A Generalization of Rosenhain's Normal Form for Hyperelliptic Curves with an Application

By Koichi TAKASE

Department of Mathematics, Miyagi University of Education

(Communicated by Shokichi IYANAGA, M. J. A., Sept. 12, 1996)

Introduction. Let C be a compact Riemann surface of genus 2. Then C has six Wierstrass points. If we normalize three of them into 0, 1 and ∞, the complex curve C is defined by

$$Y^2 = X(X-1)(X-\lambda_1)(X-\lambda_2)(X-\lambda_3).$$

Rosenhain's normal form gives λ_1, λ_2 and λ_3 as ratios of theta constants at the period matrix of C (see Remark 1.3).

In this paper, we will give a similar formula for the hyperelliptic curves over $\boldsymbol{C}$ of general genus (Theorem 1.1). As an application of the formula, we will give resolutions of a complex algebraic equation as ratios of theta constants at the period matrix of a suitable hyperelliptic curve (Theorem 3.1).

Such formulas were given by H.Umemura in [1] based on Thomae's formula. But adding to Thomae's formula, we have Frobenius' theta formula [1, Theorem 7.1] and a criterion of vanishing of theta constant at the period matrix of the hyperelliptic curve [1, Corollary 6.7]. Using these results, we can simplify the formula given by Umemura.

§1 Main result. Let $f(X)$ be a separable monic polynomial with complex coefficients of degree $2g+1$. Let $a_1, a_2, \cdots, a_{2g+1}$ be the roots of $f(X) = 0$. Let $\Omega \in \mathfrak{H}_g$ be the period matrix of the hyperelliptic curve $Y^2 = f(X)$. Here $\mathfrak{H}_g$ denotes the Siegel upper half space of genus g. The ordering of the roots of $f(X) = 0$ determines the classical basis of the first cohomology group of the hyperelliptic curve. The basis in turn defines the period matrix Ω. A theta function is defined by

$$\vartheta[\alpha](\Omega, w) = \sum_{l \in \boldsymbol{Z}^g} \exp 2\pi\sqrt{-1} \left\{\frac{1}{2}\langle l+\alpha', (l+\alpha')\Omega\rangle + \langle l+\alpha', w+\alpha''\rangle\right\},$$

where $w \in \boldsymbol{C}^g$ and $\alpha = (\alpha', \alpha'') \in \boldsymbol{R}^{2g}$ are row vectors with $\alpha', \alpha'' \in \boldsymbol{R}^g$, and $\langle x, y\rangle = x \cdot {}^t y$.

Put

$$B = \{1, 2, 3, \cdots, 2g+1\},$$
$$U = \{1, 3, 5, \cdots, 2g+1\}.$$

Define theta characteristics $\eta_k = (\eta'_k, \eta''_k) \in \frac{1}{2}\boldsymbol{Z}^{2g}$ $(k = 1,2,\cdots, 2g+1)$ by

$$\eta'_{2i-1} = \Big(0, \cdots, 0, \overset{\overset{i}{\vee}}{\tfrac{1}{2}}, 0, \cdots, 0\Big),$$

$$\eta''_{2i-1} = \Big(\frac{1}{2}, \cdots, \frac{1}{2}, \overset{\overset{i}{\vee}}{0}, 0, \cdots, 0\Big),$$

$(\eta'_{2g+1} = (0, 0, \cdots, 0))$ and

$$\eta'_{2i} = \Big(0, \cdots, 0, \overset{\overset{i}{\vee}}{\tfrac{1}{2}}, 0, \cdots, 0\Big),$$

$$\eta''_{2i} = \Big(\frac{1}{2}, \cdots, \frac{1}{2}, \overset{\overset{i}{\vee}}{\tfrac{1}{2}}, 0, \cdots, 0\Big).$$

For any subset T of B, put

$$\eta_T = (\eta'_T, \eta''_T) = \sum_{k \in T} \eta_k \in \frac{1}{2}\boldsymbol{Z}^{2g},$$

$(\eta_\emptyset = (0, 0, \cdots, 0))$. For any subsets S, T of B, let us denote by $S \circ T$ the symmetric difference of S, T; $S \circ T = S \cup T - S \cap T$. For the sake of the notational simplicity, let us denote by

$$\vartheta[T] = \vartheta[\eta_T](\Omega, 0)$$

the theta zero value at the period Ω with a theta characteristic η_T for any subset T of B.

Now our main result is

Theorem 1.1. *For any disjoint decomposition $B = V \sqcup W \sqcup \{k, l, m\}$ with $\# V = \# W = g-1$, we have*

$$\frac{a_k - a_l}{a_k - a_m} = \varepsilon(k; l, m) \times \left(\frac{\vartheta[U \circ (V \cup \{k, l\})] \cdot \vartheta[U \circ (W \cup \{k, l\})]}{\vartheta[U \circ (V \cup \{k, m\})] \cdot \vartheta[U \circ (W \cup \{k, m\})]}\right)^2.$$

Here

$$\varepsilon(k; l, m) = \begin{cases} 1 & \text{if } k < l, m \text{ or } l, m < k \\ -1 & \text{if } l < k < m \text{ or } m < k < l. \end{cases}$$

The proof of Theorem 1.1 will be given in the next section.

Remark 1.2 (the case of $g=1$). In this case $B=\{1,2,3\}$, $U=\{1,3\}$ and $V=W=\emptyset$ in Theorem 1.1. Then we have a classical formula

$$\frac{a_1-a_2}{a_1-a_3}=\left(\frac{\vartheta\left[\frac{1}{2},0\right](\Omega,0)}{\vartheta[0,0](\Omega,0)}\right)^4.$$

Remark 1.3 (the case of $g=2$). In this case $B=\{1,2,3,4,5\}$ and $U=\{1,3,5\}$. Putting

$$(k,l,m)=(1,3,2),\ (1,4,2),\ (1,5,2)$$

in Theorem 1.1, we have

$$\frac{a_1-a_3}{a_1-a_2}=\left(\frac{\vartheta\left[0,\frac{1}{2},0,0\right](\Omega,0)\cdot\vartheta[0,0,0,0](\Omega,0)}{\vartheta\left[\frac{1}{2},0,0,0\right](\Omega,0)\cdot\vartheta\left[\frac{1}{2},\frac{1}{2},0,0\right](\Omega,0)}\right)^2,$$

$$\frac{a_1-a_4}{a_1-a_2}=\left(\frac{\vartheta\left[0,\frac{1}{2},0,0\right](\Omega,0)\cdot\vartheta\left[0,0,0,\frac{1}{2}\right](\Omega,0)}{\vartheta\left[\frac{1}{2},0,0,\frac{1}{2}\right](\Omega,0)\cdot\vartheta\left[\frac{1}{2},\frac{1}{2},0,0\right](\Omega,0)}\right)^2,$$

$$\frac{a_1-a_5}{a_1-a_2}=\left(\frac{\vartheta[0,0,0,0](\Omega,0)\cdot\vartheta\left[0,0,0,\frac{1}{2}\right](\Omega,0)}{\vartheta\left[\frac{1}{2},0,0,\frac{1}{2}\right](\Omega,0)\cdot\vartheta\left[\frac{1}{2},0,0,0\right](\Omega,0)}\right)^2.$$

This is one of the seven hundred twenty possible formulas of Rosenhain's normal form of hyperelliptic curve of genus 2 [2].

§2 *Proof of Theorem* 1.1. A relation between the theta zero values at Ω and the roots $\{a_1,\cdots,a_{2g+1}\}$ is given by Thomae's formula [1, Th.8.1];

Proposition 2.1. *For any subset S of B such that $\#S$ is even and $\#(U\circ S)=g+1$, we have*

$$\vartheta[\eta_S](\Omega,0)^4=C\cdot(-1)^{\#(U\cap S)}\prod_{k\in U\circ S,\,l\notin U\circ S}(a_k-a_l)^{-1}.$$

Here C is a constant independent of S.

We have also a criterion of vanishing of theta constants at the hyperelliptic period Ω [1, Cor.6.7];

Proposition 2.2. *For any subset S of B such that $\#S$ is even, $\vartheta[\eta_S](\Omega,0)=0$ if and only if $\#(U\circ S)\neq g+1$.*

For the hyperelliptic period Ω, we have the following Frobenius' theta relation [1, Th.7.1];

Proposition 2.3. *For any $w_j\in\boldsymbol{C}^g$ and $b_j\in\boldsymbol{Q}^{2g}$ such that $w_1+w_2+w_3+w_4=0$ and $b_1+b_2+b_3+b_4=0$ respectively, we have*

$$\prod_{j=1}^{4}\vartheta[b_j](\Omega,w_j)=\sum_{k=1}^{2g+1}(-1)^{k-1}\prod_{j=1}^{4}\vartheta[b_j+\eta_k](\Omega,w_j).$$

Specializing this theta relation, we have

Lemma 2.4. *For any $\alpha,\beta\in\frac{1}{2}\boldsymbol{Z}^{2g}$, we have*

$$\vartheta[\alpha](\Omega,w)^2\cdot\vartheta[\beta](\Omega,w)^2=\sum_{j=1}^{2g+1}(-1)^{\langle 2\eta_j',2(\alpha''+\beta'')\rangle+j-1}\cdot\vartheta[\alpha+\eta_j](\Omega,w)^2\times\vartheta[\beta+\eta_j](\Omega,w)^2$$

for all $w\in\boldsymbol{C}^g$.

Proof. We have the following elementary relations;

$$\vartheta[\eta](\Omega,-w)=(-1)^{\langle 2\eta',2\eta''\rangle}\cdot\vartheta[\eta](\Omega,w),$$

and

$$\vartheta[\eta+r](\Omega,w)=(-1)^{\langle 2\eta',r''\rangle}\cdot\vartheta[\eta](\Omega,w)$$

for all $\eta\in\frac{1}{2}\boldsymbol{Z}^{2g}$ and $r\in\boldsymbol{Z}^{2g}$. Using these relations and Proposition 2.3, we have

$$\begin{aligned}&\vartheta[\alpha](\Omega,w)^2\cdot\vartheta[\beta](\Omega,w)^2\\&=(-1)^{\langle -2\alpha',2\alpha''\rangle+\langle -2\beta',2\beta''\rangle}\\&\times\vartheta[\alpha](\Omega,w)\vartheta[-\alpha](\Omega,w)\\&\qquad\times\vartheta[\beta](\Omega,-w)\vartheta[-\beta](\Omega,-w)\\&=(-1)^{\langle -2\alpha',2\alpha''\rangle+\langle -2\beta',2\beta''\rangle}\cdot\\&\qquad\times\sum_{j=1}^{2g+1}(-1)^{j-1}\vartheta[\alpha+\eta_j](\Omega,w)\\&\qquad\times\vartheta[-\alpha+\eta_j](\Omega,w)\vartheta[\beta+\eta_j](\Omega,-w)\\&\qquad\times\vartheta[-\beta+\eta_j](\Omega,-w).\end{aligned}$$

We get the required formula by means of the elementary relations given above. □

Proof of Theorem 1.1. For any subset S of B such that $\#S=g+1$, we have

$$\vartheta[U\circ S]^4=C\cdot(-1)^{\#(U-S)}\prod_{k\in S,\,l\notin S}(a_k-a_l)^{-1} \tag{2.1}$$

by Proposition 2.1. Then for any disjoint decomposition $B=V_1\sqcup V_2\sqcup\{k\}$ such that $\#V_1=\#V_2=g$, we have

$$\left(\frac{\vartheta[U\circ(V_1\cup\{k\})]}{\vartheta[U\circ(V_2\cup\{k\})]}\right)^4=(-1)^{k-1}\prod_{i\in V_1,\,j\in V_2}(a_k-a_i)(a_k-a_j)^{-1}. \tag{2.2}$$

In fact, put $S=V_1\cup\{k\}$ or $S=V_2\cup\{k\}$ in (2.1), and substitute in the left hand side of (2.2). Then many cancellations occur among the factors a_i-a_j, and the relation

$$\#(U\cap V_1)+\#(U\cap V_2)+g^2\equiv k-1\ (\mathrm{mod}\,2)$$

gives the formula (2.2).

Now put $V_1 = V \cup \{l\}$, $V_2 = W \cup \{m\}$ or $V_1 = V \cup \{m\}$, $V_2 = W \cup \{l\}$ in (2.2), and make a ratio of them. Then we have

$$(2.3)\quad \left(\frac{a_k - a_l}{a_k - a_m}\right)^2 = \left(\frac{\vartheta[U \circ (V \cup \{k, l\})] \cdot \vartheta[U \circ (W \cup \{k, l\})]}{\vartheta[U \circ (V \cup \{k, m\})] \cdot \vartheta[U \circ (W \cup \{k, m\})]}\right)^4.$$

We have the following theta relation;

Lemma 2.5.

$$\begin{aligned}\vartheta[U \circ (V \cup \{k, l\})]^2 \cdot \vartheta[U \circ (W \cup \{k, l\})]^2 &= (-1)^{\langle 2\eta'_k, 2(\eta''_l + \eta''_m)\rangle} \cdot \vartheta[U \circ (V \cup \{k, m\})]^2 \\ &\quad \times \vartheta[U \circ (W \cup \{k, m\})]^2 \\ &\quad + (-1)^{\langle 2\eta'_l, 2(\eta''_k + \eta''_m)\rangle} \cdot \vartheta[U \circ (V \cup \{m, l\})]^2 \\ &\quad \times \vartheta[U \circ (W \cup \{m, l\})]^2.\end{aligned}$$

Proof. Put

$$\alpha = \eta_{U \circ (V \cup \{k, l\})}, \quad \beta = \eta_{U \circ (W \cup \{k, l\})}.$$

Lemma 2.4 with $w = 0$ gives

$$(2.4)\quad \begin{aligned}&\vartheta[\alpha](\Omega, 0)^2 \vartheta[\beta](\Omega, 0)^2 \\ &= \sum_{j=1}^{2g+1} (-1)^{\langle 2\eta'_j, 2(\alpha'' + \beta'')\rangle + j - 1} \\ &\quad \times \vartheta[\alpha + \eta_j](\Omega, 0)^2 \cdot \vartheta[\beta + \eta_j](\Omega, 0)^2.\end{aligned}$$

We have

$$\begin{aligned}\alpha + \eta_j &\equiv \eta_{U \circ (V \cup \{k, l\}) \circ \{j\}} \pmod{\boldsymbol{Z}^{2g}} \\ &\equiv \eta_{U \circ (W \cup \{m\}) \circ \{j\}} \pmod{\boldsymbol{Z}^{2g}},\end{aligned}$$

and

$$(W \cup \{m\}) \circ \{j\} = \begin{cases} W \cup \{m, j\} & \text{if } j \in V \cup \{k, l\} \\ W \cup \{m\} - \{j\} & \text{if } j \notin V \cup \{k, l\}. \end{cases}$$

Then $\vartheta[\alpha + \eta_j](\Omega, 0) \neq 0$ only if $j \in V \cup \{k, l\}$ by Proposition 2.2. Similarly $\vartheta[\beta + \eta_j](\Omega, 0) \neq 0$ only if $j \in W \cup \{k, l\}$. Since $V \cap W = \emptyset$, on the right hand side of (2.4), only two terms for $j = k$ or $j = l$ remain. On the other hand we have

$$\alpha + \beta \equiv \eta_k + \eta_l + \eta_m \pmod{\boldsymbol{Z}^{2g}},$$

and

$$\langle 2\eta'_k, 2\eta''_k\rangle \equiv k - 1 \pmod 2.$$

We have the required formula. □

Now calculate the left hand side of

$$\left(\frac{a_k - a_l}{a_k - a_m}\right)^2 - \left(\frac{a_m - a_l}{a_m - a_k}\right)^2 = 2 \cdot \frac{a_k - a_l}{a_k - a_m} - 1$$

by the formula (2.3), and use Lemma 2.5 twice. Then we get

$$\frac{a_k - a_l}{a_k - a_m} = (-1)^{\langle 2\eta'_k, 2(\eta''_l + \eta''_m)\rangle} \times \left(\frac{\vartheta[U \circ (V \cup \{k, l\})] \cdot \vartheta[U \circ (W \cup \{k, l\})]}{\vartheta[U \circ (V \cup \{k, m\})] \cdot \vartheta[U \circ (W \cup \{k, m\})]}\right)^2.$$

and

$$(-1)^{\langle 2\eta'_k, 2(\eta''_l + \eta''_m)\rangle} = \begin{cases} 1 & \text{if } k < l, m \text{ or } l, m < k \\ -1 & \text{if } l < k < m \text{ or } m < k < l. \end{cases}$$

§3 Application. In this section, we will give resolutions of a complex algebraic equation

$$F(X) = X^n + c_1 X^{n-1} + \cdots + c_{n-1} X + c_n = 0 \quad (c_j \in \boldsymbol{C})$$

by theta constants.

First of all, we can suppose that $F(0) \neq 0$ and $F(1) \neq 0$ (otherwise, divide $F(X)$ by X or $X - 1$). If $F(X) = 0$ has a multiple root, calculate the (monic) greatest common divisor $F_1(X)$ of $F(X)$ and its derivative $F'(X)$ by the Euclidean algorithm, and put $F_2(X) = F(X)/F_1(X)$. Repeating the same procedure to each $F_j(X)$, we can decompose $F(X)$ into a product of separable polynomials. Then we suppose that $F(X)$ is separable. Finally we can suppose that the degree n of $F(X)$ is odd (otherwise replace $F(X)$ by $(X - c)F(X)$ with a complex number $c \neq 0,1$ such that $F(c) \neq 0$).

Let us suppose that $F(X)$ is a separable polynomial of odd degree such that $F(0) \neq 0$ and $F(1) \neq 0$. Let $\alpha_1, \alpha_2, \cdots, \alpha_n$ be the roots of $F(X) = 0$. Put $f(X) = X(X - 1)F(X)$ and

$$a_1 = 0, \quad a_2 = 1, \quad a_{2+j} = \alpha_j \ (j = 1, 2, \cdots, n).$$

Let $\Omega \in \mathfrak{H}_g$ ($g = (n + 1)/2$) be the period matrix of the hyperelliptic curve $Y^2 = f(X)$ subordinative to the ordering of the roots of $f(X)$ given above. Then we have

Theorem 3.1.

$$\alpha_j = \begin{cases} \left(\dfrac{\vartheta[0, 0, \cdots, 0](\Omega, 0) \cdot \vartheta[\eta_1 + \eta_2 + \eta_{2+j}](\Omega, 0)}{\vartheta\left[\frac{1}{2}, 0, \cdots, 0\right](\Omega, 0) \cdot \vartheta[\eta_2 + \eta_{2+j}](\Omega, 0)}\right)^2 & \text{if } j \text{ is odd}, \\ \left(\dfrac{\vartheta\left[0, \frac{1}{2}, 0, \cdots, 0\right](\Omega, 0) \cdot \vartheta[\eta_3 + \eta_{2+j}](\Omega, 0)}{\vartheta\left[\frac{1}{2}, \frac{1}{2}, 0, \cdots, 0\right](\Omega, 0) \cdot \vartheta[\eta_1 + \eta_3 + \eta_{2+j}](\Omega, 0)}\right)^2 & \text{if } j \text{ is even}. \end{cases}$$

Proof. If j is odd, put $k = 1$, $l = 2 + j$, $m = 2$ and

$$V = \{3, 5, 7, \cdots, 2g + 1\} - \{2 + j\}, \quad W = \{4, 6, 8, \cdots, 2g\}.$$

If j is even, put $k = 1$, $l = 2 + j$, $m = 2$ and

$$V = \{5, 7, 9, \cdots, 2g + 1\}, \quad W = \{3, 4, 6, 8, \cdots, 2g\} - \{2 + j\}.$$

Then Theorem 1.1 gives the formula of $\alpha_j = \dfrac{a_1 - a_{2+j}}{a_1 - a_2}$. □

References

[1] D. Mumford: Tata Lectures on Theta II. Progress in Mat., vol. 43, Birkhaüser (1984).

[2] G. Rosenhain: Abhandlung über die Functionen zweier Variabler mit vier Perioden. Ostwald's Klassiker der Exacten Wissenschaften, 65 (1895).