TSUKUBA J. MATH.
Vol. 6, No. 1 (1982), 67–77

# ON THE CURVES OF GENUS $g$ WITH AUTOMORPHISMS OF PRIME ORDER $2g+1$

By

Atsushi SEYAMA

## Introduction.

Let $k$ be an algebraically closed field, and let $C$ be a complete non-singular curve of genus $g\geqq 2$ defined over $k$. In [2], M. Homma showst hat if a prime number $q$ is the order of an automorphism of $C$, then $q\leqq g+1$ or $q=2g+1$. He determines all $C$ in the case of $q=2g+1$ as follows:

(i) If $q$ is equal to the characteristic $p$ of $k$, then $C$ is birationally equivalent to the plane curve

$$y^{2}=x^{q}-x.$$

(ii) If $q$ is not equal to $p$, then $C$ is birationally equivalent to one of the following plane curves

$$y^{m-r}(y-1)^{r}=x^{q},\quad 1\leqq r<m\leqq g+1.$$

The case (ii) shows, in particular, there may be many isomorphy classes of curves of genus $g$ which admit an automorphism of prime order $2g+1\neq p$. The aim of this paper is to classify these curves.

Fix a prime number $q\geqq 5$ different from $p$. For a pair of positive integer $(r, s)$ such that any one of $r, s$ and $r+s$ is coprime to $q$, let $C(r, s)$ be a non-singular model of the irreducible equation

$$y^{r}(y-1)^{s}=x^{q}$$

over $k$. Then the genus of $C(r, s)$ is $(q-1)/2$ and $C(r, s)$ has an automorphism of order $q$. In §1, we shall give a basis of the space of differentials of the first kind on $C(r, s)$, in forms suitable to our later use. In §2, we shall give a condition under which $C(r, s)'s$ are isomorphic in terms of $r$ and $s$. This is our main result. In particular, we see that the cardinality of the set of isomorphy classes is, $(q+5)/6$ if $q\equiv 1 \bmod 3$, and $(q+1)/6$ if $q\equiv 2 \bmod 3$. In §3, we determine the order of the group of automorphisms of $C(r, s)$ in the case of characteristic zero.

The auther should like to express his sincere thanks to Dr. T. Sekiguchi and Dr. M. Homma for their encouragement during the preparation of this paper.

Received November 18, 1981

**Notation.**

Throughout this paper, we fix an algebraically closed field $k$, and a prime number $q\geqq 5$ different from the characteristic of $k$. All curves are considered to be defined over $k$. We write $|S|$ for the cardinality of a finite set $S$. The subgroup of a group $H$ generated by a family $\{h_1, \cdots, h_m\}$ of elements of $H$ is denoted by $\langle h_1, \cdots, h_m\rangle$. As usual, $\boldsymbol{Z}$, $\boldsymbol{Q}$ and $\boldsymbol{C}$ mean the ring of rational integers, the field of rational numbers, and the field of complex numbers respectively.

## § 1. Bases of the space of differentials.

Let $r_0$ and $r_1$ be positive integers such that any one of $r_0, r_1$ and $r_0+r_1$ is coprime to $q$. We consider a complete nonsingular curve $C$ over $k$ which is birationally equivalent to the plane curve

$$y^{r_0}(y-1)^{r_1}=x^q.$$

The curve $C$ has an automorphism $\theta$ of order $q$ defined by

$$\theta^*(y)=y, \quad \theta^*(x)=\zeta x,$$

where $\zeta$ is a primitive $q$-th root of unity in $k$. Consider the ramified covering

$$\eta: C \longrightarrow \boldsymbol{P}^1=C/\langle\theta\rangle,$$

correceponding to the inclusion $k(x, y)^{\langle\theta^*\rangle}=k(y)\subset k(x, y)$. The degree of $\eta$ is $q$, and $\eta$ is ramified at excatly three points $P_0, P_1$ and $P_\infty$ lying above $0, 1$ and $\infty\in\boldsymbol{P}^1=k\cup\{\infty\}$ respectively with the ramification index $q$. Consequently the divisors of rational functions $y, y-1$ and $x$, and that of differential $dy$ are as follows:

$$\begin{aligned}
&\operatorname{div}(y)=qP_0-qP_\infty, \quad \operatorname{div}(y-1)=qP_1-qP_\infty,\\
&\operatorname{div}(x)=r_0P_0+r_1P_1-(r_0+r_1)P_\infty,\\
&\operatorname{div}(dy)=(q-1)P_0+(q-1)P_1-(q+1)P_\infty.
\end{aligned}$$

In particular, the genus $g$ of $C$ is given by $(q-1)/2$.

For any integer $e$ coprime to $q$, we denote by $e^*$ the element of $\{1, \cdots, q-1\}$ such that

$$e\equiv e^* \bmod q.$$

Then we define a subset $E$ of $\{1, \cdots, q-1\}$ by

$$E=\left\{e\in\{1, \cdots, q-1\} \;\middle|\; \begin{array}{l} 0\leqq(a+b)q+q-(r_0+r_1)e-1, \text{ where} \\ r_0e=(r_0e)^*+aq,\ r_1e=(r_1e)^*+bq \end{array}\right\}$$

For each $e\in E$ with $r_0e=(r_0e)^*+aq$ and $r_1e=(r_1e)^*+bq$, we put

$$\omega_e=\frac{y^{r_0-1-a}(y-1)^{r_1-1-b}}{x^{q-e}}dy.$$

This differential is of the first kind. In fact, we easily see

$$\operatorname{div}(\omega_e)=(r_0e-aq-1)P_0+(r_1e-bq-1)P_1+((a+b)q+q-(r_0+r_1)e-1)P_\infty\geqq 0.$$

LEMMA 1.1. *We have*

(0) $E=\left\{e\in\{1,\cdots,q-1\}\ \middle|\ \begin{array}{l}(r_0e)^*+(r_1e)^*+(r_\infty e)^*=q,\\ \textit{where } r_\infty=-(r_0+r_1).\end{array}\right\}$

(1) $|E|=g$.

PROOF. Since $(r_0e)^*+(r_1e)^*=(r_0+r_1)e-(a+b)q\geqq 1$, we have $e\in E$ if and only if $1\leqq(r_0e)^*+(r_1e)^*\leqq q-1$. That is,

$$(r_0e)^*+(r_1e)^*=((r_0+r_1)e)^*.$$

Look at the equality $(-c)^*=q-c^*$ for any integer $c$ coprime to $q$, and we see that $e\in E$ if and only if

$$(r_0e)^*+(r_1e)^*+(r_\infty e)^*=q.$$

On the other hand, the function

$$e\longmapsto(r_0e)^*+(r_1e)^*+(r_\infty e)^*$$

takes exactly two values $q$ and $2q$ on $\{1,\cdots,q-1\}$, $e\notin E$ is equivalent to

$$(r_0e)^*+(r_1e)^*+(r_\infty e)^*=2q.$$

That is,

$$q-(r_0(-e))^*+q-(r_1(-e))^*+q-(r_\infty(-e))^*=2q.$$

The last equality is equivalent to $q-e\in E$, and we have $|E|=g$.

PROPOSITION 1.2. *We have the following.*

(1) $\{\omega_e\}_{e\in E}$ *is a basis of the space of differentials of the first kind on* $C$.

(2) *For* $i=0,1,\infty$, *let* $G_i$ *be the set of gap values at* $P_i$. *Then the map* $E\longrightarrow G_i$ *defined by* $e\longmapsto(r_ie)^*$ *is bijective for any* $i=0,1,\infty$.

PROOF. Since $|E|=g$, and

$$\operatorname{div}(\omega_e)=\sum_{i=0,1,\infty}((r_ie)^*-1)P_i,$$

it suffices to show that the map $E\longrightarrow G_i$ is injective for each $i$. But this is obvious because $r_i$ is coprime to $q$.

REMARK 1.3. Let $\zeta$ be a primitive $q$-th root of unity in the complex number field $\boldsymbol{C}$, and let $\varphi_e$ be an element of Gal $(\boldsymbol{Q}(\zeta)/\boldsymbol{Q})$ defined by $\varphi_e(\zeta)=\zeta^e$, for $e\in E$. Then the proof of Lemma 1.1. shows that $(\boldsymbol{Q}(\zeta), \{\varphi_e\}_{e\in E})$ is a C.M. type. This C.M. type arises as follows. Assume $k=\boldsymbol{C}$, and let $J$ be the Jacobian variety of $C$. The automorphism $\theta$ of $C$ induces an automorphism $\tilde{\theta}$ of order $q$ of $J$, and we have an isomorphism $i$ of $\boldsymbol{Q}(\zeta)$ into $\mathrm{End}(J)\otimes\boldsymbol{Q}$ defined by $i(\zeta)=\tilde{\theta}$. Then $(J, i)$ is of type $(\boldsymbol{Q}(\zeta), \{\varphi_e\}_{e\in E})$.

## § 2. Main results.

First of all, we restrict the equations of curves which we have to classify.

PROPOSITION 2.1. *Let $r_0$ and $r_1$ be positive integers such that any one of $r_0, r_1$ and $r_0+r_1$ is coprime to $q$.*

*Then the irreducible equation $y^{r_0}(y-1)^{r_1}=x^q$ is birationally equivalent to $y^r(y-1)=x^q$, for some $r=1, \cdots, q-2$.*

PROOF. Let $s$ be a positive integer such that $r_1 s=1+qb$, and put

$$r_0 s=r+qa, \quad r=1, \cdots, q-1.$$

Since $r_0+r_1$ and $s$ are coprime to $q$, we have $r\neq q-1$.

We shall show that the function field $k(x, y)$ defined by the equation

$$y^{r_0}(y-1)^{r_1}=x^q$$

is isomorphic to the function field $k(u, v)$ defined by the equation

$$v^r(v-1)=u^q.$$

But it is easy to see that

$$\varphi(u)=x^s/y^a(y-1)^b, \varphi(v)=y,$$

gives an isomorphism, $\varphi: k(u, v) \longrightarrow k(x, y)$.

For each $r=1, \cdots, q-2$, we fix a non-singular model of $y^r(y-1)=x^q$, which is denoted by $C_r$. The curve $C_r$ is a special one of $C$ in § 1, so we use the following notation; the automorphism of order $q$ of $C_r$ is denoted by $\theta_r$, three fixed points of $\theta_r$ are denoted by $P_{r,0}, P_{r,1}$ and $P_{r,\infty}$, the set of gap values at $P_{r,i}$ is denoted by $G_{r,i}(i=0, 1, \infty)$, and the set

$$\{e\in\{1, \cdots, q-1\} \mid 0\leqq aq+q-(r+1)e-1, \text{ where } re=(re)^*+aq\}$$

is denoted by $E_r$.

PROPOSITION 2.2. *Let $C$ and $C'$ be curves of genus $g=(q-1)/2$ which admit automorphisms of order $q, \theta$ and $\theta'$ respectively. Then the following conditions are equivalent.*

(1) *$C$ and $C'$ are isomorphic.*

(2) *$(C, \langle\theta\rangle)$ and $(C', \langle\theta'\rangle)$ are isomorphic, that is, there is an isomorphism*

$$\varphi : C \longrightarrow C'$$

*such that $\langle\theta'\rangle = \varphi\langle\theta\rangle\varphi^{-1}$.*

PROOF. Since $\langle\theta'\rangle$ is a $q$-Sylow subgroup of the automorphism group of $C'$ by Corollary A.4. in [4], the statement is trivial.

The following lemma gives two sorts of isomorphisms among $(C_r, \langle\theta_r\rangle)$'s.

LEMMA 2.3. *For $r$ and $s \in \{1, \cdots, q-2\}$, we have the following.*

(1) *If $rs \equiv 1 \bmod q$, then there is an isomorphism*

$$\sigma_r : (C_r, \langle\theta_r\rangle) \longrightarrow (C_s, \langle\theta_s\rangle)$$

*such that*

$$\sigma_r(P_{r,0}) = P_{s,1},\ \sigma_r(P_{r,1}) = P_{s,0},\ \sigma_r(P_{r,\infty}) = P_{s,\infty}.$$

(2) *If $-(r+1)s \equiv r \bmod q$, then there is an isomorphism*

$$\tau_r : (C_r, \langle\theta_r\rangle) \longrightarrow (C_s, \langle\theta_s\rangle)$$

*such that*

$$\tau_r(P_{r,0}) = P_{s,0},\ \tau_r(P_{r,1}) = P_{s,\infty},\ \tau_r(P_{r,\infty}) = P_{s,1}.$$

PROOF. Let $k(x, y)$ (resp. $k(u, v)$) be the function field of $C_r$ (resp. $C_s$) with the equation $y^r(y-1) = x^q$ (resp. $v^s(v-1) = u^q$).

For (1), we put

$$rs = 1 + qb,\ d = \begin{cases} 1 & \text{if } r \text{ is even} \\ 0 & \text{if } r \text{ is odd.} \end{cases}$$

Then

$$\sigma_r^*(u) = (-1)^{b+ds} x^s / y^b,\ \sigma_r^*(v) = -y + 1$$

gives a desired isomorphism $\sigma_r$.

For (2), let $t \in \{1, \cdots, q-2\}$ be such that

$$(q-(r+1))t = 1 + qb.$$

Then $q-(t+1) = s$, and

$$\tau_r^*(u) = x^t / y^{t-b-1}(y-1),\ \tau_r^*(v) = y/(y-1)$$

gives a desired isomorphism $\tau_r$.

DEFINITION 2.4. *We define a subgroup $S$ of the group of permutations of the set $(\boldsymbol{Z}/q\boldsymbol{Z})^{*}-\{-1\}$ by*

$$S=\langle\sigma,\tau\rangle,\ \sigma(r)=1/r,\ \tau(r)=-r/(r+1),$$

*where $(\boldsymbol{Z}/q\boldsymbol{Z})^{*}$ is the group of invertible elements of the field $\boldsymbol{Z}/q\boldsymbol{Z}$.*

The group $S$ is isomorphic to the group of permutations of three letters. In fact, $S$ is consisting of the following six elements:

$$\begin{aligned} &1: r\longmapsto r, && \sigma: r\longmapsto 1/r\\ &\tau: r\longmapsto -r/(r+1), && \sigma\tau\sigma: \tau\longmapsto -(r+1)\\ &\sigma\tau: r\longmapsto -(r+1)/r, && (\sigma\tau)^{2}: \tau\longmapsto -1/(r+1). \end{aligned}$$

Then the map $\pi$ defined below gives an isomorphism of $S$ onto the group of permutations of $\{0,1,\infty\}$.

$$1\longmapsto\begin{pmatrix}0&1&\infty\\0&1&\infty\end{pmatrix},\qquad \sigma\longmapsto\begin{pmatrix}0&1&\infty\\1&0&\infty\end{pmatrix},$$

$$\tau\longmapsto\begin{pmatrix}0&1&\infty\\0&\infty&1\end{pmatrix},\qquad \sigma\tau\sigma\longmapsto\begin{pmatrix}0&1&\infty\\\infty&1&0\end{pmatrix},$$

$$\sigma\tau\longmapsto\begin{pmatrix}0&1&\infty\\1&\infty&0\end{pmatrix},\qquad (\sigma\tau)^{2}\longmapsto\begin{pmatrix}0&1&\infty\\\infty&0&1\end{pmatrix}.$$

In what follows, regarding $\{1,\cdots,q-2\}$ as a complete set of representatives, we use the notation $C_r$ etc. for $r\in(\boldsymbol{Z}/q\boldsymbol{Z})^{*}-\{-1\}$. By Lemma 2.3., we have,

COROLLARY 2.5. *For any $r\in(\boldsymbol{Z}/q\boldsymbol{Z})^{*}-\{-1\}$ and for any $\varphi\in S$, there is an isomorphism*

$$\varphi_r: (C_r,\langle\theta_r\rangle)\longrightarrow(C_{\varphi(r)},\langle\theta_{\varphi(r)}\rangle)$$

*such that*

$$\varphi_r(P_{r,i})=P_{\varphi(r),\pi(\varphi)(i)},\ i=0,1,\infty.$$

The following proposition concerning the action of $S$ on $(\boldsymbol{Z}/q\boldsymbol{Z})^{*}-\{-1\}$ is easy, so we omit the proof.

PROPOSITION 2.6.

(0) *For any $r\in(\boldsymbol{Z}/q\boldsymbol{Z})^{*}-\{-1\}$, the order of the stabilizer $S_r$ is* 1, 2 *or* 3.

(1) *We have*

$$\{r\in(\boldsymbol{Z}/q\boldsymbol{Z})^{*}-\{-1\}\mid |S_r|=2\}=\{1,g,2g-1\},$$

(2) *For any* $r\in(\boldsymbol{Z}/q\boldsymbol{Z})^*-\{-1\}$, $|S_r|=3$ *if and only if* $r^2+r+1=0$. *If there is such an* $r$, *then*

$$\{r\in(\boldsymbol{Z}/q\boldsymbol{Z})^*-\{-1\}\mid |S_r|=3\}=\{r, r^2\},$$

*and this set is the S-orbit of* $r$.
(3) *We have,*

$$|S\backslash(\boldsymbol{Z}/q\boldsymbol{Z})^*-\{-1\}|=\begin{cases}(q+5)/6, & \text{if } q\equiv 1 \bmod 3.\\ (q+1)/6, & \text{if } q\equiv 2 \bmod 3.\end{cases}$$

We see, in Corollary 2.5., that $C_r$ and $C_s$ are isomorphic if $r$ and $s$ are $S$-equivalent. The converse is also true, this is our main result. To prove it, we need a lemma.

For any $r=1,\cdots,q-2$, we call $E_r$ *primitive* if $E_r$ as a subset of $(\boldsymbol{Z}/q\boldsymbol{Z})^*$ satisfies,

$$\forall u\in(\boldsymbol{Z}/q\boldsymbol{Z})^*,\ uE_r=E_r \Rightarrow u=1.$$

For example, if $E_r$ satisfies $\sum_{e\in E_r}e\not\equiv 0 \bmod q$, then $E_r$ is primitive.

LEMMA 2.7. *For any* $r=1,\cdots,q-2$, *we have*

$$-12r(r+1)\sum_{e\in E_r}e\equiv r^2+r+1 \bmod q.$$

PROOF. By the definition of $E_r$, we see easily,

$$E_r=\bigcup_{a=0}^{r-1}\{e\in\boldsymbol{Z}\mid(qa+1)/r\leqq e\leqq(q(a+1)-1)/(r+1)\},$$

where the right hand side is disjoint. Furthermore, for $a=0,\cdots,r-1$,

$$\begin{aligned}&\{e\in\boldsymbol{Z}\mid(qa+1)/r\leqq e\leqq(q(a+1)-1)/(r+1)\}\\&=\{e\in\boldsymbol{Z}\mid[qa/r]+1\leqq e\leqq[q(a+1)/(r+1)]\},\end{aligned}$$

since $q(a+1)\not\equiv 0 \bmod r+1$, where [ ] is the Gauss symbol.

Note that the inequality $[qa/r]\leqq[q(a+1)/(r+1)]$, and we have,

$$\text{(i)}\quad\begin{aligned}\sum_{e\in E_r}e&=1/2\sum_{a=0}^{r-1}\{[q(a+1)/(r+1)]-[qa/r]\}\cdot\{q(a+1)/(r+1)]+[qa/r]+1\}\\&=1/2\sum_{a=1}^{r}\{[qa/(r+1)]^2+[qa/(r+1)]\}-1/2\sum_{a=1}^{r-1}\{[qa/r]^2+[qa/r]\}.\end{aligned}$$

On the other hand, for any $s=1,\cdots,q-1$, we see

$$\{qb-[qb/s]s\mid b=1,\cdots,s-1\}=\{1,\cdots,s-1\}$$

and then,

(ii)
$$s\sum_{b=1}^{s-1}[qb/s]\equiv -s(s-1)/2, \bmod q.$$
$$s^2\sum_{b=1}^{s-1}[qb/s]^2\equiv (s-1)s(2s-1)/6, \bmod q.$$

Our lemma is easily deduced from (i) and (ii).

THEOREM 2.8. *For any $r$ and $s\in(\boldsymbol{Z}/q\boldsymbol{Z})^*-\{-1\}$, $C_r$ and $C_s$ are isomorphic if and only if $r$ and $s$ are $S$-equivalent.*

PROOF. Assume $C_r$ and $C_s$ isomorphic. By Proposition 2.2., there is an isomorphism

$$\varphi:(C_r, \langle\theta_r\rangle)\longrightarrow(C_s, \langle\theta_s\rangle).$$

In particular, there is a permutation $\pi$ of $\{0, 1, \infty\}$ such that $\varphi(P_{r,i})=P_{s,\pi(i)}(i=0, 1, \infty)$, and then

$$G_{r,i}=G_{s,\pi(i)},\ i=0, 1, \infty.$$

Assume $E_r$ is not primitive. Then neither is $E_s$. By Lemma 2.7., these imply $r^2+r+1=s^2+s+1=0$, and $r$ and $s$ are $S$-equivalent by Proposition 2.6. (2).

Assume $E_r$ is primitive. There are six possibilities of $\pi$. For example, if

$$\pi=\begin{pmatrix}0 & 1 & \infty\\ 1 & \infty & 0\end{pmatrix},$$

then, as subsets of $(\boldsymbol{Z}/q\boldsymbol{Z})^*$, $E_r$ and $E_s$ satisfy the equalities $rE_r=E_s$, $E_r=-(s+1)E_s$ and $-(r+1)E_r=sE_s$ by Proposition 1.2. (2), and

$$srE_r=sE_s=-(r+1)E_r.$$

Since $E_r$ is primitive, we have

$$s=-(r+1)/r=(\sigma\tau)(r).$$

The other five cases are similarly treated, and the proof is completed.

As a corollary, we characterize hyperelliptic and trigonal curves in $\{C_r\}$.

COROLLARY 2.9.

(1) *The curve $C_r$ is hyperelliptic if and only if $r=1, g$ or $2g+1$.*

(2) *The curve $C_r$ is trigonal if and only if $r$ is $S$-equivalent to 2.*

PROOF. Both (1) and (2) are clear from Proposition 3.3. in [2] and the above theorem.

REMARK 2.10. Assume $k=\boldsymbol{C}$ and let $J_r$ be the Jacobian variety of $C_r$. Taking account of the theory of complex multiplication of abelian varieties [5], Lemma 2.7. shows that $J_r$ is simple if $|S_r|\neq 3$, and that $J_r$ is isogenous to the three fold product of an abelian variety $X$ of dimension $(q-1)/6$ if $|S_r|=3$. Furthermore, by the results of [3], we see that $J_r$ and $J_s$ are isogenous if and only if $r$ and $s$ are $S$-equivalent, and that $X$ as above is simple.

## § 3. Orders of automorphisms groups.

As before, let $C$ be a curve of genus $g=(q-1)/2$ with an automorphism $\theta$ of order $q$. Each element of $\mathrm{Aut}(C, \langle\theta\rangle)$ induces a permutation of the set of fixed points of $\theta$, Fix $(\theta)$, and we have a group homomorphism of $\mathrm{Aut}(C, \langle\theta\rangle)$ into the group of permutations of $\mathrm{Fix}(\theta)$.

LEMMA 3.1. *The kernel of above homomorphism is* $\langle\theta\rangle$.

PROOF. If $\varphi\in\mathrm{Aut}(C, \langle\theta\rangle)$ is identity on $\mathrm{Fix}(\theta)$, then the induced automorphism $\bar{\varphi}$ of $C/\langle\theta\rangle$ is identity on $\pi(\mathrm{Fix}(\theta))$, where $\pi$ is the projection $C\longrightarrow C/\langle\theta\rangle$. Since the genus of $C/\langle\theta\rangle$ is 0 and $|\mathrm{Fix}(\theta)|=3, \bar{\varphi}$ is identity on $C/\langle\theta\rangle$. But the natural homomorphism

$$\mathrm{Aut}(C, \langle\theta\rangle)\longrightarrow \mathrm{Aut}(C/\langle\theta\rangle)$$

has the kernel $\langle\theta\rangle$, we have $\varphi\in\langle\theta\rangle$.

PROPOSITION 3.2. *For any* $r=1, \cdots, q-2$, *we have*

$$|\mathrm{Aut}(C_r, \langle\theta_r\rangle)|=q|S_r|.$$

PROOF. Assume $|S_r|=1$. Then the cardinality of the set $G_r=\{G_{r,0}, G_{r,1}, G_{r,\infty}\}$ is 3. Hence any element of $\mathrm{Aut}(C_r, \langle\theta_r\rangle)$ is identity on $\mathrm{Fix}(\theta_r)=\{P_{r,0}, P_{r,1}, P_{r,\infty}\}$.

Suppose $|S_r|=2$. Then $|G_r|=2$, so that there is no element of $\mathrm{Aut}(C_r, \langle\theta_r\rangle)$ of order 3.

If $|S_r|=3$, then it suffices to show that there is no element of $\mathrm{Aut}(C_r, \langle\theta_r\rangle)$ of order 2. Let $i$ be an automorphism of $\mathrm{Aut}(C_r, \langle\theta_r\rangle)$ of order 2. Then the genus $g'$ of $C_r/\langle i\rangle$ satisfies

$$(*)\qquad 1\leqq g'<g,$$

because $C_r$ is not hyperelliptic. Since $i$ induces a permutation of order 2 on the set $\mathrm{Fix}(\theta_r)$ of cardinality 3, $i$ and $\theta_r$ have a common fixed point. Let $H$ be the stabilizer of this point in $\mathrm{Aut}(C_r)$, and let $p$ be the characteristic exponent of the ground field $k$. Since $p$-Sylow subgroups of $H$ are normal and the quotient group of $H$ by the $p$-Sylow subgroup is cyclic, we see that the order of $i\theta_r i^{-1}\theta_r^{-1}$ is a power of $p$.

On the other hand, $i$ normalizes $\langle\theta_r\rangle$, so that $i\theta_r i^{-1}\theta_r^{-1}\in\langle\theta_r\rangle$. Hence we have

$$i\theta_r=\theta_r i$$

because of $(p, q)=1$. Consequently, $\theta_r$ induces an automorphism of order $q$ on $C_r/\langle i\rangle$ with a fixed point. This contradicts (*).

Now, we consider the full automorphism group $\mathrm{Aut}(C)$ in the case of characteristic zero. When the genus is 2 or 3, $\mathrm{Aut}(C)$ is well known. If the genus is 2, then all curves in question are isomorphic and the order of $\mathrm{Aut}(C)$ is 10. If the genus is 3, there are two isomorphy classes, hyperelliptic one and non-hyperelliptic one. In the first case, the order is 14. In the second case, the order is 168, and the curves are isomorphic to well known Klein curve. In general, we have the following.

THEOREM 3.3. *Assume the characteristic of the ground field is zero. Then for any* $r=1, \cdots, q-2$, *we have*

$$|\mathrm{Aut}(C_r)|=q|S_r|$$

*except that* $C_r$ *is isomorphic to Klein curve.*

REMARK. By the result of §2, $C_r$ is isomorphic to Klein curve if and only if $g=3$ and $r=2$ or 4.

PROOF. Let $C$ be a curve of genus $g=(q-1)/2$ with an automorphism $\theta$ of order $q$. It suffices to show that $\langle\theta\rangle$ is normal in $\mathrm{Aut}(C)$ provided $g\geqq 5$.

Put $G=\mathrm{Aut}(C)$. Assume $\langle\theta\rangle$ is not normal in $G$. Then the cardinality of the set of $q$-Sylow subgroups is at least $q+1$, and we have

$$(*)\qquad (2g+1)(2g+2)=q(q+1)\leqq|G|.$$

On the other hand, let $\{Q_1, \cdots, Q_n\}$ be a maximal set of inequivalent fixed points of $G-\{1_C\}$ and let $m_i$ be the order of the stabilizer of $Q_i$ in $G$. We may assume $m_1\leqq\cdots\leqq m_n$. Since the genus of $C/G$ is zero, Hurwitz formula gives

$$2g-2=|G|\left(n-2-\sum_{i=1}^{n}1/m_i\right).$$

Using above formula, we see easily

$$(1)\qquad |G|\leqq 24(g-1)$$

except the following two cases;

(2) $n=3$ and $m_1=2, m_3=5$.

(3) $n=3$ and $m_3 \geqq 7$.

(For example, see [1].)

The inequality (1) contradicts (*) because of $g \geqq 5$. The case (2) does not occur, since one of $m_1, m_2$ and $m_3$ is divisible by $q \geqq 11$. For the same reason, we have following inequality in the case (3),

$$|G| \leqq (2g-2)/(1-1/2-1/3-1/11) < 27(g-1).$$

This contradicts (*) again.

## References

[1] Farkas, H.M. and Kra, I., Riemann surfaces, G.T.M. Springer-Verlag, 1980.

[2] Homma, M., Automorphisms of prime order of curves, Manuscripta Math. **33** (1980), 99-109.

[3] Kobliz, N. and Rohrlich, D., Simple factors in the Jacobian of a Fermat curve, Can. J. Math., **30** (1978) 1183-1205.

[4] Sekiguchi, T., On the field of rationality for curves and for their jacobian varieties, to appear.

[5] Shimura, G. and Taniyama, Y., Complex multiplication of abelian varieties and its applications to number theory, Math. Soc. Japan, Tokyo, 1961.

Institute of Mathematics
University of Tsukuba
Ibaraki, 305 Japan