TSUKUBA J. MATH.
Vol. 31 No. 1 (2007), 1–37

THE AUTOMORPHISM GROUP OF A CYCLIC p-GONAL CURVE

By

Naonori ISHII and Katsuaki YOSHIDA

Abstract. Let M be a cyclic p-gonal curve with a positive prime number p, and let V be the automorphism of order p satisfying $M/\langle V\rangle \simeq \boldsymbol{P}^1$. It is well-known that finite subgroups H of $\mathrm{Aut}(\boldsymbol{P}^1)$ are classified into five types. In this paper, we determine the defining equation of M with $H \subset \mathrm{Aut}(M/\langle V\rangle)$ for each type of H, and we make a list of hyperelliptic curves of genus 2 and cyclic trigonal curves of genus 5, 7, 9 with $H = \mathrm{Aut}(M/\langle V\rangle)$.

1 Introduction

Let M be a compact Riemann surface defined by

$$y^p - (x-a_1)^{r_1}\cdots(x-a_s)^{r_s} = 0, \tag{1}$$

where p is a positive prime integer, a_i's are distinct complex numbers, and r_i's are integers satisfying $1 \le r_i < p$ $(i = 1,\dots,s)$. Put $\mathscr{S} := \{a_1,\dots,a_s\}$ (resp. $\{a_1,\dots,a_s,a_{s+1}=\infty\}$) when $\sum_{i=1}^{s} r_i \equiv 0 \pmod{p}$ (resp. $\sum_{i=1}^{s} r_i \not\equiv 0 \pmod{p}$). Then the genus g of M is $\frac{(\#\mathscr{S}-2)(p-1)}{2}$. Let $\boldsymbol{C}(M)$ denote the function field $\boldsymbol{C}(x,y)$ of M. For an automorphism $\sigma \in \mathrm{Aut}(M)$, σ^* represents the action on $\boldsymbol{C}(M)$ induced by σ. Let V be the automorphism on M defined by

$$V^*x = x \quad \text{and} \quad V^*y = \zeta_p y$$

with the primitive p-th root $\zeta_p = \exp 2\pi i/p$ of unity. The inclusion $\boldsymbol{C}(x) \subset \boldsymbol{C}(M)$ corresponds to the cyclic normal covering $x : M \to \boldsymbol{P}^1(x)$ of degree p, and its covering group is $\langle V\rangle$. Then x is (totally) ramified over a point $a \in \boldsymbol{P}^1(x)$ if and only if $a \in \mathscr{S}$.

2000 Mathematical Subject Classification: 14H05, 14H30, 14H37.
Key words: Compact Riemann surface, Automorophisms, Coverings.
Received June 6, 2005.
Revised May 9, 2006.

In general, a compact Riemann surface of genus g is called a n-gonal curve when M has a meromorphic function of degree n and does not have any non-trivial meromorphic functions whose degree is smaller than n. It is known that M becomes a p-gonal curve provided $(p-1)(p-2) < g$ with a prime number p [10].

From now on, we always assume that M is a compact Riemann surface defined by (1). From the fact mentioned above, M becomes a p-gonal curve when $2p-2 < \#\mathscr{S}$.

Let g_d^1 denote a linear system of degree d and dimension 1, then the linear system $|(x)_\infty|$ is g_p^1. Here $(x)_\infty$ is the pole divisor of x on M. We also assume that $|(x)_\infty|$ is unique as g_p^1. In fact the uniqueness of g_p^1 is satisfied when $(p-1)^2 < g$, i.e., $2p < \#\mathscr{S}$ [10]. The uniqueness of g_p^1 on a cyclic p-gonal curve M implies that $\langle V \rangle$ is normal in $\mathrm{Aut}(M)$. Moreover we will see that V is in the center of $\mathrm{Aut}(M)$. Therefore, for a subgroup G of $\mathrm{Aut}(M)$ containing V, we have an exact sequence

$$1 \to \langle V \rangle \to G \xrightarrow{\pi} H \to 1, \qquad (*)$$

where $H = G/\langle V \rangle$.

On the other hand, it is well known that a finite subgroup H of $\mathrm{Aut}(\boldsymbol{P}^1)$ is isomorphic to cyclic $\mathbf{C}_n$, dihedral $\mathbf{D}_{2n}$, tetrahedral $\mathbf{A}_4$, octahedral $\mathbf{S}_4$ or icosahedral $\mathbf{A}_5$. Then it can be said that the group G above is obtained as an extension of these five groups by a cyclic group $\langle V \rangle$ of order p. Consequently there exist special relations among $a_1, \dots, a_s$ of (1) depending on H.

First we will give a necessary and sufficient condition that the sequence $(*)$ is split.

Next, by applying the concrete representations of finite subgroup H of $\mathrm{Aut}(\boldsymbol{P}^1(x))$ given by Klein, we determine a defining equation of M which satisfies the condition $H \subset \mathrm{Aut}(M)/\langle V \rangle$ for a given H.

Finally, as applications, we give a classification of hyperelliptic curves M of genus 2 and cyclic tigonal curves of genus $g = 5, 7, 9$ based on the types of H contained in $\mathrm{Aut}(M)/\langle V \rangle$.

2 A Necessary and Sufficient Condition in Which the Exact Sequence (*) is Split

Let M be a cyclic p-gonal curve defined by the equation (1), and the linear system $|(x)_\infty|$ is assumed to be unique as g_p^1. The symbols G, H, $\mathscr{S}$ etc. are same as in the previous section. We prepare more notations.

Notation 1. *Let denote $\tilde{T}$ the element of $H = G/\langle V \rangle \subset \mathrm{Aut}(\boldsymbol{P}^1(x))$ induced by some element $T \in G$. Let $FP(H)$ (resp. $FP(G)$) denote the set of points on*

$M/\langle V\rangle \simeq \boldsymbol{P}^1(x)$ (resp. M) fixed by a non-trivial element of H (resp. G), and let $FG(a)$ denote the set of automorphisms of $\boldsymbol{P}^1(x)$ which fixes a point $a \in \boldsymbol{P}^1(x)$. By corresponding $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL(2, \boldsymbol{C})$ to $A(x) := \frac{\alpha x+\beta}{\gamma x+\delta}$, we have an isomorphism $SL(2, \boldsymbol{C})/\{\pm 1\} \simeq \mathrm{Aut}(\boldsymbol{P}^1(x))$. We use the same symbol "A" for both a matrix and an element of $\mathrm{Aut}(\boldsymbol{P}^1(x))$. Let $\langle A\rangle a$ denote the orbit of $a \in \boldsymbol{P}^1(x)$ by the subgroup $\langle A\rangle$ generated by $A \in SL(2, \boldsymbol{C})$.

For $a \in FP(H)$, $FG(a)$ is a cyclic group and $FP(FG(a))$ consists of two points a and a' with $a \neq a'$. If $FG(a)$ is generated by an element A of order n, then, by changing the coordinate x suitably, we may assume $A(x) = \zeta_n x$ and $FP(\langle A\rangle) = \{0, \infty\}$, where $\zeta_n = \exp(\frac{2\pi i}{n})$.

We start with the following lemma.

LEMMA 2.1. (i) *The group H acts on $\mathscr{S}$.*

(ii) *Let a_i and a_j be in $\mathscr{S}$. If there exists an element $T \in G$ satisfying $\tilde{T}a_i = a_j$, then we have $r_i = r_j$. Here we define r_{s+1} by $r_{s+1} \equiv -\sum_{i=1}^{s} r_i \pmod p$ and $0 < r_{s+1} < p$ when $\sum_{i=1}^{s} r_i \not\equiv 0 \pmod p$.*

(iii) *The automorphism V is contained in the center of G.*

PROOF. (i) Let T be an arbitrary automorphism on M. From the uniqueness of g_p^1, we have a diagram

$$\begin{array}{ccc} M & \xrightarrow{\ x\ } & M/\langle V\rangle \simeq \boldsymbol{P}^1(x) \\ {\scriptstyle T}\downarrow\wr & & \downarrow\wr{\scriptstyle \tilde{T}} \\ M & \xrightarrow[\ x\ ]{} & M/\langle V\rangle \simeq \boldsymbol{P}^1(x), \end{array}$$

and this implies that $\tilde{T}$ acts on S.

(ii) Refer to [6], [11].

(iii) Suppose ord $\tilde{T} = n$. Then we may assume that $\tilde{T}$ is defined by $\tilde{T}^* x = \zeta_n x$, and then $FP(\langle T\rangle) = \{0, \infty\}$. For $a \in M/\langle V\rangle \simeq \boldsymbol{P}^1(x)$ with $a \notin \{0, \infty\}$, the orbit $\langle \tilde{T}\rangle a$ is $\{a, \zeta_n a, \ldots, \zeta_n^{p-1} a\}$. The set $\mathscr{S}$ is decomposed into orbits of $\langle \tilde{T}\rangle$ depending on the order $\#\mathscr{S} \cap \{0, \infty\}$.

(a) $\underline{\#\{\mathscr{S} \cap \{0, \infty\}\} = 2}$ $\mathscr{S} = \{0\} \cup \{\infty\} \cup \langle \tilde{T}\rangle b_1 \cup \cdots \cup \langle \tilde{T}\rangle b_t$,

(b) $\underline{\#\{\mathscr{S} \cap \{0, \infty\}\} = 1}$ (we may assume $\mathscr{S} \cap \{0, \infty\} = \{0\}$), $\mathscr{S} = \{0\} \cup \langle \tilde{T}\rangle b_1 \cup \cdots \cup \langle \tilde{T}\rangle b_t$,

(c) $\underline{\#\{\mathscr{S} \cap \{0, \infty\}\} = 0}$ $\mathscr{S} = \langle \tilde{T}\rangle b_1 \cup \cdots \cup \langle \tilde{T}\rangle b_t$, where $b_1, \dots, b_t$ are non-zero elements in $\mathscr{S}$ with $b_i \neq \infty$ and $\langle \tilde{T} \rangle b_i \cap \langle \tilde{T} \rangle b_j = \emptyset$ for $i \neq j$.

In case (a), from (i) of this lemma, M is defined by

$$y^p = x(x^n - b_1^n)^{u_1} \cdots (x^n - b_t^n)^{u_t}, \tag{2}$$

with $n \sum_{i=1}^t u_i + 2 \equiv 0 \pmod{p}$. In case (b), M is also defined by (2) with $n \sum_{i=1}^t u_i + 1 \equiv 0 \pmod{p}$. In both cases (a) and (b), by acting T^* on (2), we have

$$(T^*y)^p = \tilde{T}^*(x)(\tilde{T}^*(x)^n - b_1^n)^{u_1} \cdots (\tilde{T}^*(x)^n - b_t^n)^{u_t} = \zeta_n y^p.$$

Then T is defined by $T^*x = \zeta_n x$ and $T^*y = \varepsilon y$, where ε satisfies $\varepsilon^p = \zeta_n$. Since $V^*x = x$ and $V^*y = \zeta_p y$, we have $V^*T^* = T^*V^*$.

In case (c), we can also prove as above. □

Lemma 2.1 (i) and (ii) imply the following.

Lemma 2.2. *Assume $\mathscr{S} \not\ni \infty$. Let $\mathscr{S} = \bigcup_{i=1}^u Hb_i^{(1)}$ (disjoint) be the decomposition of $\mathscr{S}$ into orbits $Hb_i^{(1)} = \{b_i^{(1)}, \dots, b_i^{(s_i)}\} (\subset \boldsymbol{C})$. Then the equation (1) is transformed into*

$$y^p = \prod_{i=1}^u \{(x - b_i^{(1)}) \cdots (x - b_i^{(s_i)})\}^{r_i} \tag{3}$$

with $1 \leq r_i < p$ and $\sum_{i=1}^u s_i r_i \equiv 0 \pmod{p}$.

Let $\tilde{\pi} : \boldsymbol{P}^1(x) \to \boldsymbol{P}^1(u)$ be a normal covering defined by $u = f_1(x)/f_0(x)$ with a Galois group H, where $f_0(x)$ and $f_1(x)$ are polynomials relatively prime to each other. We write $(b_0 : b_1)$ for a point of u-plane $\boldsymbol{P}^1(u)$ with $u = \dfrac{b_1}{b_0}$. Then we have the following theorem.

Theorem 2.1. *Let M be defined by the equation (1). Then the exact sequence $(*)$ is split if and only if*

(A) *$FP(H) \cap \mathscr{S} = \emptyset$, or*

(B) *for $a \in FP(H) \cap \mathscr{S}$, $\#FG(a)$ is not divisible by p.*

Proof. Put $\#H = n$. Then $\#G = pn$. We may assume $\mathscr{S} \not\ni \infty$. Then M is defined by (3) in Lemma 2.2. We regard M/G as a u-plane $\boldsymbol{P}^1(u)$, and consider the normal covering

$$M/\langle V\rangle \simeq \boldsymbol{P}^1(x) \xrightarrow{\tilde{\pi}} M/G \simeq \boldsymbol{P}^1(u),$$

whose covering group is H. We assume $u = f_1(x)/f_0(x)$. We can also assume that the image $\tilde{\pi}(\mathscr{S})$ does not contain $\infty(\in \boldsymbol{P}^1(u))$.

Now we assume that $(*)$ is split. Then $G = \langle V\rangle \times H$. We have a commutative diagram and canonical isomorphisms

$$(\natural)\quad \begin{array}{ccc} M & \xrightarrow{x} & M/\langle V\rangle \\ \pi\downarrow & & \downarrow\tilde{\pi} \\ M/H & \xrightarrow[u]{} & M/G, \end{array} \qquad \begin{cases} \mathrm{Gal}(\pi) \simeq \mathrm{Gal}(\tilde{\pi}) \simeq H \\ \mathrm{Gal}(x) \simeq \mathrm{Gal}(u) \simeq \langle V\rangle \\ \boldsymbol{C}(M) \simeq \boldsymbol{C}(M/H) \underset{\boldsymbol{C}(u)}{\otimes} \boldsymbol{C}(x), \end{cases}$$

where $\mathrm{Gal}(\psi)$ means the covering group of a given normal covering $\psi : M_1 \to M_2$ of compact Riemann surfaces M_i. Put $\tilde{\pi}(\mathscr{S}) = \{(1 : b_1), \dots, (1 : b_u)\}$, where b_i $(i = 1 \cdots u)$ are distinct complex numbers. Then we may assume that M/H is defined by

$$y^p = (u - b_1)^{t_1} \cdots (u - b_u)^{t_u} \quad \text{with} \quad \sum_{i=1}^{u} t_i \equiv 0 \text{ and } 0 < t_i < p. \tag{4}$$

The isomorphism $\boldsymbol{C}(M) \simeq \boldsymbol{C}(M/H) \underset{\boldsymbol{C}(u)}{\otimes} \boldsymbol{C}(x)$ implies that x and y have a relation

$$y^p = \left(\frac{f_1(x)}{f_0(x)} - b_1\right)^{t_1} \cdots \left(\frac{f_1(x)}{f_0(x)} - b_u\right)^{t_u}. \tag{5}$$

By replacing $f_0^{(\sum_{i=1}^{u} t_i)/p} y$ with y, we have

$$y^p = (f_1(x) - b_1 f_0(x))^{t_1} \cdots (f_1(x) - b_u f_0(x))^{t_u}, \tag{6}$$

and this equation defines M. Let $\mathscr{S}_i = \{b_i^{(1)}, \dots, b_i^{(s_i)}\}$ $(i = 1, \dots, u)$ be the set of points b in $\boldsymbol{P}^1(x)$ satisfying $\tilde{\pi}(b) = b_i$. Then, by the assumptions $\infty \notin \mathscr{S}$ and $\infty \notin \tilde{\pi}(\mathscr{S})$, we have factorizations

$$f_1(x) - b_i f_0(x) = C_i\{(x - b_i^{(1)}) \cdots (x - b_i^{(s_i)})\}^{m_i} \quad \text{with } n = m_i s_i \text{ and } C_i \neq 0.$$

The positive integers m_i are ramification indices of $\tilde{\pi}$ over $(1 : b_i)$ and $m_i = \# FG(b_i^{(k)})$. So the equation (6) may assume to be transformed into

$$y^p = \prod_{i=1}^{u} \{(x - b_i^{(1)}) \cdots (x - b_i^{(s_i)})\}^{m_i t_i}, \tag{7}$$

and we have $\mathscr{S} \subset \bigcup_{i=1}^{t} \mathscr{S}_i$. If some m_i is divisible by p, we can omit the term $\{(x - b_i^{(1)}) \cdots (x - b_i^{(s_i)})\}^{m_i t_i}$ of (7) by replacing y with $y/\{\prod_{k=1}^{s_i} (x - b_i^{(k)})\}^{m_i t_i/p}$.

Further we can delete the term $(u-b_i)^{t_i}$ from the equation (4). Finally we can get the equation (4) satisfying $\mathscr{S}=\bigcup_{i=1}^{t}\mathscr{S}_i$ and $(m_i,p)=1$.

Conversely assume that (A) or (B) is satisfied and M is be defined by the equation (3) in Lemma 2.2. Put $b_i=\tilde{\pi}(b_i^{(1)})$ $(i=1,\dots,u)$. Then, for each b_i, we have $f_1(x)-b_if_0(x)=C_i\{(x-b_i^{(1)})\cdots(x-b_i^{(s_i)})\}^{m_i}$ again. The assumption (A) or (B) implies $(m_i,p)=1$. Then, from $(r_i,p)=1$ and $(m_i,p)=1$, there exists an integer s_i satisfying $0<s_i<p$ and $s_ir_i\equiv m_i \pmod{p}$ for each i. Put $s=\prod_{i=1}^{u}s_i$. Then there exist two integers u_i and M_i satisfying $sr_i=u_im_i+M_ip$. Raising both sides of (3) to s-th power and replacing $y^s/\{\prod_{i=1}^{u}\{(x-b_i^{(1)})\cdots(x-b_i^{(s_i)})\}^{M_i}\}$ with y again, we have

$$y^p=\prod_{i=1}^{u}\{(x-b_i^{(1)})\cdots(x-b_i^{(s_i)})\}^{u_im_i}=C\prod_{i=1}^{u}(f_1(x)-b_if_0(x))^{u_i},$$

where C is a non-zero constant. Therefore we may assume that M is defined by $y^p=\prod_{i=1}^{u}(f_1(x)-b_if_0(x))^{u_i}$, and then $\boldsymbol{C}(M)=\boldsymbol{C}(M/H)\underset{\boldsymbol{C}(u)}{\otimes}\boldsymbol{C}(x)$. □

3 Defining Equations of p-gonal Curves M with an Exact Sequence $(*)$

In this section, we give defining equations of M and representations of G according to each type of finite subgroups H of $\mathrm{Aut}(\boldsymbol{P}^1)$ classified by Klein [8].

Let $A=\begin{pmatrix}\alpha&\beta\\ \gamma&\delta\end{pmatrix}\in SL(2,\boldsymbol{C})$. As in the previous section, we also write A for the element $\{\pm A\}$ in $SL(2,\boldsymbol{C})/\{\pm 1\}\simeq \mathrm{Aut}(\boldsymbol{P}^1(x))$ as long as there is no confusion. Although there are p distinct elements of G which induce $A\in H$, we also use the symbol A abusively for an element of G which induces $A\in H$. In order to determine the action of A^* on the function field $\boldsymbol{C}(x,y)$, it is sufficient to investigate A^*y.

Let $\tilde{\pi}:\boldsymbol{P}^1(x)\to\boldsymbol{P}^1(u)$ be a finite normal covering defined by a rational function $u=\frac{f_1(x)}{f_0(x)}$ with $(f_0,f_1)=1$, and let H be is its covering group. Put $\#H=s$. Take $(b_0:b_1)\in\boldsymbol{P}^1(u)$. Let $m\geq 1$ be the ramification index of $\tilde{\pi}$ over $(b_0:b_1)$. Then there are three types of factorizations of the polynomial

$$\tilde{P}_{(b_o:b_1)}:=b_0f_1(x)-b_1f_0(x).$$

That is:

$$\tilde{P}_{(b_o:b_1)}=\begin{cases}\text{(i)}\ \ C\prod_{i=1}^{t}(x-a_i)^m & \text{with } t\geq 1 \text{ and } mt=s,\\ \text{(ii)}\ \ C\prod_{i=1}^{t-1}(x-a_i)^m & \text{with } t-1\geq 1 \text{ and } mt=s,\\ \text{(iii)}\ \ C, & \end{cases}$$

where C is a non-zero constant. Type (i) (resp. (ii)) happens when $\tilde{\pi}(\infty) \neq (b_0 : b_1)$ (resp. $\tilde{\pi}(\infty) = (b_0 : b_1)$ and $m < s$). Type (iii) happens when $\tilde{\pi}(\infty) = (b_0 : b_1)$ and $m = s$. Then H must be a cyclic group.

Define a polynomial $P_{(b_0:b_1)}$ and a positive integer $d_{(b_0:b_1)}$ as follows.

(i) $P_{(b_0:b_1)}(x) = \prod_{i=1}^{t}(x - a_i)$, $d_{(b_0:b_1)} = t$ if $\tilde{P}_{(b_o:b_1)}$ is of type (i),
(ii) $P_{(b_0:b_1)}(x) = \prod_{i=1}^{t-1}(x - a_i)$, $d_{(b_0:b_1)} = t$ if $\tilde{P}_{(b_o:b_1)}$ is of type (ii),
(iii) $P_{(b_0:b_1)}(x) = 1$, $d_{(b_0:b_1)} = s$ if $\tilde{P}_{(b_o:b_1)}$ is of type (iii).

The following lemma comes form the consideration similar to that of the previous section.

Lemma 3.1. *Let M be a cyclic p-gonal curve defined by* (1) *with $\#\mathscr{S} > 2p$ (therefore M has a unique g_p^1). Assume* $\mathrm{Aut}(M)/\langle V\rangle$ *contains the finite subgroup H above. Then there exists a finite set $\{(b_{0,i} : b_{1,i}) \mid 1 \leq i \leq r\}$ of distinct points in $\boldsymbol{P}^1(u)$, and M can be defined by*

$$y^p = \prod_{i=1}^{r} P_{(b_{0,i}:b_{1,i})}^{u_i}, \quad 1 \leq u_i \leq p-1, \tag{8}$$

$$\sum_{i=1}^{r} u_i d_{(b_{0,i}:b_{1,i})} \equiv 0 \pmod p, \quad \#\mathscr{S} = \sum_{i=1}^{r} d_{(b_{0,i}:b_{1,i})} > 2p.$$

Moreover the number of $P_{(b_{0,i},b_{1,i})}$ of type (i) *among $P_{(b_{0,i},b_{1,i})}$ $(1 \leq i \leq r)$ is at least $(r-1)$. If there is a $P_{(b_{0,i},b_{1,i})}$ of type* (iii), *H is a cyclic group.*

Next we introduce the results from F. Klein.

Lemma 3.2 ([8], [4]). *Let $\tilde{\pi} : \boldsymbol{P}^1(x) \to \boldsymbol{P}^1(u)$ be a finite normal covering defined by a rational function $u = \frac{f_1(x)}{f_0(x)}$. Then the covering group H of $\tilde{\pi}$ is cyclic, dihedral, tetrahedral, octahedral or icosahedral. And, by choosing coordinates x and u suitably, $u = \frac{f_1(x)}{f_0(x)}$ and the generators of H can be represented as in Table* 1 *of Appendix.*

Proposition 3.1. *Let H be one of the groups in Table* 1. *Then the polynomials $P_{(b_0:b_1)}$ in each type of H are given in Table* 2 *of Appendix.*

Proof. For example, when $H = \mathbf{A}_4$ and $u = \frac{(x^4 - 2\sqrt{3}ix^2+1)^3}{(x^4+2\sqrt{3}ix^2+1)^3}$,

$$\tilde{P}_{(1:1)}(x) = (x^4 - 2\sqrt{3}ix^2 + 1)^3 - (x^4 + 2\sqrt{3}ix^2 + 1)^3 = \{x(x^4 - 1)\}^2$$

and 0, ± 1, $\pm i$ and ∞ are points over $(1:1)$ with ramification index 2. Then $P_{(1:1)}(x) = x(x^4 - 1)$ is of type (ii).

When $H = \mathbf{A}_5$ and $u = \frac{f_1(x)}{f_0(x)} = \frac{\{-x^{20}-1+228(x^{15}-x^5)-494x^{10}\}^3}{1728x^5(x^{10}+11x^5-1)^5}$, we have

$$\begin{aligned}\tilde{P}_{(1:1)} &= \{-x^{20} - 1 + 228(x^{15} - x^5) - 494x^{10})\}^3 - \{1728x^5(x^{10} + 11x^5 - 1)\}^5 \\ &= -(x^{30} + 522x^{25} - 10005x^{20} - 10005x^{10} - 522x^5 + 1)^2,\end{aligned}$$

and $P_{(1:1)} = x^{30} + 522x^{25} - 10005x^{20} - 10005x^{10} - 522x^5 + 1$ is of type (i). In any other cases, we can calculate by the same way as above. □

By this proposition and Lemma 3.1, we can get defining equations of M with H of Table 1, and they are written in Theorem 3.1.

We can get the representation A^*y for the generators A of H in Table 1, by letting A act on both sides of the defining equations of M directly. But, before practicing the calculation, we will make closer observations on the action of A.

DEFINITION 1. *For $A = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in SL(2, \mathbf{C})$. Define $j(A, x) := \gamma x + \delta$ with a variable x on $\mathbf{C}$. When $A\infty = \infty$ (i.e., $\gamma = 0$), define $j(A, \infty) := j(DAD^{-1}, 0) = \alpha$, where $D = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. And when $A\infty \neq \infty$, define $j(A, \infty) := 1$. Of course an automorphism of $\mathbf{P}^1(x)$ induced by a matrix A is also induced by $-A$, and $j(-A, x) = -j(A, x)$ for a variable x.*

First we will write down several properties of $j(A, x)$.

LEMMA 3.3. *Let $A = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ and B be in $SL(2, \mathbf{C})$, and let x be a variable on $\mathbf{C}$. Then*

(i) $j(AB, x) = j(A, Bx)j(B, x)$.

(ii) $\alpha - \gamma A(x) = j(A, x)^{-1}$.

(iii) $j(A, x)j(A^{-1}, A(x)) = 1$.

(iv) *Assume that the order of $A \in \mathrm{Aut}(\mathbf{P}^1)$ is l (i.e., l is the least positive integer satisfying $A^l = \pm\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$). Take $a \in \mathbf{P}^1(x)$ such that $a \notin FP(\langle A \rangle)$.*

(a) *Assume $\infty \notin \langle A \rangle a$. Then*

$$\prod_{i=1}^{l} j(A^{-1}, A^i(a)) = j(A^l, x) = \begin{cases} 1 & \text{if } A^l = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \\ -1 & \text{if } A^l = -\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right). \end{cases}$$

(b) *Assume $a = \infty$. Then $j(A^{-1}, A(a)) = 0$ and*

$$\prod_{i=2}^{l} j(A^{-1}, A^{i}(a)) = -j(A^{l}, x) = \begin{cases} -1 & \text{if } A^{l} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \\ 1 & \text{if } A^{l} = -\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \end{cases}$$

(v) *For* $a \in FP(\langle A \rangle)$, $j(A, a) = j(BAB^{-1}, B(a))$.

(vi) *Let* $FP(\langle A \rangle) = \{a_1, a_2\}$. *Then* $j(A, a_1)$ *and* $j(A, a_2)$ *are primitive* l (*resp.* $2l$)*-th roots of* 1 *if* $A^{l} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ (*resp.* $-\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$). *And* $j(A, a_1)j(A, a_2) = 1$.

PROOF. We can prove (i), (ii) and (iii) by simple calculations.

(iv) We will prove only (b). Assume $a = \infty$. As $\gamma \neq 0$ and $A(a) = \frac{\alpha}{\gamma}$, we have $j(A^{-2}, A(a)) = -1$ and $j(A^{-1}, A(a)) = 0$. Since $j(A^{-1}, A^{i}(a)) = j(A^{i-2}, A(a))/j(A^{i-1}, A(a))$ $(2 \le i \le l-1)$ and $j(A^{-1}, A^{l}(a)) = j(A^{-1}, \infty) = 1$ by the definition, we have

$$\prod_{i=2}^{l} j(A^{-1}, A^{i}(a)) = \prod_{i=2}^{l-1} \frac{j(A^{i-2}, A(a))}{j(A^{i-1}, A(a))} = \frac{1}{j(A^{l-2}, A(a))}$$

$$= \frac{1}{j(A^{l}, A^{-2}A(a))j(A^{-2}, A(a))} = -\frac{1}{j(A^{l}, A^{-2}(a))} = -j(A^{l}, x).$$

(v) Since $A(a) = a$, the assertion comes from (i), (iii) and $j(A, \infty) = \alpha$.

(vi) By (v), we may assume $a_1 = 0$, $a_2 = \infty$ and $A = \begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{pmatrix}$ where ε is a primitive l or $2l$-th root of 1. Then $j(A, 0) = \varepsilon^{-1}$ and $j(A, \infty) = \varepsilon$. □

Let $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in H$. First we observe the action of A^* on polynomials $P_{(b_0:b_1)}$.

LEMMA 3.4. *Assume that* $A \in \mathrm{Aut}(\boldsymbol{P}^1(x))$ *has an order* l. *Let* $P_{(b_0:b_1)}$ *be a polynomial of type* (i) *or* (ii) *above. Put* $\mathscr{U} := \{a_1, \dots, a_t\}$ (*resp.* $\{a_1, \dots, a_{t-1}, \infty\}$) *when* $P_{(b_0:b_1)}$ *is of type* (i) (*resp.* (ii)). *Then* A^* *acts on* $P_{(b_0:b_1)}$ *in the following manner.*

(I) *If* $\mathscr{U} \cap FP(\langle A \rangle) = \varnothing$, *then* $t \equiv 0 \pmod{l}$ *and*

$$A^*(P_{(b_0:b_1)}(x)) = P_{(b_0:b_1)}(A(x)) = j(A, x)^{-t} j(A^{l}, x)^{t/l} P_{(b_0:b_1)}(x).$$

(II) *If* $\mathscr{U} \cap FP(\langle A \rangle)$ *consists of one fixed point* $c \in \boldsymbol{P}^1(x)$ *of* A, *then* $t - 1 \equiv 0 \pmod{l}$ *and*

$$A^*(P_{(b_0:b_1)}(x)) = j(A^{-1}, c) j(A, x)^{-t} j(A^{l}, x)^{(t-1)/l} P_{(b_0:b_1)}(x).$$

(III) *If* $\mathscr{U} \cap FP(\langle A \rangle)$ *consists of two points* c, c' *of* A, *then* $t - 2 \equiv 0 \pmod{l}$, *and*

$$A^*(P_{(b_0:b_1)}(x)) = j(A,x)^{-t} j(A^l,x)^{(t-2)/l} P_{(b_0:b_1)}(x).$$

These representations are independent from the choice of matrix A or $-A$.

Proof. (I) Assume $\mathscr{U} \ni \infty$ (i.e., $P_{(b_0:b_1)}$ is of type (ii)). Let

$$\mathscr{U} = \{\infty, A(\infty), \dots, A^{l-1}(\infty)\} \cup (\textstyle\bigcup_{k=2}^{r} \langle A \rangle c_k)$$

be the decomposition of $\mathscr{U}$ into the orbits of $\langle A \rangle$. Then $lr = t$, $\gamma \neq 0$ and

$$P_{(b_0:b_1)}(x) = \prod_{i=1}^{l-1}(x - A^i(\infty)) \prod_{k=2}^{r}\prod_{i=1}^{l}(x - A^i(c_k)).$$

By acting A^* on both sides of this equation, we have

$$A^*(P_{(b_0:b_1)}(x)) = \underbrace{\prod_{i=1}^{l-1}\left(\frac{\alpha x+\beta}{\gamma x+\delta} - A^i(\infty)\right)}_{(A)} \underbrace{\prod_{k=2}^{r}\prod_{i=1}^{l}\left(\frac{\alpha x+\beta}{\gamma x+\delta} - A^i(c_k)\right)}_{(B)}.$$

Since $A(\infty) = \frac{\alpha}{\gamma}$ and $-\gamma A(\infty) + \alpha = 0$,

$$\text{the term } (A) = j(A,x)^{-(l-1)} \prod_{i=1}^{l-1}\{(-\gamma A^i(\infty)+\alpha)x - (\delta A^i(\infty) - \beta)\}$$

$$= j(A,x)^{-(l-1)}\left(-\delta\frac{\alpha}{\gamma} + \beta\right) \prod_{i=2}^{l-1}\{(-\gamma A^i(\infty)+\alpha)x - (\delta A^i(\infty) - \beta)\}$$

$$= j(A,x)^{-(l-1)}\left(-\delta\frac{\alpha}{\gamma} + \beta\right) \prod_{i=2}^{l} j(A^{-1}, A^i(\infty))$$

$$\times \prod_{i=2}^{l-1}\left\{x - \frac{(\delta A^i(\infty) - \beta)}{(-\gamma A^i(\infty)+\alpha)}\right\}$$

$$= j(A,x)^{-(l-1)}\left(-\delta\frac{\alpha}{\gamma} + \beta\right)(-j(A^l,x)) \prod_{i=2}^{l-1}\{x - A^{i-1}(\infty)\}. \qquad (\star)$$

The last equality comes from Lemma 3.1 iv) (b). On the other hand, by Lemma 3.1 iv) (a),

$$\text{the term } (B) = j(A,x)^{-l(r-1)} j(A^l,x)^{(r-1)} \prod_{k=2}^{r}\prod_{i=1}^{l}(x - A^{i-1}(c_k)). \qquad (\star\star)$$

By multiplying ($\star$) and ($\star\star$), we have

$$A^*(P_{(b_0:b_1)}(x)) = j(A,x)^{-(t-1)}\left(-\delta\frac{\alpha}{\gamma}+\beta\right)(-j(A^l,x)^r)$$

$$\times\prod_{i=2}^{l-1}(x-A^{i-1}(\infty))\prod_{k=2}^{r}\prod_{i=1}^{l}(x-A^{i-1}(c_k)).$$

Moreover, by $\alpha\delta-\beta\gamma=1$ and $(x-A^{l-1}(\infty))^{-1}=\gamma j(A,x)^{-1}$, we have

$$A^*(P_{(b_0:b_1)}(x)) = j(A,x)^{-(t-1)}\left(-\delta\frac{\alpha}{\gamma}+\beta\right)(-j(A^l,x)^r)(x-A^{l-1}(\infty))^{-1}$$

$$\times\prod_{i=2}^{l}(x-A^{i-1}(\infty))\prod_{k=2}^{r}\prod_{i=1}^{l}(x-A^{i-1}(c_k))$$

$$= j(A,x)^{-t}j(A^l,x)^rP_{(b_0:b_1)}.$$

In case $\infty\notin\mathscr{U}$, the calculation is much easier than the case above.

(II) Let $\mathscr{U}=\{c\}\cup(\bigcup_{k=1}^{r}\langle A\rangle c_k)(t=lr+1)$ be the decomposition of $\mathscr{U}$ into the orbits of $\langle A\rangle$. There are three cases

i) $c\neq\infty$ and $c_k\neq\infty$ $(k=1,\dots,r)$, ii) $c=\infty$, iii) $c_k=\infty$ for some k, to be considered respectively. But the calculations can be carried out by the same way as in (I), and then we omit the details.

(III) Let $\mathscr{U}=\{c\}\cup\{c'\}\cup(\bigcup_{k=1}^{r}\langle A\rangle c_k)(t=lr+2)$ be the decomposition of $\mathscr{U}$ into the orbits of $\langle A\rangle$. And we have

$$A^*(P_{(b_0:b_1)}(x)) = j(A^{-1},c)j(A^{-1},c')j(A,x)^{-t}j(A^l,x)^{(t-2)/l}P_{(b_0:b_1)}(x).$$

By Lemma 3.1 (vi), we have the equality of III. □

The following theorem is from these lemmas above. In this theorem we use the symbols $\prod_{i=m}^{m-1}$ and $\sum_{i=m}^{m-1}$ as

$$\prod_{i=m}^{m-1}*:=1 \quad\text{and}\quad \sum_{i=m}^{m-1}*:=0 \quad\text{for an positive integer } m.$$

THEOREM 3.1. *Let H be one of the groups in Table 1. Let M be a cyclic p-gonal curve with $\#\mathscr{S}>2p$. Assume* $\mathrm{Aut}(M)/\langle V\rangle$ *contains H. Then the defining equation of M and A^*y for the generators $A\in H$ of Table 1 are given as follows.*

(Case $H = \mathbf{C}_n$). *M is defined by*

$$y^p = P_{(0:1)}^{u_1} P_{(1:0)}^{u_2} \prod_{i=3}^{d} P_{(1:b_i)}^{u_i} = x^{u_2} \prod_{i=3}^{d} (x^n - b_i)^{u_i}, \tag{9}$$

$$\#\mathscr{S} = \varepsilon_1 + \varepsilon_2 + n \sum_{i=3}^{d} 1, \quad u_1 + u_2 + n \sum_{i=3}^{d} u_i \equiv 0 \pmod{p},$$

where $0 \le u_1, u_2 < p$, $0 < u_i < p$ $(i \ge 3)$, $b_i \ne 0$, *and put* $\varepsilon_k = 1$ (*resp.* $\varepsilon_k = 0$) *if* $u_k > 0$ (*resp.* $u_k = 0$) $(k = 1, 2)$. *In this case* $d \ge 3$ *since* $\#\mathscr{S} > 2p \ge 4$.

For the generator S_n *of* $\mathbf{C}_n$,

- $S_n^* y = \eta_{S_n} y$, *where* $(\eta_{S_n})^p = \zeta_n^{u_2}$.

(Case $H = \mathbf{D}_{2n}$). *M is defined by*

$$\begin{aligned} y^p &= P_{(1:2)}^{u_1} P_{(1:-2)}^{u_2} P_{(0:1)}^{u_3} \prod_{i=4}^{d} P_{(1:b_i)}^{u_i} \\ &= (x^n - 1)^{u_1} (x^n + 1)^{u_2} x^{u_3} \prod_{i=4}^{d} (x^{2n} - b_i x^n + 1)^{u_i}, \end{aligned} \tag{10}$$

$$\#S = n\varepsilon_1 + n\varepsilon_2 + 2\varepsilon_3 + 2n \sum_{i=4}^{d} 1, \quad nu_1 + nu_2 + 2u_3 + 2n \sum_{i=4}^{d} u_i \equiv 0 \pmod{p},$$

where $d \ge 3$ (*according to the notation above*), $0 \le u_1, u_2, u_3 < p$, *and* $0 < u_i < p$ $(i \ge 4)$, $b_i \ne \pm 2$, *and put* $\varepsilon_k = 1$ (*resp.* $\varepsilon_k = 0$) *if* $u_k > 0$ (*resp.* $u_k = 0$) $(k = 1, 2, 3)$.

For the generators S_n *and* T *of* $\mathbf{D}_{2n}$,

- $S_n^* y = \eta_{S_n} y$ *where* $(\eta_{S_n})^p = \zeta_n^{u_3}$
- $T^* y = \eta_T x^{-(nu_1 + nu_2 + 2u_3 + 2n\sum_{i=4}^{d} u_i)/p} y$, *where* $(\eta_T)^p = (-1)^{u_1}$

(Case $H = \mathbf{A}_4$). *M is defined by*

$$\begin{aligned} y^p &= P_{(1:0)}^{u_1} P_{(1:1)}^{u_2} P_{(0:1)}^{u_3} \prod_{i=4}^{d} P_{(1:b_i)}^{u_i} \\ &= (x^4 - 2\sqrt{3}ix^2 + 1)^{u_1} \{x(x^4 - 1)\}^{u_2} (x^4 + 2\sqrt{3}ix^2 + 1)^{u_3} \\ &\quad \times \prod_{i=4}^{d} \frac{1}{1 - b_i} \{(x^4 - 2\sqrt{3}ix^2 + 1)^3 - b_i (x^4 + 2\sqrt{3}ix^2 + 1)^3\}^{u_i}, \end{aligned} \tag{11}$$

$$\#\mathscr{S} = 4\varepsilon_1 + 6\varepsilon_2 + 4\varepsilon_3 + 12 \sum_{i=4}^{d} 1, \quad 4u_1 + 6u_2 + 4u_3 + 12 \sum_{i=4}^{d} u_i \equiv 0 \pmod{p},$$

where $d \geq 3$, $0 \leq u_1, u_2, u_3 < p$, $0 < u_i < p$ $(i \geq 4)$, $b_i \neq 0, 1$, *and put* $\varepsilon_k = 1$ (*resp.* $\varepsilon_k = 0$) *if* $u_k > 0$ (*resp.* $u_k = 0$) $(k = 1, 2, 3)$.

For the generators U, W *of* $\mathbf{A}_4$,

- $U^* y = \eta_U \{\frac{1-i}{2}(x+1)\}^{(-4u_1 - 6u_2 - 4u_3 - 12\sum_{i=4}^{d} u_i)/p} y,$

  where $(\eta_U)^p = (-1)^{u_2 + u_3} \exp(\frac{1}{3}\pi i)^{u_2} \exp(\frac{5}{3}\pi i)^{u_3}$.
- $W^* y = \eta_W \{\frac{1+i}{2}(x+i)\}^{(-4u_1 - 6u_2 - 4u_3 - 12\sum_{i=4}^{d} u_i)/p} y,$

  where $(\eta_W)^p = \exp(\frac{2}{3}\pi i)^{u_2} \exp(\frac{4}{3}\pi i)^{u_3}$.

(*Case* $H = \mathbf{S}_4$). *M is defined by*

$$\begin{aligned} y^p &= P_{(1:0)}^{u_1} P_{(1:1)}^{u_2} P_{(0:1)}^{u_3} \prod_{i=4}^{d} P_{(1:b_i)}^{u_i} \\ &= (x^8 + 14x^4 + 1)^{u_1} (x^{12} - 33x^8 - 33x^4 + 1)^{u_2} \{x(x^4 - 1)\}^{u_3} \\ &\quad \times \prod_{i=4}^{d} \{(x^8 + 14x^4 + 1)^3 - 108 b_i (x^4 (x^4 - 1)^4)\}^{u_i}, \end{aligned} \tag{12}$$

$$\#\mathscr{S} = 8\varepsilon_1 + 12\varepsilon_2 + 6\varepsilon_3 + 24\sum_{i=4}^{d} 1, \quad 8u_1 + 12u_2 + 6u_3 + 24\sum_{i=4}^{d} u_i \equiv 0 \pmod{p},$$

where $d \geq 3$, $0 \leq u_1, u_2, u_3 < p$, $0 < u_i < p$ $(i \geq 4)$, $b_i \neq 0, 1$ *and put* $\varepsilon_k = 1$ (*resp.* $\varepsilon_k = 0$) *if* $u_k > 0$ (*resp.* $u_k = 0$) $(k = 1, 2, 3)$.

For the generators W, R *of* $\mathbf{S}_4$,

- $W^* y = \eta_W \{\frac{1+i}{2}\}^{(-8u_1 - 12u_2 - 6u_3 - 24\sum_{i=4}^{n} u_i)/p} (x+i)^{(-8u_1 - 12u_2 - 6u_3 - 24\sum_{i=4}^{n} u_i)/p} y,$

  where $(\eta_W)^p = 1$.
- $R^* y = \eta_R x^{-(8u_1 + 12u_2 + 6u_3 + 24\sum_{i=4}^{n} u_i)/p} y,$ *where* $(\eta_R)^p = i^{u_3}$.

(*Case* $H = \mathbf{A}_5$). *M is defined by*

$$\begin{aligned} y^p &= P_{(1:0)}^{u_1} P_{(1:1)}^{u_2} P_{(0:1)}^{u_3} \prod_{i=4}^{d} P_{(1:b_i)}^{u_i} \\ &= \{x^{20} + 1 - 228(x^{15} - x^5) + 494x^{10}\}^{u_1} \\ &\quad \times \{x^{30} + 522x^{25} - 10005x^{20} - 10005x^{10} - 522x^5 + 1\}^{u_2} \{x(x^{10} + 11x^5 - 1)\}^{u_3} \\ &\quad \times \prod_{i=4}^{t} [\{x^{20} + 1 - 228(x^{15} - x^5) + 494x^{10}\}^3 \\ &\qquad + 1728 b_i x^5 (x^{10} + 11x^5 - 1)^5]^{u_i}, \end{aligned} \tag{13}$$

$$\#\mathscr{S} = 20\varepsilon_1 + 30\varepsilon_2 + 12\varepsilon_3 + 60\sum_{i=4}^{d} 1, \quad 20u_1 + 30u_2 + 12u_3 + 60\sum_{i=4}^{t} u_i \equiv 0 \pmod p,$$

where $d \geq 3$, $0 \leq u_1, u_2, u_3 < p$, $0 < u_i < p$ $(i \geq 4)$, $b_i \neq 0, 1$, *and put* $\varepsilon_k = 1$ (*resp.* $\varepsilon_k = 0$) *if* $u_k > 0$ (*resp.* $u_k = 0$) $(k = 1, 2, 3)$.

For the generators K, Z *of* $\mathbf{A}_5$,

- $K^*y = \eta_K\left[\frac{1}{\sqrt{5}}\{(1-\zeta_5^2)x + (\zeta_5 - \zeta_5^2)\}\right]^{(-20u_1-30u_2-12u_3-60\sum_{i=4}^{n}u_i)/p} y$ *where* $(\eta_K)^p = 1$.
- $Z^*y = \eta_Z y$, *where* $(\eta_Z)^p = \zeta_5^{u_3}$.

Proof. Here we only deal with several cases as examples.

Case $H = \mathbf{A}_4$. Let M be defined by $y^p = P_{(1:0)}^{u_1} P_{(1:1)}^{u_2} P_{(0:1)}^{u_3} \prod_{i=4}^{d} P_{(1:b_i)}^{u_i}$, where $P_{(b_0:b_1)}$ are as in Table 2. Let A be $U = \frac{1-i}{2}\begin{pmatrix} i & -i \\ 1 & 1 \end{pmatrix}$ (resp. $W = \frac{1+i}{2}\begin{pmatrix} -1 & i \\ 1 & i \end{pmatrix}$). Then

$$\begin{cases} A^3 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \text{ (resp. } \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\text{)}, & j(A^3, x) = -1 \text{ (resp. } 1\text{)}, \\ j(A, x) = \frac{1-i}{2}(x+1) \text{ (resp. } \frac{1+i}{2}(x+i)\text{)}. \end{cases}$$

Two fixed points a_1, a_2 of $A = U$ (resp. W) are

$$(\natural) \quad \begin{cases} a_1 = \frac{(-1+\sqrt{3})(1-i)}{2} \text{ (resp. } \frac{(-1-\sqrt{3})(1+i)}{2}\text{)}, & j(A^{-1}, a_1) = \exp\left(\frac{1}{3}\pi i\right) \\ & \text{(resp. } \exp\left(\frac{2}{3}\pi i\right)\text{)}, \\ a_2 = \frac{(-1-\sqrt{3})(1-i)}{2} \text{ (resp. } \frac{(-1+\sqrt{3})(1+i)}{2}\text{)}, & j(A^{-1}, a_2) = \exp\left(\frac{5}{3}\pi i\right) \\ & \text{(resp. } \exp\left(\frac{4}{3}\pi i\right)\text{)}. \end{cases}$$

and we have $P_{(1:0)}(a_1) = 0$ and $P_{(0:1)}(a_2) = 0$.

In case $A = U$, by Lemma 3.2, we have

$$\begin{cases} U^*P_{(1:0)} = j(U^{-1}, a_1)j(U, x)^{-4}j(U^3, x)P_{(1:0)} \\ \qquad = \exp\left(\frac{1}{3}\pi i\right)\left\{\frac{1-i}{2}(x+1)\right\}^{-4}(-1)P_{(1:0)}, \\ U^*P_{(1:1)} = j(U, x)^{-6}j(U^{-3}, x)^2 P_{(1:1)} = \left\{\frac{1-i}{2}(x+1)\right\}^{-6}(-1)^2 P_{(1:1)}, \\ U^*P_{(0:1)} = j(U^{-1}, a_2)j(U, x)^{-4}j(U^3, x)P_{(0:1)} \\ \qquad = \exp\left(\frac{5}{3}\pi i\right)\left\{\frac{1-i}{2}(x+1)\right\}^{-4}(-1)P_{(0:1)}, \\ U^*P_{(1:b_i)} = j(U, x)^{-12}j(U^3, x)^4 P_{(1:b_i)} \\ \qquad = \left\{\frac{1-i}{2}(x+1)\right\}^{-12}(-1)^4 P_{(1:b_i)} \quad (b_i \neq 0, 1). \end{cases}$$

Then

$$U^*y^p = (-1)^{u_1+u_3}\exp\left(\frac{1}{3}\pi i\right)^{u_1}\exp\left(\frac{5}{3}\pi i\right)^{u_3} \times \left\{\frac{1-i}{2}(x+1)\right\}^{(-4u_1-6u_2-4u_3-12\sum_{i=4}^{n}u_i)} y, \tag{14}$$

and

$$U^*y = \eta\left\{\frac{1-i}{2}(x+1)\right\}^{(-4u_1-6u_2-4u_3-12\sum_{i=4}^{n}u_i)/p} y,$$

where η satisfies $\eta^p = (-1)^{u_1+u_3}\exp(\frac{1}{3}\pi i)^{u_1}\exp(\frac{5}{3}\pi i)^{u_3}$.

We can calculate W^*y by the same way as above.

Case $H = \mathbf{S}_4$. H is generated by W and R. The fixed points $\frac{(-1\pm\sqrt{3})(1+i)}{2}$ of W are zeros of $P_{(1:0)}$. Then, by Lemma 3.2 (III), we get the representation of W^*y.

Case $H = \mathbf{A}_5$. We may assume that M is defined by $y^p = P_{(1:0)}^{u_1}P_{(1:1)}^{u_2}P_{(0:1)}^{n_3}\prod_{i=4}^{d}P_{(1:b_i)}^{u_i}$, $20u_1 + 30u_2 + 12u_3 + 60\sum_{i=2}^{d}u_i \equiv 0 \pmod p$. Assume $A = K$. Then $K^3 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ and $j(K^3, x) = -1$. Let a_1 and a_2 be fixed points of K. As $\deg P_{(1:0)} = 20 \equiv 2 \pmod 3$, a_1 and a_2 are roots of $P_{(1:0)}$. Then we can apply Lemma 3.2 (III) to $P_{(1:0)}$, and we have

$$\begin{aligned} K^*y^p &= j(K,x)^{(-20u_1-30u_2-12u_3-60\sum_{i=4}^{n}u_i)}j(K^3,x)^{(6u_1+10u_2+4u_3+20\sum_{i=4}^{n}u_i)}y^p \\ &= \left\{\frac{1}{\sqrt{5}}((1-\zeta_5^2)x + (\zeta_5-\zeta_5^2))\right\}^{(-20u_1-30u_2-12u_3-60\sum_{i=4}^{n}u_i)} y^p. \end{aligned}$$ □

Here we give several examples of defining equations of cyclic p-gonal curves having a split exact sequence $(*)$.

Corollary 3.1.1. *Let M be a p-gonal curve defined by*

$$y^p = (x^n-1)^{u_1}(x^n+1)^{u_2}x^{u_3}\prod_{i=4}^{d}(x^{2n}-b_ix^n+1)^{u_i},$$

$$nu_1 + nu_2 + 2u_3 + 2n\sum_{i=4}^{d}u_i \equiv 0 \pmod p,$$

where $d \geq 3$ and $0 \leq u_i < p$ $(1 \leq i \leq 3, b_i \neq \pm 2)$. Then $\mathrm{Aut}(M)/\langle V\rangle$ contains $H = \mathbf{D}_{2n}$. Moreover the exact sequence $(*)$ is split if and only if the prime number p is taken according to the following way. That is; take a prime number p such that $(p,2) = 1$ in case $u_3 \neq 0$, $(p,n) = 1$ in case $u_1 \neq 0$ or $u_2 \neq 0$ and any prime p in case $u_1 = u_2 = u_3 = 0$. And a map $\iota : H \to G$ defined by

$$S_n \mapsto \{S_n^* x = \zeta_n x, S_n^* y = \zeta_n^{ru_3} y\},$$
$$T \mapsto \{T^* x = 1/x, T^* y = (-1)^{u_1} x^{-(nu_1+nu_2+2u_3+2n\sum_{i=4}^{d} u_i)/p} y\}$$

gives a section of $(*)$, *where* r *is an integer satisfying* $rp \equiv 1 \pmod{n}$.

PROOF. The first half of our assertion is from Theorem 3.1 and Theorem 2.1.

Here we only check that the given map $\imath : H \to G$ is a section in case $(2p, n) = 1$ and $u_1 u_2 u_3 \neq 0$. In Theorem 3.1 (Case $H = \mathbf{D}_{2n}$), put $\eta_T = (-1)^{u_1}$ and $\eta_{S_n} = \zeta_n^{ru_3}$ with an integer r satisfying $rp \equiv 1 \pmod{n}$. Then $(\eta_{S_n})^p = (\zeta_n)^{u_3}$, $(\eta_T)^p = (-1)^{u_1}$. Meanwhile $\mathbf{D}_{2n}$ is defined by relations $S_n^n = 1$, $T^2 = 1$ and $TS_nT = S_n^{-1}$. But $(S_n^*)^n y = \eta_{S_n}^n y = y$ and $(T^*)^2 y = \eta_T^2 y = y$ hold. Therefore if $T^* S_n^* T^* y = S_n^{*-1} y$ holds, then $\imath$ is a group homomorphism. In fact, by the definiton of $\imath$,

$$\begin{aligned} T^* S_n^* T^* y &= T^* S_n^* (\eta_T x^{-(nu_1+nu_2+2u_3+2n\sum_{i=4}^{d} u_i)/p} y) \\ &= T^* (\eta_T \eta_{S_n} (\zeta_n x)^{-(nu_1+nu_2+2u_3+2n\sum_{i=4}^{d} u_i)/p} y) \\ &= (\eta_T)^2 \eta_{S_n} (\zeta_n)^{-(nu_1+nu_2+2u_3+2n\sum_{i=4}^{d} u_i)/p} y \\ &= ((-1)^{u_1})^2 \zeta_n^{ru_3} (\zeta_n)^{\{-(nu_1+nu_2+2u_3+2n\sum_{i=4}^{d} u_i)/p\}pr} y \\ &= \zeta_n^{-ru_3} y. \end{aligned}$$

Then $T^* S_n^* T^* y = S_n^{*-1} y$ holds. The equation $\pi \circ \imath = id_H$ is trivial from the definiton. □

COROLLARY 3.1.2. (1) *The compact Riemann surface* M *defined by the following equations* (14) *or* (15) *has* $\mathrm{Aut}(M)$ *isomorphic to* $\mathbf{A}_5 \times \langle V \rangle$.

$$y^p = x^{20} + 1 - 228(x^{15} - x^5) + 494x^{10} \quad (p = 2, 5). \tag{15}$$

$$y^p = x(x^{10} + 11x^5 - 1) \quad (p = 2, 3). \tag{16}$$

(2) *The compact Riemann surface* M *defined by*

$$y^p = x^{30} + 522x^{25} - 10005x^{20} - 10005x^{10} - 522x^5 + 1 \quad (p = 2, 3, 5), \tag{17}$$

satisfies $\mathrm{Aut}(M)/\langle V \rangle \simeq \mathbf{A}_5$. *Moreover* $\mathrm{Aut}(M) \simeq \mathbf{A}_5 \times \langle V \rangle$ *provided* $p = 3, 5$. *But when* $p = 2$, *the exact sequence* $(*)$ *is not split.*

PROOF. The right hand side of (14) is $P_{(1:0)}$ of A_5 in Table 2. Then, by Theorem 3.1, $\mathrm{Aut}(M)/\langle V\rangle \simeq \mathbf{A}_5$ if $20 \equiv 0 \pmod p$. So $p = 2$ or 5. Moreover if a is a root of $P_{(1:0)} = 0$, then $\# FG(a) = 3$. Therefore the exact sequence $(*)$ is split by Theorem 2.1. The remains of the assertion can be proved by the same manner. □

4 Hyperelliptic Curves of Genus 2 with an Exact Sequence $(*)$

In this section, we assume that M is a hyperelliptic curve (i.e., $p = 2$) of genus $g = 2$. By applying the results in the previous sections, we will determine all possible types of $\mathrm{Aut}(M)/\langle V\rangle$ and their standard defining equations of M. We start with the following proposition.

PROPOSITION 4.1. *Let M be a hyperelliptic curve of genus $g = 2$. Let H be a subgroup of* $\mathrm{Aut}(M)/\langle V\rangle$, *and we consider the exact sequence* $(*)$.

Then H is isomorphic to $\mathbf{C}_n$ $(n = 2,3,4,5,6)$, $\mathbf{D}_{2n}$ $(n = 2,3,4,6)$, $\mathbf{A}_4$ or $\mathbf{S}_4$. And according to each type of H, we can get a standard defining equation of M as in the following list.

$H = \langle$*generators*$\rangle$	*defining equation of M*	$(*)$ *is split* (S) *or not split* (NS)
$\mathbf{C}_2 = \langle S_2\rangle$	$y^2 = (x^2-1)(x^2-a^2)(x^2-b^2)$	S
$\mathbf{C}_2 = \langle S_2\rangle$	$y^2 = x(x^2-1)(x^2-a^2)$	NS
$\mathbf{D}_4 = \langle S_2, \overline{T}\rangle$	$y^2 = x(x^2-1)(x^2-a^2)$	NS
$\mathbf{C}_3 = \langle S_3\rangle$	$y^2 = (x^3-1)(x^3-a^3)$	S
$\mathbf{D}_6 = \langle S_3, \overline{T}\rangle$	$y^2 = (x^3-1)(x^3-a^3)$	S
$\mathbf{C}_4 = \langle S_4\rangle$	$y^2 = x(x^4-1)$	NS
$\mathbf{D}_8 = \langle S_4, T\rangle$	$y^2 = x(x^4-1)$	NS
$\mathbf{A}_4 = \langle U, W\rangle$	$y^2 = x(x^4-1)$	NS
$\mathbf{S}_4 = \langle W, R\rangle$	$y^2 = x(x^4-1)$	NS
$\mathbf{C}_5 = \langle S_5\rangle$	$y^2 = x(x^5-1) \underset{birational}{\sim} y^2 = x^5-1$	S
$\mathbf{C}_6 = \langle S_6\rangle$	$y^2 = (x^6-1)$	S
$\mathbf{D}_{12} = \langle S_6, T\rangle$	$y^2 = (x^6-1)$	NS

where the symbols S_n, T, U, W and R are defined in Appendix, and $\overline{T}$ is defined by $\overline{T}(x) = \dfrac{a}{x}$.

In particular

$$\mathbf{C}_4 \subset \mathrm{Aut}(M)/\langle V\rangle \quad \textit{if and only if} \quad \mathbf{S}_4 = \mathrm{Aut}(M)/\langle V\rangle,$$
$$\mathbf{C}_6 \subset \mathrm{Aut}(M)/\langle V\rangle \quad \textit{if and only if} \quad \mathbf{D}_{12} = \mathrm{Aut}(M)/\langle V\rangle,$$
$$\mathbf{C}_3 \subset \mathrm{Aut}(M)/\langle V\rangle \quad \textit{if and only if} \quad \mathbf{D}_6 \subset \mathrm{Aut}(M)/\langle V\rangle,$$

and
$$\begin{cases} \mathbf{C}_2 \subset \mathrm{Aut}(M)/\langle V\rangle \\ \textit{and } (*) \textit{ is NS} \end{cases} \quad \textit{if and only if} \quad \mathbf{D}_4 \subset \mathrm{Aut}(M)/\langle V\rangle.$$

Proof. H is isomorphic to $\mathbf{C}_n$, $\mathbf{D}_{2n}$, $\mathbf{A}_4$, $\mathbf{S}_4$ or $\mathbf{A}_5$. But, for $g=2$, M is defined by $y^2=(x-a_1)\cdots(x-a_s)$ with $s=5$ or 6, and then $H=\mathbf{S}_4, \mathbf{A}_4, \mathbf{D}_{2n}, \mathbf{C}_n$ $(n\le 6)$ are the only groups which are possibly contained in $\mathrm{Aut}(M)/\langle V\rangle$.

Assume $\mathrm{Aut}(M)/\langle V\rangle \supset H=\mathbf{C}_n$ with $n\le 6$. We may assume that $\mathbf{C}_n$ is generated by the automorphism S_n defined by $S_n^*x=\zeta_n x$ and the set $\mathscr{S}$ defined in §1 contains 1. For example, assume $\mathrm{Aut}(M)/\langle V\rangle \supset \mathbf{C}_2$. Then the decomposition of $\mathscr{S}$ into orbits by $\mathbf{C}_2$ may assume to be $\mathscr{S}=\{\pm 1\}\cup\{\pm a\}\cup\{\pm b\}$ or $\mathscr{S}=\{\infty\}\cup\{0\}\cup\{\pm 1\}\cup\{\pm a\}$. Therefore M is defined by $y^2=(x^2-1)(x^2-a^2)(x^2-b^2)$ or $y^2=x(x^2-1)(x^2-a^2)$, where a, b, 0, ± 1 are distinct. For $n>2$, by the same manner as above, we find that M can be defined by one of the following equations when $\mathrm{Aut}(M)/\langle V\rangle$ contains $H=\mathbf{C}_n$.

(a) $H=\mathbf{C}_2$, $y^2=(x^2-1)(x^2-a^2)(x^2-b^2)$ (0, 1, a^2, b^2 are distinct).
(b) $H=\mathbf{C}_2$, $y^2=x(x^2-1)(x^2-a^2)$ $(a^2\ne 0,1)$.
(c) $H=\mathbf{C}_3$, $y^2=(x^3-1)(x^3-a^3)$ $(a^3\ne 0,1)$.
(d) $H=\mathbf{C}_4$, $y^2=x(x^4-1)$.
(e) $H=\mathbf{C}_5$, $y^2=x(x^5-1)$.
(f) $H=\mathbf{C}_6$, $y^2=(x^6-1)$.

Assume that M is defined by (f). We can see that M has an automorphism T defined by $T^*x=1/x$ and $T^*y=ix^3y$. Then T and S_6 generate $\mathbf{D}_{12}$. Moreover since $\mathbf{D}_{12}\not\subset\mathbf{A}_4$ and $\mathbf{D}_{12}\not\subset\mathbf{S}_4$, we have $\mathrm{Aut}(M)/\langle V\rangle=\mathbf{D}_{12}$. As $\pm 1\in \boldsymbol{P}^1(x)$ are fixed points of T and the order of T is 2, the exact sequence $(*)$ with $H=\mathrm{Aut}(M)/\langle V\rangle=\mathbf{D}_{12}$ is not split by Theorem 2.1.

Assume M is defined by (e). Among four types of groups $\mathbf{S}_4$, $\mathbf{A}_4$, $\mathbf{D}_{2n}$, $\mathbf{C}_n$ $(n\le 6)$, $\mathbf{C}_5$ and $\mathbf{D}_{10}$ are the only groups which contain $\mathbf{C}_5$. Therefore $\mathrm{Aut}(M)/\langle V\rangle$ is isomorphic to $\mathbf{C}_5$ or $\mathbf{D}_{10}$. On the other hand the exponent u_1 (resp. u_3) of (x^5-1) (resp. x) in (e) is equal to 1, and $5u_1+2u_3=7\not\equiv 0 \pmod 2$. Then, from Theorem 3.1, $\mathrm{Aut}(M)/\langle V\rangle$ does not contain $\mathbf{D}_{10}$ and $\mathrm{Aut}(M)/\langle V\rangle=\mathbf{C}_5$. As $\mathscr{S}\cap FP(\langle S_5\rangle)=\{0\}$ and $(5,2)=1$, $(*)$ is split from Theorem 2.1.

Assume M is defined by (d), then, from (13) in Theorem 3.1, $\mathrm{Aut}(M)/\langle V\rangle$

$= \mathbf{S}_4$ and $H = \mathbf{C}_4, \mathbf{D}_8, \mathbf{A}_4$ or $\mathbf{S}_4$. Moreover the exact sequence $(*)$ is not split since H contains S_2 of order 2 and $FP(\langle S_2 \rangle) \cap \mathscr{S} = \{0, \infty\}$.

Assume M is defined by (c). Then M has an automorphism $\bar{T}$ defined by $\bar{T}^*x = a/x$ and $\bar{T}^*y = a^{-3/2}x^3y$, and the group $H_1 = \langle S, \bar{T} \rangle$ is isomorphic to $\mathbf{D}_6$. So we can say that $\mathrm{Aut}(M)/\langle V \rangle$ contains a subgroup $\mathbf{D}_6$ if and only if $\mathrm{Aut}(M)/\langle V \rangle$ contains $\mathbf{C}_3$. Since $FP(H_1) \cap \mathscr{S} = \emptyset$, $(*)$ is split with $H = \langle S, \bar{T} \rangle$.

Assume M is defined by (b). Then M also has an automorphism $\bar{T}$ defined by $\bar{T}^*x = a/x$ and $\bar{T}^*y = a^{-3/2}x^3y$. Therefore $\mathbf{D}_4 \subset \mathrm{Aut}(M)/\langle V \rangle$ if and only if $\mathbf{C}_2 \subset \mathrm{Aut}(M)/\langle V \rangle$. Since $FP(\langle S_2 \rangle) \cap \mathscr{S} = \{0, \infty\}$ and the order of S_2 is 2, $(*)$ is not split by Theorem 2.1. □

By this proposition, we can get the list of $\mathrm{Aut}(M)/\langle V \rangle$ as follows.

THEOREM 4.1. *Let M be a hyperelliptic curve of genus $g = 2$. Assume that* $\mathrm{Aut}(M)/\langle V \rangle$ *is non-trivial. Then* $\mathrm{Aut}(M)/\langle V \rangle$ *is isomorphic to* $\mathbf{C}_2$, $\mathbf{C}_5$, $\mathbf{D}_4$, $\mathbf{D}_6$, $\mathbf{D}_{12}$ *or* $\mathbf{S}_4$. *And according to each type of* $\mathrm{Aut}(M)/\langle V \rangle$, *we can get a standard equation of M as follows.*

Case $\mathrm{Aut}(M)/\langle V \rangle \simeq \mathbf{S}_4$.

M is defined by $$y^2 = x(x^4 - 1). \tag{18}$$

Case $\mathrm{Aut}(M)/\langle V \rangle \simeq \mathbf{C}_5$. $$M : y^2 = x(x^5 - 1) \underset{birational}{\sim} y^2 = x^5 - 1. \tag{19}$$

Case $\mathrm{Aut}(M)/\langle V \rangle \simeq \mathbf{D}_{12}$. $$M : y^2 = (x^6 - 1). \tag{20}$$

Case $\mathrm{Aut}(M)/\langle V \rangle \simeq \mathbf{D}_4$. $$M : y^2 = x(x^2 - 1)(x^2 - a^2) \quad \textit{with } a^2 \neq 0, \pm 1. \tag{21}$$

#-1). *The curve* (21) has $\mathrm{Aut}(M)/\langle V \rangle \simeq \mathbf{S}_4$ if and only if $a^2 = -1$.

Case $\mathrm{Aut}(M)/\langle V \rangle \simeq \mathbf{D}_6$. $$M : y^2 = (x^3 - 1)(x^3 - a^3) \tag{22}$$

with $a^3 \neq \pm 1$ *and* $a^3 \neq \left(\frac{1 \pm \sqrt{3}}{1 \mp \sqrt{3}}\right)^3$.

#-2). *The curve* (22) has $\mathrm{Aut}(M)/\langle V \rangle \simeq \mathbf{D}_{12}$ if and only if $a^3 = -1$.

#-3). $\mathrm{Aut}(M)/\langle V \rangle \simeq \mathbf{S}_4$ if and if $a^3 = \left(\frac{1 \pm \sqrt{3}}{1 \mp \sqrt{3}}\right)^3$.

In fact we can give a birational map F from $M : y^2 = (x^3 - 1)(x^3 - a^3)$ to

$$M' : y^2 = x(x^4 - 1)$$

by the following way.

Let $a_1 = \frac{(1+i)(-1-\sqrt{3})}{2}$ and $a_2 = \frac{(1+i)(-1+\sqrt{3})}{2}$ be fixed points of $W = \frac{1+i}{2}\begin{pmatrix} -1 & i \\ 1 & i \end{pmatrix}$. If $a^3 = \left(\frac{a_1}{a_2}\right)^3 = \left(\frac{1+\sqrt{3}}{1-\sqrt{3}}\right)^3$ (resp. $a^3 = \left(\frac{a_2}{a_1}\right)^3 = \left(\frac{1-\sqrt{3}}{1+\sqrt{3}}\right)^3$), the equalities

$$F^*x = \frac{a_2x - a_1}{x-1}, \quad F^*y = \{a_2(a_2^4 - 1)\}^{1/2}\frac{y}{(x-1)^3} \tag{23}$$

$$(resp.\ F^*x = \frac{a_1x - a_2}{x-1}, F^*y = \{a_1(a_1^4 - 1)\}^{1/2}\frac{y}{(x-1)^3})$$

define a birational map F from M to M'.

Consequently any birational map from M to M' has a form $F \circ \phi = \psi \circ F$ with some $\phi \in \mathrm{Aut}(M)$, $\psi \in \mathrm{Aut}(M')$.

Case $\mathrm{Aut}(M)/\langle V\rangle \simeq \mathbf{C}_2$. $\quad M : y^2 = (x^2-1)(x^2-a^2)(x^2-b^2), \quad (24)$

where a and b satisfy the following three conditions (I), (II) and (III).

(I) For each $\{i,j,k\} = \{-1,0,1\}$, there is no pair (α,η) which satisfies

$$a^2 = \left(\frac{\sqrt{\alpha}+\eta}{\sqrt{\alpha}-\eta}\right)^{2i}\bigg/\left(\frac{\sqrt{\alpha}+\eta}{\sqrt{\alpha}-\eta}\right)^{2k},$$
$$b^2 = \left(\frac{\sqrt{\alpha}+\eta}{\sqrt{\alpha}-\eta}\right)^{2j}\bigg/\left(\frac{\sqrt{\alpha}+\eta}{\sqrt{\alpha}-\eta}\right)^{2k} \quad \text{and} \quad \eta^4 = 1. \tag{25}$$

(II) For each $\{i,j,k\} = \{0,1,2\}$, there is no pair (α,η) which satisfies

$$a^2 = \left(\frac{\sqrt{\alpha}-\zeta_3^i\eta}{\sqrt{\alpha}+\zeta_3^i\eta}\right)^2\bigg/\left(\frac{\sqrt{\alpha}-\zeta_3^k\eta}{\sqrt{\alpha}+\zeta_3^k\eta}\right)^2,$$
$$b^2 = \left(\frac{\sqrt{\alpha}-\zeta_3^j\eta}{\sqrt{\alpha}+\zeta_3^j\eta}\right)^2\bigg/\left(\frac{\sqrt{\alpha}-\zeta_3^k\eta}{\sqrt{\alpha}+\zeta_3^k\eta}\right)^2 \quad \text{and} \quad \eta^6 = 1. \tag{26}$$

(III) $\{1,a^2,b^2\} \neq \{1,\zeta_3,\zeta_3^2\}$.

#-4). Assume there exists α and η which satisfy (25) for some $\{i,j,k\} = \{-1,0,1\}$. Then $\alpha^2 \neq 0,1$, and the equalities

$$F^*x = \frac{\eta\sqrt{\alpha}(x+\delta)}{-x+\delta}, \quad F^*y = (\eta\sqrt{\alpha})^{3/2}(\alpha-\eta^2)\frac{y}{(x-\delta)^3} \tag{27}$$

with $\delta^2 = \left(\frac{\sqrt{\alpha}+\eta}{\sqrt{\alpha}-\eta}\right)^{-2k}$ define a birational map F from M to

$$M' : y^2 = x(x^2-1)(x^2-\alpha^2).$$

Therefore, under the existence of (α, η) satisfying (25),

#-4-i) $\mathrm{Aut}(M)/\langle V\rangle \simeq \mathbf{D}_4$ if and only if $\alpha^2 \neq -1$,
#-4-ii) $\mathrm{Aut}(M)/\langle V\rangle \simeq \mathbf{S}_4$ if and only if $\alpha^2 = -1$.

#-5). Assume there exists α which satisfies (26) for some $\{i, j, k\} = \{0, 1, 2\}$. Then $\alpha^3 \neq 0, 1$, and the equalities

$$F^*x = \frac{\eta\sqrt{\alpha}(x+\delta)}{-x+\delta}, \quad F^*y = (\eta\sqrt{\alpha})^{3/2}(\eta^3 + \sqrt{\alpha}^3)\frac{y}{(x-\delta)^3} \tag{28}$$

with $\delta^2 = \left(\frac{\sqrt{\alpha}-\eta\zeta_3^k}{\sqrt{\alpha}+\eta\zeta_3^k}\right)^{-2}$ define a birational map F from M to

$$M' : y^2 = (x^3 - 1)(x^3 - \alpha^3).$$

Therefore, under the existence of α satisfying (26),

#-5-i) $\mathrm{Aut}(M)/\langle V\rangle \simeq \mathbf{D}_6$ if and only if $\alpha^3 \neq -1$ and $\alpha^3 \neq \frac{(1\pm\sqrt{3})^3}{(1\mp\sqrt{3})^3}$,
#-5-ii) $\mathrm{Aut}(M)/\langle V\rangle \simeq \mathbf{D}_{12}$ if and only if $\alpha^3 = -1$,
#-5-iii) $\mathrm{Aut}(M)/\langle V\rangle \simeq \mathbf{S}_4$ if and only if $\alpha^3 = \frac{(1\pm\sqrt{3})^3}{(1\mp\sqrt{3})^3}$.

#-6). If $\{1, a^2, b^2\} = \{1, \zeta_3, \zeta_3^2\}$, then $\mathrm{Aut}(M)/\langle V\rangle \simeq \mathbf{D}_{12}$.

PROOF. Let $\mathscr{A}$ denote $\mathrm{Aut}(M)/\langle V\rangle$.

Cases $\mathscr{A} \simeq \mathbf{S}_4, \mathbf{C}_5$ and $\mathbf{D}_{12}$. The equations (18), (19), (20) come from Proposition 4.1.

Case $\mathscr{A} \simeq \mathbf{D}_4$. By Proposition 4.1, a curve

$$M : y^2 = x(x^2 - 1)(x^2 - a^2) \quad (a^2 \neq 0, 1)$$

satisfies $\mathbf{D}_4 = \langle S_2, \bar{T}\rangle \subset \mathscr{A}$, where $\bar{T}^*x = a/x$.

If $\mathbf{D}_4 \subsetneq \mathscr{A}$, then, also by Proposition 4.1, $\mathscr{A}$ must be isomorphic to $\mathbf{S}_4$. Now take an element $D \in \mathscr{A}$ of order 4. Then D acts on $\mathscr{S} = \{0, \infty, \pm 1, \pm a\}$ and has two fixed points in $\mathscr{S}$.

First assume $D(a) = a$ and $D(-a) = -a$. Put $J = \begin{pmatrix} 1 & -a \\ 1 & a \end{pmatrix}$. Then JDJ^{-1} fixes $x = 0$ and ∞, we have $(JDJ^{-1})^*x = \pm\sqrt{-1}x$. As JDJ^{-1} acts on $J(\{0, \infty, +1, -1\}) = \left\{\pm 1, \frac{1-a}{1+a}, \left(\frac{1-a}{1+a}\right)^{-1}\right\}$, we have $\sqrt{-1} = \frac{1-a}{1+a}$ or $\left(\frac{1-a}{1+a}\right)^{-1}$ and $a^2 = -1$. Therefore $y^2 = x(x^2-1)(x^2-a^2)$ coincides with (18).

Next assume $D(0) = 0$ and $D(1) = 1$. Put $J = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}$. Then $(JDJ^{-1})^*x = \pm\sqrt{-1}x$ and JDJ^{-1} acts on $J(\{\infty, -1, a, -a\}) = \left\{1, \frac{1}{2}, \frac{a}{a-1}, \frac{a}{a+1}\right\}$. This does not happen.

By checking any other possibilities of fixed points of D in $\mathscr{S}$, we can see that $\mathscr{A} = \mathbf{S}_4$ if and only if $a^2 = -1$.

Case $\mathscr{A} \simeq \mathbf{D}_6$. From Proposition 4.1, the curve

$$M : y^2 = (x^3 - 1)(x^3 - a^3) \quad (a^3 \neq 0, 1)$$

satisfies $\mathbf{D}_6 = \langle S_3, \bar{T} \rangle \subset \mathscr{A}$. If $\mathbf{D}_6 \subsetneq \mathscr{A}$, then $\mathscr{A} \simeq \mathbf{D}_{12}$ or $\mathscr{A} \simeq \mathbf{S}_4$.

Assume $\mathscr{A} \simeq \mathbf{D}_{12}$. By the structure of $\mathbf{D}_{12}$ there exists an element S' of order 6 in $\mathscr{A}$ such that S'^2 coincides with the element $S_3 \in \mathscr{A}$. For $S_3^* x = \zeta_3 x$, $S'^* x = \eta x$ with $\eta^2 = \zeta_3$. As S' acts on $\mathscr{S} = \{1, \zeta_3, \zeta_3^2, a, \zeta_3 a, \zeta_3^2 a\}$, a must be a primitive 6-th root of unity and $\mathscr{S} = \{1, \eta, \dots, \eta^5\}$. So we arrive at #-2).

Assume $\mathscr{A} \simeq \mathbf{S}_4$. Then there is a birational map F from M to

$$M' : y^2 = x(x^4 - 1).$$

Let $\tilde{F} : M/\langle V \rangle \to M'/\langle V \rangle$ be the morphism induced by F. Put $D = \tilde{F} \circ S_3 \circ \tilde{F}^{-1} \in \mathrm{Aut}(M')/\langle V \rangle$. From the structure of $\mathbf{S}_4$, there are 8 elements of order 3 in $\mathbf{S}_4$, and they are represented by matrices $R^t W^s R^{-t}$ $(s = 1, 2, t = 0, 1, 2, 3)$ in $\mathrm{Aut}(M')/\langle V \rangle$ (see Table 1). Assume $D = R^t W^s R^{-t}$. Then D fixes $a_1 \cdot i^t$, and $a_2 \cdot i^t$ with $a_1 = \frac{(1+i)(-1-\sqrt{3})}{2}$ and $a_2 = \frac{(1+i)(-1+\sqrt{3})}{2}$. As $\tilde{F}$ sends fixed points of S_3 to those of D, we have $\tilde{F}(\{0, \infty\}) = \{a_1 \cdot i^t, a_2 \cdot i^t\}$ and then $F^* x = Ax$ with a matrix $A = \begin{pmatrix} a_2 \cdot i^t & \delta \cdot a_1 \cdot i^t \\ 1 & \delta \end{pmatrix}$ or $\begin{pmatrix} a_1 \cdot i^t & \delta \cdot a_2 \cdot i^t \\ 1 & \delta \end{pmatrix}$ (δ is a suitable number).

First we assume $F^* x = Ax = \frac{i^t \cdot a_2 x + \delta i^t \cdot a_1}{x + \delta}$. From $y^2 = x(x^4 - 1)$, we have $(F^* y)^2 = F^* x((F^* x)^4 - 1)$. By further calculations, we have

$$\begin{aligned} F^* x((F^* x)^4 - 1) &= i^t a_2 (a_2^4 - 1)(x + \delta)^{-6} \\ &\quad \times \left\{ \left(x + \delta \frac{a_1}{a_2} \right) \left(x + \delta \frac{a_1 - 1}{a_2 - 1} \right) \left(x + \delta \frac{a_1 - i}{a_2 - i} \right) \right\} \\ &\quad \times \left\{ (x + \delta) \left(x + \delta \frac{a_1 + 1}{a_2 + 1} \right) \left(x + \delta \frac{a_1 + i}{a_2 + i} \right) \right\}. \end{aligned}$$

On the other hand, by direct calculations, we have

$$\frac{a_1 - 1}{a_2 - 1} = \frac{a_1}{a_2} \zeta_3^2, \quad \frac{a_1 + 1}{a_2 + 1} = \zeta_3^2, \quad \frac{a_1 - i}{a_2 - i} = \frac{a_1}{a_2} \zeta_3, \quad \frac{a_1 + i}{a_2 + i} = \zeta_3.$$

Thus the equation $(F^* y)^2 = F^* x((F^* x)^4 - 1)$ is transformed into

$$\{\mathrm{C}(x + \delta)^3 (F^* y)\}^2 = (x^3 + \delta^3) \left(x^3 + \delta^3 \cdot \left(\frac{a_1}{a_2} \right)^3 \right), \tag{29}$$

where $\mathrm{C}^2 = [(i^t a_2)\{(a_2)^4 - 1\}]^{-1}$.

Put $Y := C(x+\delta)^3(F^*y)$, $X := x$. Then $X, Y \in \boldsymbol{C}(M)$ and (29) becomes

$$Y^2 = (X^3+\delta^3)\left(X^3+\delta^3\left(\frac{a_1}{a_2}\right)^3\right). \tag{30}$$

Since $\mathscr{S} = \{1, \zeta_3, \zeta_3^2, a, a\zeta_3, a\zeta_3^2\}$ consists of branch points of the function $X = x \in \boldsymbol{C}(M)$, (30) implies

$$\mathscr{S} = \left\{-\delta, -\delta\zeta_3, -\delta\zeta_3^2, -\delta\left(\frac{a_1}{a_2}\right), -\delta\left(\frac{a_1}{a_2}\right)\zeta_3, -\delta\left(\frac{a_1}{a_2}\right)\zeta_3^2\right\}.$$

Then "$\delta^3 = -1$ and $\delta^3\left(\frac{a_1}{a_2}\right)^3 = -a^3$" or "$\delta^3 = -a^3$ and $\delta^3\left(\frac{a_1}{a_2}\right)^3 = -1$". Therefore $a^3 = \left(\frac{1\pm\sqrt{3}}{1\mp\sqrt{3}}\right)^3$. Using $\begin{pmatrix} a_1 \cdot i' & \delta \cdot a_2 \cdot i' \\ 1 & \delta \end{pmatrix}$ for A, we can get the same result. Therefore $\mathscr{A} \simeq \mathbf{D}_6$ implies $a^3 \neq \left(\frac{1\pm\sqrt{3}}{1\mp\sqrt{3}}\right)^3$.

Conversely, by the same argument as above, we can also see that (23) define a birational morphism when $a^3 = \left(\frac{1\pm\sqrt{3}}{1\mp\sqrt{3}}\right)^3$. Thus we get #-3).

<u>$\mathscr{A} \simeq \mathbf{C}_2$.</u> From Proposition 4.1, the curve

$$M : y^2 = (x^2-1)(x^2-a^2)(x^2-b^2) \tag{31}$$

satisfies $\mathscr{A} \supset \langle S_2 \rangle \simeq \mathbf{C}_2$. If $\mathbf{C}_2 \subsetneq \mathscr{A}$, then $\mathscr{A} = \mathbf{D}_4, \mathbf{D}_6, \mathbf{D}_{12}$ or $\mathbf{S}_4$.

Assume $\mathscr{A} \simeq \mathbf{D}_4 \supset \langle S_2 \rangle$. There is a birational morphism F from M to

$$M' : y^2 = x(x^2-1)(x^2-\alpha^2) \quad (\alpha^2 \neq 0, \pm 1).$$

By Proposition 4.1, $\mathrm{Aut}(M')/\langle V \rangle = \langle S_2, \bar{T} \rangle$ with $\bar{T}^*x = \alpha/x$. Let $\tilde{F} : M/\langle V \rangle \to M'/\langle V \rangle$ be the morphism induced by F. Put $J := \tilde{F} \circ S_2 \circ \tilde{F}^{-1} (\in \mathrm{Aut}(M')/\langle V \rangle)$. Then $\tilde{F}(\mathscr{S}) = \{0, \infty, \pm 1, \pm\alpha\}$ ($\mathscr{S} = \{\pm 1, \pm a, \pm b\}$), and $\tilde{F}$ sends a fixed point of S_2 (on $M/\langle V \rangle$) to a fixed point of J (on $M'/\langle V \rangle$). From the fact that S_2 (on $M/\langle V \rangle$) has no fixed point in $\mathscr{S}$ but S_2 (on $M'/\langle V \rangle$) fixes 0 and ∞ in $\tilde{F}(\mathscr{S})$, we can see $J \neq S_2$ (on $M'/\langle V \rangle$). Therefore $J^*x = \pm\alpha/x$, and $\tilde{F}(\{0, \infty\}) = \{\pm\sqrt{\alpha}\}$ (resp. $\{\pm\sqrt{-1}\sqrt{\alpha}\}$) provided $J^*x = \alpha/x$ (resp. $J^*x = -\alpha/x$). So

$$F^*x = A(x) = \frac{\eta\sqrt{\alpha}x + \delta\eta\sqrt{\alpha}}{-x+\delta}, \quad A := \begin{pmatrix} \eta\sqrt{\alpha} & \delta\eta\sqrt{\alpha} \\ -1 & \delta \end{pmatrix},$$

with suitable numbers δ and η satisfying $\eta^4 = 1$.

The equation $(F^*y)^2 = F^*x((F^*x)^2-1)((F^*x)^2-\alpha^2)$ is transformed as follows.

$$
\begin{aligned}
(F^*y)^2 &= A(x)(A(x)^2-1)(A(x)^2-\alpha^2) \\
&= (\eta\sqrt{\alpha})^3(\alpha-\eta^2)^2(x-\delta)^{-6}(x-\delta)(x+\delta) \\
&\quad \times \left(x+\delta\left(\frac{\eta\sqrt{\alpha}+1}{\eta\sqrt{\alpha}-1}\right)\right)\left(x+\delta\left(\frac{\eta\sqrt{\alpha}-1}{\eta\sqrt{\alpha}+1}\right)\right) \\
&\quad \times \left(x-\delta\left(\frac{\sqrt{\alpha}+\eta}{\sqrt{\alpha}-\eta}\right)\right)\left(x-\delta\left(\frac{\sqrt{\alpha}-\eta}{\sqrt{\alpha}+\eta}\right)\right) \\
&= (\eta\sqrt{\alpha})^3(\alpha-\eta^2)^2(x-\delta)^{-6}(x^2-\delta^2) \\
&\quad \times \left(x^2-\delta^2\left(\frac{\sqrt{\alpha}+\eta}{\sqrt{\alpha}-\eta}\right)^2\right)\left(x^2-\delta^2\left(\frac{\sqrt{\alpha}-\eta}{\sqrt{\alpha}+\eta}\right)^2\right).
\end{aligned}
$$

As $\mathscr{S}$ consists of the branch points of x, we have

$$
\{1, a^2, b^2\} = \left\{\delta^2, \delta^2\left(\frac{\sqrt{\alpha}+\eta}{\sqrt{\alpha}-\eta}\right)^2, \delta^2\left(\frac{\sqrt{\alpha}+\eta}{\sqrt{\alpha}-\eta}\right)^{-2}\right\},
$$

and the pair (α, η) satisfies (25). Thus $\mathscr{A} \not\simeq \mathbf{D}_4$ implies the condition (I).

Conversely assume that there is a pair (α, η) satisfies (25). Since a^2, b^2, 1 are distinct, we can see $\alpha^2 \neq 0, 1$. And (27) gives a birational morphism from M to M' even if $\alpha^2 = -1$. So we get #-4) from (21) and #-1).

Assume $\mathscr{A} \simeq \mathbf{D}_6$. There is a birational map F from M to

$$
M' : y^2 = (x^3-1)(x^3-\alpha^3), \qquad \left(\alpha^3 \neq -1, \left(\frac{1\pm\sqrt{3}}{1\mp\sqrt{3}}\right)^3\right).
$$

Let $\tilde{F}$ be as before. Put $J := \tilde{F}\circ S_2 \circ \tilde{F}^{-1}$. On the other hand, as $\mathrm{Aut}(M')/\langle V\rangle = \langle S_3, \overline{T}\rangle$, $J^*x = \zeta_3^s\alpha/x$ for some $0 \le s \le 2$. Since the fixed points of J are $\pm\zeta_3^{2s}\sqrt{\alpha}$, we have $\tilde{F}(\{0,\infty\}) = \{\zeta_3^{2s}\sqrt{\alpha}, -\zeta_3^{2s}\sqrt{\alpha}\}$ and

$$
F^*x = B(x) = \frac{\eta\sqrt{\alpha}x + \delta\eta\sqrt{\alpha}}{-x+\delta}, \quad B := \begin{pmatrix} \eta\sqrt{\alpha} & \delta\eta\sqrt{\alpha} \\ -1 & \delta \end{pmatrix},
$$

where $\eta = \pm\zeta_3^{2s}$.

The equation $(F^*y)^2 = ((F^*x)^3-1)((F^*x)^3-\alpha^3)$ is transformed as follows.

$$
\begin{aligned}
(F^*y)^2 &= (-x+\delta)^{-6}\eta^3\sqrt{\alpha}^3\{\sqrt{\alpha}^3(x+\delta)^3 - \eta^3(-x+\delta)^3\} \\
&\quad \times \{(\eta^3(x+\delta)^3 - \sqrt{\alpha}^3(-x+\delta)^3\}
\end{aligned}
$$

$$= (-x+\delta)^{-6}\eta^3\sqrt{\alpha}^3$$

$$\times \prod_{t=0}^{2}\{\sqrt{\alpha}(x+\delta) - \zeta_3^t\eta(-x+\delta)\}\prod_{t=0}^{2}\{-\sqrt{\alpha}(-x+\delta) + \zeta_3^t\eta(x+\delta)\}$$

$$= (-x+\delta)^{-6}\eta^3\sqrt{\alpha}^3$$

$$\times \prod_{t=0}^{2}(\sqrt{\alpha}+\zeta_3^t\eta)\left\{x+\delta\left(\frac{\sqrt{\alpha}-\zeta_3^t\eta}{\sqrt{\alpha}+\zeta_3^t\eta}\right)\right\}\prod_{t=0}^{2}(\sqrt{\alpha}+\zeta_3^t\eta)\left\{x-\delta\left(\frac{\sqrt{\alpha}-\zeta_3^t\eta}{\sqrt{\alpha}+\zeta_3^t\eta}\right)\right\}$$

$$= (-x+\delta)^{-6}\eta^3\sqrt{\alpha}^3(\eta^3+\sqrt{\alpha}^3)^2$$

$$\times \left(x^2-\delta^2\left(\frac{\sqrt{\alpha}-\eta}{\sqrt{\alpha}+\eta}\right)^2\right)\left(x^2-\delta^2\left(\frac{\sqrt{\alpha}-\zeta_3\eta}{\sqrt{\alpha}+\zeta_3\eta}\right)^2\right)$$

$$\times \left(x^2-\delta^2\left(\frac{\sqrt{\alpha}-\zeta_3^2\eta}{\sqrt{\alpha}+\zeta_3^2\eta}\right)^2\right).$$

Then we have

$$\{1,a^2,b^2\} = \left\{\delta^2\left(\frac{\sqrt{\alpha}-\eta}{\sqrt{\alpha}+\eta}\right)^2, \delta^2\left(\frac{\sqrt{\alpha}-\zeta_3\eta}{\sqrt{\alpha}+\zeta_3\eta}\right)^2, \delta^2\left(\frac{\sqrt{\alpha}-\zeta_3^2\eta}{\sqrt{\alpha}+\zeta_3^2\eta}\right)^2\right\},$$

and the pair (α,η) satisfies (26). Thus $\mathscr{A} \not\simeq \mathbf{D}_6$ implies the condition (II).

Conversely if there exists α^3 satisfying (26) for some $\{i,j,k\} = \{0,1,2\}$, then $\alpha^3 \neq 0,1$ and the equalities (28) defines a birational map even if $\alpha^3 = -1$ or $\left(\frac{1\pm\sqrt{3}}{1\mp\sqrt{3}}\right)$. Thus we get #-5) from (22), #-2) and #-3).

Next assume $\mathscr{A} \simeq \mathbf{D}_{12}$. There is a birational map F from M to

$$M' : y^2 = (x^6-1).$$

Put $J := \tilde{F}\circ S_2 \circ \tilde{F}^{-1}$ as above. Then $J^*x = \frac{\zeta_6^s}{x}$ $(0 \le s \le 5)$ or $J^*x = -x$ on M'. But when $J^*x = \zeta_6^k/x$, we can follow the same argument in the case of $\mathscr{A} \simeq \mathbf{D}_6$, and we can get the relation (26) with $\alpha^3 = -1$. (28) gives a birational map from M to M' again.

When $J^*x = -x$, the set of fixed points of J is $\{0,\infty\}$. Since $\tilde{F}$ sends $\{0,\infty\}$ (the set of fixed points of S_2) to $\{0,\infty\}$ (the fixed points of J), we have $F^*x = \delta x$ or $F^*x = \delta/x$ for some number δ. At the same time $\tilde{F}$ sends $\{\pm 1, \pm a, \pm b\}$ to $\{\pm 1, \pm\zeta_3, \pm\zeta_3^2\}$, so we know that $\delta = \zeta_3^k$ and $\{1,a^2,b^2\} = \{1,\zeta_3,\zeta_3^2\}$. Thus we get #-6). Overall, we know that $\mathscr{A} \simeq \mathbf{C}_2$ if and only if the three conditions (I), (II) and (III) are satisfied at the same time. □

5 Cyclic Trigonal Curves of Genus 5, 7, 9

Let M be a cyclic trigonal curve defined by

$$y^3 - (x-a_1)^{r_1} \cdots (x-a_s)^{r_s} = 0 \quad (1 \le r_i \le 2,\ a_i\text{'s are distinct}). \tag{32}$$

The genus g of M is $\#\mathscr{S} - 2$. We also assume $g \ge 5$ (i.e., M has unique g_3^1).

In this section we study M with odd g. In particular we will determine all possible types of $\mathrm{Aut}(M)/\langle V \rangle$ and their standard defining equations of M for $g = 5, 7, 9$. We start with the following lemma.

Lemma 5.1. *Assume that the genus g of M is odd. Then*
(i) $\mathrm{Aut}(M)/\langle V \rangle$ *is isomorphic to a cyclic group or a dihedral group,*
(ii) *If* $\mathrm{Aut}(M)/\langle V \rangle \simeq \mathbf{D}_{2n}$, *then n is odd.*

Proof. (i) Assume $\mathbf{A}_4 \subset \mathrm{Aut}(M)/\langle V \rangle$. The equation $\#\mathscr{S} = 4\varepsilon_1 + 6\varepsilon_2 + 4\varepsilon_3 + 12\sum 1$ for $H = \mathbf{A}_4$ in Theorem 3.1 indicates that $\#\mathscr{S}$ and g are even. This is a contradiction. So $\mathbf{A}_4 \not\subset \mathrm{Aut}(M)/\langle V \rangle$, and then $\mathbf{A}_5, \mathbf{S}_4 \not\subset \mathrm{Aut}(M)/\langle V \rangle$.

(ii) The equality $\#\mathscr{S} = n\varepsilon_1 + n\varepsilon_2 + 2\varepsilon_3 + 2n\sum_{i=4}^{d} 1$ for $H = \mathbf{D}_{2n}$ in Theorem 3.1 implies that odd g does not happen for even n. □

Next we will investigate cyclic trigonal curves with $g = 5, 7, 9$.

Theorem 5.1. *Let M be a cyclic trigonal curve* (32) *with $g = 5, 7$ or 9. Assume that* $\mathscr{A} := \mathrm{Aut}(M)/\langle V \rangle$ *is non-trivial. Then the type of $\mathscr{A}$ and a standard defining equation of M are as follows.*

I. $g = 9$.

<u>$\mathscr{A} \simeq \mathbf{C}_{10}$.</u> *$M$ is defined by*

$$y^3 = x(x^{10} - 1)^2, \qquad \text{the exact sequence } (*) \text{ is split.} \tag{33}$$

<u>$\mathscr{A} \simeq \mathbf{C}_9$.</u> $y^3 = x(x^9 - 1)^r$ $(r = 1, 2)$, $(*)$ *is non-split.* (34)

<u>$\mathscr{A} \simeq \mathbf{C}_5$.</u> $y^3 = x(x^5 - 1)^2(x^5 - a^5)^2$ $(a^5 \ne 0, \pm 1)$, $(*)$ *is split.* (35)

♭-1) The curve (35) has $\mathscr{A} \simeq \mathbf{C}_{10}$ if and only if $a^5 = -1$.

<u>$\mathscr{A} \simeq \mathbf{C}_3$.</u> $y^3 = x(x^3 - 1)^{u_3}(x^3 - a^3)^{u_4}(x^3 - b^3)^{u_5}$, $(*)$ is non-split, (36)

where 0, 1, a^3, b^3 are distinct, and a, b, u_3, u_4, u_5 satisfy one of the following two conditions a), b).

a) $u_i \neq u_j$ for some $i, j \in \{3,4,5\}$.
b) b-i) $u_3 = u_4 = u_5$ and b-ii) $\{a^3, b^3\} \neq \{\zeta_3, \zeta_3^2\}$.

$\mathfrak{b}$-2) $\mathscr{A} \simeq \mathbf{C}_9$ if and only if $\{a^3, b^3\} = \{\zeta_3, \zeta_3^2\}$ and $u_3 = u_4 = u_5$ hold. In this case (36) coincides with (34).

$\underline{\mathscr{A} \simeq \mathbf{C}_2.}$ M is defined by

$$y^3 = x(x^2-1)^{u_3}(x^2-a^2)^{u_4}(x^2-b^2)^{u_5}(x^2-c^2)^{u_6}(x^2-d^2)^{u_7}, \quad (*) \text{ is split,} \tag{37}$$

where 0, 1, a^2, b^2, c^2, d^2 are distinct, and a, b, c, d, $u_3, \dots, u_7$ satisfy one of the following two conditions a), b).

a) a-i) $u_3 = \cdots = u_7 = 2$ and a-ii) $\{1, a^2, b^2, c^2, d^2\} \neq \{\zeta_5^k \mid 0 \leq k \leq 4\}$.
b) $u_i = u_j = u_k = 1$, $u_l = u_m = 2$ for some $\{i, j, k, l, m\} = \{3,4,5,6,7\}$.

$\mathfrak{b}$-3) $\mathscr{A} \simeq \mathbf{C}_{10}$ if and only if $u_3 = \cdots = u_7 = 2$ and $\{1, a^2, b^2, c^2, d^2\} = \{\zeta_5^k \mid 0 \leq k \leq 4\}$ hold. In this case (37) coincides with (33).

II. $g = 7$.

$\underline{\mathscr{A} \simeq \mathbf{D}_{18}.}$ M is defined by

$$y^3 = (x^9-1), \quad (*) \text{ is split.} \tag{38}$$

$\underline{\mathscr{A} \simeq \mathbf{C}_8.}$ $y^3 = x(x^8-1)$, $(*)$ is split. (39)

$\underline{\mathscr{A} \simeq \mathbf{D}_{14}.}$ $y^3 = x(x^7-1)$, $(*)$ is split. (40)

$\underline{\mathscr{A} \simeq \mathbf{C}_4.}$ $y^3 = x(x^4-1)(x^4-a^4)$ $(a^4 \neq 0, \pm 1)$, $(*)$ is split. (41)

$\mathfrak{b}$-4) $\mathscr{A} \simeq \mathbf{C}_8$ if and only if $a^4 = -1$. In this case (41) coincides with (39).

$\underline{\mathscr{A} \simeq \mathbf{D}_6.}$

$$y^3 = (x^3-1)(x^6-bx^3+1)^u \quad (\text{“}b \neq \pm 2\text{” and “}u \neq 1 \text{ or } b \neq -1\text{”}), \quad (*) \text{ is split.} \tag{42}$$

$\mathfrak{b}$-5) $\mathscr{A} \simeq \mathbf{D}_{18}$ if and only if $u = 1$ and $b = -1$ hold. And (42) coincides with (38).

$\underline{\mathscr{A} \simeq \mathbf{C}_3.}$ $y^3 = (x^3-1)(x^3-a_1^3)^{v_1}(x^3-a_2^3)^{v_2}$, $(*)$ is split. (43)

Here 1, a_1^3, a_2^3 are distinct, and a_1, a_2, v_1, v_2 satisfy the following three conditions a), b) and c) at once.

a) $a_1^3 a_2^3 \neq 1$ or $v_1 \neq v_2$, b) $a_1^3 \neq a_2^6$ or $v_1 \neq 1$, c) $a_1^6 \neq a_2^3$ or $v_2 \neq 1$.

$\flat$-6) Assume $a_1^3a_2^3 = 1$ and $v_1 = v_2$. Then (43) becomes

$$y^3 = (x^3 - 1)\{x^6 - (a_1^3 + a_2^3)x^3 + 1\}^{v_1}.$$

Therefore

$\flat$-6-i) $\mathscr{A} \simeq \mathbf{D}_6$ if and only if $a_1^3 + a_2^3 \neq -1$ or $v_1 \neq 1$ (in this case (43) becomes (42) with $b = a_1^3 + a_2^3$), and

$\flat$-6-ii) $\mathscr{A} \simeq \mathbf{D}_{18}$ if and only if $a_1^3 + a_2^3 = -1$ and $v_1 = 1$ hold (in this case (43) coincides with (38)).

$\flat$-7) Assume $a_i^3 = a_j^6$ and $v_i = 1$ for $\{i, j\} = \{1, 2\}$. Then there is a birational morphism F from M to

$$M' : y^3 = \{x^6 - (a_j^3 + a_j^{-3})x^3 + 1\}(x^3 - 1)^{v_j}.$$

defined by

$$F^*x = a_j^{-1}x, \quad F^* = a_j^{-2-v_j}x.$$

Therefore

$\flat$-7-i) $\mathscr{A} \simeq \mathbf{D}_6$ if and only if $a_j^3 \neq \zeta_3^{\pm 1}$ or $v_j \neq 1$ (in this case (43) is birational to (42) with $b = a_j^3 + a_j^{-3} (\neq -1)$), and

$\flat$-7-ii) $\mathscr{A} \simeq \mathbf{D}_{18}$ if and only if $a_j^3 = \zeta_3^{\pm 1}$ and $v_j = 1$ hold ((43) is birational to (38)).

<u>$\mathscr{A} \simeq \mathbf{C}_2$.</u>

$$M : y^3 = x(x^2 - 1)^{u_3}(x^2 - c_4^2)^{u_4}(x^2 - c_5^2)^{u_5}(x^2 - c_6^2)^{u_6}, \quad (*) \text{ is split}, \quad (44)$$

where 1, c_4^2, c_5^2, c_6^2 are distinct, and u_3, u_4, u_5, u_6, c_4, c_5, c_6 satisfy one of the following conditions a) or b). Here we put $c_3 := 1$.

a)
- a-i) $u_3 = u_4 = u_5 = u_6 = 1$,
- a-ii) there is no number α satisfying
$$\{c_4^2, c_5^2, c_6^2\} = \{-1, \alpha^2, -\alpha^2\}, \qquad (\star)$$
and
- a-iii) for each $\{i, j, k, l\} = \{3, 4, 5, 6\}$, there is no number α satisfying
$$c_i^2 : c_j^2 : c_k^2 : c_l^2 = 3 : -\left(\frac{\alpha - 1}{\alpha + 1}\right)^2 : -\left(\frac{\zeta_3\alpha - 1}{\zeta_3\alpha + 1}\right)^2 : -\left(\frac{\zeta_3^2\alpha - 1}{\zeta_3^3\alpha + 1}\right)^2. \qquad (\star\star)$$

b)
- b-i) $u_i = 1$, $u_j = u_k = u_l = 2$ with $\{i, j, k, l\} = \{3, 4, 5, 6\}$, and
- b-ii) there is no number α satisfying $(\star\star)$ for the same i, j, k, l in b-i).

$\flat$-8) Assume a-i) and there is α satisfying $(\star)$. Then

$\flat$-8-i) $\mathscr{A} \simeq \mathbf{C}_4$ if and only if $\alpha^4 \neq -1$,

$\flat$-8-ii) $\mathscr{A} \simeq \mathbf{C}_8$ if and only if $\alpha^4 = -1$.

$\flat$-9) Assume a-i) and there is α satisfying ($\star\star$) for some $\{i,j,k,l\} = \{3,4,5,6\}$. Then (44) is birational to

$$M' : y^3 = (x^3-1)\{x^6 - (\alpha^3+\alpha^{-3})x^3 + 1\}.$$

In fact the equalities

$$F^*x = \frac{x+\gamma}{-x+\gamma}, \quad F^*y = 2^{1/3}\alpha^{-1}(1+\alpha^3)^{2/3}y(-x+\gamma)^{-3} \quad \text{with } \gamma = c_i/\sqrt{-3} \tag{45}$$

give a birational morphism from M to M'. And then

$\flat$-9-i) $\mathscr{A} \simeq \mathbf{D}_6$ if and only if $\alpha^3 \neq \zeta_3^{\pm 1}$,
$\flat$-9-ii) $\mathscr{A} \simeq \mathbf{D}_{18}$ if and only if $\alpha^3 = \zeta_3^{\pm 1}$.

$\flat$-10) Assume b-i) for some $\{i,j,k,l\} = \{3,4,5,6\}$.

Then $\mathscr{A} = \mathbf{D}_6$ if and only if there is a number α satisfying ($\star\star$) for the i, j, k, l in b-i). And (44) becomes birational to

$$y^3 = x(x^3-1)\{x^6 - (\alpha^3+\alpha^{-3})x^3 + 1\}^2.$$

In fact the equalities

$$F^*x = \frac{x+\gamma}{-x+\gamma}, \quad F^*y = 2^{1/3}\alpha^{-2}(1+\alpha^3)^{4/3}y(-x+\gamma)^{-5} \quad \text{with } \gamma = c_i/\sqrt{-3} \tag{46}$$

give a birational morphism from M to M'.

III. $g = 5$

<u>$\mathscr{A} \simeq \mathbf{D}_{10}$.</u>

$$M : y^3 = x^2(x^5-1), \quad (*) \text{ is split.}$$

<u>$\mathscr{A} \simeq \mathbf{C}_2$.</u>

$$M : y^3 = x(x^2-1)^{u_3}(x^2-c_4^2)^{u_4}(x^2-c_5^2)^{u_5}, \quad (*) \text{ is split,}$$

where $u_i = 2$, $u_j = u_k = 1$ for $\{i,j,k\} = \{3,4,5\}$, and $\{c_j^2, c_k^2\} \neq \left\{c_i^2\left(\frac{1-\zeta_5}{1+\zeta_5}\right)^2, c_i^2\left(\frac{1-\zeta_5^2}{1+\zeta_5^2}\right)\right\}$. Here we denote $c_3 = 1$.

$\flat$-11) If $u_i = 2$, $u_j = u_k = 1$ and $\{c_j^2, c_k^2\} = \left\{c_i^2\left(\frac{1-\zeta_5}{1+\zeta_5}\right)^2, c_i^2\left(\frac{1-\zeta_5^2}{1+\zeta_5^2}\right)\right\}$, then M is birational to $M' : y^3 = x^2(x^5-1)$ and $\mathscr{A} \simeq \mathbf{D}_{10}$.

In fact

$$F^*x = \frac{x+c_i}{-x+c_i}, \quad F^*y = \sqrt{2}y(-x+c_i)^{-3} \tag{47}$$

give a birational morphism from M to M'.

Proof. Assume $\mathscr{A} \supset \mathbf{C}_n$ with $n \geq 2$. Then, from Theorem 3.1, M can be defined by

$$y^3 = 1^{u_1} x^{u_2} \prod_{i=3}^{d} (x^n - b_i)^{u_i}, \quad \mathscr{A} \supset \mathbf{C}_n = \langle S_n \rangle, \tag{48}$$

$$\begin{cases} \text{(48-I)} \quad \#\mathscr{S} = \varepsilon_1 + \varepsilon_2 + n \sum_{i=3}^{d} 1, \\ \text{(48-II)} \quad u_1 + u_2 + n \sum_{i=3}^{d} u_i \equiv 0 \pmod 3, \end{cases}$$

where 0 and b_i $(3 \leq i \leq d)$ are distinct, $0 \leq u_1, u_2 < 3$, $u_i = 1, 2$ $(i \geq 3)$, and $\varepsilon_k = 1$ (resp. $\varepsilon_k = 0$) if $u_k > 0$ (resp. $u_k = 0$) $(k = 1, 2)$.

<u>$g = 9$.</u>

Then $\#\mathscr{S} = 11$. For $n = 8, 7, 6, 4$ and $n \geq 12$, there are no ε_i $(i = 1, 2)$ or d, which satisfy (48-I) with $\#\mathscr{S} = 11$. When $n = 11$, $\varepsilon_1 = \varepsilon_2 = 0$ and $d = 3$ satisfy (48-I) with $\#\mathscr{S} = 11$. Therefore $u_1 = u_2 = 0$ and $u_3 = 1$ or 2. But they do not satisfy (48-II). Thus a number n satisfying $\mathscr{A} \supset \mathbf{C}_n$ is among 10, 9, 5, 3, 2. Moreover Lemma 5.1 implies that only $\mathbf{D}_6$, $\mathbf{D}_{10}$, $\mathbf{D}_{18}$ are candidates for $\mathscr{A}$ among dihedral groups.

<u>Case $\mathscr{A} \supset \mathbf{C}_{10}$.</u> From (48-I), we have $d = 3$ and $\varepsilon_1 + \varepsilon_2 = 1$. And then (48-II) holds if and only if "$u_1 = 2$, $u_2 = 0$, $u_3 = 1$", "$u_1 = 0$, $u_2 = 2$, $u_3 = 1$", "$u_1 = 1$, $u_2 = 0$, $u_3 = 2$" or "$u_1 = 0$, $u_2 = 1$, $u_3 = 2$". These solutions define one curve up to birational morphisms. That is

$$y^3 = x(x^{10} - 1)^2, \quad \mathscr{A} \supset \mathbf{C}_{10} = \langle S_{10} \rangle.$$

By Lemma 5.1, we have $\mathscr{A} \simeq \mathbf{C}_{10}$.

<u>Case $\mathscr{A} \supset \mathbf{C}_9$.</u> We have $d = 3$ and $\varepsilon_1 = \varepsilon_2 = 1$. (48-II) holds if and only if "$u_1 = 1$, $u_2 = 2$" or "$u_1 = 2$, $u_2 = 1$". Then M is defined by

$$y^3 = x(x^9 - 1)^r, \quad \mathscr{A} \supset \mathbf{C}_9 = \langle S_9 \rangle, \quad \text{with } r = 1, 2 \tag{49}$$

up to birational morphisms. From Lemma 5.1, we have $\mathscr{A} \simeq \mathbf{C}_9$ or $\mathbf{D}_{18}$.

Assume $\mathscr{A} \simeq \mathbf{D}_{18}$. Let $\mathscr{A} = \langle S_9, T' \rangle$ with $T'^2 = 1$ and $T' S_9 T'^{-1} = S_9^{-1}$. Then $T'(0) = \infty$ and $T'^* x = \alpha / x$ with some number α. But, since $2 + 9r \not\equiv 0 \pmod 3$, there does not exist an automorphism of M which induces T'. Thus $\mathscr{A} \supset \mathbf{C}_9$ means $\mathscr{A} \simeq \mathbf{C}_9$.

Case $\mathscr{A} \supset \mathbf{C}_5$. Then $d = 4$ and $\varepsilon_1 + \varepsilon_2 = 1$. (48-II) holds if and only if "$u_1 = 2$ (resp. 0), $u_2 = 0$ (resp. 2) and $u_3 = u_4 = 1$" or "$u_1 = 1$ (resp. 0), $u_2 = 0$ (resp. 1) and $u_3 = u_4 = 2$". Then M is defined by

$$y^3 = x(x^5 - 1)^2(x^5 - a^5)^2, \quad \mathscr{A} \supset \mathbf{C}_5 = \langle S_5 \rangle \tag{50}$$

up to birational morphisms. If $\mathscr{A} \supsetneqq \mathbf{C}_5$, then $\mathscr{A} \simeq \mathbf{C}_{10}$ or $\mathbf{D}_{10}$.

When $\mathscr{A} \simeq \mathbf{C}_{10}$, there is an element $S' \in \mathscr{A}$ such that $S'^2 = S_5$. Necessarily $S'^*x = \eta x$ holds with a primitive 10-th root η of 1, and then $a^5 = -1$.

When $\mathscr{A} \simeq \mathbf{D}_{10}$, $\mathscr{A} = \langle S_5, T' \rangle$ with $T'^2 = 1$ and $T' S_5 T'^{-1} = S_5^{-1}$. By the same argument as in Case $\mathscr{A} \supset \mathbf{C}_9$, we can deduce a contradiction from $2 \cdot 1 + 2 \cdot 5 + 2 \cdot 5 \not\equiv 0 \pmod 3$. So $\mathscr{A} \simeq \mathbf{D}_{10}$ does not happen. Thus we get b-1).

Case $\mathscr{A} \supset \mathbf{C}_3$. Then $d = 5$ and $\varepsilon_1 = \varepsilon_2 = 1$. (48-II) holds if and only if "$u_1 + u_2 = 3$". Therefore M is defined by

$$y^3 = x(x^3 - 1)^{u_3}(x^3 - a^3)^{u_4}(x^3 - b^3)^{u_5}, \quad \mathscr{A} \supset \mathbf{C}_3 = \langle S_3 \rangle. \tag{51}$$

If $\mathscr{A} \supsetneqq \mathbf{C}_3$, then $\mathscr{A} \simeq \mathbf{C}_9, \mathbf{D}_6$ or $\mathbf{D}_{18}$. The case $\mathscr{A} \simeq \mathbf{D}_{18}$ has already been eliminated when we considered the case $\mathscr{A} \supset \mathbf{C}_9$.

Assume $\mathscr{A} \simeq \mathbf{D}_6$. Let $\mathscr{A} = \langle S_3, T' \rangle$ with $T'^2 = 1$, and $T' S_3 T'^{-1} = S_3^2$. Then, by the same argument as in Case $\mathscr{A} \supset \mathbf{C}_9$, we can deduce a contradiction.

Assume $\mathscr{A} \simeq \mathbf{C}_9$. There exists $S' \in \mathscr{A}$ such that $S'^3 = S_3$. Then $S'^*x = \eta x$ with a primitive 9-th root of 1, and we can see that $u_3 = u_4 = u_5$ and $\{a^3, b^3\} = \{\zeta_3, \zeta_3^2\}$. Then (51) coincides with (34). Thus we get b-2).

Case $\mathscr{A} \supset \mathbf{C}_2$. Then $d = 7$ and $\varepsilon_1 + \varepsilon_2 = 1$. (48-II) holds if and only if

1) $u_1 = 0$ (resp. 1), $u_2 = 1$ (resp. 0), $u_3 = \cdots = u_7 = 2$,
2) $u_1 = 0$ (resp. 2), $u_2 = 2$ (resp. 0), $u_3 = \cdots = u_7 = 1$,
3) $u_1 = 0$ (resp. 1), $u_2 = 1$ (resp. 0), $u_i = u_j = u_k = 1$, $u_l = u_m = 2$ with $\{i, j, k, l, m\} = \{3, 4, 5, 6, 7\}$,

or

4) $u_1 = 0$ (resp. 2), $u_2 = 2$ (resp. 0), $u_i = u_j = u_k = 2$, $u_l = u_m = 1$ with $\{i, j, k, l, m\} = \{3, 4, 5, 6, 7\}$.

Therefore, up to birational isomorphisms, we have two types of equations with $\mathscr{A} \supset \mathbf{C}_2 = \langle \zeta_2 \rangle$. That is:

$y^3 = x(x^2-1)^2(x^2-a)^2(x^2-b)^2(x^2-c)^2(x^2-d)^2$ (from 1) and 2))

$y^3 = x(x^2-1)^{u_3}(x^2-a^2)^{u_4}(x^2-b^2)^{u_5}(x^2-c^2)^{u_6}(x^2-d^2)^{u_7}$

with $u_i = u_j = u_k = 1$, $u_l = u_m = 2$ for $\{i,j,k,l,m\} = \{3,4,5,6,7\}$.

(from 3) and 4)).

Assume $\mathscr{A} \supsetneqq \mathbf{C}_2$. The possibility of $\mathscr{A} \simeq \mathbf{D}_6, \mathbf{D}_{10}$ or $\mathbf{D}_{18}$ has already been eliminated when we considered $\mathscr{A} \supsetneqq \mathbf{C}_3, \mathbf{C}_5$. Then $\mathscr{A} \simeq \mathbf{C}_{10}$. By the same way as in Case $\mathscr{A} \supset \mathbf{C}_9$, we know $\{1, a^2, b^2, c^2, d^2\} = \{\zeta_5^k \mid 1 \le k \le 5\}$ and $u_3 = \cdots = u_7$. Thus we get b-3).

<u>g = 7.</u>

Then $\#\mathscr{S} = 9$. For $n = 6, 5$ and $n \ge 10$, there are no ε_i $(i = 1,2)$ or d, which satisfy (48-I) with $\#\mathscr{S} = 9$. Thus a number n satisfying $\mathscr{A} \supset \mathbf{C}_n$ is among 9, 8, 7, 4, 3, 2. Moreover, by Lemma 5.1, only $\mathbf{D}_{18}$, $\mathbf{D}_{14}$, $\mathbf{D}_6$, among dihedral groups, are candidates for $\mathscr{A}$.

<u>Case $\mathscr{A} \supset \mathbf{C}_9$.</u> Then $M : y^3 = (x^9 - 1)$ and $\mathscr{A} \simeq \mathbf{D}_{18}$.

<u>Case $\mathscr{A} \supset \mathbf{C}_8$.</u> Then $M : y^3 = x(x^8 - 1)$ and $\mathscr{A} \simeq \mathbf{C}_8$.

<u>Case $\mathscr{A} \supset \mathbf{C}_7$.</u> Then $M : y^3 = x(x^7 - 1)$ and $\mathscr{A} \simeq \mathbf{D}_{14}$.

<u>Case $\mathscr{A} \supset \mathbf{C}_4$.</u> Then $M : y^3 = x(x^4-1)(x^4-a^4)$. If $\mathscr{A} \supsetneqq \mathbf{C}_4$, we have $\mathscr{A} \simeq \mathbf{C}_8$. By the same way as in Case $\mathscr{A} \supset \mathbf{C}_5$ of $g = 9$, we have $a^4 = -1$. Then we get b-4).

<u>Case $\mathscr{A} \supset \mathbf{D}_6$.</u> Then, from (10) in Theorem 3.1, M can be defined by

$$y^3 = (x^3-1)(x^6 - bx^3 + 1)^u \ (b \ne \pm 2), \quad \mathscr{A} \supset \mathbf{D}_6 = \langle S_3, T \rangle.$$

If $\mathscr{A} \supsetneqq \mathbf{D}_6$, $\mathscr{A} \simeq \mathbf{D}_{18}$. There is an element $S' \in \mathscr{A}$ satisfying $S'^3 = S_3$. Then $S'^* x = \eta x$ with a primitive 9-th root η of 1. Thus $\mathscr{S} = \{\zeta_9^k \mid 0 \le k \le 8\}$, $b = -1$ and $u = 1$. Then we get b-5).

<u>Case $\mathscr{A} \supset \mathbf{C}_3$.</u> We have

$$y^3 = (x^3-1)(x^3-a_1^3)^{v_1}(x^3-a_2^3)^{v_2}, \quad \mathscr{A} \supset \mathbf{C}_3 = \langle S_3 \rangle. \tag{52}$$

If $\mathscr{A} \supsetneqq \mathbf{C}_3$, then $\mathscr{A} \simeq \mathbf{D}_6$ or $\mathscr{A} \simeq \mathbf{D}_{18}$.

Assume $\mathscr{A} \supset \mathbf{D}_6 = \langle S_3, T' \rangle$ with $T'^2 = 1$ and $T' S_3 T'^{-1} = S_3^2$.

Put $H = \{\zeta_3^k \mid 0 \le k \le 2\}$, $H_1 = \{a_1 \zeta_3^k \mid 0 \le k \le 2\}$, $H_2 = \{a_2 \zeta_3^k \mid 0 \le k \le 2\}$ and $\mathscr{H} = \{H, H_1, H_2\}$. Then T' acts on $\mathscr{H}$, and T' fixes exactly one element in $\mathscr{H}$ because T' is of order 2 and it has just two fixed points. For example,

$T'H = H_i$ and $T'H_j = H_j$ with $\{i,j\} = \{1,2\}$. From $T'H = H_i$ and $T'(0) = \infty$, $T'^*x = (\zeta_3^k a_i)/x$ $(0 \le k \le 2)$ and $v_i = 1$. $T'H_j = H_j$ implies that T' has a fixed point in H_j, and then we need $a_i^3 = a_j^6$. Thus (52) becomes

$$M : y^3 = \{x^6 - (a_i^3 + 1)x^3 + a_i^3\}(x^3 - a_j^3)^{v_j} \quad \text{with } a_i^3 = a_j^6. \tag{53}$$

Moreover $F^*x = a_j^{-1}x$ and $F^*y = a_j^{-2-v_j}y$ define a birational morphism from M to

$$M' : y^3 = \{x^6 - (a_j^3 + a_j^{-3})x^3 + 1\}(x^3 - 1)^{v_j}.$$

From (42) and $\flat$-5), we get $\flat$-7).

In case $T'H = H$ we obtain $\flat$-6).

<u>Case $\mathscr{A} \supset \mathbf{C}_2$.</u> M is defined by

$$y^3 = x(x^2 - 1)^{u_3}(x^2 - c_4^2)^{u_4}(x^2 - c_5^2)^{u_5}(x^2 - c_6^2)^{u_6}, \quad \mathscr{A} \supset \mathbf{C}_2 = \langle S_2 \rangle$$

$$\text{with } \begin{cases} \text{a-i) } u_3 = u_4 = u_5 = u_6 = 1, \text{ or} \\ \text{b-i) } u_i = 1,\ u_j = u_k = u_l = 2 \quad \text{for } \{i,j,k,l\} = \{3,4,5,6\}. \end{cases}$$

If $\mathscr{A} \supsetneqq \mathbf{C}_2$, then $\mathscr{A} \simeq \mathbf{C}_4, \mathbf{C}_8, \mathbf{D}_6, \mathbf{D}_{14}$ or $\mathbf{D}_{18}$. But the possibility of $\mathbf{D}_{18}$ has been eliminated.

Assume that $\mathscr{A} \simeq \mathbf{C}_4$ (resp. $\mathbf{C}_8$). By the same argument as in Case $\mathscr{A} \supset \mathbf{C}_5$ of $g = 9$, we can see $\mathscr{A} = \langle S_4 \rangle$ (resp. $\langle S_8 \rangle$). Thus we get $\flat$-8).

Assume $\mathscr{A} \simeq \mathbf{D}_6$. From (42), there exists a birational map F from M to

$$M' : y^3 = (x^3 - 1)(x^6 - bx^3 + 1)^u \quad (b \ne \pm 2 \text{ and "} u \ne 1 \text{ or } b \ne -1\text{"}). \tag{54}$$

Let $\tilde{F}$ denote the induced morphism as before, and put $T' = \tilde{F} \circ S_2 \circ \tilde{F}^{-1} \in \mathrm{Aut}(M')/\langle V \rangle = \langle T, S_3 \rangle$. Then $T'^*x = \zeta_3^e/x$ for some $0 \le e \le 2$. Let

$$\mathscr{S}' := \{1, \zeta_3, \zeta_3^2, \alpha, \alpha\zeta_3, \alpha\zeta_3^2, \alpha^{-1}, \alpha^{-1}\zeta_3, \alpha^{-1}\zeta_3^2\}$$

with a root α of the equation $x^6 - bx^3 + 1 = 0$. As $b \ne \pm 2$ and then $\alpha^3 \ne \pm 1$, T' has only one fixed point ζ_3^{2e} $(0 \le e \le 2)$ in $\mathscr{S}'$. On the other hand S_2 has only one fixed point 0 in $\mathscr{S}$ on M. Since $\tilde{F}$ sends $\{0, \infty\}$ (fixed points of S_2) and $\mathscr{S}$ to $\{\pm\zeta_3^{2e}\}$ (fixed points of T') and $\mathscr{S}'$ respectively, we have $\tilde{F}(0) = \zeta_3^{2e}$, $\tilde{F}(\infty) = -\zeta_3^{2e}$ and

$$F^*x = Ax \quad \text{with } A = \begin{pmatrix} \zeta_3^{2e} & \gamma\zeta_3^{2e} \\ -1 & \gamma \end{pmatrix} \quad (\gamma\text{: a suitable number}).$$

Since $\tilde{F}$ also sends the orbit decomposition of $\mathscr{S}$ by $\langle S_2 \rangle$ to that of $\mathscr{S}'$ by $\langle T' \rangle$, we have

$$\{A^{-1}(\zeta_3^{2f}), A^{-1}(\zeta_3^{2g})\} = \{c_i, -c_i\}, \quad \{A^{-1}\alpha, A^{-1}(\alpha^{-1})\} = \{c_j, -c_j\},$$

$$\{A^{-1}(\zeta_3\alpha), A^{-1}(\zeta_3^2\alpha^{-1})\} = \{c_k, -c_k\}, \quad \{A(\zeta_3\alpha), A(\zeta_3^2\alpha^{-1})\} = \{c_l, -c_l\},$$

where $\{f, g\} = \{0, 1, 2\} - \{e\}$, $\{i, j, k, l\} = \{3, 4, 5, 6\}$, and we denote $c_3 = 1$. From these relations, we have $\gamma^2 = \left(\frac{\zeta_3^{(e-g)}+1}{\zeta_3^{(e-g)}-1}\right)^2 c_i^2 = -c_i^2/3$ and

$$c_i^2 : c_j^2 : c_k^2 : c_l^2 = 3 : -\left(\frac{\alpha - \zeta_3^{2e}}{\alpha + \zeta_3^{2e}}\right)^2 : -\left(\frac{\zeta_3\alpha - \zeta_3^{2e}}{\zeta_3\alpha + \zeta_3^{2e}}\right)^2 : -\left(\frac{\zeta_3^2\alpha - \zeta_3^{2e}}{\zeta_3^2\alpha + \zeta_3^{2e}}\right)^2.$$

By permuting j, k, l suitably, we get the relation ($\star\star$).

Conversely we assume that there exists α satisfying ($\star\star$) for some $\{i, j, k, l\} = \{1, 2, 3, 4\}$.

When a-i) is satisfied, $\alpha^3 \neq \zeta_3^{\pm 1}$ or $\alpha^3 = \zeta_3^{\pm 1}$, we can see that (45) defines birational morphism from M to

$$M' : y^3 = (x^3 - 1)\{x^6 - (\alpha^3 + \alpha^{-3})x^3 + 1\}$$

by direct calculations. Then, from (42) and ♭-5), $\mathscr{A} \simeq \mathbf{D}_6$ (resp. $\mathscr{A} \simeq \mathbf{D}_{18}$) provided $\alpha^3 \neq \zeta_3^{\pm 1}$ (resp. $\alpha^3 = \zeta_3^{\pm 1}$). Thus we get ♭-9).

When b-i) is satisfied with the same i, j, k, l in the relation ($\star\star$), we can check that (46) gives a birational morphism from M to

$$M' : y^3 = (x^3 - 1)\{x^6 - (\alpha^3 + \alpha^{-1})x^3 + 1\}^2.$$

Thus we get ♭-10).

$\underline{\mathbf{g = 5}}$.

Then $\#\mathscr{S} = 7$. For $n = 4, 3$ and $n \geq 6$, there are no ε_i $(i = 1, 2)$ and d satisfying (48-I, II) with $\#\mathscr{S} = 7$. Thus non-trivial $\mathscr{A}$ is possibly isomorphic to $\mathbf{C}_2$, $\mathbf{C}_5$ or $\mathbf{D}_{10}$.

Case $\mathscr{A} \supset \mathbf{C}_5 = \langle S_5 \rangle$. Then M is defined by $y^3 = x^2(x^5 - 1)$. Moreover we can see $\mathscr{A} = \mathbf{D}_{10} = \{S_5, T\}$.

Case $\mathscr{A} \supset \mathbf{C}_2 = \langle S_2 \rangle$. Then M is defined by

$$M : y^3 = x(x^2 - 1)^{u_3}(x^2 - c_3^2)^{u_4}(x^2 - c_2^2)^{u_5},$$

where $u_i = 2$, $u_j = u_k = 1$ for $\{i, j, k\} = \{3, 4, 5\}$.

Assume $\mathscr{A} \supsetneq \mathbf{C}_2$. Then $\mathscr{A} \simeq \mathbf{D}_{10}$. Let F be a birational morphism from M to

$$M' : y^3 = x^2(x^5 - 1).$$

Put $J := \tilde{F} \circ S_2 \circ \tilde{F}^{-1}$ as before. Then $J^*x = \zeta_5^k/x$ $(0 \leq k \leq 4)$ and J fixes $\pm\zeta_5^{3k}$. Only 0 is fixed by S_2 in $\mathscr{S} = \{0, \pm c_3, \pm c_4, \pm c_5\}$, and only ζ_5^{3k} is fixed by J in

$\mathscr{S}' = \{0, \infty, 1, \zeta_3, \dots, \zeta_3^4\}$. Therefore $\tilde{F}(0) = \zeta_5^{3k}$, $\tilde{F}(\infty) = -\zeta_5^{3k}$ and

$$F^*x = \frac{\zeta_5^{3k}x + \delta\zeta_5^{3k}}{-x+\delta} \quad \text{(with a suitable number } \delta).$$

By the same calculations as before, we have

$$(F^*x)^2((F^*x)^5 - 1) = 2\zeta_5^k(-x+\delta)^{-9}x(x^2-\delta^2)^2$$
$$\times \left\{x^2 - \delta^2\left(\frac{1-\zeta_5}{1+\zeta_5}\right)^2\right\}\left\{x^2 - \delta^2\left(\frac{1-\zeta_5^2}{1+\zeta_5^2}\right)^2\right\}. \tag{55}$$

Then $\{c_3^2, c_4^2, c_5^2\} = \left\{\delta^2, \delta^2\left(\frac{1-\zeta_5}{1+\zeta_5}\right)^2, \delta^2\left(\frac{1-\zeta_5^2}{1+\zeta_5^2}\right)^2\right\}$. As $u_i = 2$ and $u_j = u_k = 1$, we can see $\delta^2 = c_i$ and $\{c_j^2, c_k^2\} = \left\{c_i^2\left(\frac{1-\zeta_5}{1+\zeta_5}\right)^2, c_i^2\left(\frac{1-\zeta_5^2}{1+\zeta_5^2}\right)^2\right\}$ from (55).

Conversely we can check that (47) defines a birational morphism from M to M'. Overall we proved $\flat$-11). □

Appendix

Here S_n, T, U, W, R, K, Z are elements of $SL_2(\boldsymbol{C})$ defined by $S_n = \begin{pmatrix}\zeta_{2n} & 0\\ 0 & \zeta_{2n}^{-1}\end{pmatrix}$, $T = \begin{pmatrix}0 & i\\ i & 0\end{pmatrix}$, $U = \frac{1-i}{2}\begin{pmatrix}i & -i\\ 1 & 1\end{pmatrix}$, $W = \frac{1+i}{2}\begin{pmatrix}-1 & i\\ 1 & i\end{pmatrix}$, $R = \begin{pmatrix}\frac{1+i}{\sqrt{2}} & 0\\ 0 & \frac{1-i}{\sqrt{2}}\end{pmatrix}$, $Z = \zeta_{10}^{-1}\begin{pmatrix}\zeta_5 & 0\\ 0 & 1\end{pmatrix}$, $K = \frac{1}{\sqrt{5}}\begin{pmatrix}\zeta_5^4-\zeta_5^3 & \zeta_5^3-1\\ 1-\zeta_5^2 & \zeta_5-\zeta_5^2\end{pmatrix}$. And the symbol $\begin{Bmatrix}n_1 & n_2 & \cdots\\ \alpha_1 & \alpha_2 & \cdots\end{Bmatrix}$ means that $\tilde{\pi}$ is ramified over α_i with ramification index n_i.

Table 1: Finite subgroups of Aut($\boldsymbol{P}^1$).

group H [$\#H$]	$f_1(x)/f_0(x)$, $\begin{Bmatrix}\text{ramification indeces}\\ \text{branch points}\end{Bmatrix}$	generators $A = \begin{pmatrix}a & b\\ c & d\end{pmatrix}$ ($\in SL(2,\boldsymbol{C})/\{\pm 1\}$)
cyclic $\mathbf{C}_n$, [n]	$\frac{x^n}{1}$, $\begin{Bmatrix}n & n\\ 0 & \infty\end{Bmatrix}$	S_n
dihedral $\mathbf{D}_{2n}$, [$2n$]	$\frac{x^{2n}+1}{x^n}$, $\begin{Bmatrix}2 & 2 & n\\ -2 & 2 & \infty\end{Bmatrix}$	S_n, T
tetrahedral $\mathbf{A}_4$, [12]	$\frac{(x^4-2\sqrt{3}ix^2+1)^3}{(x^4+2\sqrt{3}ix^2+1)^3}$, $\begin{Bmatrix}3 & 2 & 3\\ 0 & 1 & \infty\end{Bmatrix}$	U, W
octahedral $\mathbf{S}_4$, [24]	$\frac{(x^8+14x^4+1)^3}{108x^4(x^4-1)^4}$, $\begin{Bmatrix}3 & 3 & 4\\ 0 & 1 & \infty\end{Bmatrix}$	W, R
icosahedral $\mathbf{A}_5$, [60]	$\frac{\{-x^{20}-1+228(x^{15}-x^5)-494x^{10}\}^3}{1728x^5(x^{10}+11x^5-1)^5}$, $\begin{Bmatrix}3 & 2 & 5\\ 0 & 1 & \infty\end{Bmatrix}$	K, Z

Table 2: Types of $P_{(b_0:b_1)}$.

group	$(b_0 : b_1) \in \boldsymbol{P}^1(u)$	ramification index over $(b_0 : b_1)$	$P_{(b_0:b_1)}$	type of $P_{(b_0:b_1)}$
$\mathbf{C}_n$	$(0:1)$	n	$P_{(0:1)} = 1$	(iii)
	$(1:0)$	n	$P_{(1:0)} = x$	(ii)
	$(1:b)$ $(b \neq 0)$	1	$P_{(1:b)} = x^n - b$	(i)
$\mathbf{D}_{2n}$	$(1:2)$	2	$P_{(1:2)} = x^n - 1$	(i)
	$(1:-2)$	2	$P_{(1:-2)} = x^n + 1$	(i)
	$(0:1)$	n	$P_{(0:1)} = x$	(ii)
	$(1:b)$ $(b \neq \pm 2)$	1	$P_{(1:b)} = x^{2n} - bx^n + 1$	(i)
$\mathbf{A}_4$	$(1:0)$	3	$P_{(1:0)} = (x^4 - 2\sqrt{3}ix^2 + 1)$	(i)
	$(1:1)$	2	$P_{(1:1)} = x(x^4 - 1)$	(ii)
	$(0:1)$	3	$P_{(0:1)} = (x^4 + 2\sqrt{3}ix^2 + 1)$	(i)
	$(1:b)$ $(b \neq 0, 1)$	1	$P_{(1:b)} = \frac{1}{1-b}\{(x^4 - 2\sqrt{3}ix^2 + 1)^3 - b(x^4 + 2\sqrt{3}ix^2 + 1)^3\}$	(i)
$\mathbf{S}_4$	$(1:0)$	3	$P_{(1:0)} = x^8 + 14x^4 + 1$	(i)
	$(1:1)$	2	$P_{(1:1)} = x^{12} - 33x^8 - 33x^4 + 1$	(i)
	$(0:1)$	4	$P_{(0:1)} = x(x^4 - 1)$	(ii)
	$(1:b)$ $(b \neq 0, 1)$	1	$P_{(1:b)} = (x^8 + 14x^4 + 1)^3 - 108b\{x(x^4 - 1)\}^4$	(i)
$\mathbf{A}_5$	$(1:0)$	3	$P_{(1:0)} = x^{20} + 1 + 228(x^{15} - x^5) + 494x^{10}$	(i)
	$(1:1)$	2	$P_{(1:1)} = x^{30} + 522x^{25} - 10005x^{20} - 10005x^{10} - 522x^5 + 1$	(i)
	$(0:1)$	5	$P_{(0:1)} = x(x^{10} + 11x^5 - 1)$	(ii)
	$(1:b)$ $(b \neq 0, 1)$	1	$P_{(1:b)} = \{x^{20} + 1 - 228(x^{15} - x^5) + 494x^{10}\}^3 - 1728b\{x(x^{10} + 11x^5 - 1)\}^5$	(i)

References

[1] Accola, R. D. M., Strongly branched coverings of closed Riemann Surfaces, Proc. Amer. Soc. **26** (1970), 315–322.

[2] Arbarello, E., Cormallba, M., Griffiths, P. A. and Harris, J., Geometry of Algebraic Curves Vol. I Springer-Verlag (1985).

[3] Farkas, H. M. and Kra, I., Riemann Surfaces, Graduate Texts in Mathematics 71, Springer-Verlag (1980).

[4] Horiuchi, R., Normal coverings of hyperelliptic Riemann surfaces, J. Math. Kyoto Univ. **19**-3 (1979), 497–523.

[5] Ishii, N., Covering over d-gonal curves, Tsukuba J. Math. Vol. 16, No. 1 (1992), 173–189.

[6] Ishii, N., Remarks on d-gonal curves, Tsukuba J. Math. Vol. 19, No. 2 (1995), 329–345.
[7] Kato, T., Conformal equivalence of compact Riemann surfaces, Japan J. Math. 7-2 (1981), 281–289.
[8] Klein, F., Lectures on the icosahedron and the solution of equations of fifth degree, Dover (1956), (translation).
[9] Machlachlan, C., Smooth coverings of hyperelliptic surfaces, Qurt. J. Math. Oxford (2), **22** (1971), 117–123.
[10] Namba, M., Families of meromorphic functioins on compact Riemann surfaces, Lecture Notes in Math. **767** (1979), Springer-Verlag.
[11] Namba, M., Equivalence problem and automorphism groups of certain compact Riemann surfaces, Tsukuba J. Math. Vol. 5, No. 2 (1981), 319–338.

Mathematical Division of General Education
College of Science and Technology
Nihon University, Narashinodai 7-24-1
Funabashi-shi, Chiba 274-8501
Japan
ishii@penta.ge.cst.nihon-u.ac.jp
yoshida@penta.ge.cst.nihon-u.ac.jp.