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 $M/\langle V \rangle \simeq \mathbb{P}^1$. It is well-known that finite subgroups $H$ of $\text{Aut}(\mathbb{P}^1)$ are classified into five types. In this paper, we determine the defining equation of $M$ with $H \subset \text{Aut}(M/\langle V \rangle)$ 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 $H = \text{Aut}(M/\langle V \rangle)$.

1 Introduction

Let $M$ be a compact Riemann surface defined by

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

where $p$ is a positive prime integer, $a_i$'s are distinct complex numbers, and $r_i$'s are integers satisfying $1 \leq r_i < p$ ($i = 1, \ldots, s$). Put $\mathcal{S} := \{a_1, \ldots, a_s\}$ (resp. $\{a_1, \ldots, a_s, a_{s+1} = \infty\}$) 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 $\frac{(\#\mathcal{S} - 2)(p-1)}{2}$. Let $C(M)$ denote the function field $C(x, y)$ of $M$. For an automorphism $\sigma \in \text{Aut}(M)$, $\sigma^*$ represents the action on $C(M)$ induced by $\sigma$. 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 $\zeta_p = \exp \frac{2\pi i}{p}$ of unity. The inclusion $C(x) \subset C(M)$ corresponds to the cyclic normal covering $x : M \rightarrow \mathbb{P}^1(x)$ of degree $p$, and its covering group is $\langle V \rangle$. Then $x$ is (totally) ramified over a point $a \in \mathbb{P}^1(x)$ if and only if $a \in \mathcal{S}$.

2000 Mathematical Subject Classification: 14H05, 14H30, 14H37.
Key words: Compact Riemann surface, Automorphisms, 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 \( 2p - 2 < \#\mathcal{F} \).

Let \( g_1^p \) denote a linear system of degree \( d \) and dimension 1, then the linear system \( |(x)_\infty| \) is \( g_1^p \). Here \((x)_\infty\) is the pole divisor of \( x \) on \( M \). We also assume that \( |(x)_\infty| \) is unique as \( g_1^p \). In fact the uniqueness of \( g_1^p \) is satisfied when \((p - 1)^2 < g\), i.e., \( 2p < \#\mathcal{F} \) [10]. The uniqueness of \( g_1^p \) on a cyclic \( p \)-gonal curve \( M \) implies that \( \langle V \rangle \) is normal in \( \text{Aut}(M) \). Moreover we will see that \( V \) is in the center of \( \text{Aut}(M) \). Therefore, for a subgroup \( G \) of \( \text{Aut}(M) \) containing \( V \), we have an exact sequence

\[
1 \to \langle V \rangle \to G \xrightarrow{\pi} H \to 1,
\]

where \( H = G/\langle V \rangle \).

On the other hand, it is well known that a finite subgroup \( H \) of \( \text{Aut}(\mathbb{P}^1) \) is isomorphic to cyclic \( C_n \), dihedral \( D_{2n} \), tetrahedral \( A_4 \), octahedral \( S_4 \) or icosahedral \( A_5 \). 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 \( a_1, \ldots, a_s \) of (1) depending on \( H \).

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

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

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

2 A Necessary and Sufficient Condition in Which the Exact Sequence (\ast) 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 \( g_1^p \). The symbols \( G, H, \mathcal{F} \) etc. are same as in the previous section. We prepare more notations.

**Notation 1.** Let denote \( \tilde{T} \) the element of \( H = G/\langle V \rangle \subset \text{Aut}(\mathbb{P}^1(x)) \) induced by some element \( T \in G \). Let \( FP(H) \) (resp. \( FP(G) \)) denote the set of points on
The automorphism group of a cyclic \( p \)-gonal curve

\( M/\langle V \rangle \simeq \mathbb{P}^1(x) \) (resp. \( M \)) fixed by a non-trivial element of \( H \) (resp. \( G \)), and let \( \text{FG}(a) \) denote the set of automorphisms of \( \mathbb{P}^1(x) \) which fixes a point \( a \in \mathbb{P}^1(x) \).

By corresponding \( A = \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \in \text{SL}(2, \mathbb{C}) \) to \( A(x) := \frac{ax+b}{cx+d} \), we have an isomorphism \( \text{SL}(2, \mathbb{C})/\{\pm1\} \simeq \text{Aut}(\mathbb{P}^1(x)) \). We use the same symbol "\( A \)" for both a matrix and an element of \( \text{Aut}(\mathbb{P}^1(x)) \). Let \( \langle A \rangle a \) denote the orbit of \( a \in \mathbb{P}^1(x) \) by the subgroup \( \langle A \rangle \) generated by \( A \in \text{SL}(2, \mathbb{C}) \).

For \( a \in \text{FP}(H) \), \( \text{FG}(a) \) is a cyclic group and \( \text{FP}(\text{FG}(a)) \) consists of two points \( a \) and \( a' \) with \( a \neq a' \). If \( \text{FG}(a) \) 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 \( \text{FP}(\langle A \rangle) = \{0, \infty\} \), where \( \zeta_n = \exp \left( \frac{2\pi i}{n} \right) \).

We start with the following lemma.

**Lemma 2.1.** (i) The group \( H \) acts on \( \mathcal{S} \).

(ii) Let \( a_i \) and \( a_j \) be in \( \mathcal{S} \). If there exists an element \( T \in G \) satisfying \( T a_i = a_j \), 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 \( \sum_{i=1}^s r_i \neq 0 \pmod{p} \).

(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 \( g_1^x \), we have a diagram

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

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

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

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

(a) \#\( \mathcal{S} \cap \{0, \infty\} \) = 2 \( \mathcal{S} = \{0\} \cup \{\infty\} \cup <\tilde{T}>b_1 \cup \cdots \cup <\tilde{T}>b_t \),

(b) \#\( \mathcal{S} \cap \{0, \infty\} \) = 1 (we may assume \( \mathcal{S} \cap \{0, \infty\} = \{0\} \)), \( \mathcal{S} = \{0\} \cup <\tilde{T}>b_1 \cup \cdots \cup <\tilde{T}>b_t \),

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

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

\[
y^p = x(x^n - b_1^n)^{u_1} \cdots (x^n - b_i^n)^{u_i},
\]

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

\[
(T^*y)^p = (T^*)^n(x^n - b_1^n)^{u_1} \cdots (T^*)^n(x^n - b_i^n)^{u_i} = \zeta_n y^p.
\]

Then \( T \) is defined by \( T^*x = \zeta_n x \) and \( T^*y = \epsilon y \), where \( \epsilon \) satisfies \( \epsilon^p = \zeta_n \). 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. \( \square \)

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

**Lemma 2.2.** Assume \( S \neq \emptyset \). Let \( S = \bigcup_{i=1}^u Hb_i^{(1)} \) (disjoint) be the decomposition of \( S \) into orbits \( Hb_i^{(1)} = \{b_i^{(1)}, \ldots, b_i^{(s_i)}\} \subset C \). Then the equation (1) is transformed into

\[
y^p = \prod_{i=1}^u \{(x - b_i^{(1)}) \cdots (x - b_i^{(s_i)}) \}^{r_i}
\]

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

Let \( \bar{u} : P^1(x) \to P^1(u) \) 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 \( P^1(u) \) with \( u = \frac{b_1}{b_0} \). 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) \( FP(H) \cap S = \emptyset \), or

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

**Proof.** Put \( \#H = n \). Then \( \#G = pn \). We may assume \( S \neq \emptyset \). Then \( M \) is defined by (3) in Lemma 2.2. We regard \( M / G \) as a \( u \)-plane \( P^1(u) \), and consider the normal covering
The automorphism group of a cyclic \( p \)-gonal curve 5

\[ M/\langle V \rangle \simeq P^1(\alpha) \xrightarrow{\tilde{\pi}} M/G \simeq P^1(u), \]

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

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

\[
\begin{array}{ccc}
M & \xrightarrow{x} & M/\langle V \rangle \\
\downarrow{\pi} & & \downarrow{\tilde{\pi}} \\
M/H & \xrightarrow{u} & M/G,
\end{array}
\]

\[
\begin{aligned}
\text{Gal}(\pi) & \simeq \text{Gal}(\tilde{\pi}) \simeq H \\
\text{Gal}(x) & \simeq \text{Gal}(\alpha) \simeq \langle V \rangle \\
C(M) & \simeq C(M/H) \otimes C(x),
\end{aligned}
\]

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

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

The isomorphism \( C(M) \simeq C(M/H) \otimes C(x) \) implies that \( x \) and \( y \) have a relation

\[ y^p = \prod_{i=1}^{u} \left( f_1(x) - b_1 \right)^{t_1} \cdots \left( f_1(x) - b_u \right)^{t_u}. \quad (5) \]

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

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

and this equation defines \( M \). Let \( \mathcal{S} = \{b_1^{(1)}, \ldots, b_u^{(s_i)}\} \) \( (i = 1, \ldots, u) \) be the set of points \( b \) in \( P^1(x) \) satisfying \( \tilde{\pi}(b) = b_i \). Then, by the assumptions \( \infty \notin \mathcal{S} \) and \( \infty \notin \tilde{\pi}(\mathcal{S}) \), we have factorizations

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

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

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

and we have \( \mathcal{S} \subset \bigcup_{i=1}^{u} \mathcal{S}_i \). 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 \((u - b_i)^t\) from the equation (4). Finally we can get the equation (4) satisfying \(\mathcal{S} = \bigcup_{i=1}^{t} \mathcal{S}_i\) 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 \(b_i = \pi(b_i^{(1)})\ (i = 1, \ldots, u)\). Then, for each \(b_i\), we have \(f_i(x) - b_if_0(x) = C_i\{x - b_i^{(1)}\} \cdots \{x - b_i^{(s_i)}\}\) 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 \(sri = u_im_i + M_ip\). Raising both sides of (3) to \(s\)-th power and replacing \(y^s/\{\prod_{i=1}^{u} \{x - b_i^{(1)}\} \cdots \{x - b_i^{(s_i)}\}\}\) with \(y\) again, we have

\[
y^p = \prod_{i=1}^{u} \{x - b_i^{(1)}\} \cdots \{x - b_i^{(s_i)}\}\} \cdot \prod_{i=1}^{u} (f_i(x) - b_if_0(x))^{u_i},
\]

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

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 \(\text{Aut}(\mathbb{P}^1)\) classified by Klein [8].

Let \(A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \text{SL}(2, \mathbb{C})\). As in the previous section, we also write \(A\) for the element \(\{\pm A\}\) in \(\text{SL}(2, \mathbb{C})/\{\pm 1\} \simeq \text{Aut}(\mathbb{P}^1(x))\) 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 \(C(x, y)\), it is sufficient to investigate \(A^*y\).

Let \(\tilde{\pi} : \mathbb{P}^1(x) \to \mathbb{P}^1(u)\) be a finite normal covering defined by a rational function \(u = f_1(x) / f_0(x)\) with \((f_0, f_1) = 1\), and let \(H\) be its covering group. Put \(\#H = s\). Take \((b_0 : b_1) \in \mathbb{P}^1(u)\). 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

\[
\tilde{P}_{(b_0, b_1)} := b_0f_1(x) - b_1f_0(x).
\]

That is:

\[
\tilde{P}_{(b_0, b_1)} = \begin{cases} 
(i) & C \prod_{i=1}^{t} (x - a_i)^m \quad \text{with } t \geq 1 \text{ and } mt = s, \\
(ii) & C \prod_{i=1}^{t-1} (x - a_i)^m \quad \text{with } t - 1 \geq 1 \text{ and } mt = s, \\
(iii) & C.
\end{cases}
\]
The automorphism group of a cyclic \( p \)-gonal curve

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 \( \pi(\infty) = (b_0 : b_1) \) 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) \( P_{(b_0,b_1)}(x) = \prod_{i=1}^{r}(x - a_i), \quad d_{(b_0,b_1)} = t \) if \( \tilde{P}_{(b_0,b_1)} \) is of type (i),

(ii) \( P_{(b_0,b_1)}(x) = \prod_{i=1}^{r}(x - a_i), \quad d_{(b_0,b_1)} = t \) if \( \tilde{P}_{(b_0,b_1)} \) is of type (ii),

(iii) \( P_{(b_0,b_1)}(x) = 1, \quad d_{(b_0,b_1)} = s \) if \( \tilde{P}_{(b_0,b_1)} \) is of type (iii).

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

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

\[
y^p = \prod_{i=1}^{r} P_{(b_{0,i},b_{1,i})}^{u_i}, \quad 1 \leq u_i \leq p - 1,
\]

\[
\sum_{i=1}^{r} u_i d_{(b_{0,i},b_{1,i})} \equiv 0 \pmod{p}, \quad \#F = \sum_{i=1}^{r} d_{(b_{0,i},b_{1,i})} > 2p.
\]

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 \( \tilde{\pi} : P^1(x) \to P^1(u) \) 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 \( H = A_4 \) 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, ±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 $H = A_5$ and $u = f_1(x) = \frac{-x^{30} - 228(x^{15} - x^5) - 494x^{10}}{1728x^5(x^{10} + 11x^5 - 1)^2}$, we have

$$\bar{P}_{(1:1)} = \{-x^{20} - 1 + 228(x^{15} - x^5) - 494x^{10}\}^3 - \{1728x^5(x^{10} + 11x^5 - 1)\}^5$$

$$= -(x^{30} + 522x^{25} - 10005x^{20} - 10005x^{10} - 522x^5 + 1)^2,$$

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 $A = (\begin{smallmatrix} a & \beta \\ \gamma & \delta \end{smallmatrix}) \in SL(2, \mathbb{C})$. Define $j(A, x) := \gamma x + \delta$ with a variable $x$ on $\mathbb{C}$. When $A \infty = \infty$ (i.e., $\gamma = 0$), define $j(A, \infty) := j(DAD^{-1}, 0) = a$, where $D = (\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix})$. And when $A \infty \neq \infty$, define $j(A, \infty) := 1$. Of course an automorphism of $P^1(x)$ 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 $A = (\begin{smallmatrix} a & \beta \\ \gamma & \delta \end{smallmatrix})$ and $B$ be in $SL(2, \mathbb{C})$, and let $x$ be a variable on $\mathbb{C}$. Then

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

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

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

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

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

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

(b) Assume $a = \infty$. Then $j(A^{-1}, A(a)) = 0$ and
The automorphism group of a cyclic $p$-gonal curve

\[ \prod_{i=2}^{l} j(A^{-1}, A^i(a)) = -j(A^l, x) = \begin{cases} -1 & \text{if } A^l = \left( \begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right), \\ 1 & \text{if } A^l = -\left( \begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right). \end{cases} \]

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

(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 $A^l = \left( \begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right)$ (resp. $-\left( \begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right)$). 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 $A(a) = \frac{\xi}{\nu}$, we have $j(A^{-2}, A(a)) = -1$ and $j(A^{-1}, A(a)) = 0$. Since $j(A^{-1}, A^i(a)) = j(A^{i-2}, A(a))/j(A^{i-1}, A(a))$ ($2 \leq i \leq l - 1$) and $j(A^{-1}, A^l(a)) = j(A^{-1}, \infty) = 1$ by the definition, we have

\[ \prod_{i=2}^{l} j(A^{-1}, A^i(a)) = \prod_{i=2}^{l-1} \frac{j(A^{i-2}, A(a))}{j(A^{i-1}, A(a))} = \frac{1}{j(A^{l-2}, A(a))j(A^{-2}, A(a))} = -j(A^l, x). \]

(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 $A = \left( \begin{array}{cc} \xi & 0 \\ 0 & \epsilon^{-1} \end{array} \right)$ where $\epsilon$ is a primitive $l$ or $2l$-th root of $1$. Then $j(A, 0) = \epsilon^{-1}$ and $j(A, \infty) = \epsilon$. \qed

Let $A = \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \in H$. First we observe the action of $A^*$ on polynomials $P_{(b_0:b_1)}$.

**Lemma 3.4.** Assume that $A \in \text{Aut}(P^1(x))$ has an order $l$. Let $P_{(b_0:b_1)}$ be a polynomial of type (i) or (ii) above. Put $\mathcal{U} := \{a_1, \ldots, a_t\}$ (resp. $\{a_1, \ldots, a_{t-1}, \infty\}$) 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 $\mathcal{U} \cap FP(\langle A \rangle) = \emptyset$, then $t \equiv 0 \pmod{l}$ and

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

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

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

(III) If $\mathcal{U} \cap FP(\langle A \rangle)$ consists of two points $c, c'$ of $A$, then $t - 2 \equiv 0 \pmod{l}$, and
These representations are independent from the choice of matrix $A$ or $-A$.

**Proof.** (I) Assume $\mathcal{U} \ni \infty$ (i.e., $P_{(b^2:b^3)}$ is of type (ii)). Let

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

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

$$P_{(b^2:b^3)}(x) = \prod_{i=1}^{l-1} (x - A^i(\infty)) \prod_{k=2}^{r} \prod_{i=1}^{l} (x - A^i(c_k)).$$

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

$$A^*(P_{(b^2:b^3)}(x)) = \prod_{i=1}^{l-1} \frac{\alpha x + \beta}{\gamma x + \delta - A^i(\infty)} \prod_{k=2}^{r} \prod_{i=1}^{l} \frac{\alpha x + \beta}{\gamma x + \delta - A^i(c_k)}.$$

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

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

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

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

the term $(B) = j(A, x)^{-(l-1)} j(A^l, x)^{(r-1)} \prod_{k=2}^{r} \prod_{i=1}^{l} (x - A^{i-1}(c_k)). \quad (**)$
By multiplying (\*) and (\**), we have

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

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

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

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

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

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

1) $c \neq \infty$ and $c_k \neq \infty$ ($k = 1, \ldots, r$), 2) $c = \infty$, 3) $c_k = \infty$ 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 $\mathcal{U} = \{c\} \cup \{c'\} \cup (\bigcup_{k=1}^{r} \langle A \rangle c_k)(t = lr + 2)$ be the decomposition of $\mathcal{U}$ into the orbits of $\langle A \rangle$. And we have

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

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

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 $\#\mathcal{S} > 2p$. Assume $\text{Aut}(M)/\langle V \rangle$ 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 $H = C_n$). $M$ is defined by
\[
y^p = P_{u_1}^{u_1} P_{u_2}^{u_2} \prod_{i=3}^{d} P_{u_i}^{u_i} = x^n \prod_{i=3}^{d} (x^n - b_i)^{u_i},
\]

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

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

For the generator $S_n$ of $C_n$,
\begin{itemize}
  \item $S_n^* = \eta_{S_n}$, where $(\eta_{S_n})^p = \zeta_n^{u_3}$.
\end{itemize}

(Case $H = D_{2n}$). $M$ is defined by
\[
y^p = P_{u_1}^{u_1} P_{u_2}^{u_2} P_{u_3}^{u_3} \prod_{i=4}^{d} P_{u_i}^{u_i} = (x^n - 1)^{u_1} (x^n + 1)^{u_2} x^{u_3} \prod_{i=4}^{d} (x^{2n} - b_i x^n + 1)^{u_i},
\]

\[
\#S = ne_1 + 2e_2 + 2e_3 + 2n \sum_{i=4}^{d} 1, \quad nu_1 + nu_2 + 2u_3 + 2n \sum_{i=4}^{d} u_i \equiv 0 \pmod{p},
\]

where $d \geq 3$ (according to the notation above), $0 \leq u_1, u_2, u_3 < p$, and $0 < u_i < p$ ($i \geq 4$), $b_i \neq \pm 2$, 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 $D_{2n}$,
\begin{itemize}
  \item $S_n^* = \eta_{S_n}$, where $(\eta_{S_n})^p = \zeta_n^{u_3}$.
  \item $T^* = \eta_T x^{-(nu_1 + nu_2 + 2u_3 + 2n \sum_{i=4}^{d} u_i)/p} y$, where $(\eta_T)^p = (-1)^{u_1}$
\end{itemize}

(Case $H = A_4$). $M$ is defined by
\[
y^p = P_{u_1}^{u_1} P_{u_2}^{u_2} P_{u_3}^{u_3} \prod_{i=4}^{d} P_{u_i}^{u_i} = (x^4 - 2\sqrt{3}ix^2 + 1)^{u_1} \{x(x^4 - 1)^{u_1} (x^4 + 2\sqrt{3}ix^2 + 1)^{u_3}
\]

\[
\times \prod_{i=4}^{d} \frac{1}{1 - b_i} \{ (x^4 - 2\sqrt{3}ix^2 + 1)^3 - b_i (x^4 + 2\sqrt{3}ix^2 + 1)^3 \}^{u_i},
\]

\[
\#S = 4e_1 + 6e_2 + 4e_3 + 12 \sum_{i=4}^{d} 1, \quad 4u_1 + 6u_2 + 4u_3 + 12 \sum_{i=4}^{d} u_i \equiv 0 \pmod{p},
\]
The automorphism group of a cyclic p-gonal curve

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 \( \epsilon_k = 1 \) (resp. \( \epsilon_k = 0 \)) if \( u_k > 0 \) (resp. \( u_k = 0 \)) (\( k = 1,2,3 \)).

For the generators \( U, W \) of \( A_4 \),

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

(Case \( H = S_4 \)). \( M \) is defined by

\[
y^p = P_{(1:0)}^{u_1} P_{(1:1)}^{u_2} P_{(0:1)}^{u_3} \prod_{i=4}^{d} P_{(1:b_i)}^{u_i} \\
= (x^8 + 14x^4 + 1)^{u_1} (x^{12} - 33x^8 - 33x^4 + 1)^{u_2} (x(x^4 - 1))^{u_3} \\
\times \prod_{i=4}^{d} ((x^8 + 14x^4 + 1)^3 - 108b_i(x^4(x^4 - 1)^4))^r, \tag{12}
\]

\( \# p = 8u_1 + 12u_2 + 6u_3 + 24 \sum_{i=4}^{d} 1, \) \( 8u_1 + 12u_2 + 6u_3 + 24 \sum_{i=4}^{d} u_i \equiv 0 \) (mod \( p \)),

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 \( \epsilon_k = 1 \) (resp. \( \epsilon_k = 0 \)) if \( u_k > 0 \) (resp. \( u_k = 0 \)) (\( k = 1,2,3 \)).

For the generators \( W, R \) of \( S_4 \),

- \( W^* y = \eta_W \left( \frac{1+i}{2} \right)^{(8u_1-12u_2-6u_3-24\sum u_i)/p} (x + i)^{(8u_1-12u_2-6u_3-24\sum u_i)/p} y \), where \( (\eta_W)^p = 1 \).
- \( R^* y = \eta_R x^{-(8u_1+12u_2+6u_3+24\sum u_i)/p} y \), where \( (\eta_R)^p = i^{u_3} \).

(Case \( H = A_5 \)). \( M \) is defined by

\[
y^p = P_{(1:0)}^{u_1} P_{(1:1)}^{u_2} P_{(0:1)}^{u_3} \prod_{i=4}^{d} P_{(1:b_i)}^{u_i} \\
= \{x^{20} + 1 - 228(x^{15} - x^5) + 494x^{10}\}^{u_1} \\
\times \{x^{30} + 522x^{25} - 10005x^{20} - 10005x^{10} - 522x^5 + 1\}^{u_2} (x(x^{10} + 11x^5 - 1))^{u_3} \\
\times \prod_{i=4}^{d} \{x^{20} + 1 - 228(x^{15} - x^5) + 494x^{10}\}^3 \\
+ 1728b_i x^5(x^{10} + 11x^5 - 1)^5, \tag{13}
\]
# \( \bar{\gamma} = 20c_1 + 30c_2 + 12c_3 + 60 \sum_{i=4}^{d} 1, \quad 20u_1 + 30u_2 + 12u_3 + 60 \sum_{i=4}^{f} u_i \equiv 0 \pmod{p}, \)

where \( d \geq 3, 0 \leq u_1, u_2, u_3 < p, 0 < u_1 < p \) (\( i \geq 4 \)), \( b_i \neq 0, 1 \), 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 \( A_5 \),

\[
\begin{align*}
\text{\( K^*y = \eta_K \left( \frac{1}{\sqrt{5}} \{ (1 - \zeta_5^2)x + (\zeta_5 - \zeta_5^2) \} \right)^{(20u_1 - 30u_2 - 12u_3 - 60\sum_{i=4}^{d} u_i)/p} \) & \quad \text{where } (\eta_K)^p = 1. \\
\text{\( Z^*y = \eta_Z y \) & \quad \text{where } (\eta_Z)^p = \varepsilon_5^u.}
\end{align*}
\]

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

**Case \( H = A_4 \).** Let \( M \) be defined by \( y^p = P_{(1:0)}^{u_1} P_{(0:1)}^{u_2} \prod_{i=4}^{d} P_{(1:b_i)}^{u_i} \), where \( P_{(b_i:b_i)} \) are as in Table 2. Let \( A \) be \( U = \frac{1+i}{2} \left( \begin{array}{cc} 1 & 1 \\ 1 & 1 \end{array} \right) \) (resp. \( W = \frac{1+i}{2} \left( \begin{array}{cc} 1 & -1 \\ 1 & -1 \end{array} \right) \)). Then

\[
\begin{align*}
A^2 &= \left( \begin{array}{cc} -1 & 0 \\ 0 & -1 \end{array} \right) \quad \text{(resp. \( \frac{-1-\sqrt{3}}{2}(1+i) \))}, \quad j(A^3, x) = -1 \quad \text{(resp. \( 1 \))}, \\
j(A, x) &= \frac{1+i}{2} (x + 1) \quad \text{(resp. \( \frac{1-i}{2} (x + i) \))}.
\end{align*}
\]

Two fixed points \( a_1, a_2 \) of \( A \) (resp. \( W \)) are

\[
\begin{align*}
a_1 &= \frac{(1+i)(1-i)}{2} \quad \text{(resp. \( \frac{-1-\sqrt{3}}{2}(1+i) \))}, \quad j(A^{-1}, a_1) = \exp(\frac{1}{3} \pi i) \\
(\ddagger) \quad a_2 &= \frac{(1-\sqrt{3})(1-i)}{2} \quad \text{(resp. \( \frac{-1+\sqrt{3}}{2}(1+i) \))}, \quad j(A^{-1}, a_2) = \exp(\frac{5}{3} \pi i)
\end{align*}
\]

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

\[
\begin{align*}
U^*P_{(1:0)} &= j(U^{-1}, a_1) j(U, x)^{-4} j(U^3, x) P_{(1:0)} \\
&= \exp \left( \frac{1}{3} \pi i \right) \left( \frac{1 - i}{2} (x + 1) \right)^{-4} (-1)^2 P_{(1:0)}, \\
U^*P_{(1:1)} &= j(U, x)^{-6} j(U^3, x)^2 P_{(1:1)} = \left( \frac{1 - i}{2} (x + 1) \right)^{-6} (-1)^2 P_{(1:1)}, \\
U^*P_{(0:1)} &= j(U^{-1}, a_2) j(U, x)^{-4} j(U^3, x) P_{(0:1)} \\
&= \exp \left( \frac{5}{3} \pi i \right) \left( \frac{1 - i}{2} (x + 1) \right)^{-4} (-1)^2 P_{(0:1)}, \\
U^*P_{(1:b_i)} &= j(U, x)^{-12} j(U^3, x)^4 P_{(1:b_i)} \\
&= \left( \frac{1 - i}{2} (x + 1) \right)^{-12} (-1)^4 P_{(1:b_i)} \quad (b_i \neq 0, 1).
\end{align*}
\]
Then
\[ U^* y^p = (-1)^{u_1+u_2} \exp\left(\frac{1}{3} \pi i\right)^{u_1} \exp\left(\frac{5}{3} \pi i\right)^{u_3} \times \left\{ \frac{1-i}{2} (x+1) \right\}^{(-4u_1-6u_2-4u_3-12\sum_{i=4}^{d} u_i)} y, \] (14)
and
\[ U^* y = \eta \left\{ \frac{1-i}{2} (x+1) \right\}^{(-4u_1-6u_2-4u_3-12\sum_{i=4}^{d} u_i)/p} y, \]
where \( \eta \) satisfies \( \eta^p = (-1)^{u_1+u_2} \exp\left(\frac{1}{3} \pi i\right)^{u_1} \exp\left(\frac{5}{3} \pi i\right)^{u_3} \).

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

Case \( H = S_4 \). \( H \) is generated by \( W \) and \( R \). The fixed points \( \frac{(-1+\sqrt{3})i}{2} \) of \( W \) are zeros of \( P_{(1:0)} \). Then, by Lemma 3.2 (III), we get the representation of \( W^* y \).

Case \( H = A_5 \). We may assume that \( M \) is defined by
\[ \sum_{i=4}^{d} U_i + \sum_{i=4}^{d} U_2 + 2U_3 + 60 \sum_{i=4}^{d} U_i \equiv 0 \pmod{p}, \]
and assume \( A = K \). Then \( K^3 = (\frac{1}{0} - \frac{1}{0}) \) 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
\[ K^* y^p = j(K, x)^{(-20u_1-30u_2-12u_3-60\sum_{i=4}^{d} u_i)} j(K^3, x)^{(6u_1+10u_2+4u_3+20\sum_{i=4}^{d} u_i)} y^p \]
\[ = \left\{ \frac{1}{\sqrt{5}} ((1-\zeta_5^2)x + (\zeta_5 - \zeta_5^2)) \right\}^{(-20u_1-30u_2-12u_3-60\sum_{i=4}^{d} u_i)} y^p. \]

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
\[
y^p = (x^n - 1)^{u_1} (x^n + 1)^{u_2} x^{u_3} \prod_{i=4}^{d} (x^{2n} - b_i x^n + 1)^{u_i},
\]
where \( d \geq 3 \) and \( 0 \leq u_i < p \) \( (1 \leq i \leq 3, b_i \neq \pm 2) \). Then \( \text{Aut}(M)/\langle V \rangle \) contains \( H = D_{2n} \). 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
\[ S_n \mapsto \{ S_n^* x = \zeta_n x, S_n^* y = \zeta_n^{-1} y \}, \]
\[ T \mapsto \{ T^* x = \frac{1}{x}, T^* y = (-1)^{u_1} x^{-(n u_1 + n u_2 + 2 u_3 + 2 n \sum_{d=1}^{d} u_d)} / p y \} \]
gives a section of (\star), 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 \( \iota : H \to G \) is a section in case \((2p, n) = 1 \) and \( u_1 u_2 u_3 \neq 0 \). In Theorem 3.1 (Case \( H = D_{2n} \)), put \( \eta_T = (-1)^{u_1} \) and \( \eta_{S_n} = \zeta_n^{u_1} \) with an integer \( r \) satisfying \( rp \equiv 1 \pmod{n} \). Then \( \eta_{S_n}^{p} = (\zeta_n)^{u_1} \), \( \eta_T^{p} = (-1)^{u_1} \). Meanwhile \( D_{2n} \) is defined by relations \( S_n^n = 1, T^2 = 1 \) and \( T S_n T = S_n^{-1} \). But \( (S_n^*)^{y} = \eta_S^3 y = y \) and \( (T^*)^{y} = \eta_T^2 y = y \) hold. Therefore if \( T^* S_n^* T^* y = S_n^{*-1} y \) holds, then \( \iota \) is a group homomorphism. In fact, by the definition of \( \iota \),
\[ T^* S_n^* T^* y = T^* S_n^* (\eta_T x^{-(n u_1 + n u_2 + 2 u_3 + 2 n \sum_{d=1}^{d} u_d)} / p y) \]
\[ = T^* (\eta_T \eta_{S_n} (\zeta_n x)^{-(n u_1 + n u_2 + 2 u_3 + 2 n \sum_{d=1}^{d} u_d)} / p y) \]
\[ = (\eta_T)^2 \eta_{S_n} (\zeta_n)^{-(n u_1 + n u_2 + 2 u_3 + 2 n \sum_{d=1}^{d} u_d)} / p y \]
\[ = ((-1)^{u_1})^2 \eta_{S_n} (\zeta_n)^{-(n u_1 + n u_2 + 2 u_3 + 2 n \sum_{d=1}^{d} u_d)} / p r y \]
\[ = \zeta_n^{-r u_3} y. \]

Then \( T^* S_n^* T^* y = S_n^{*-1} y \) holds. The equation \( \pi \circ \iota = \text{id}_H \) is trivial from the definition.

**Corollary 3.1.2.** (1) The compact Riemann surface \( M \) defined by the following equations (14) or (15) has \( \text{Aut}(M) \) isomorphic to \( A_5 \times \langle V \rangle \).
\[ y_p = x^{20} + 1 - 228(x^{15} - x^5) + 494x^{10} \quad (p = 2, 5). \quad (15) \]
\[ y_p = x(x^{10} + 11x^5 - 1) \quad (p = 2, 3). \quad (16) \]

(2) The compact Riemann surface \( M \) defined by
\[ y_p = x^{30} + 522x^{25} - 10005x^{20} - 10005x^{10} - 522x^5 + 1 \quad (p = 2, 3, 5), \quad (17) \]
satisfies \( \text{Aut}(M) / \langle V \rangle \cong A_5 \). Moreover \( \text{Aut}(M) \cong A_5 \times \langle V \rangle \) provided \( p = 3, 5 \).
But when \( p = 2 \), the exact sequence (\star) is not split.
The automorphism group of a cyclic $p$-gonal curve

PROOF. The right hand side of (14) is $P_{(1:0)}$ of $A_5$ in Table 2. Then, by Theorem 3.1, $\text{Aut}(M)/<V> \simeq A_5$ 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 $\text{Aut}(M)/<V>$ 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 $\text{Aut}(M)/<V>$, and we consider the exact sequence (*).

Then $H$ is isomorphic to $C_n$ ($n = 2, 3, 4, 5, 6$), $D_{2n}$ ($n = 2, 3, 4, 6$), $A_4$ or $S_4$. And according to each type of $H$, we can get a standard defining equation of $M$ as in the following list.

<table>
<thead>
<tr>
<th>$H = \langle generators \rangle$</th>
<th>defining equation of $M$</th>
<th>$(\ast)$ is split ($S$) or not split ($NS$)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$C_2 = \langle S_2 \rangle$</td>
<td>$y^2 = (x^2 - 1)(x^2 - a^2)(x^2 - b^2)$</td>
<td>$S$</td>
</tr>
<tr>
<td>$C_2 = \langle S_2 \rangle$</td>
<td>$y^2 = x(x^2 - 1)(x^2 - a^2)$</td>
<td>$NS$</td>
</tr>
<tr>
<td>$D_4 = \langle S_2, \bar{T} \rangle$</td>
<td>$y^2 = x(x^2 - 1)(x^2 - a^2)$</td>
<td>$NS$</td>
</tr>
<tr>
<td>$C_3 = \langle S_3 \rangle$</td>
<td>$y^2 = (x^3 - 1)(x^3 - a^3)$</td>
<td>$S$</td>
</tr>
<tr>
<td>$D_6 = \langle S_3, \bar{T} \rangle$</td>
<td>$y^2 = (x^3 - 1)(x^3 - a^3)$</td>
<td>$S$</td>
</tr>
<tr>
<td>$C_4 = \langle S_4 \rangle$</td>
<td>$y^2 = x(x^4 - 1)$</td>
<td>$NS$</td>
</tr>
<tr>
<td>$D_8 = \langle S_4, T \rangle$</td>
<td>$y^2 = x(x^4 - 1)$</td>
<td>$NS$</td>
</tr>
<tr>
<td>$A_4 = \langle U, W \rangle$</td>
<td>$y^2 = x(x^4 - 1)$</td>
<td>$NS$</td>
</tr>
<tr>
<td>$S_4 = \langle W, R \rangle$</td>
<td>$y^2 = x(x^4 - 1)$</td>
<td>$NS$</td>
</tr>
<tr>
<td>$C_5 = \langle S_5 \rangle$</td>
<td>$y^2 = x(x^5 - 1)$ $\sim$ $y^2 = x^5 - 1$</td>
<td>$S$</td>
</tr>
<tr>
<td>$C_6 = \langle S_6 \rangle$</td>
<td>$y^2 = (x^6 - 1)$</td>
<td>$S$</td>
</tr>
<tr>
<td>$D_{12} = \langle S_6, T \rangle$</td>
<td>$y^2 = (x^6 - 1)$</td>
<td>$NS$</td>
</tr>
</tbody>
</table>

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

In particular

\begin{align*}
C_4 &\subset \text{Aut}(M)/\langle V \rangle \text{ if and only if } S_4 = \text{Aut}(M)/\langle V \rangle, \\
C_6 &\subset \text{Aut}(M)/\langle V \rangle \text{ if and only if } D_{12} = \text{Aut}(M)/\langle V \rangle, \\
C_3 &\subset \text{Aut}(M)/\langle V \rangle \text{ if and only if } D_6 = \text{Aut}(M)/\langle V \rangle,
\end{align*}
and
\begin{align*}
\{ C_2 &\subset \text{Aut}(M)/\langle V \rangle \text{ if and only if } D_4 = \text{Aut}(M)/\langle V \rangle. \\
\text{and } (\ast) \text{ is NS} &\}
\end{align*}

PROOF. \( H \) is isomorphic to \( C_n, D_{2n}, A_4, S_4 \) or \( A_5 \). But, for \( g = 2 \), \( M \) is defined by \( y^2 = (x - a_1) \cdots (x - a_s) \) with \( s = 5 \) or \( 6 \), and then \( H = S_4, A_4, D_{2n}, C_n \) \((n \leq 6)\) are the only groups which are possibly contained in \( \text{Aut}(M)/\langle V \rangle \).

Assume \( \text{Aut}(M)/\langle V \rangle \supset H = C_n \) with \( n \leq 6 \). We may assume that \( C_n \) is generated by the automorphism \( S_n \) defined by \( S_n x = \zeta_n x \) and the set \( \mathcal{S} \) defined in §1 contains 1. For example, assume \( \text{Aut}(M)/\langle V \rangle \supset C_2 \). Then the decomposition of \( \mathcal{S} \) into orbits by \( C_2 \) may assume to be \( \mathcal{S} = \{ \pm 1 \} \cup \{ \pm a \} \cup \{ \pm b \} \) or \( \mathcal{S} = \{ \infty \} \cup \{ \pm 1 \} \cup \{ \pm a \} \). 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 \( a, b, 0, \pm 1 \) 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 \( \text{Aut}(M)/\langle V \rangle \) contains \( H = C_n \).

\begin{align*}
(a) \ H &\subset C_2, \quad y^2 = (x^2 - 1)(x^2 - a^2)(x^2 - b^2) \quad (0, 1, a^2, b^2 \text{ are distinct}). \\
(b) \ H &\subset C_2, \quad y^2 = x(x^2 - 1)(x^2 - a^2) \quad (a^2 \neq 0, 1). \\
(c) \ H &\subset C_3, \quad y^2 = (x^3 - 1)(x^3 - a^3) \quad (a^3 \neq 0, 1). \\
(d) \ H &\subset C_4, \quad y^2 = x(x^4 - 1). \\
(e) \ H &\subset C_5, \quad y^2 = x(x^5 - 1). \\
(f) \ H &\subset C_6, \quad y^2 = (x^6 - 1).
\end{align*}

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 \( D_{12} \). Moreover since \( D_{12} \not\subset A_4 \) and \( D_{12} \not\subset S_4 \), we have \( \text{Aut}(M)/\langle V \rangle = D_{12} \). As \( \pm 1 \in P^1(x) \) are fixed points of \( T \) and the order of \( T \) is 2, the exact sequence \( (\ast) \) with \( H = \text{Aut}(M)/\langle V \rangle = D_{12} \) is not split by Theorem 2.1.

Assume \( M \) is defined by \( (e) \). Among four types of groups \( S_4, A_4, D_{2n}, C_n \) \((n \leq 6)\), \( C_5 \) and \( D_{10} \) are the only groups which contain \( C_5 \). Therefore \( \text{Aut}(M)/\langle V \rangle \) is isomorphic to \( C_5 \) or \( D_{10} \). On the other hand the exponent \( u_1 \) (resp. \( u_3 \)) of \( x^5 - 1 \) (resp. \( x \)) in \( (e) \) is equal to 1, and \( 5u_1 + 2u_3 = 7 \neq 0 \) (mod 2). Then, from Theorem 3.1, \( \text{Aut}(M)/\langle V \rangle \) does not contain \( D_{10} \) and \( \text{Aut}(M)/\langle V \rangle = C_5 \). As \( \mathcal{S} \cap FP(\langle S_5 \rangle) = \{ 0 \} \) and \( (5, 2) = 1 \), \( (\ast) \) is split from Theorem 2.1.

Assume \( M \) is defined by \( (d) \), then, from (13) in Theorem 3.1, \( \text{Aut}(M)/\langle V \rangle \).
= S_4 and H = C_4, D_8, A_4 or S_4. Moreover the exact sequence (*) is not split since H contains S_2 of order 2 and FP(\langle S_2 \rangle) \cap \mathcal{S} = \{0, \infty\}.

Assume M is defined by (c). Then M has an automorphism \overline{T} defined by \overline{T}^*x = a/x and \overline{T}^*y = a^{-3/2}x^3y, and the group H_1 = \langle S, \overline{T} \rangle is isomorphic to D_6. So we can say that Aut(M)/\langle V \rangle contains a subgroup D_6 if and only if Aut(M)/\langle V \rangle contains C_3. Since FP(H_1) \cap \mathcal{S} = \emptyset, (*) is split with H = \langle S, \overline{T} \rangle.

Assume M is defined by (b). Then M also has an automorphism \overline{T} defined by \overline{T}^*x = a/x and \overline{T}^*y = a^{-3/2}x^3y. Therefore D_4 c Aut(M)/\langle V \rangle if and only if C_2 c Aut(M)/\langle V \rangle. Since FP(\langle S_2 \rangle) \cap \mathcal{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 Aut(M)/\langle V \rangle as follows.

**Theorem 4.1.** Let M be a hyperelliptic curve of genus g = 2. Assume that Aut(M)/\langle V \rangle is non-trivial. Then Aut(M)/\langle V \rangle is isomorphic to C_2, C_5, D_4, D_6, D_{12} or S_4. And according to each type of Aut(M)/\langle V \rangle, we can get a standard equation of M as follows.

---

**Case** Aut(M)/\langle V \rangle \simeq S_4.

M is defined by

\[ y^2 = x(x^4 - 1). \] (18)

**Case** Aut(M)/\langle V \rangle \simeq C_5.

M: \[ y^2 = x(x^5 - 1) \sim \text{birationally} \quad y^2 = x^5 - 1. \] (19)

**Case** Aut(M)/\langle V \rangle \simeq D_{12}.

M: \[ y^2 = (x^6 - 1). \] (20)

**Case** Aut(M)/\langle V \rangle \simeq D_6.

M: \[ y^2 = x(x^2 - 1)(x^2 - a^2) \quad \text{with } a^2 \neq 0, \pm 1. \] (21)

---

#-1). The curve (21) has Aut(M)/\langle V \rangle \simeq S_4 if and only if \( a^2 = -1 \).

**Case** Aut(M)/\langle V \rangle \simeq D_6.

M: \[ y^2 = (x^3 - 1)(x^3 - a^3) \] (22)

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

---

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

---

#-3). Aut(M)/\langle V \rangle \simeq S_4 if and if \( a^3 = \left(\frac{1 + \sqrt{3}}{1 + \sqrt{3}}\right)^3 \).

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 $W = \frac{1+i}{2} (1 \ 1)$. If $a_3 = \left(\frac{a_1}{a_1}\right)^3 = \left(\frac{1+i}{1+\sqrt{3}}\right)^3$ (resp. $a_3 = \left(\frac{a_2}{a_2}\right)^3 = \left(\frac{1-\sqrt{3}}{1+\sqrt{3}}\right)^3$), the equalities 

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

(23)

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

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 $\phi \in \text{Aut}(M)$, $\psi \in \text{Aut}(M')$.

Case $\text{Aut}(M)/\langle V \rangle \approx \mathbb{C}_2$. $M : y^2 = (x^2 - 1)(x^2 - a^2)(x^2 - b^2)$, 

(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 $(\alpha, \eta)$ which satisfies 

$$a^2 = \left(\frac{\sqrt{\alpha + \eta}}{\sqrt{\alpha - \eta}}\right)^{2i} \left(\frac{\sqrt{\alpha + \eta}}{\sqrt{\alpha - \eta}}\right)^{2k},$$

$$b^2 = \left(\frac{\sqrt{\alpha + \eta}}{\sqrt{\alpha - \eta}}\right)^{2j} \left(\frac{\sqrt{\alpha + \eta}}{\sqrt{\alpha - \eta}}\right)^{2k} \quad \text{and} \quad \eta^4 = 1.$$ 

(25)

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

$$a^2 = \left(\frac{\sqrt{\alpha - \zeta_3^j \eta}}{\sqrt{\alpha + \zeta_3^j \eta}}\right)^{2i} \left(\frac{\sqrt{\alpha - \zeta_3^k \eta}}{\sqrt{\alpha + \zeta_3^k \eta}}\right)^{2k},$$

$$b^2 = \left(\frac{\sqrt{\alpha - \zeta_3^j \eta}}{\sqrt{\alpha + \zeta_3^j \eta}}\right)^{2j} \left(\frac{\sqrt{\alpha - \zeta_3^k \eta}}{\sqrt{\alpha + \zeta_3^k \eta}}\right)^{2k} \quad \text{and} \quad \eta^6 = 1.$$ 

(26)

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

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

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

(27)

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

$$M' : y^2 = x(x^2 - 1)(x^2 - \alpha^2).$$
The automorphism group of a cyclic p-gonal curve

Therefore, under the existence of \((\alpha, \eta)\) satisfying (25),

\[
\begin{align*}
\text{#-4-i)} & \quad \text{Aut}(M)/\langle V \rangle \simeq D_4 \text{ if and only if } \alpha^2 \neq -1, \\
\text{#-4-ii)} & \quad \text{Aut}(M)/\langle V \rangle \simeq S_4 \text{ if and only if } \alpha^2 = -1.
\end{align*}
\]

\[
\begin{align*}
\text{#-5). Assume there exists } \alpha \text{ which satisfies (26) for some } \{i, j, k\} = \{0, 1, 2\}. \text{ Then } \alpha^3 \neq 0, 1, \text{ and the equalities}
\end{align*}
\]

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

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

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

Therefore, under the existence of \(\alpha\) satisfying (26),

\[
\begin{align*}
\text{#-5-i)} & \quad \text{Aut}(M)/\langle V \rangle \simeq D_6 \text{ if and only if } \alpha^3 \neq -1 \text{ and } \alpha^3 \neq \frac{(1 + \sqrt{3})}{(1 + \sqrt{3})^3}, \\
\text{#-5-ii)} & \quad \text{Aut}(M)/\langle V \rangle \simeq D_{12} \text{ if and only if } \alpha^3 = -1, \\
\text{#-5-iii)} & \quad \text{Aut}(M)/\langle V \rangle \simeq S_4 \text{ if and only if } \alpha^3 = \frac{(1 + \sqrt{3})}{(1 + \sqrt{3})^3}.
\end{align*}
\]

\[
\text{#-6). If } \{1, a^2, b^2\} = \{1, \zeta_3, \zeta_3^2\}, \text{ then } \text{Aut}(M)/\langle V \rangle \simeq D_{12}.
\]

**Proof.** Let \(\mathcal{A}\) denote \(\text{Aut}(M)/\langle V \rangle\).

**Cases \(\mathcal{A} \simeq S_4, C_5\) and \(D_{12}\).** The equations (18), (19), (20) come from Proposition 4.1.

**Case \(\mathcal{A} \simeq D_4\).** By Proposition 4.1, a curve

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

satisfies \(D_4 = \langle S_2, \bar{T} \rangle \subset \mathcal{A}\), where \(\bar{T}^*x = a/x\).

If \(D_4 \subset \mathcal{A}\), then, also by Proposition 4.1, \(\mathcal{A}\) must be isomorphic to \(S_4\). Now take an element \(D \in \mathcal{A}\) of order 4. Then \(D\) acts on \(\mathcal{S} = \{0, \infty, \pm 1, \pm a\}\) and has two fixed points in \(\mathcal{S}\).

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 \(\infty\), 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 \(J = \begin{pmatrix} 1 & 0 \\ 1 & -a \end{pmatrix}\). Then \((JDJ^{-1})^*x = \pm \sqrt{-1}x\) and \(JDJ^{-1}\) acts on \(J([\infty, -1, a, -a]) = \left\{ 1, \frac{a}{a+1}, \frac{a}{a-1} \right\}\). This does not happen.
By checking any other possibilities of fixed points of $D$ in $\mathcal{P}$, we can see that $\mathcal{A} = S_4$ if and only if $a^2 = -1$.

**Case $\mathcal{A} \simeq D_6$.** From Proposition 4.1, the curve

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

satisfies $D_6 = \langle S_3, T \rangle \subset \mathcal{A}$. If $D_6 \not\subseteq \mathcal{A}$, then $\mathcal{A} \simeq D_{12}$ or $\mathcal{A} \simeq S_4$.

Assume $\mathcal{A} \simeq D_{12}$. By the structure of $D_{12}$ there exists an element $S'$ of order 6 in $\mathcal{A}$ such that $S'^2$ coincides with the element $S_3 \in \mathcal{A}$. For $S_3^*x = \zeta_3x$, $S'^*x = \eta x$ with $\eta^2 = \zeta_3$. As $S'$ acts on $\mathcal{P} = \{1, \zeta_3, \zeta_3^2, a, \zeta_3a, \zeta_3^2a\}$, $a$ must be a primitive 6-th root of unity and $\mathcal{P} = \{1, \eta, \ldots, \eta^5\}$. So we arrive at $\#-2$.

Assume $\mathcal{A} \simeq S_4$. Then there is a birational map $F$ from $M$ to

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

Let $\bar{F} : M/\langle V \rangle \to M'/\langle V \rangle$ be the morphism induced by $F$. Put $D = \bar{F} \circ S_3 \circ \bar{F}^{-1} \in \text{Aut}(M'/\langle V \rangle)$. From the structure of $S_4$, there are 8 elements of order 3 in $S_4$, and they are represented by matrices $R^t W^s R^{-t}$ ($s = 1, 2, t = 0, 1, 2, 3$) in $\text{Aut}(M'/\langle V \rangle)$ (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 $\bar{F}$ sends fixed points of $S_3$ to those of $D$, we have $\bar{F}(\{0, \infty\}) = \{a_1 \cdot i^t, a_2 \cdot i^t\}$ and then $F^*x = Ax$ with a matrix $A = \left( \begin{array}{cc} a_1i^t & \delta a_1i^t \\ 1 & \delta \end{array} \right)$ or $\left( \begin{array}{cc} a_2i^t & \delta a_2i^t \\ 1 & \delta \end{array} \right)$ ($\delta$ is a suitable number).

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

$$F^*x((F^*x)^4 - 1) = i'a_2(a_2^3 - 1)(x + \delta)^{-6}$$

$$\times \left\{ \left( x + \delta \frac{a_1}{a_2} \right) \left( x + \delta \frac{a_1 - 1}{a_2 - 1} \right) \left( x + \delta \frac{a_1 - i}{a_2 - i} \right) \right\}$$

$$\times \left\{ \left( x + \delta \right) \left( x + \delta \frac{a_1 + 1}{a_2 + 1} \right) \left( x + \delta \frac{a_1 + i}{a_2 + i} \right) \right\}.$$
The automorphism group of a cyclic $p$-gonal curve

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

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

(30)

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

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

Then "$\delta^3 = -1$ and $\delta \left(\frac{a_1}{a_2}\right)^3 = -a^3$" or "$\delta^3 = -a^3$ and $\delta \left(\frac{a_1}{a_2}\right)^3 = -1$". Therefore $a^3 = \left(1 + \sqrt[3]{3}\right)$ Using $\left(\frac{a_1 \pm i}{1 + \sqrt[3]{3}}\right)$ for $A$, we can get the same result. Therefore $\mathcal{A} \simeq D_6$ implies $a^3 \neq \left(1 + \sqrt[3]{3}\right)$.

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

$\mathcal{A} \simeq C_2$. From Proposition 4.1, the curve

$$M : y^2 = (x^2 - 1)(x^2 - a^2)(x^2 - b^2)$$

(31)

satisfies $\mathcal{A} \supset \langle S_2 \rangle \simeq C_2$. If $C_2 \subseteq \mathcal{A}$, then $\mathcal{A} = D_4, D_6, D_{12}$ or $S_4$.

Assume $\mathcal{A} \simeq D_4 \supset \langle S_2 \rangle$. There is a birational morphism $F$ from $M$ to

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

By Proposition 4.1, $\text{Aut}(M')/\langle V \rangle = \langle S_2, T \rangle$ with $T^*x = a/x$. Let $\tilde{F} : M/\langle V \rangle \to M'/\langle V \rangle$ be the morphism induced by $F$. Put $J := \tilde{F} \circ S_2 \circ \tilde{F}^{-1}(\in \text{Aut}(M')/\langle V \rangle)$. Then $\tilde{F}(\mathcal{S}) = \{0, \infty, \pm 1, \pm a\} \quad (\mathcal{S} = \{\pm 1, \pm a, \pm b\})$, 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 $\mathcal{S}$ but $S_2$ (on $M'/\langle V \rangle$) fixes $0$ and $\infty$ in $\tilde{F}(\mathcal{S})$, we can see $J \neq S_2$ (on $M'/\langle V \rangle$). Therefore $J^*x = \pm a/x$, and $\tilde{F}(\{0, \infty\}) = \{\pm \sqrt{a}\}$ (resp. $\{\pm \sqrt{-1 a}\}$) provided $J^*x = \alpha/x$ (resp. $J^*x = -\alpha/x$). So

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

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

The equation $(F^*y)^2 = F^*x((F^*x)^2 - 1)((F^*x)^2 - a^2)$ is transformed as follows.
\[(F*y)^2 = A(x)(A(x)^2 - 1)(A(x)^2 - \alpha^2)\]
\[= (\eta\sqrt{\alpha}^3(\alpha - \eta^2)^2(x - \delta)^6(x - \delta)(x + \delta)\]
\[\times \left( x + \delta \left( \frac{\eta\sqrt{\alpha} + 1}{\eta\sqrt{\alpha} - 1} \right) \right)\left( x + \delta \left( \frac{\eta\sqrt{\alpha} - 1}{\eta\sqrt{\alpha} + 1} \right) \right)\]
\[\times \left( x - \delta \left( \frac{\sqrt{\alpha} + \eta}{\sqrt{\alpha} - \eta} \right) \right)\left( x - \delta \left( \frac{\sqrt{\alpha} - \eta}{\sqrt{\alpha} + \eta} \right) \right)\]
\[= (\eta\sqrt{\alpha}^3(\alpha - \eta^2)^2(x - \delta)^6(x^2 - \delta^2)\]
\[\times \left( x^2 - \delta^2 \left( \frac{\sqrt{\alpha} + \eta}{\sqrt{\alpha} - \eta} \right)^2 \right)\left( x^2 - \delta^2 \left( \frac{\sqrt{\alpha} - \eta}{\sqrt{\alpha} + \eta} \right)^2 \right).
\]

As \(\mathcal{S}\) 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 \((\alpha, \eta)\) satisfies (25). Thus \(\mathcal{A} \neq D_3\) implies the condition (I).

Conversely assume that there is a pair \((\alpha, \eta)\) 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 \(\mathcal{A} \simeq D_6\). There is a birational map \(F\) from \(M\) to

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

Let \(\tilde{F}\) be as before. Put \(J := \tilde{F} \circ S_2 \circ \tilde{F}^{-1}\). On the other hand, as \(\text{Aut}(M')/\langle V \rangle = \langle S_3, \bar{T} \rangle\), \(J^*x = \zeta^s_3 \alpha/x\) for some \(0 \leq s \leq 2\). Since the fixed points of \(J\) are \(\pm \zeta^{2s}_3 \sqrt{\alpha}\), we have \(\tilde{F}(\{0, \infty\}) = \{ \zeta^{2s}_3 \sqrt{\alpha}, -\zeta^{2s}_3 \sqrt{\alpha} \}\) and

\[F^*x = B(x) = \frac{\eta\sqrt{\alpha}x + \delta \eta\sqrt{\alpha}}{-x + \delta}, \quad B := \left( \begin{array}{cc} \eta\sqrt{\alpha} & \delta \eta\sqrt{\alpha} \\ -1 & \delta \end{array} \right),\]

where \(\eta = \pm \zeta^{2s}_3\).

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

\[(F*y)^2 = (-x + \delta)^{-6} \eta^3 \sqrt{\alpha}^3 \{(\sqrt{\alpha}^3 (x + \delta)^3 - \eta^3 (-x + \delta)^3)\}
\times \{ (\eta^3 (x + \delta)^3 - \sqrt{\alpha}^3 (-x + \delta)^3)\}\]
The automorphism group of a cyclic $p$-gonal curve

\[ (-x + \delta)^{-6} \eta^3 \sqrt{\alpha^3} \]
\[ \times \prod_{t=0}^{2} \{ \sqrt{\alpha(x + \delta) - \zeta_3^t \eta(-x + \delta)} \} \prod_{t=0}^{2} \{ -\sqrt{\alpha(-x + \delta) + \zeta_3^t \eta(x + \delta)} \} \]
\[ = (-x + \delta)^{-6} \eta^3 \sqrt{\alpha^3} \]
\[ \times \prod_{t=0}^{2} (\sqrt{\alpha + \zeta_3^t \eta}) \left\{ x + \delta \left( \frac{\sqrt{\alpha - \zeta_3^t \eta}}{\sqrt{\alpha + \zeta_3^t \eta}} \right) \right\} \prod_{t=0}^{2} (\sqrt{\alpha + \zeta_3^t \eta}) \left\{ x - \delta \left( \frac{\sqrt{\alpha - \zeta_3^t \eta}}{\sqrt{\alpha + \zeta_3^t \eta}} \right) \right\} \]
\[ = (-x + \delta)^{-6} \eta^3 (\eta^3 + \sqrt{\alpha^3})^2 \]
\[ \times \left( x^2 - \delta^2 \left( \frac{\sqrt{\alpha - \eta}}{\sqrt{\alpha + \eta}} \right)^2 \right) \left( x^2 - \delta^2 \left( \frac{\sqrt{\alpha - \zeta_3 \eta}}{\sqrt{\alpha + \zeta_3 \eta}} \right)^2 \right) \]
\[ \times \left( x^2 - \delta^2 \left( \frac{\sqrt{\alpha - \zeta_5 \eta}}{\sqrt{\alpha + \zeta_5 \eta}} \right)^2 \right). \]

Then we have
\[ \{1, a^2, b^2\} = \left\{ \delta^2 \left( \frac{\sqrt{\alpha - \eta}}{\sqrt{\alpha + \eta}} \right)^2, \delta^2 \left( \frac{\sqrt{\alpha - \zeta_3 \eta}}{\sqrt{\alpha + \zeta_3 \eta}} \right)^2, \delta^2 \left( \frac{\sqrt{\alpha - \zeta_5 \eta}}{\sqrt{\alpha + \zeta_5 \eta}} \right)^2 \right\}, \]
and the pair $(\alpha, \eta)$ satisfies (26). Thus $\mathcal{A} \neq \mathcal{D}_6$ implies the condition (II).

Conversely if there exists $\alpha^3$ 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 $\left( \frac{1 \pm \sqrt{3}}{1 + \sqrt{3}} \right)$. Thus we get $\#-5$ from (22), $\#-2$ and $\#-3$.

Next assume $\mathcal{A} \simeq \mathcal{D}_{12}$. There is a birational map $F$ from $M$ to $M' : y^2 = (x^6 - 1)$.

Put $J := \bar{F} \circ S_2 \circ \bar{F}^{-1}$ as above. Then $J^* x = \zeta_6^s / x$ $(0 \leq s \leq 5)$ or $J^* x = -x$ on $M'$. But when $J^* x = \zeta_6^s / x$, we can follow the same argument in the case of $\mathcal{A} \simeq \mathcal{D}_6$, 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 $\bar{F}$ 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 $\delta$. At the same time $\bar{F}$ sends $\{ \pm 1, \pm \zeta_3, \pm \zeta_5 \}$ to $\{ \pm 1, \pm \zeta_3, \pm \zeta_5 \}$, so we know that $\delta = \zeta_3^k$ and $\{1, a^2, b^2\} = \{1, \zeta_3, \zeta_5^2 \}$. Thus we get $\#-6$. Overall, we know that $\mathcal{A} \simeq \mathcal{C}_2$ 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
\[ y^3 - (x - a_1)^{r_1} \cdots (x - a_i)^{r_i} = 0 \quad (1 \leq r_i \leq 2, \text{ } a_i\text{'s are distinct}). \] (32)
The genus $g$ of $M$ is $\#\mathcal{P} - 2$. We also assume $g \geq 5$ (i.e., $M$ has unique $g_1^1$).

In this section we study $M$ with odd $g$. In particular we will determine all possible types of $\text{Aut}(M)/\langle V \rangle$ 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) $\text{Aut}(M)/\langle V \rangle$ is isomorphic to a cyclic group or a dihedral group,
(ii) If $\text{Aut}(M)/\langle V \rangle \cong D_{2n}$, then $n$ is odd.

**Proof.** (i) Assume $A_4 \subseteq \text{Aut}(M)/\langle V \rangle$. The equation $\#\mathcal{P} = 4e_1 + 6e_2 + 4e_3 + 12 \sum 1$ for $H = A_4$ in Theorem 3.1 indicates that $\#\mathcal{P}$ and $g$ are even. This is a contradiction. So $A_4 \not\subseteq \text{Aut}(M)/\langle V \rangle$, and then $A_5, S_4 \not\subseteq \text{Aut}(M)/\langle V \rangle$.

(ii) The equality $\#\mathcal{P} = ne_1 + ne_2 + 2e_3 + 2n \sum e_i = 4$ for $H = D_{2n}$ 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 $\mathcal{A} := \text{Aut}(M)/\langle V \rangle$ is non-trivial. Then the type of $\mathcal{A}$ and a standard defining equation of $M$ are as follows.

I. $g = 9$.

$\mathcal{A} \cong C_{10}$. $M$ is defined by
\[ y^3 = x(x^{10} - 1)^2, \quad \text{the exact sequence (\star) is split}. \] (33)

$\mathcal{A} \cong C_9$. $y^3 = x(x^9 - 1)^r$ ($r = 1, 2$), \quad (\star) is non-split. \] (34)

$\mathcal{A} \cong C_5$. $y^3 = x(x^5 - 1)^2(x^5 - a_5)^2 (a_5 \neq 0, \pm 1)$, \quad (\star) is split. \] (35)

b-1) The curve (35) has $\mathcal{A} \cong C_{10}$ if and only if $a_5 = -1$.

$\mathcal{A} \cong C_3$. $y^3 = x(x^3 - 1)^u_9(x^3 - a^3)^u_4(x^3 - b^3)^u_5$, \quad (\star) 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).
The automorphism group of a cyclic \( p \)-gonal curve

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) \( \{a^3, b^3\} \neq \{\zeta_3, \zeta_3^2\} \).

b-2) \( \mathcal{A} \cong C_2 \) 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).

\( \mathcal{A} \cong C_2 \). \( M \) is defined by

\[ y^3 = x(x^2 - 1)^{u_1}(x^2 - a^2)^{u_4}(x^2 - b^2)^{u_5}(x^2 - c^2)^{u_6}(x^2 - d^2)^{u_7}, \quad (\ast) \text{ is split,} \quad (37) \]

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

b-i) \( u_3 = \cdots = u_7 = 2 \) and b-ii) \( \{1, a^2, b^2, c^2, d^2\} \neq \{\zeta_3^k | 0 \leq k \leq 4\} \).

b-3) \( \mathcal{A} \cong C_{10} \) if and only if \( u_3 = \cdots = u_7 = 2 \) and \( \{1, a^2, b^2, c^2, d^2\} = \{\zeta_3^k | 0 \leq k \leq 4\} \) hold. In this case (37) coincides with (33).

II. \( g = 7 \).

\( \mathcal{A} \cong D_{18} \). \( M \) is defined by

\[ y^3 = (x^9 - 1), \quad (\ast) \text{ is split.} \quad (38) \]

\( \mathcal{A} \cong C_8 \). \( y^3 = x(x^8 - 1), \quad (\ast) \text{ is split.} \quad (39) \]

\( \mathcal{A} \cong D_{14} \). \( y^3 = x(x^7 - 1), \quad (\ast) \text{ is split.} \quad (40) \]

\( \mathcal{A} \cong C_4 \). \( y^3 = x(x^4 - 1)(x^4 - a^4) \quad (a^4 \neq 0, \pm 1), \quad (\ast) \text{ is split.} \quad (41) \]

b-4) \( \mathcal{A} \cong C_8 \) if and only if \( a^4 = -1 \). In this case (41) coincides with (39).

\( \mathcal{A} \cong D_6 \).

\[ y^3 = (x^3 - 1)(x^6 - bx^3 + 1)^u \quad ("b \neq \pm 2" \text{ and } "u \neq 1 \text{ or } b \neq -1"), \quad (\ast) \text{ is split.} \quad (42) \]

b-5) \( \mathcal{A} \cong D_{18} \) if and only if \( u = 1 \) and \( b = -1 \) hold. And (42) coincides with (38).

\( \mathcal{A} \cong C_3 \). \( y^3 = (x^3 - 1)(x^3 - a_1^3)^{v_1}(x^3 - a_2^3)^{v_2}, \quad (\ast) \text{ is split.} \quad (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 \( v_2 \neq 1 \).
b-6) Assume $a_1^3 a_2^3 = 1$ 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

b-6-i) $\mathcal{A} \cong D_6$ 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

b-6-ii) $\mathcal{A} \cong D_{18}$ if and only if $a_1^3 + a_2^3 = -1$ and $v_1 = 1$ hold (in this case (43) coincides with (38)).

b-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

b-7-i) $\mathcal{A} \cong D_6$ if and only if $a_j^3 \neq \xi_3^\pm 1$ or $v_j \neq 1$ (in this case (43) is birational to (42) with $b = a_j^3 + a_j^{-3}(\neq -1)$), and

b-7-ii) $\mathcal{A} \cong D_{18}$ if and only if $a_j^3 = \xi_3^\pm 1$ and $v_j = 1$ hold ((43) is birational to (38)).

$\mathcal{A} \cong C_2.$

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

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 $c_3 := 1$.

\[
\begin{aligned}
a-i) & \quad u_3 = u_4 = u_5 = u_6 = 1, \\
a-ii) & \quad \text{there is no number } \alpha \text{ satisfying} \\
& \quad \{ c_4^2, c_5^2, c_6^2 \} = \{-1, \alpha^2, -\alpha^2\}, \quad (\star)
\end{aligned}
\]

and

\[
\begin{aligned}
a-iii) & \quad \text{for each } \{i,j,k,l\} = \{3,4,5,6\}, \text{ there is no number } \alpha \text{ satisfying} \\
& \quad c_i^2 : c_j^2 : c_k^2 = 3 : -\left( \frac{\alpha - 1}{\alpha + 1} \right)^2 : -\left( \frac{\xi_3^3 \alpha - 1}{\xi_3^3 \alpha + 1} \right)^2 = -\left( \frac{\xi_3^2 \alpha - 1}{\xi_3^2 \alpha + 1} \right)^2. \quad (\star\star)
\end{aligned}
\]

b) \[
\begin{aligned}
b-i) & \quad u_i = 1, u_j = u_k = u_l = 2 \text{ with } \{i,j,k,l\} = \{3,4,5,6\}, \text{ and} \\
b-ii) & \quad \text{there is no number } \alpha \text{ satisfying } (\star\star) \text{ for the same } i,j,k,l \text{ in b-i).}
\end{aligned}
\]

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

b-8-i) $\mathcal{A} \cong C_4$ if and only if $\alpha^4 \neq -1$,

b-8-ii) $\mathcal{A} \cong C_8$ if and only if $\alpha^4 = -1$. 

b-9) Assume a-i) and there is $\alpha$ satisfying $(**)$ 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

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

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

- b-9-i) $\mathcal{A} \simeq D_6$ if and only if $\alpha^3 \neq \zeta_3^{\pm 1},$
- b-9-ii) $\mathcal{A} \simeq D_{18}$ if and only if $\alpha^3 = \zeta_3^{\pm 1}.$

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

Then $\mathcal{A} = D_6$ if and only if there is a number $\alpha$ satisfying $(**)$ 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

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

give a birational morphism from $M$ to $M'$.

III. $g = 5$

$\mathcal{A} \simeq D_{10}$:

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

$\mathcal{A} \simeq C_2$:

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

where $u_i = 2, u_j = u_k = 1$ for $\{i, j, k\} = \{3, 4, 5\},$ and $\{c_4^2, c_5^2\} \neq \left\{c_i^2\left(\frac{1 + \zeta_5}{1 + \zeta_5}\right)^2, \frac{1 - \zeta_5}{1 + \zeta_5}\right\}$. Here we denote $c_3 = 1$.

b-11) If $u_i = 2, u_j = u_k = 1$ and $\{c_4^2, c_5^2\} = \left\{c_i^2\left(\frac{1 + \zeta_5}{1 + \zeta_5}\right)^2, c_i^2\left(\frac{1 - \zeta_5}{1 + \zeta_5}\right)\right\}$, then $M$ is birational to $M' : y^3 = x^2(x^5 - 1)$ and $\mathcal{A} \simeq D_{10}$.

In fact

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

give a birational morphism from $M$ to $M'$. 

PROOF. Assume $\mathcal{A} \supset C_n$ with $n \geq 2$. Then, from Theorem 3.1, $M$ can be defined by

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

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. $u_k = 0$) ($k = 1, 2$).

$g = 9.$

Then $\# \mathcal{A} = 11$. For $n = 8, 7, 6, 4$ and $n \geq 12$, there are no $\varepsilon_i$ ($i = 1, 2$) or $d$, which satisfy (48-I) with $\# \mathcal{A} = 11$. When $n = 11$, $\varepsilon_1 = \varepsilon_2 = 0$ and $d = 3$ satisfy (48-I) with $\# \mathcal{A} = 11$. Therefore $u_1 = u_2 = 0$ and $u_3 = 1$ or 2. But they do not satisfy (48-II). Thus a number $n$ satisfying $\mathcal{A} \supset C_n$ is among 10, 9, 5, 3, 2. Moreover Lemma 5.1 implies that only $D_6, D_{10}, D_{18}$ are candidates for $\mathcal{A}$ among dihedral groups.

Case $\mathcal{A} \supset C_{10}$. 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

$$y^3 = x(x^{10} - 1)^2, \quad \mathcal{A} \supset C_{10} = \langle S_{10} \rangle.$$

By Lemma 5.1, we have $\mathcal{A} \simeq C_{10}$.

Case $\mathcal{A} \supset C_9$. 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

$$y^3 = x(x^9 - 1)^r, \quad \mathcal{A} \supset C_9 = \langle S_9 \rangle, \quad \text{with } r = 1, 2 \tag{49}$$

up to birational morphisms. From Lemma 5.1, we have $\mathcal{A} \simeq C_9$ or $D_{18}$.

Assume $\mathcal{A} \simeq D_{18}$. Let $\mathcal{A} = \langle S_9, T' \rangle$ with $T'^2 = 1$ and $T'S_9T'^{-1} = S_9^{-1}$. Then $T'(0) = \infty$ and $T'^n x = \alpha/x$ with some number $\alpha$. But, since $2 + 9r \neq 0$ (mod 3), there does not exist an automorphism of $M$ which induces $T'$. Thus $\mathcal{A} \supset C_9$ means $\mathcal{A} \simeq C_9$. 

Case $\mathcal{A} \supset C_5$. Then $d = 4$ and $e_1 + e_2 = 1$. (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
$$y^3 = x(x^3 - 1)^2(x^3 - a^3)^2, \quad \mathcal{A} \supset C_5 = \langle S_5 \rangle$$
(50)
up to birational morphisms. If $\mathcal{A} \supseteq C_5$, then $\mathcal{A} \simeq C_{10}$ or $D_{10}$.

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

When $\mathcal{A} \simeq D_{10}$, $\mathcal{A} = \langle S_5, T' \rangle$ with $T'^2 = 1$ and $T'S_5T'^{-1} = S_5^{-1}$. By the
same argument as in Case $\mathcal{A} \supset C_9$, we can deduce a contradiction from
$2 \cdot 1 + 2 \cdot 5 + 2 \cdot 5 \neq 0$ (mod 3). So $\mathcal{A} \simeq D_{10}$ does not happen. Thus we get $b=1$.

Case $\mathcal{A} \supset C_3$. Then $d = 5$ and $e_1 = e_2 = 1$. (48-II) holds if and only if
"$u_1 + u_2 = 3$". Therefore $M$ is defined by
$$y^3 = x(x^3 - 1)^a(x^3 - a^3)^u(x^3 - b^3)^w, \quad \mathcal{A} \supset C_3 = \langle S_3 \rangle.$$ (51)
If $\mathcal{A} \supseteq C_3$, then $\mathcal{A} \simeq C_9, D_6$ or $D_{18}$. The case $\mathcal{A} \simeq D_{18}$ has already been eliminated when we considered the case $\mathcal{A} \supset C_9$.

Assume $\mathcal{A} \simeq D_6$. Let $\mathcal{A} = \langle S_3, T' \rangle$ with $T'^2 = 1$, and $T'S_5T'^{-1} = S_5^2$. Then, by
the same argument as in Case $\mathcal{A} \supset C_9$, we can deduce a contradiction.

Assume $\mathcal{A} \simeq C_9$. There exists $S' \in \mathcal{A}$ 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\} = \{ζ_3, ζ_3^2\}. Then (51) coincides with (34). Thus we get $b=2$.

Case $\mathcal{A} \supset C_2$. Then $d = 7$ and $e_1 + e_2 = 1$. (48-II) holds if and only if
$$\begin{cases}
1) \quad u_1 = 0 \text{ (resp. 1)}, \ u_2 = 1 \text{ (resp. 0)}, \ u_3 = \ldots = u_7 = 2, \\
2) \quad u_1 = 0 \text{ (resp. 2)}, \ u_2 = 2 \text{ (resp. 0)}, \ u_3 = \ldots = u_7 = 1, \\
3) \quad u_1 = 0 \text{ (resp. 1)}, \ u_2 = 1 \text{ (resp. 0)}, \ u_i = u_j = u_k = 1, \ u_l = u_m = 2 \text{ with} \\
\{i, j, k, l, m\} = \{3, 4, 5, 6, 7\}, \\
or \\
4) \quad u_1 = 0 \text{ (resp. 2)}, \ u_2 = 2 \text{ (resp. 0)}, \ u_i = u_j = u_k = 2, \ u_l = u_m = 1 \text{ with} \\
\{i, j, k, l, m\} = \{3, 4, 5, 6, 7\}.
\end{cases}$$

Therefore, up to birational isomorphisms, we have two types of equations with $\mathcal{A} \supset C_2 = \langle ζ_2 \rangle$. That is:
$$y^3 = x(x^2 - 1)^2(x^2 - a)^2(x^2 - b)^2(x^2 - c)^2(x^2 - d)^2 \quad \text{(from 1 and 2)}$$

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

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 $\mathcal{A} \supseteq C_2$. The possibility of $\mathcal{A} \simeq D_6, D_{10}$ or $D_{18}$ has already been eliminated when we considered $\mathcal{A} \supseteq C_3, C_5$. Then $\mathcal{A} \simeq C_{10}$. By the same way as in Case $\mathcal{A} \supseteq C_9$, we know $\{1, a^2, b^2, c^2, d^2\} = \{\zeta_5^k | 1 \leq k \leq 5\}$ and $u_3 = \cdots = u_7$. Thus we get b-3).

$g = 7$.

Then $\#\mathcal{S} = 9$. For $n = 6, 5$ and $n \geq 10$, there are no $e_i$ ($i = 1, 2$) or $d$, which satisfy (48-1) with $\#\mathcal{S} = 9$. Thus a number $n$ satisfying $\mathcal{A} \supseteq C_n$ is among $9, 8, 7, 4, 3, 2$. Moreover, by Lemma 5.1, only $D_{18}, D_{14}, D_6$, among dihedral groups, are candidates for $\mathcal{A}$.

Case $\mathcal{A} \supseteq C_9$. Then $M: y^3 = (x^9 - 1)$ and $\mathcal{A} \simeq D_{18}$.

Case $\mathcal{A} \supseteq C_8$. Then $M: y^3 = x(x^8 - 1)$ and $\mathcal{A} \simeq C_8$.

Case $\mathcal{A} \supseteq C_7$. Then $M: y^3 = x(x^7 - 1)$ and $\mathcal{A} \simeq D_{14}$.

Case $\mathcal{A} \supseteq C_6$. Then $M: y^3 = x(x^6 - 1)(x^4 - a^4)$. If $\mathcal{A} \supseteq C_4$, we have $\mathcal{A} \simeq C_8$. By the same way as in Case $\mathcal{A} \supseteq C_5$ of $g = 9$, we have $a^4 = -1$. Then we get b-4).

Case $\mathcal{A} \supseteq D_6$. Then, from (10) in Theorem 3.1, $M$ can be defined by

$$y^3 = (x^3 - 1)(x^6 - bx^3 + 1)^u \quad (b \neq \pm 2), \quad \mathcal{A} \supseteq D_6 = \langle S_3, T \rangle.$$

If $\mathcal{A} \supseteq D_6, \mathcal{A} \simeq D_{18}$. There is an element $S' \in \mathcal{A}$ satisfying $S'^3 = S_3$. Then $S'^x = \eta x$ with a primitive 9-th root $\eta$ of 1. Thus $\mathcal{S} = \{\zeta_9^k | 0 \leq k \leq 8\}, b = -1$ and $u = 1$. Then we get b-5).

Case $\mathcal{A} \supseteq C_3$. We have

$$y^3 = (x^3 - 1)(x^3 - a_1^3)^n(x^3 - a_2^3)^m, \quad \mathcal{A} \supseteq C_3 = \langle S_3 \rangle. \quad (52)$$

If $\mathcal{A} \supseteq C_3$, then $\mathcal{A} \simeq D_6$ or $\mathcal{A} \simeq D_{18}$.

Assume $\mathcal{A} \supseteq D_6 = \langle S_3, T' \rangle$ with $T'^2 = 1$ and $T'S_3T'^{-1} = S_3^2$.

Put $H = \{\zeta_3^k | 0 \leq k \leq 2\}$, $H_1 = \{a_1\zeta_3^k | 0 \leq k \leq 2\}$, $H_2 = \{a_2\zeta_3^k | 0 \leq k \leq 2\}$ and $\mathcal{K} = \{H, H_1, H_2\}$. Then $T'$ acts on $\mathcal{K}$, and $T'$ fixes exactly one element in $\mathcal{K}$ because $T'$ is of order 2 and it has just two fixed points. For example,
The automorphism group of a cyclic $p$-gonal curve

$T'H = H_i$ and $T'H_j = H_j$ with $\{i, j\} = \{1, 2\}$. From $T'H = H_i$ and $T'(0) = \infty$, $T''x = (\zeta_k^2 a_i)/x$ ($0 \leq k \leq 2$) 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

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

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

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

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

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

Case $\mathcal{A} \supset \mathbb{C}_2$. $M$ is defined by

$$y^3 = x(x^2 - 1)^u (x^2 - c_4^3)u_s (x^2 - c_5^2)u_s (x^2 - c_6^2)u_s, \quad \mathcal{A} \supset \mathbb{C}_2 = \langle S_2 \rangle$$

with

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

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

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

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

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

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

$$\mathcal{Q}' := \{1, \zeta_3, \zeta_3^2, \zeta_3^3, \alpha, \alpha \zeta_3, \alpha \zeta_3, \alpha \zeta_3^2, \alpha^{-1} \zeta_3, \alpha^{-1} \zeta_3^2, \zeta_3^3 \}$$

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

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

Since $\tilde{F}$ also sends the orbit decomposition of $\mathcal{Q}$ by $\langle S_2 \rangle$ to that of $\mathcal{Q}'$ by $\langle T' \rangle$, we have
\[ \{A^{-1}(\zeta_3^2), A^{-1}(\zeta_3^2g)\} = \{c_i, -c_i\}, \quad \{A^{-1}a, A^{-1}(a^{-1})\} = \{c_j, -c_j\}, \]
\[ \{A^{-1}(\zeta_3a), A^{-1}(\zeta_3^2x^{-1})\} = \{c_k, -c_k\}, \quad \{A(\zeta_3a), A(\zeta_3^2x^{-1})\} = \{c_i, -c_i\}, \]

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 
\[ y^2 = \left( \frac{\zeta_3^{i+j+1}}{\zeta_3^{i+j-1}} \right) c_i^2 = -c_i^2/3 \]
and 
\[ c_i^2 : c_j^2 : c_k^2 : c_l^2 = 3 : -\left( \frac{\alpha - \zeta_3^{2e}}{\alpha + \zeta_3^{2e}} \right)^2 : -\left( \frac{\zeta_3^3x - \zeta_3^{2e}}{\zeta_3^3x + \zeta_3^{2e}} \right)^2 : -\left( \frac{\zeta_3^{2e} - \zeta_3^{2e}}{\zeta_3^{2e} + \zeta_3^{2e}} \right)^2. \]

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

Conversely we assume that there exists \( \alpha \) satisfying (**) 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 b-5), \( \mathcal{A} \simeq D_6 \) (resp. \( \mathcal{A} \simeq D_{18} \)) provided \( \alpha^3 \neq \zeta_3^{\pm 1} \) (resp. \( \alpha^3 = \zeta_3^{\pm 1} \)). Thus we get b-9).

When b-i) is satisfied with the same \( i, j, k, l \) in the relation (**), 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 b-10).

\( g = 5 \).

Then \( \#\mathcal{S} = 7 \). For \( n = 4, 3 \) and \( n \geq 6 \), there are no \( \varepsilon_i \) \( (i = 1, 2) \) and \( d \) satisfying (48-I, II) with \( \#\mathcal{S} = 7 \). Thus non-trivial \( \mathcal{A} \) is possibly isomorphic to \( C_2, C_5 \) or \( D_{10} \).

Case \( \mathcal{A} \supset C_2 = \langle S_5 \rangle \). Then \( M \) is defined by \( y^3 = x^2(x^5 - 1) \). Moreover we can see \( \mathcal{A} = D_{10} = \{S_5, T\} \).

Case \( \mathcal{A} \supset C_2 = \langle S_2 \rangle \). Then \( M \) is defined by
\[ M : y^3 = x(x^2 - 1)^u_1(x^2 - c_3^2)^u_2(x^2 - c_2^2)^u_5, \]
where \( u_i = 2, u_j = u_k = 1 \) for \( \{i, j, k\} = \{3, 4, 5\} \).

Assume \( \mathcal{A} \not\supset C_2 \). Then \( \mathcal{A} \simeq D_{10} \). 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 \( \pm \zeta_5^k \).

Only 0 is fixed by \( S_2 \) in \( \mathcal{S} = \{0, \pm c_3, \pm c_4, \pm c_5\} \), and only \( \zeta_5^k \) is fixed by \( J \) in
The automorphism group of a cyclic $p$-gonal curve

$\mathcal{C}' = \{0, \infty, 1, \zeta_3, \ldots, \zeta_3^2\}$. Therefore $\bar{F}(0) = \zeta_3^{2k}$, $\bar{F}(\infty) = -\zeta_3^{2k}$ and

$$F^*x = \frac{\zeta_3^{2k} x + \delta \zeta_3^{2k}}{-x + \delta} \text{ (with a suitable number } \delta).$$

By the same calculations as before, we have

$$(F^*x)^2((F^*x)^5 - 1) = 2\zeta_5^k(-x + \delta)^{-9}x(x^2 - \delta^2)^2$$

$$\times \left\{ x^2 - \delta^2 \left( \frac{1 - \zeta_5}{1 + \zeta_5} \right)^2 \right\} \left\{ x^2 - \delta^2 \left( \frac{1 - \zeta_5^2}{1 + \zeta_5^2} \right)^2 \right\}. \quad (55)$$

Then $\{c_2^2, c_2^2, c_2^2\} = \left\{ \delta^2, \delta^2 \left( \frac{1 - \zeta_5}{1 + \zeta_5} \right)^2, \delta^2 \left( \frac{1 - \zeta_5^2}{1 + \zeta_5^2} \right)^2 \right\}$. As $u_i = 2$ and $u_j = u_k = 1$, we can see $\delta^2 = c_2$ and $\{c_2^2, c_2^2\} = \left\{ c_2^2 \left( \frac{1 - \zeta_5}{1 + \zeta_5} \right)^2, c_2^2 \left( \frac{1 - \zeta_5^2}{1 + \zeta_5^2} \right)^2 \right\}$ from (55).

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

Appendix

Here $S_n, T, U, W, R, K, Z$ are elements of $SL_2(\mathbb{C})$ defined by $S_n = (\zeta_n^0 \ 0)$, $T = \begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix}$, $U = \frac{1+i}{2} (i \ -i)$, $W = \frac{1+i}{2} (\ -1 \\ i)$, $R = \begin{pmatrix} \frac{-i}{\sqrt{3}} & 0 \\ 0 & \frac{i}{\sqrt{3}} \end{pmatrix}$, $Z = \zeta_4^{-1}(\zeta_4^0 \ 0)$, $K = \frac{1}{\sqrt{5}}(\zeta_4^1 - \zeta_4^3 \ 1 - \zeta_4^1 \ -\zeta_4^3 \ \zeta_4^1 \ -\zeta_4^3)$. And the symbol $\left\{ n_1 \ n_2 \ldots \right\}$ means that $\pi$ is ramified over $\alpha_i$ with ramification index $n_i$.

<table>
<thead>
<tr>
<th>group $H$</th>
<th>$#H$</th>
<th>generators $A = (a \ b \ c) \ (a \in SL(2, \mathbb{C})/(\pm 1))$</th>
</tr>
</thead>
<tbody>
<tr>
<td>cyclic $C_n$, $[n]$</td>
<td>$x^n$</td>
<td>$\left{ n \ n \right}$</td>
</tr>
<tr>
<td>dihedral $D_{2n}$, $[2n]$</td>
<td>$x^{2n} + 1$</td>
<td>$\left{ 2 \ 2 \ n \right}$</td>
</tr>
<tr>
<td>tetrahedral $A_4$, $[12]$</td>
<td>$(x^4 - 2\sqrt{3}x^2 + 1)^3$</td>
<td>$\left{ 3 \ 2 \ 3 \right}$</td>
</tr>
<tr>
<td>octahedral $S_4$, $[24]$</td>
<td>$108x^4(x^4 - 1)^4$</td>
<td>$\left{ 3 \ 3 \ 4 \right}$</td>
</tr>
<tr>
<td>icosahedral $A_5$, $[60]$</td>
<td>$-x^{20} - 1 + 228(x^{15} - x^5) - 494x^{10} + 1728x^5(x^{10} + 11x^5 - 1)^2$</td>
<td>$\left{ 3 \ 2 \ 5 \right}$</td>
</tr>
</tbody>
</table>
Table 2: Types of $P_{(b_0:b_1)}$.

<table>
<thead>
<tr>
<th>group</th>
<th>$(b_0 : b_1) \in P^1(u)$</th>
<th>ramification index over $(b_0 : b_1)$</th>
<th>$P_{(b_0:b_1)}$</th>
<th>type of $P_{(b_0:b_1)}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$C_n$</td>
<td>$(0 : 1)$</td>
<td>$n$</td>
<td>$P_{(0:1)} = 1$</td>
<td>(iii)</td>
</tr>
<tr>
<td></td>
<td>$(1 : 0)$</td>
<td>$n$</td>
<td>$P_{(1:0)} = x$</td>
<td>(ii)</td>
</tr>
<tr>
<td></td>
<td>$(1 : b)$ ($b \neq 0$)</td>
<td>$1$</td>
<td>$P_{(1:b)} = x^n - b$</td>
<td>(i)</td>
</tr>
<tr>
<td>$D_{2n}$</td>
<td>$(1 : 2)$</td>
<td>$2$</td>
<td>$P_{(1:2)} = x^n - 1$</td>
<td>(i)</td>
</tr>
<tr>
<td></td>
<td>$(1 : -2)$</td>
<td>$2$</td>
<td>$P_{(1:-2)} = x^n + 1$</td>
<td>(i)</td>
</tr>
<tr>
<td></td>
<td>$(0 : 1)$</td>
<td>$n$</td>
<td>$P_{(0:1)} = x$</td>
<td>(ii)</td>
</tr>
<tr>
<td></td>
<td>$(1 : b)$ ($b \neq \pm 2$)</td>
<td>$1$</td>
<td>$P_{(1:b)} = x^{2n} - bx^n + 1$</td>
<td>(i)</td>
</tr>
<tr>
<td>$A_4$</td>
<td>$(1 : 0)$</td>
<td>$3$</td>
<td>$P_{(1:0)} = (x^4 - 2\sqrt{3}ix^2 + 1)$</td>
<td>(i)</td>
</tr>
<tr>
<td></td>
<td>$(1 : 1)$</td>
<td>$2$</td>
<td>$P_{(1:1)} = x(x^4 - 1)$</td>
<td>(ii)</td>
</tr>
<tr>
<td></td>
<td>$(0 : 1)$</td>
<td>$3$</td>
<td>$P_{(0:1)} = (x^4 + 2\sqrt{3}ix^2 + 1)$</td>
<td>(i)</td>
</tr>
<tr>
<td></td>
<td>$(1 : b)$ ($b \neq 0, 1$)</td>
<td>$1$</td>
<td>$P_{(1:b)} = \frac{1}{12}((x^4 - 2\sqrt{3}ix^2 + 1)^3 - b(x^4 + 2\sqrt{3}ix^2 + 1)^3)}$</td>
<td>(i)</td>
</tr>
<tr>
<td>$S_4$</td>
<td>$(1 : 0)$</td>
<td>$3$</td>
<td>$P_{(1:0)} = x^8 + 14x^4 + 1$</td>
<td>(i)</td>
</tr>
<tr>
<td></td>
<td>$(1 : 1)$</td>
<td>$2$</td>
<td>$P_{(1:1)} = x^{12} - 33x^8 - 33x^4 + 1$</td>
<td>(i)</td>
</tr>
<tr>
<td></td>
<td>$(0 : 1)$</td>
<td>$4$</td>
<td>$P_{(0:1)} = x(x^4 - 1)$</td>
<td>(ii)</td>
</tr>
<tr>
<td></td>
<td>$(1 : b)$ ($b \neq 0, 1$)</td>
<td>$1$</td>
<td>$P_{(1:b)} = (x^8 + 14x^4 + 1)^3 - 108b(x(x^4 - 1))^4$</td>
<td>(i)</td>
</tr>
<tr>
<td>$A_5$</td>
<td>$(1 : 0)$</td>
<td>$3$</td>
<td>$P_{(1:0)} = x^{20} + 1 + 228(x^{15} - x^5) + 494x^{10}$</td>
<td>(i)</td>
</tr>
<tr>
<td></td>
<td>$(1 : 1)$</td>
<td>$2$</td>
<td>$P_{(1:1)} = x^{30} + 522x^{25} - 10005x^{20} - 10005x^{10} - 522x^5 + 1$</td>
<td>(i)</td>
</tr>
<tr>
<td></td>
<td>$(0 : 1)$</td>
<td>$5$</td>
<td>$P_{(0:1)} = x(x^{10} + 11x^5 - 1)$</td>
<td>(ii)</td>
</tr>
<tr>
<td></td>
<td>$(1 : b)$ ($b \neq 0, 1$)</td>
<td>$1$</td>
<td>$P_{(1:b)} = {x^{20} + 1 - 228(x^{15} - x^5) + 494x^{10}}^3 - 1728b(x(x^{10} + 11x^5 - 1))^5$</td>
<td>(i)</td>
</tr>
</tbody>
</table>

References

The automorphism group of a cyclic $p$-gonal curve


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.