{-1}$, $\mu_7 = \mu_0^{-1}\big(\mu_1\mu_2\mu_3\mu_4\mu_5\big)^{-3}$.

On the other hand, the second congruence subgroup of $\mathrm{Sp}_4(\mathbb{Z})$

$$\Gamma_2(4) \ := \ \big\{\mu \in \mathrm{Sp}_4(\mathbb{Z}) : \ \mu \equiv I_{4\times 4} \bmod 2\big\}$$

can be defined as follows: first $\mu_1^2, \ldots, \mu_5^2$ generate some subgroup $\Gamma \in \Gamma_2(4)$, then one normalizes Γ to obtain $\Gamma_2(4)$ spanned by $\mu_1^2, \ldots, \mu_5^2$, $\mu_6^2 = \mu_1^{-2}\mu_5\mu_4\mu_3^2\mu_5^{-2}\mu_4^{-1}\mu_5^{-1}$ and $\mu_7\mu_6^2\mu_7^{-1}$ [13]. The factor-group $\mathrm{Sp}_4(\mathbb{Z})\big/\Gamma_2(4)$ will be identified as $\mathrm{Sp}_4(\mathbb{F}_2)$, where $\mathbb{F}_2$ denotes the field with two elements: 0 and 1 modulo 2.

Proposition 4.1 [14] *The factor-group* $\mathrm{Sp}_4(\mathbb{F}_2)$ *turns out to be isomorphic with the symmetric group* $\mathcal{S}_6$ *(via the correspondence* $b_i \leftrightarrow \mu_i$, $i = 1, \ldots, 5$*).*

Sketch of the proof. As we have a surjective homomorphism $\mathcal{B}_6 \to \mathrm{Sp}_4(\mathbb{Z})$ and the congruence subgroups $\widehat{\mathcal{B}}_6$ and $\Gamma_2(4)$ are generated in an identical manner, the homomorphism $\mathcal{S}_6 \to \mathrm{Sp}_4(\mathbb{F}_2)$ is surjective, too. To establish the isomorphism, we must prove that the group $\mathrm{Sp}_4(\mathbb{F}_2)$ has order 720, like $\mathcal{S}_6$ does.

As usual, consider the chain of subgroups

$$\mathrm{Sp}_4(\mathbb{F}_2) \ \supset \ G_1 \ \supset \ G_2 \ \supset \ G_3 \ ,$$

$$G_1 := \begin{pmatrix} 1 & 0 & 0 & 0 \\ * & * & * & * \\ * & * & * & * \\ * & * & * & * \end{pmatrix}, \quad G_2 := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & * & * & * \\ 0 & * & * & * \\ 0 & * & * & * \end{pmatrix}, \quad G_3 := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & * & 0 & 1 \end{pmatrix},$$

the stars $*$ stand for 0 or 1. Given an arbitrary symplectic matrix μ, there always exist suitable left and right multiplications by certain symplectic matrix to include the products successively in G_1, G_2 and G_3.

The index of the subgroup G_1 in $\mathrm{Sp}_4(\mathbb{F}_2)$ equals 15, since the first row of μ is not equal to $(0,0,0,0)$. The index $[G_1 : G_2] = 8$. The index $[G_2 : G_3] = 3$ as the second row could be $(0,1,0,0)$, $(0,1,0,1)$ or $(0,0,0,1)$. The subgroup G_3 has order two. All these facts give the order of $\mathrm{Sp}_4(\mathbb{F}_2)$ to be 15.8.3.2=720. $\square$

Having the isomorphisms $\mathcal{S}_6 \cong \mathrm{Sp}_4(\mathbb{F}_2)$, we may formulate:

Theorem 4.2 *The monodromy group of the family of genus two algebraic curves $w^2 = P_6(z)$ is the second congruence subgroup $\Gamma_2(4) \subset \mathrm{Sp}_4(\mathbb{Z})$, while the extended monodromy group for this family coincides with the Siegel modular group $\mathrm{Sp}_4(\mathbb{Z})$. More precisely, $\Gamma_2(4)$ leaves the root tuples $(z_1, \ldots, z_6)$ of $P_6(z)$ invariant, whereas the factor-group*

$$\mathrm{Sp}_4(\mathbb{F}_2) \;=\; \mathrm{Sp}_4(\mathbb{Z})/\Gamma_2(4) \;\cong\; \mathcal{S}_6$$

permutes effectively and transitively these roots.

There also exists an exact commutative diagram

$$\begin{array}{ccccccccc}
1 & \to & \widehat{\mathcal{B}}_6 & \to & \mathcal{B}_6 & \to & \mathcal{S}_6 & \to & 1 \\
 & & \downarrow & & \downarrow & & \updownarrow & & \\
1 & \to & \Gamma_2(4) & \to & \mathrm{Sp}_4(\mathbb{Z}) & \to & \mathrm{Sp}_4(\mathbb{F}_2) & \to & 1 \\
 & & \downarrow & & \downarrow & & & & \\
 & & 1 & & 1 & & & &
\end{array}$$

which relates the monodromy to the braids groups $\mathcal{B}_6$ and $\widehat{\mathcal{B}}_6$.

To complete the point, let us fix a symplectic matrix $\mu := \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{Sp}_4(\mathbb{Z})$, where a, b, c and d are (2×2) integer matrices. Give a hat $\widehat{}$ for every new object arising after the μ-change $(\widehat{A}_1, \widehat{A}_2, \widehat{B}_1, \widehat{B}_2)^t := \mu.(A_1, A_2, B_1, B_2)^t$ of the basis of cycles on R. Then [9]

$$\widehat{\sigma} = \sigma a^t + \rho b^t\,, \qquad \widehat{\rho} = \sigma c^t + \rho d^t\,, \qquad \widehat{\Omega} = (c + d\Omega)(a + b\Omega)^{-1},$$

$$\widehat{\mathcal{A}}(Q) = \mathcal{A}(Q)(a + b\Omega)^{-1}, \;\; \widehat{u} = (\widehat{u}_1, \widehat{u}_2) := (u_1, u_2)(a + b\Omega)^{-1} = u.(a + b\Omega)^{-1},$$

$$[\,\widehat{\eta}\,] \;=\; \begin{bmatrix} \widehat{\alpha} \\ \widehat{\beta} \end{bmatrix} := \begin{bmatrix} \alpha a^t - \beta b^t \\ -\alpha c^t + \beta d^t \end{bmatrix} + \frac{1}{2}\begin{bmatrix} (ab^t)_{11} & (ab^t)_{22} \\ (cd^t)_{11} & (cd^t)_{22} \end{bmatrix},$$

$$\widehat{\theta}[\,\widehat{\eta}\,](\widehat{u}, \widehat{\Omega}) \;=\; \kappa.\sqrt{\det(a + b\Omega)}\,.\exp \pi i\, \widehat{u}\, b\, u^t.\,\theta[\,\eta\,](u, \Omega),$$

$$\Big(\widehat{\theta}_1[\,\widehat{\eta}\,]\,, \widehat{\theta}_2[\,\widehat{\eta}\,]\Big) \;=\; \kappa.\sqrt{\det(a + b\Omega)}\,.\Big(\theta_1[\,\eta\,]\,, \theta_2[\,\eta\,]\Big).(a^t + \Omega b^t)\,,$$

where κ is certain eight root of unity, independent on u and Ω. The last equality between theta-function-gradients yields for every $m = 1, 2, \ldots, 6$ the equality

$$\Big(\widehat{\theta}_1\big[\widehat{\eta}_m\big]\,,\,\widehat{\theta}_2\big[\widehat{\eta}_m\big]\Big).\,\widehat{\sigma}^{-1} \;=\; \kappa.\sqrt{\det(a+b\Omega)}\,.\Big(\theta_1\big[\eta_{\widehat{m}}\big]\,,\,\theta_2\big[\eta_{\widehat{m}}\big]\Big).\,\sigma^{-1}$$

and, henceforth, the invariant equality

$$\widehat{z}_m = -\frac{\widehat{\sigma}^{11}\,\widehat{\theta}_1\big[\widehat{\eta}_m\big] + \widehat{\sigma}^{21}\,\widehat{\theta}_2\big[\widehat{\eta}_m\big]}{\widehat{\sigma}^{12}\,\widehat{\theta}_1\big[\widehat{\eta}_m\big] + \widehat{\sigma}^{22}\,\widehat{\theta}_2\big[\widehat{\eta}_m\big]} = -\frac{\sigma^{11}\,\theta_1\big[\eta_{\widehat{m}}\big] + \sigma^{21}\,\theta_2\big[\eta_{\widehat{m}}\big]}{\sigma^{12}\,\theta_1\big[\eta_{\widehat{m}}\big] + \sigma^{22}\,\theta_2\big[\eta_{\widehat{m}}\big]} = z_{\widehat{m}}$$

where $\widehat{m} := (b_{i_1}b_{i_2}\ldots b_{i_n})(m)$ iff $\mu = \mu_{i_1}\mu_{i_2}\ldots\mu_{i_n}$.

5 A resolution of degree less than six algebraic equations

1. All derived formulas for the roots of $P_6(z)$ remain true for each degree five polynomial $P_5(z) = a_1z^5 + a_2z^4 + \cdots + a_6$ with simple roots and $a_1 \neq 0$; just assume $a_0 = 0$ and the root $z_6 = \infty$, i.e. the denominator $\sigma_{12}\theta_1[\,\eta_6\,] - \sigma_{11}\theta_2[\,\eta_6\,]$ vanishes, which defines both integrals $\sigma_{11}\,, \sigma_{12}$ up to a multiplicative constant ξ.

According to the classical Rosenhain formulas [15], for $m, s = 1, \ldots, 6$, $m < s$,

$$\theta_1[\,\eta_m\,]\,\theta_2[\,\eta_s\,] - \theta_2[\,\eta_m\,]\,\theta_1[\,\eta_s\,] \;=\; \pi^2\,\theta[\,e_1^{m,s}\,]\,\theta[\,e_2^{m,s}\,]\,\theta[\,e_3^{m,s}\,]\,\theta[\,e_4^{m,s}\,]\,,$$

where $[\,e_1^{m,s}\,], \ldots, [\,e_4^{m,s}\,]$ are the even half-periods for which $[\,e_i^{m,s}\,] + [\,\eta_m\,] + [\,\eta_s\,]$ is an odd half-period, $\theta[e] := \theta[e](0,\Omega)$. Using $z_1 + \cdots + z_5 = -\frac{a_2}{a_1}$ to evaluate the constant ξ, we compute explicitly the roots of $P_5(z)$:

$$z_1 = \frac{\sigma_{22}\,\theta_1\begin{bmatrix}\frac12 & \frac12\\ 0 & \frac12\end{bmatrix} - \sigma_{21}\,\theta_2\begin{bmatrix}\frac12 & \frac12\\ 0 & \frac12\end{bmatrix}}{\xi\,\theta\begin{bmatrix}\frac12 & 0\\ 0 & \frac12\end{bmatrix}\theta\begin{bmatrix}\frac12 & 0\\ 0 & 0\end{bmatrix}\theta\begin{bmatrix}0 & \frac12\\ \frac12 & 0\end{bmatrix}\theta\begin{bmatrix}0 & \frac12\\ 0 & 0\end{bmatrix}}\,, \quad z_2 = \frac{\sigma_{22}\,\theta_1\begin{bmatrix}0 & \frac12\\ 0 & \frac12\end{bmatrix} - \sigma_{21}\,\theta_2\begin{bmatrix}0 & \frac12\\ 0 & \frac12\end{bmatrix}}{\xi\,\theta\begin{bmatrix}0 & 0\\ 0 & \frac12\end{bmatrix}\theta\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}\theta\begin{bmatrix}\frac12 & \frac12\\ 0 & 0\end{bmatrix}\theta\begin{bmatrix}0 & \frac12\\ \frac12 & 0\end{bmatrix}}\,,$$

$$z_3 = \frac{\sigma_{22}\,\theta_1\begin{bmatrix}0 & \frac12\\ \frac12 & \frac12\end{bmatrix} - \sigma_{21}\,\theta_2\begin{bmatrix}0 & \frac12\\ \frac12 & \frac12\end{bmatrix}}{\xi\,\theta\begin{bmatrix}0 & 0\\ \frac12 & \frac12\end{bmatrix}\theta\begin{bmatrix}0 & 0\\ \frac12 & 0\end{bmatrix}\theta\begin{bmatrix}\frac12 & \frac12\\ 0 & 0\end{bmatrix}\theta\begin{bmatrix}0 & \frac12\\ 0 & 0\end{bmatrix}}\,, \quad z_4 = \frac{\sigma_{22}\,\theta_1\begin{bmatrix}\frac12 & 0\\ \frac12 & \frac12\end{bmatrix} - \sigma_{21}\,\theta_2\begin{bmatrix}\frac12 & 0\\ \frac12 & \frac12\end{bmatrix}}{\xi\,\theta\begin{bmatrix}\frac12 & \frac12\\ \frac12 & \frac12\end{bmatrix}\theta\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}\theta\begin{bmatrix}0 & 0\\ \frac12 & 0\end{bmatrix}\theta\begin{bmatrix}\frac12 & 0\\ 0 & 0\end{bmatrix}}\,,$$

$$z_5 = \frac{\sigma_{22}\,\theta_1\begin{bmatrix}\frac12 & 0\\ \frac12 & 0\end{bmatrix} - \sigma_{21}\,\theta_2\begin{bmatrix}\frac12 & 0\\ \frac12 & 0\end{bmatrix}}{\xi\,\theta\begin{bmatrix}\frac12 & \frac12\\ \frac12 & \frac12\end{bmatrix}\theta\begin{bmatrix}0 & 0\\ 0 & \frac12\end{bmatrix}\theta\begin{bmatrix}0 & 0\\ \frac12 & \frac12\end{bmatrix}\theta\begin{bmatrix}\frac12 & 0\\ 0 & \frac12\end{bmatrix}}\,, \quad \xi := -\frac{a_1}{a_2}\sum_{m=1}^{5}\frac{\sigma_{22}\,\theta_1[\,\eta_m\,] - \sigma_{21}\,\theta_2[\,\eta_m\,]}{\theta[e_1^{m,6}]\,\theta[e_2^{m,6}]\,\theta[e_3^{m,6}]\,\theta[e_4^{m,6}]}\,.$$

In case $a_2 = 0$ we define ξ with the help of Viète's formulas.

2. Similar arguments hold for the polynomials $P_4(z) = a_2z^4 + a_3z^3 + \cdots + a_6$, $a_2a_6 \neq 0$, with four different roots: in addition to $z_6 = \infty$, we shall consider $z_5 = 0$, that is the above z_5–numerator $\sigma_{22}\,\theta_1\begin{bmatrix}\frac12 & 0\\ \frac12 & 0\end{bmatrix} - \sigma_{21}\,\theta_2\begin{bmatrix}\frac12 & 0\\ \frac12 & 0\end{bmatrix}$ vanishes, to conclude the roots of $P_4(z)$ equal

$$z_1 = \zeta\cdot\frac{\theta\begin{bmatrix}0 & 0\\ \frac12 & 0\end{bmatrix}\theta\begin{bmatrix}\frac12 & \frac12\\ 0 & 0\end{bmatrix}\theta\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}}{\theta\begin{bmatrix}0 & \frac12\\ \frac12 & 0\end{bmatrix}\theta\begin{bmatrix}\frac12 & 0\\ 0 & 0\end{bmatrix}\theta\begin{bmatrix}0 & \frac12\\ 0 & 0\end{bmatrix}}\,, \qquad z_2 = \zeta\cdot\frac{\theta\begin{bmatrix}0 & 0\\ \frac12 & 0\end{bmatrix}\theta\begin{bmatrix}\frac12 & 0\\ 0 & 0\end{bmatrix}\theta\begin{bmatrix}0 & \frac12\\ 0 & 0\end{bmatrix}}{\theta\begin{bmatrix}0 & \frac12\\ \frac12 & 0\end{bmatrix}\theta\begin{bmatrix}\frac12 & \frac12\\ 0 & 0\end{bmatrix}\theta\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}}\,,$$

$$z_3 = \zeta\cdot\frac{\theta\begin{bmatrix}0 & \frac12\\ \frac12 & 0\end{bmatrix}\theta\begin{bmatrix}\frac12 & 0\\ 0 & 0\end{bmatrix}\theta\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}}{\theta\begin{bmatrix}0 & 0\\ \frac12 & 0\end{bmatrix}\theta\begin{bmatrix}\frac12 & \frac12\\ 0 & 0\end{bmatrix}\theta\begin{bmatrix}0 & \frac12\\ 0 & 0\end{bmatrix}}\,, \qquad z_4 = \zeta\cdot\frac{\theta\begin{bmatrix}0 & \frac12\\ \frac12 & 0\end{bmatrix}\theta\begin{bmatrix}\frac12 & \frac12\\ 0 & 0\end{bmatrix}\theta\begin{bmatrix}0 & \frac12\\ 0 & 0\end{bmatrix}}{\theta\begin{bmatrix}0 & 0\\ \frac12 & 0\end{bmatrix}\theta\begin{bmatrix}\frac12 & 0\\ 0 & 0\end{bmatrix}\theta\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}}\,,$$

where the identity $z_1 + z_2 + z_3 + z_4 = -\frac{a_3}{a_2}$ (or some other formulas of Viète if $a_3 = 0$) defines unambiguously the constant ζ.

Multiplying by the least common denominator of z_1, z_2, z_3, z_4 simplifies the above expressions:

$$z_1 = \zeta_1\cdot\theta\begin{bmatrix}0 & 0\\ \frac12 & 0\end{bmatrix}^2\theta\begin{bmatrix}\frac12 & \frac12\\ 0 & 0\end{bmatrix}^2\theta\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}^2\,, \qquad z_2 = \zeta_1\cdot\theta\begin{bmatrix}0 & 0\\ \frac12 & 0\end{bmatrix}^2\theta\begin{bmatrix}\frac12 & 0\\ 0 & 0\end{bmatrix}^2\theta\begin{bmatrix}0 & \frac12\\ 0 & 0\end{bmatrix}^2\,,$$

$$z_3 = \zeta_1\cdot\theta\begin{bmatrix}0 & \frac12\\ \frac12 & 0\end{bmatrix}^2\theta\begin{bmatrix}\frac12 & 0\\ 0 & 0\end{bmatrix}^2\theta\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}^2\,, \qquad z_4 = \zeta_1\cdot\theta\begin{bmatrix}0 & \frac12\\ \frac12 & 0\end{bmatrix}^2\theta\begin{bmatrix}\frac12 & \frac12\\ 0 & 0\end{bmatrix}^2\theta\begin{bmatrix}0 & \frac12\\ 0 & 0\end{bmatrix}^2\,,$$

the constant ζ_1 specified like ζ did.

3. In order to solve the cubic equation $P_3(z) = a_3z^3 + a_4z^2 + a_5z + a_6 = 0$ (subject $a_3a_6 \neq 0$ and $z_j \neq 1$) via two-dimensional theta constants, we regard the polynomial $P_4(z) := (z-1)P_3(z)$, namely suppose that $z_4 = 1$ and the constant ζ specified upon the identity $\zeta\,\theta\begin{bmatrix}0 & \frac12\\ \frac12 & 0\end{bmatrix}\theta\begin{bmatrix}\frac12 & \frac12\\ 0 & 0\end{bmatrix}\theta\begin{bmatrix}0 & \frac12\\ 0 & 0\end{bmatrix} = \theta\begin{bmatrix}0 & 0\\ \frac12 & 0\end{bmatrix}\theta\begin{bmatrix}\frac12 & 0\\ 0 & 0\end{bmatrix}\theta\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}$, whence

$$z_1 = \frac{\theta\begin{bmatrix}0 & 0\\ \frac12 & 0\end{bmatrix}^2\theta\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}^2}{\theta\begin{bmatrix}0 & \frac12\\ \frac12 & 0\end{bmatrix}^2\theta\begin{bmatrix}0 & \frac12\\ 0 & 0\end{bmatrix}^2}\,, \qquad z_2 = \frac{\theta\begin{bmatrix}0 & 0\\ \frac12 & 0\end{bmatrix}^2\theta\begin{bmatrix}\frac12 & 0\\ 0 & 0\end{bmatrix}^2}{\theta\begin{bmatrix}0 & \frac12\\ \frac12 & 0\end{bmatrix}^2\theta\begin{bmatrix}\frac12 & \frac12\\ 0 & 0\end{bmatrix}^2}\,, \qquad z_3 = \frac{\theta\begin{bmatrix}\frac12 & 0\\ 0 & 0\end{bmatrix}^2\theta\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}^2}{\theta\begin{bmatrix}\frac12 & \frac12\\ 0 & 0\end{bmatrix}^2\theta\begin{bmatrix}0 & \frac12\\ 0 & 0\end{bmatrix}^2}\,.$$

Remark that these three exact squares would be the roots of cubic polynomials due to Umemura [13], compare with [4] too.

6 Torelli theorem for genus two Riemann surfaces

Every genus two Riemann surface R is hyperelliptic and there always exist two meromorphic functions $w, z : R \to \mathbb{CP}^1$ such that $w^2 = P_6(z)$ for some degree six polynomial $P_6(z)$ with different roots $z_1, \dots, z_6$ [7]. In accordance with our construction, fix the order of the six roots of $P_6(z)$ and compute the matrix of the periods $\Omega = \Omega(R)$ to define the rank four lattice

$$\Lambda(\Omega) := \left\{ M + N\Omega \mid M, N \in \mathbb{Z}^2 \right\} \subset \mathbb{C}^2.$$

Then the classical Torelli theorem [7] claims that the Riemann surface R can be restored by its Jacobian $J(R) = \mathbb{C}^2/\Lambda(\Omega)$, or, which is the same, by $\Lambda(\Omega)$.

On the other side, each (2×2) symmetric matrix Ω with $\operatorname{Im}\Omega > 0$ defines a two-dimensional complex torus $T := \mathbb{C}^2/\Lambda(\Omega)$ and then the Riemann surface

$$R(\Omega) \ : \quad w^2 = \prod_{m=1}^{6} \left(z - \frac{\theta_1\left[\eta_m\right]}{\theta_2\left[\eta_m\right]} \right) \tag{3}$$

has Jacobian $J(R) = T$. This formula effectively solves the Torelli theorem for genus two Riemann surfaces, see also [4].

The symplectic group $\mathrm{Sp}_4(\mathbb{Z})$ leaves $\Lambda(\Omega)$ and thus the Riemann surface $R(\Omega)$ invariant, while the group-action

$$z \mapsto \frac{h_{11}z + h_{12}}{h_{21}z + h_{22}}\,, \qquad \begin{pmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \end{pmatrix} \in \mathrm{PGL}_2(\mathbb{C}) \ \cong \ \mathrm{Aut}(\mathbb{CP}^1)$$

leaves $R(\Omega)$ invariant in sense that any Riemann surface

$$R_h(\Omega) \ : \quad w^2 = \prod_{m=1}^{6} \left(\frac{h_{11}z + h_{12}}{h_{21}z + h_{22}} - \frac{\theta_1\left[\eta_m\right]}{\theta_2\left[\eta_m\right]} \right)$$

remains algebraically isomorphic to $R(\Omega)$.

Alternatively, any two different rank four lattices $\Lambda(\Omega)$ and $\Lambda(\Omega')$ in $\mathbb{C}^2$ must define algebraically non-isomorphic Riemann surfaces $R(\Omega)$ and $R(\Omega')$ by (3). The moduli space, i.e. the variety of all algebraically non-isomorphic genus two Riemann surfaces

$$\begin{aligned} \mathcal{M}_2 \ &= \ \left\{ 2 \times 2 \text{ symmetric matrix } \Omega \text{ with } \operatorname{Im}\Omega > 0 \right\} \text{ modulo } \mathrm{Sp}_4(\mathbb{Z}) - \text{action} \\ &= \ \mathrm{PGL}_2(\mathbb{C}) \setminus \left\{ \text{degree 6 polynomials with different roots} \right\} / \, \mathcal{S}_6 \\ &= \ \left\{ (\xi_1, \xi_2, \xi_3),\ \xi_j \in \mathbb{C} - \{0, 1\},\ \xi_{1,2,3} \text{ are different} \right\} \text{ modulo } \mathcal{S}_6' - \text{action}, \end{aligned}$$

where the $\mathcal{S}_6$-elements reorder the roots of $P_6(z)$, an unique element of $\mathrm{PGL}_2(\mathbb{C})$ normalizes them in the form $(0, 1, \infty, \xi_1, \xi_2, \xi_3)$; then we forget for $0, 1, \infty$ to obtain a $\mathcal{S}_6'$–action on triples (ξ_1, ξ_2, ξ_3). In general, there are 720 $\mathcal{S}_6'$–equivalent triples (ξ_1, ξ_2, ξ_3).

Acknowledgements. The author wishes to thank R.-P. Holzapfel for his clarifying comments during the preparation of this paper.

References

[1] Abel N. H., Beweis der Unmöglichkeit algebraische Gleichungen von höheren Graden als dem vierten allgemein aufzulösen. – J. reine angew. Math., Bd.1, 1826, 65–84.

[2] Artin E., Theory of braids. – Ann. Math. 48, 1926, 101–106.

[3] Behr H., Eine endliche Präsentation der symplektischen Gruppe $\mathrm{Sp}_4(\mathbb{Z})$. – Math. Z., 141, 1975, 47–56.

[4] Belokolos E., Enol'skii V., Solutions of algebraically integrable nonlinear equations and theta–constants. – Preprint IMP.9.86, Inst. for Metal Phys., Kiev, 1986.

[5] Coxeter H., Moser W., Generators and Relations for discrete Groups. – Springer–Verlag, Berlin Heidelberg New York, 1972.

[6] Galois E., Ecrits et mémoires mathématiques. – Gautier–Villars, Paris, 1962.

[7] Griffiths P., Harris J., Principles of algebraic geometry. – Willey-Intersci. Publ., 1978.

[8] Hermite Ch., Sur la résolution de l'équation du cinquième degré. – C. R. Acad. Sci., t.46, 1858, 508–515.

[9] Igusa J., Theta functions. – Grund. Math. Wiss., 194, Springer, 1972.

[10] Jordan C., Traité des substitution et des équation algébrique. – Gautier–Villars, Paris, 1870.

[11] Klein F., Gleichungen vom siebenten und achten Grade. – Math. Ann., 1879, Bd.15, 251–282.

[12] Kronecker L., Sur la résolution de l'équation du cinquième degré. – C. R. Acad. Sci., t.46, 1858, 1150–1152.

[13] Mumford D., Tata Lectures on Theta II. – Birkhäuser, Boston Basel Stuttgart, 1984.

[14] O'Meara O., Lectures on Symplectic Groups. Univ. of Notre Dame, 1976.

[15] Rosenhain G., Abhandlung über die Functionen zweiter Variabler mit vier Perioden. – Mem. des savants, Bd.IX, 1851.

[16] Thomae J., Beitrag zur Bestimmung von $\theta(0, 0, \ldots, 0)$ durch die Klassenmoduln algebraischer Functionen. – J. reine angew. Math., Bd.71, 1870, 201–222.

[17] Weber H., Lehrbuch der Algebra, Reprint. – Chelsea, New York.