TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 303, Number 2, October 1987

p-RANKS AND AUTOMORPHISM GROUPS OF ALGEBRAIC CURVES

SHŌICHI NAKAJIMA

Dedicated to Professor Nagayoshi Iwahori on his 60th birthday

ABSTRACT. Let X be an irreducible complete nonsingular curve of genus g over an algebraically closed field k of positive characteristic p. If $g \geq 2$, the automorphism group $\mathrm{Aut}(X)$ of X is known to be a finite group, and moreover its order is bounded from above by a polynomial in g of degree four (Stichtenoth). In this paper we consider the p-rank γ of X and investigate relations between γ and $\mathrm{Aut}(X)$. We show that γ affects the order of a Sylow p-subgroup of $\mathrm{Aut}(X)$ (§3) and that an inequality $|\mathrm{Aut}(X)| \leq 84(g-1)g$ holds for an ordinary (i.e. $\gamma = g$) curve X (§4).

1. Introduction. Let k be an algebraically closed field. We consider a connected complete nonsingular algebraic curve X over k. The genus and the automorphism group of X are denoted by g_X and $\mathrm{Aut}(X)$, respectively. It is a classical fact that $\mathrm{Aut}(X)$ is a finite group when $g_X \geq 2$. Further it is known that, for any finite group G, there exists a curve X with $G = \mathrm{Aut}(X)$ (see Madden and Valentini [**5**]). But if we consider a fixed curve X, the order of $\mathrm{Aut}(X)$ (we denote it by $|\mathrm{Aut}(X)|$) is bounded from above by a polynomial of g_X. When $\mathrm{char}\, k = 0$, there is a well-known inequality of Hurwitz ($g_X \geq 2$):

$$|\mathrm{Aut}(X)| \leq 84(g_X - 1). \tag{1.1}$$

When $p = \mathrm{char}\, k$ is positive, the inequality (1.1) holds if $2 \leq g_X \leq p-2$, except for a curve $y^2 = x^p - x$ (Roquette [**7**]). But when g_X is large, (1.1) is no longer valid, and instead we have the results of Stichtenoth [**11**] and Singh [**10**]. Stichtenoth's theorem[1] states that

$$|\mathrm{Aut}(X)| \leq 16g_X^4 \tag{1.2}$$

holds when $g_X \geq 2$ except for the curves below. The exceptional curves are the complete nonsingular models of $y^q + y = x^{q+1}$ where q runs over all powers of $p = \mathrm{char}\, k$. (For the above curve X, $g_X = q(q-1)/2$ and $|\mathrm{Aut}(X)| = q^3(q^3+1)(q^2-1)$.) From this we see that $|\mathrm{Aut}(X)|$ may be very large in the case $\mathrm{char}\, k > 0$, as compared with the case $\mathrm{char}\, k = 0$. (Its cause is appearance of wild ramification.)

When $p = \mathrm{char}\, k$ is positive, we have an important invariant of X other than g_X. It is the p-rank γ_X of X (namely, the p-rank of the Jacobian of X). Concerning γ_X, it was observed [**11**, **13**] that, for curves X with large $\mathrm{Aut}(X)$, it often occurs

Received by the editors April 9, 1986 and, in revised form, November 12, 1986.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 14H05, 14H30; Secondary 14H45.

[1]Stichtenoth's result was improved by Henn [**3**]. But his proof contains a gap (last paragraph of p. 104). I do not know if the gap can be covered.

$\gamma_X = 0$. This suggests that γ_X may affect the size of $\mathrm{Aut}(X)$ in some way. The purpose of this paper is to show that actually γ_X has influence on $|\mathrm{Aut}(X)|$.

After explaining notation in §2, we show in §3 that γ_X directly influences the sizes of p-subgroups ($p = \mathrm{char}\, k$) of $\mathrm{Aut}(X)$, and prove, as its consequence, that $|\mathrm{Aut}(X)|$ must be small for certain values of γ_X. In particular, we may see that the case $\gamma_X = 0$ is really exceptional. In §4 we treat ordinary (i.e. $g_X = \gamma_X$) curves, which occupy an open dense subset in the moduli space of curves of given genus. Our result is that, when restricted to ordinary curves, we have an inequality $|\mathrm{Aut}(X)| \leq 84(g_X - 1)g_X$ ($g_X \geq 2$), which is better than the general estimate (1.2). A noteworthy fact about an ordinary curve X is that, for any finite subgroup G of $\mathrm{Aut}(X)$ and $P \in X$, the second ramification group $G_2(P)$ (cf. §2) is always trivial (Theorem 2(i)). The main tools of the proofs are the Riemann-Hurwitz formula and the Deuring-Šafarevič formula (see §2). Our arguments proceed by applying these formulas to various coverings of curves.

2. Notation and formulas. To begin with, we explain the notation which will be used throughout the paper. We fix an algebraically closed field k of positive characteristic and put $p = \mathrm{char}\, k$. A "curve" always means a connected complete nonsingular algebraic curve over k. For a curve X, the symbols $g_X, \gamma_X, \mathrm{Aut}(X)$ and $k(X)$ denote, respectively, the genus, the p-rank, the automorphism group and the function field over k, of X. The integer γ_X is, by definition, the p-rank of the Jacobian of X. When a curve X, a finite subgroup G of $\mathrm{Aut}(X)$ and a point P of X are given, we define the ramification groups $G_i(P)$ ($i \geq 0$) by

$$G_0(P) = \{\sigma \in G \,|\, \sigma \cdot P = P\}$$

and for $i \geq 1$,

$$G_i(P) = \{\sigma \in G_0(P) \,|\, \mathrm{ord}_P(\sigma \cdot \pi_P - \pi_P) \geq i + 1\},$$

where π_P is a local uniformizing parameter at P and ord_P means the order at P. For properties of $G_i(P)$, we refer to [**9**, Chapter IV]. When a covering $X \to Y$ of curves is given, we denote its covering morphism by $\pi_{X/Y}: X \to Y$. Further, if $X \to Y$ is a Galois covering, its Galois group is denoted by $\mathrm{Gal}(X/Y)$. For natural numbers a and b, (a, b) denotes the greatest common divisor of a and b, and for a finite set S, $|S|$ means its cardinality. When q is a power of p, $\mathbf{F}_q$ denotes the field with q elements.

Next we review the Riemann-Hurwitz formula and the Deuring-Šafarevič formula for Galois coverings of curves. Suppose that a finite Galois covering $X \to Y$ is given. For a point $Q \in Y$, we define e_Q (ramification index) and d_Q (different exponent) in the following way: Put $G = \mathrm{Gal}(X/Y)$ and take $P \in X$ which satisfies $\pi_{X/Y}(P) = Q$. Then, $e_Q = |G_0(P)|$ and $d_Q = \sum_{i=0}^{\infty}(|G_i(P)| - 1)$. Since $X \to Y$ is a Galois covering, e_Q and d_Q do not depend on choice of P. We note that $d_Q \geq e_Q - 1$ is always true and $d_Q \geq e_Q$ holds if and only if Q (i.e. P) is widly ramified in $X \to Y$. With notation as above, the Riemann-Hurwitz formula is the following (see e.g. [**11**, p. 529]):

$$\frac{2g_X - 2}{|G|} = 2g_Y - 2 + \sum_{Q \in Y} \frac{d_Q}{e_Q}. \tag{2.1}$$

We further assume that $G = \mathrm{Gal}(X/Y)$ is a p-group ($p = \mathrm{char}\, k$). Then we have the following equality, which is called the Deuring-Šafarevič formula (see e.g. [**4**, **6**, **12**]):

$$\frac{\gamma_X - 1}{|G|} = \gamma_Y - 1 + \sum_{Q \in Y} \left(1 - e_Q^{-1}\right). \tag{2.2}$$

These formulas will be used to estimate $|G|$ from above.

3. γ_X and p-subgroups of $\mathrm{Aut}(X)$. Let X be a curve. In this section we investigate how the values of the p-rank γ_X and the difference $g_X - \gamma_X$ affect the sizes of p-subgroups of $\mathrm{Aut}(X)$.

First we deal with γ_X. Namely, we prove the following

THEOREM 1. *Let X be a curve with $g_X \geq 2$, and let H be a Sylow p-subgroup of $\mathrm{Aut}(X)$. Then the following hold.*

(i) *When $\gamma_X \geq 2$, we have*

$$|H| \leq c_p (\gamma_X - 1), \tag{3.1}$$

where $c_p = p/(p-2)$ $(p \geq 3)$ and $c_2 = 4$.

(ii) *When $\gamma_X = 1$ and $p \geq 3$, H is a cyclic p-group and $|H|$ divides $g_X - 1$. Further the covering $X \to X/H$ is unramified.*

(iii) *When $\gamma_X = 1$ and $p = 2$, we have $|H| \leq 4(g_X - 1)$.*

(iv) *When $\gamma_X = 0$, we have*

$$|H| \leq \max\left\{g_X, \frac{4p}{(p-1)^2} g_X^2\right\}.$$

PROOF. We put $Z = X/H$ and denote by e_S $(S \in Z)$ the ramification index of S with respect to $X \to Z$. Set $\lambda = (\gamma_X - 1)/|H|$. Then by formula (2.2),

$$\lambda = \gamma_Z - 1 + \sum_{S \in Z} \left(1 - e_S^{-1}\right). \tag{3.2}$$

Here we note that if $e_S > 1$, then $e_S \geq p$ holds, because H is a p-group. Assume that $\gamma_X \geq 2$, i.e. $\lambda > 0$. We should prove $\lambda \geq c_p^{-1}$. If $\gamma_Z \geq 2$, (3.2) shows $\lambda \geq 1 > c_p^{-1}$. If $\gamma_Z = 1$, there exists $S_1 \in Z$ with $e_{S_1} > 1$, since $\lambda > 0$. Then from (3.2), $\lambda \geq 1 - e_{S_1}^{-1} \geq 1 - p^{-1} > c_p^{-1}$. If $\gamma_Z = 0$ and $p \geq 3$, there are two points S_1, $S_2 \in Z$ with e_{S_1}, $e_{S_2} > 1$, since $\lambda > 0$. Then we have $\lambda \geq -1 + 2(1 - p^{-1}) = c_p^{-1}$. If $\gamma_Z = 0$ and $p = 2$, we have two cases; (a) there are S_1, $S_2 \in Z$ with $e_{S_1} \geq 4$ and $e_{S_2} \geq 2$ (note that e_S is a power of $p = 2$), (b) there are S_1, S_2, $S_3 \in Z$ with $e_{S_i} \geq 2$ $(i = 1, 2, 3)$. In both cases (a) and (b), we obtain from (3.2), $\lambda \geq \frac{1}{4}$ and $\lambda \geq \frac{1}{2}$, respectively. Thus (i) is proved. Next assume that $\gamma_X = 1$, i.e. $\lambda = 0$. Then, from (3.2), $\gamma_Z = 0$ or 1. If $\gamma_Z = 1$, we have $e_S = 1$ for all $S \in Z$, i.e. $X \to Z$ is unramified. Since $\gamma_Z = 1$, an unramified p-covering of Z must be cyclic (cf. [**8**, **2**]). Hence $H = \mathrm{Gal}(X/Z)$ is a cyclic p-group. Further, (2.1) gives $2g_X - 2 = |H|(2g_Z - 2)$, which shows that $|H|$ divides $g_X - 1$. In particular, $|H| \leq g_X - 1$. The case $\gamma_Z = 0$ cannot occur if $p \geq 3$, because we have $\frac{2}{3} \leq 1 - p^{-1} \leq 1 - e_S^{-1} < 1$ when $e_S > 1$, and hence $\sum_{S \in Z}(1 - e_S^{-1}) \neq 1$. This proves (ii). In the case $\gamma_Z = 0$ and $p = 2$, we have $e_{S_1} = e_{S_2} = 2$ for S_1, $S_2 \in Z$ and $e_S = 1$ if $S \neq S_1$, S_2. Hence (2.1) shows

$$(2g_X - 2)/|H| = 2g_Z - 2 + \tfrac{1}{2}(d_{S_1} + d_{S_2}).$$

The right-hand side of this equality is not smaller than $\frac{1}{2}$ because it is a positive rational number with denominator at most 2. This settles (iii). Finally, assume that $\gamma_X = 0$, i.e. $\lambda < 0$. Then $\gamma_Z = 0$ from (3.2). If $e_{S_1}, e_{S_2} > 1$ for two points S_1, $S_2 \in Z$, the right-hand side of (3.2) is not smaller than $-1 + 2(1 - p^{-1}) = (p-2)/p \geq 0$, which contradicts $\lambda < 0$. Consequently $e_S = 1$ when $S \neq S_1$ for a point $S_1 \in Z$. In this case $\lambda = -e_{S_1}^{-1}$, i.e. $e_{S_1} = |H|$. Take $P_1 \in X$ satisfying $\pi_{X/Z}(P_1) = S_1$. Then the above fact shows that P_1 is the only ramification point of $X \to Z$ and it is totally ramified. Therefore, from [**11**, Teil I, Satz 1(a), (c)], we obtain the assertion (iv).

Theorem 1 shows, in particular, that the order of Sylow p-subgroups of $\mathrm{Aut}(X)$ is bounded from above by a linear polynomial of g_X except when $\gamma_X = 0$. If $\gamma_X = 0$, the upper bound $4pg_X^2/(p-1)^2$ can really be attained ([**11**, p. 533, Bemerkung 1]), which demonstrates that $\mathrm{Aut}(X)$ may be especially large when $\gamma_X = 0$.

We give a corollary of Theorem 1, which exhibits influence of γ_X on the whole group $\mathrm{Aut}(X)$.

COROLLARY. *Let X be a curve with $g_X \geq 2$ and put $G = \mathrm{Aut}(X)$.*

(i) *Assume $\gamma_X = 1$ and $p \geq 3$. Then the covering $X \to X/G$ is tamely ramified, i.e. $G_1(P) = \{1\}$ for all $P \in X$.*

(ii) *Assume $2 \leq \gamma_X \leq p-2$ (necessarily $p \geq 5$). Then $|G|$ is not divisible by p. In particular $X \to X/G$ is tamely ramified.*

(iii) *In both cases* (i) *and* (ii), *the Hurwitz inequality $|G| \leq 84(g_X - 1)$ holds.*

PROOF. (i) By Theorem 1(ii), $X \to X/H$ is unramified for any p-subgroup H of G. This is equivalent to the assertion that $X \to X/G$ is tamely ramified.

(ii) Let H be the same as in Theorem 1. Then from Theorem 1(i) and $\gamma_X \leq p-2$, we have $|H| \leq p(p-3)/(p-2) < p$. Hence we have $|H| = 1$ because $|H|$ is a power of p. This shows that $|G|$ is not divisible by p.

(iii) In (i) and (ii), the covering $X \to X/G$ is tamely ramified. In that case the classical argument of Hurwitz is valid and we have $|G| \leq 84(g_X - 1)$ (cf. [**11**, Teil I, Satz 3]).

Next we consider the difference $g_X - \gamma_X$. Our result is given in the following

THEOREM 2. (i) *Assume that X is an ordinary curve (i.e. $g_X = \gamma_X$), and let G be a finite subgroup of $\mathrm{Aut}(X)$. Then for every point $P \in X$, we have $G_2(P) = \{1\}$. (For the definition of $G_2(P)$, see §2.)*

(ii) *Let X be a curve with $g_X \geq 2$, and assume that $1 \leq g_X - \gamma_X \leq (p-2)/2$ holds (necessarily $p \geq 5$). Then $|\mathrm{Aut}(X)|$ is not divisible by p. In particular $X \to X/\mathrm{Aut}(X)$ is tamely ramified and $|\mathrm{Aut}(X)| \leq 84(g_X - 1)$ holds.*

PROOF. Let H be a p-subgroup of G. (In the case (ii), we put $G = \mathrm{Aut}(X)$.) We consider the covering $X \to Z = X/H$ and apply to it the formulas (2.1) and (2.2). Consequently we have

$$\frac{2g_X - 2}{|H|} = 2g_Z - 2 + \sum_{S \in Z} \frac{d_S}{e_S}$$

and

$$\frac{\gamma_X - 1}{|H|} = \gamma_Z - 1 + \sum_{S \in Z} \left(1 - e_S^{-1}\right).$$

From these equalities we obtain

$$\frac{2(g_X - \gamma_X)}{|H|} = 2(g_Z - \gamma_Z) + \sum_{S \in Z} \frac{r_S}{e_S}, \tag{3.3}$$

where $r_S = d_S - 2(e_S - 1)$. For $S \in Z$, take $P \in X$ satisfying $\pi_{X/Z}(P) = S$. Then we have $d_S = \sum_{i=0}^{\infty}(|H_i(P)| - 1)$ and $e_S = |H_0(P)|$. We note that also the equality $e_S = |H_1(P)|$ holds since H is a p-group (cf. [**9**, p. 75, Corollary 1]). Therefore we obtain

$$r_S = \sum_{i=2}^{\infty}(|H_i(P)| - 1).$$

In particular $r_S \geq 0$. Hereafter we assume that $g_X - \gamma_X \leq (p-2)/2$ holds. For any $S \in Z$, (3.3) shows (recall $g_Z - \gamma_Z \geq 0$),

$$r_S \leq (2e_S/|H|)(g_X - \gamma_X) \leq p - 2.$$

From this we may conclude that $H_2(P) = \{1\}$, i.e. $r_S = 0$. For, if $H_2(P) \neq \{1\}$, then $|H_2(P)| \geq p$ and hence $r_S \geq p - 1$ must hold. Now we apply the above result to the cases (i) and (ii). In the case (i), put $H = G_1(P)$. Then the above argument shows $G_2(P) = H_2(P) = \{1\}$, which is the assertion of (i). In the case (ii), let H be a Sylow p-subgroup of $G = \mathrm{Aut}(X)$. Since $r_S = 0$ for all $S \in Z$, (3.3) gives an equality $g_X - \gamma_X = |H|(g_Z - \gamma_Z)$. Accordingly, $g_X - \gamma_X$ is a multiple of p if $|H| > 1$. But, that is impossible because of the assumption $1 \leq g_X - \gamma_X \leq (p-2)/2$. Therefore we have $|H| = 1$, i.e. $|\mathrm{Aut}(X)|$ is not divisible by p. As in the Corollary to Theorem 1, we obtain $|\mathrm{Aut}(X)| \leq 84(g_X - 1)$.

Finally, we mention a direct consequence of Theorem 2.

COROLLARY. *Let X be an ordinary curve and $\sigma \in \mathrm{Aut}(X)$ an element of order p^l $(l \geq 1)$. If σ fixes at least one point of X, then $l = 1$.*

PROOF. Let $G = \langle\sigma\rangle$ be the group generated by σ, and let $P \in X$ be a point which is fixed by σ. Then $G = G_1(P)$. Theorem 2(i) shows $G_2(P) = \{1\}$. Hence $G = G_1(P)/G_2(P)$. On the other hand, $G_1(P)/G_2(P)$ must be an elementary abelian p-group (cf. [**9**, p. 75, Corollary 3]). Accordingly, G is both cyclic and elementary abelian, i.e. $l = 1$.

4. Ordinary curves. In the moduli space of curves of given genus, ordinary curves form a Zariski dense open subset, i.e. general curves are ordinary. So it seems worthwhile making closer investigation for ordinary curves. When we restrict ourselves to ordinary curves, the general estimate (1.2) can be much improved. Namely, we have

THEOREM 3. *Let X be an ordinary curve with $g_X \geq 2$. Then the following inequality holds*;

$$|\mathrm{Aut}(X)| \leq 84(g_X - 1)g_X. \tag{4.1}$$

REMARK. Whether the estimate (4.1) for ordinary curves is best possible or not is an open question. However, we know that $|\mathrm{Aut}(X)|$ cannot be bounded from above by any polynomial in g_X of degree one. That fact was first shown by Subrao [**12**]. As examples of ordinary curves with large automorphism groups, he pointed out the complete nonsingular models of $(y^q - y)(x^q - x) = 1$, where q runs

over all powers of p. Here we refer to another kind of ordinary curves with large automorphism groups. Let q be a power of p and let X be the complete nonsingular model of $y^{q^2}-y=x^q+x^{-1}$. Then in view of the Claim below, we see that $|\mathrm{Aut}(X)|$ cannot be bounded from above by a linear polynomial in g_X, even for ordinary X.

CLAIM. *The above X is an ordinary curve with $g_X=q^2-1$, and* $|\mathrm{Aut}(X)|\geq (g_X+1)(\sqrt{g_X+1}+1)$.

PROOF. We put $z=y^q+y$ and denote by V and W the complete nonsingular curves corresponding to the function fields $k(x,z)$ and $k(x)$, respectively. (Note that W is isomorphic to $\mathbf{P}^1$ and the function field of X is $k(x,y)$.) The coverings $V\to W$ and $X\to V$ are defined by the equations $z^q-z=x^q+x^{-1}$ and $y^q+y=z$, respectively. Hence, putting $H=\mathrm{Gal}(V/W)$ and $H'=\mathrm{Gal}(X/V)$, we have $H\simeq H'\simeq(\mathbf{Z}/p\mathbf{Z})^n$, where $q=p^n$. The covering $V\to W$ is also defined by $(z')^q-z'=x+x^{-1}$, where $z'=z-x$. Therefore, in $V\to W$, exactly two points $x=0$ and $x=\infty$ of W ramify completely and the other points are unramified. Denote by Q_0 and Q_∞ the points of V lying over $x=0$ and $x=\infty$, respectively. Then by the same method as in [**1**] and [**11**], we obtain $H_1(Q_0)=H_1(Q_\infty)=H$ and $H_2(Q_0)=H_2(Q_\infty)=\{1\}$ (for notation see §2). By applying formulas (2.1) and (2.2) to $V\to W$, we see that V is an ordinary curve of genus $q-1$. Now we consider $X\to V$. From the equation $(z')^q-z'=x+x^{-1}$ $(z'=z-x)$, we get $(z')_\infty=Q_0+Q_\infty$ and $(z)_\infty=Q_0+qQ_\infty$, where $(z')_\infty$ and $(z)_\infty$ are the pole-divisors on V of z' and z, respectively. Therefore the points of V other than Q_0 and Q_∞ are unramified in $X\to V$. The equation $y^q+y=z$ shows that Q_0 is completely ramified in $X\to V$ (recall $(z)_\infty=Q_0+qQ_\infty$). Further, letting P_0 be the point of X lying over Q_0, we obtain $H_1'(P_0)=H'$ and $H_2'(P_0)=\{1\}$ (cf. [**1** or **11**]; $H'=\mathrm{Gal}(X/V)$). Rewriting $y^q+y=z$ in the form $(y-z')^q+(y-z')=-z'-x^{-1}$, we obtain $H_1'(P_\infty)=H'$ and $H_2'(P_\infty)=\{1\}$, where P_∞ is the point of X lying over Q_∞ (recall $(z')_\infty=Q_0+Q_\infty$). Then applying (2.1) and (2.2) to $X\to V$, we can conclude that X is ordinary and $g_X=q^2-1$. For any $\xi,\zeta\in\mathbf{F}_{q^2}$ satisfying $\zeta^{q+1}=1$, the transformation $x\to\zeta x, y\to\zeta^{-1}y+\xi$ induces an automorphism of X. Hence we have $|\mathrm{Aut}(X)|\geq q^2(q+1)=(g_X+1)(\sqrt{g_X+1}+1)$.

From now on we shall prove Theorem 3. The fundamental fact for the proof is Theorem 2(i). Put $G=\mathrm{Aut}(X)$ and $Y=X/G$. For $Q\in Y$, we denote by e_Q the ramification index of Q with respect to $X\to Y$. Then by [**11**, Teil I, Satz 3], we have $|G|\leq 84(g_X-1)$ except for the four cases below:

(I) $p\geq 3$ and $g_Y=0$; $e_Q=1$ if $Q\neq Q_1,Q_2,Q_3\in Y$; p divides e_{Q_1}, and $e_{Q_2}=e_{Q_3}=2$.

(II) $g_Y=0$; $e_Q=1$ if $Q\neq Q_1,\ Q_2\in Y$; p divides both e_{Q_1} and e_{Q_2}.

(III) $g_Y=0$; $e_Q=1$ if $Q\neq Q_1\in Y$; p divides e_{Q_1}.

(IV) $g_Y=0$; $e_Q=1$ if $Q\neq Q_1,\ Q_2\in Y$; p divides e_{Q_1} and $(p,e_{Q_2})=1$.

We shall prove (4.1) in each of the above cases. The following Proposition 1 is useful for the proof. It will be used only in the case $G_2(P)=\{1\}$.

PROPOSITION 1. *Let X be a curve and G be a finite subgroup of* $\mathrm{Aut}(X)$. *For $P\in X$, put $E=|G_0(P)/G_1(P)|$ and $q=|G_1(P)/G_2(P)|$. Then $q-1$ is a multiple of E.*

PROOF. Proposition 1 is merely a special case of [**3**, Lemma 1] (take care, notation is different). But we give another proof here. There exist injective

homomorphisms $\theta_0\colon G_0(P)/G_1(P) \to k^\times$ and $\theta_1\colon G_1(P)/G_2(P) \to k$, for which Image $\theta_0 = \mu_E$ (the group of Eth roots of unity) and

$$\theta_1\left(\tau\sigma\tau^{-1}\right) = \theta_0(\bar{\tau})\theta_1(\sigma) \qquad (\tau \in G_0(P), \sigma \in G_1(P)/G_2(P)) \tag{4.2}$$

hold (cf. [**9**, Chapter IV, §2]). Let $\mathbf{F}_{q_0}$ be the field generated by μ_E over $\mathbf{F}_p$. Then by (4.2), Image θ_1 is an $\mathbf{F}_{q_0}$-vector space. Accordingly, $q = |\operatorname{Image}\theta_1| = q_0^l$, where l is the dimension over $\mathbf{F}_{q_0}$ of Image θ_1. From definition, $q_0 - 1$ is a multiple of E. Hence $q - 1 = q_0^l - 1$ is also a multiple of E.

Now we consider the case (I). Put $e_{Q_1} = Eq$, where $(p, E) = 1$ and q is a power of p, i.e. $E = |G_0(P_1)/G_1(P_1)|$ and $q = |G_1(P_1)|$ for $P_1 \in X$ satisfying $\pi_{X/Y}(P_1) = Q_1$. Note that $q > 1$ holds since p divides e_{Q_1}. By virtue of Theorem 2(i), $d_{Q_1} = Eq - 1 + q - 1 = Eq + q - 2$. Since $d_{Q_2} = d_{Q_3} = 2 - 1 = 1$ (recall $p \geq 3$), the formula (2.1) gives

$$(2g_X - 2)/|G| = (q - 2)/Eq.$$

From this equality we obtain $q \leq 2g_X$ because Eq divides $|G|$. Then, since $q > 1$, Proposition 1 and Theorem 2(i) shows $E \leq q - 1 \leq 2g_X - 1$. Hence we obtain (note that $q \geq p \geq 3$),

$$\begin{aligned} |G| &= \frac{2Eq}{q-2}(g_X - 1) \leq \frac{2q}{q-2}(g_X - 1)(2g_X - 1) \\ &\leq 6(g_X - 1)(2g_X - 1). \end{aligned}$$

A fortiori, (4.1) holds.

Next we consider the case (II). Put $e_{Q_i} = E_i q_i$ $(i = 1, 2)$, where $(p, E_i) = 1$ and q_i is a power of p. Then, as in (I), we have $d_{Q_i} = E_i q_i + q_i - 2$ $(i = 1, 2)$ and

$$\frac{2g_X - 2}{|G|} = \frac{q_1 - 2}{E_1 q_1} + \frac{q_2 - 2}{E_2 q_2}.$$

The equality $q_1 = q_2 = 2$ contradicts the assumption $g_X \geq 2$. Hence we may assume $q_1 \geq 3$. Further, the above equality shows

$$(2g_X - 2)/|G| \geq (q_1 - 2)/E_1 q_1.$$

Then, by the same argument as in (I), we obtain the estimate (4.1).

In the case (III), let $e_{Q_1} = Eq$ be the same as in (I). Then we have $d_{Q_1} = Eq + q - 2$ and (2.1) gives

$$(2g_X - 2)/|G| = (q - Eq - 2)/Eq.$$

However, the right-hand side of the above equality is clearly negative, contradicting the assumption $g_X \geq 2$. That is to say, the case (III) does not occur when X is ordinary, and so we have nothing to prove.

Finally we proceed to the most difficult case (IV). We put $e_{Q_1} = Eq$ and $e_{Q_2} = e$, where $(p, E) = 1$ and q is a power of p. Then, as before, $d_{Q_1} = Eq + q - 2$ and $d_{Q_2} = e - 1$. So (2.1) gives

$$(2g_X - 2)/|G| = ((e - E)q - 2e)/Eqe. \tag{4.3}$$

To begin with, we settle the case $E = 1$.

LEMMA 1. *Assume that* $E = 1$. *Then we have* $|G| \leq 24(g_X - 1)$.

PROOF. Setting $E = 1$ in (4.3), we obtain $2g_X - 2 = \nu|G|$, where $\nu = 1 - e^{-1} - 2q^{-1}$. So we should show $\nu \geq \frac{1}{12}$. Since $g_X \geq 2$, $\nu > 0$ holds. Accordingly, $e \geq 2$. If $e = 2$, we have $q \geq 5$ and $\nu \geq 1 - \frac{1}{2} - \frac{2}{5} = \frac{1}{10}$. If $e = 3$, we have $q \geq 4$ and $\nu \geq 1 - \frac{1}{3} - \frac{2}{4} = \frac{1}{6}$. If $e \geq 4$, we have $q \geq 3$ and $\nu \geq 1 - \frac{1}{4} - \frac{2}{3} = \frac{1}{12}$. In all cases the inequality $\nu \geq \frac{1}{12}$ is true.

Hereafter we assume $E \geq 2$. The estimate of $|G|$ will be carried out by use of the following

LEMMA 2. *Assume* $E \geq 2$. *Then the following inequalities hold:*

$$|G| \leq 14Eq\,(g_X - 1) \tag{4.4}$$

and

$$|G| \leq 21E^2\,(g_X - 1)\,. \tag{4.5}$$

PROOF. We put $d = (q-1)/E$ and $\varepsilon = e - E$. By Proposition 1 and Theorem 2(i), d is an integer. Further, $d \geq 1$ holds since $q > 1$. The assumption $g_X \geq 2$ and the formula (4.3) show $\varepsilon \geq 1$. Now (4.3) gives the equalities $2Eq(g_X - 1) = \lambda|G|$ and $2E^2(g_X - 1) = \mu|G|$, where

$$\lambda = \frac{dE\varepsilon - 2E - \varepsilon}{E + \varepsilon} \quad \text{and} \quad \mu = \frac{dE\varepsilon - 2E - \varepsilon}{(d + E^{-1})(E + \varepsilon)}.$$

So what we should prove is $\lambda \geq \frac{1}{7}$ and $\mu \geq \frac{2}{21}$. Here we give the proof of $\mu \geq \frac{2}{21}$. The proof of $\lambda \geq \frac{1}{7}$ is similar and easier. To estimate μ, we often use the fact that $(\alpha x - \beta)(\gamma x + \delta)^{-1}$ is a nondecreasing function of x for $\alpha, \beta, \gamma, \delta \geq 0$. First we consider the case $d,\ \varepsilon \geq 2$. Then, if $E \geq \varepsilon$, we have

$$\mu \geq \frac{dE\varepsilon - 3E}{(d + \frac{1}{2})(2E)} = \frac{d\varepsilon - 3}{2d + 1} \geq \frac{1}{5},$$

and if $E \leq \varepsilon$, we have

$$\mu \geq \frac{dE\varepsilon - 3\varepsilon}{(d + \frac{1}{2})(2\varepsilon)} = \frac{dE - 3}{2d + 1} \geq \frac{1}{5}.$$

In both cases $\mu > \frac{2}{21}$. Next assume that $d = 1$. Then

$$\mu = (E\varepsilon - 2E - \varepsilon)/(1 + E^{-1})(E + \varepsilon).$$

Since $\mu > 0$, $\varepsilon \geq 3$ holds. When $E = 2, \mu = 2(\varepsilon - 4)/3(\varepsilon + 2)$. Then we have $\varepsilon \geq 5$ and hence $\mu \geq \frac{2}{21}$. When $E = 3$, $\mu = 3(\varepsilon - 3)/2(\varepsilon + 3)$. Then $\varepsilon \geq 4$ and $\mu \geq \frac{3}{14} > \frac{2}{21}$. When $E \geq 4$, we have from $\varepsilon \geq 3$, $\mu \geq \frac{4}{35} > \frac{2}{21}$. Finally, assume that $\varepsilon = 1$. Then $\mu = ((d-2)E - 1)/(d + E^{-1})(E + 1)$. Since $\mu > 0$, we have $d \geq 3$. From $E \geq 2$ and $d \geq 3$, we obtain easily $\mu \geq \frac{2}{21}$. After all, $\mu \geq \frac{2}{21}$ is true for all $d, \varepsilon \geq 1$ and $E \geq 2$.

We take and fix a point $P_1 \in X$ which satisfies $\pi_{X/Y}(P_1) = Q_1$. Put $H = G_1(P_1)$ ($|H| = q$) and $Z = X/H$. Then the following holds.

LEMMA 3. *If $g_Z \geq 1$, then the estimate* (4.1) *is valid.*

PROOF. We note that $q = |H| = \deg \pi_{X/Z}$ and $H_0(P_1) = H_1(P_1) = H$. Hence applying (2.1) to $X \to Z$, we obtain an inequality $2g_X - 2 \geq q(2g_Z - 2) + 2(q-1) = 2qg_Z - 2$. Namely,

$$qg_Z \leq g_X. \tag{4.6}$$

On the other hand, $G_0(P_1)/G_1(P_1)$, which is a cyclic group of order E, may be regarded as a subgroup of $\mathrm{Aut}(Z)$ which fixes $\pi_{X/Z}(P_1) \in Z$. Accordingly, the assumption $g_Z \geq 1$ admits an estimate $E \leq 4g_Z + 2 \leq 6g_Z$ (see [**11**, Teil I, Satz 2], [**14**]). Combined with (4.6), this shows $Eq \leq 6g_X$. Therefore, in view of (4.4) we obtain (4.1).

Hereafter we assume $g_Z = 0$. We put $W = X/G_0(P_1)$. Then $Z \to W$ is a cyclic covering of degree E and $\mathrm{Gal}(Z/W) = G_0(P_1)/G_1(P_1)$. From the assumption $g_Z = 0$ and $E \geq 2$, we see that, in $Z \to W$, just two points are totally ramified and the other points are unramified. (This follows easily by applying (2.1) to $Z \to W$; cf. [**11**, p. 538, Lemma].) One of the ramification points is $R_1 = \pi_{X/W}(P_1) \in W$. Let the other be $R_2 \in W$. Here we prove

LEMMA 4. *If there exists a point $R_3 \in W$ $(R_3 \neq R_1, R_2)$ which ramifies in $X \to W$, then we have $|G| \leq 56(g_X - 1)^2$. In particular,* (4.1) *holds in this case.*

PROOF. Since R_3 is unramified in $Z \to W$, it ramifies in $X \to Z$, i.e. R_3 is wildly ramified in $X \to W$ ($q = \deg \pi_{X/Z}$ is a power of p). We apply (2.1) to the covering $X \to W$. We have $d_{R_1} \geq e_{R_1}$, $d_{R_2} \geq e_{R_2} - 1$ and $d_{R_3} \geq e_{R_3}$ because R_1 and R_3 are wildly ramified in $X \to W$. Further $g_W = 0$ holds since $g_Z = 0$. Consequently we obtain

$$2g_X - 2 \geq Eq(1 - e_{R_2}^{-1}) \geq Eq/2.$$

This shows the inequality $|G| \leq 56(g_X - 1)^2$ in view of (4.4).

From now on we assume that R_1 and R_2 are the only ramification points of the covering $X \to W$. We fix $P_2 \in X$ which satisfies $\pi_{X/W}(P_2) = R_2$. Further, we put $N = H_1(P_2)$, $q' = |N|$ and $q'' = |H/N|$. (We have $q = q'q''$ and the ramification index of P_2 with respect to $X \to W$ is Eq'.) Then the following lemma holds.

LEMMA 5. (i) *E divides both $q' - 1$ and $q'' - 1$.*
(ii) *If $q'' \geq 2$, then $|G| \leq 21(g_X - 1)^2$.*

PROOF. We first prove that N is a normal subgroup of $G' = \mathrm{Gal}(X/W) = G_0(P_1)$. For $\tau \in G'$, we have $\tau N \tau^{-1} = H_1(\tau \cdot P_2)$ because τ normalizes $H = G_1(P_1)$. By definition we have $\pi_{X/W}(\tau \cdot P_2) = \pi_{X/W}(P_2) = R_2$. Then $\pi_{X/Z}(\tau \cdot P_2) = \pi_{X/Z}(P_2)$ holds because R_2 is totally ramified in $Z \to W$. Accordingly, there exists $\sigma \in H = \mathrm{Gal}(X/Z)$ for which $\tau \cdot P_2 = \sigma \cdot P_2$ holds. Therefore, since H is abelian (cf. Theorem 2(i)), we obtain $\tau N \tau^{-1} = H_1(\tau \cdot P_2) = H_1(\sigma \cdot P_2) = \sigma H_1(P_2)\sigma^{-1} = H_1(P_2) = N$. This shows that N is normal in G'. Now we prove (i). Applying Proposition 1 to $P_2 \in X$ and $\mathrm{Gal}(X/W)$, we see that E divides $q' - 1$. Next, put $V = X/N$. Then, since N is normal in $G' = \mathrm{Gal}(X/W)$, $V \to W$ is a Galois covering of degree Eq''. Put $D = \mathrm{Gal}(V/W) = G'/N$ and $T_1 = \pi_{X/V}(P_1) \in V$. We note that T_1 is totally ramified in $V \to W$. Theorem 2(i) shows $G_2'(P_1) = \{1\}$, and hence $D_2(T_1) = \{1\}$ holds as easily calculated by using Herbrand's theorem (see

[**9**, p. 82, Lemme 5]). Therefore, applying Proposition 1 to $T_1 \in V$ and D, we see that E divides $q'' - 1$. To prove (ii), we apply (2.1) to $X \to Z$. Then we have

$$2g_X - 2 = q\left\{-2 + \frac{2(q-1)}{q} + \frac{2(q'-1)}{q'}\right\} = 2\{(q'-1)(q''-1) + q' - 2\}, \tag{4.7}$$

since $H_2(P_1) = H_2(P_2) = \{1\}$ by Theorem 2(i). From (4.7) and the assumption $g_X \geq 2$, we have $q' \geq 2$. Hence, from (i) above, $E \leq q' - 1$. We also have $E \leq q'' - 1$ since we are assuming $q'' \geq 2$. Consequently (4.7) shows $g_X - 1 \geq (q'-1)(q''-1) \geq E^2$. Therefore $|G| \leq 21(g_X - 1)^2$ holds by virtue of (4.5).

Lemma 5(ii) shows, in particular, that (4.1) is true when $q'' \geq 2$. Now we consider the final case $q'' = 1$. Namely, we assume that, in $X \to W$, P_1 and P_2 are totally ramified and the other points are unramified. In this case (4.7) gives

$$g_X = q - 1. \tag{4.8}$$

We shall prove (4.1) by use of (4.5). To estimate E, we need the following argument.

For a divisor D on X, we put $\mathcal{L}(D) = \{x \in k(X) \mid (x) \geq -D\}$, where (x) denotes the divisor of x. ($\mathcal{L}(D)$ is a finite-dimensional vector space over k.) Further, for $x \in k(X)$, we denote by $\mathrm{ord}_{P_i}(x)$ the order of x at P_i $(i = 1, 2)$. We first prove

LEMMA 6. (i) $\dim_k \mathcal{L}((q-1)P_1) = 1$.
(ii) $\dim_k \mathcal{L}((q-1)P_1 + P_2) \geq 2$.

PROOF. (i) We follow the argument of [**3**, p. 104]. Let $l \geq 1$ be the smallest integer for which $\dim_k \mathcal{L}(lP_1) = 2$ holds, and take $x \in \mathcal{L}(lP_1)$ with $\mathrm{ord}_{P_1}(x) = -l$. For every $\sigma \in H = \mathrm{Gal}(X/Z)$, $c_\sigma = \sigma \cdot x - x$ belongs to $\mathcal{L}(lP_1)$ and $\mathrm{ord}_{P_1}(c_\sigma) \geq -l+1$ holds because $\sigma \in H = H_1(P_1)$. Hence by the minimality of l, c_σ is a constant function, i.e. $c_\sigma \in k$. Furthermore, from $H = H_1(P_2)$ and $\mathrm{ord}_{P_2}(x) \geq 0$, we have $\mathrm{ord}_{P_2}(c_\sigma) \geq 1$. This shows that $c_\sigma = 0$ for all $\sigma \in H$. Consequently $x \in k(Z)$, and hence l is a multiple of q. In particular we have $l \geq q$, which proves (i).

(ii) The Riemann-Roch theorem shows $\dim_k \mathcal{L}((q-1)P_1 + P_2) \geq q - g_X + 1$. Hence by (4.8), we obtain $\dim_k \mathcal{L}((q-1)P_1 + P_2) \geq 2$.

Let $d \geq 1$ be the smallest integer for which $\dim_k \mathcal{L}(dP_1 + P_2) = 2$ holds. Then Lemma 6(ii) shows

$$d \leq q - 1. \tag{4.9}$$

We take an element $\tau \in \mathrm{Gal}(X/W)$ of order E. (Since $(E, q) = 1$, the sequence $1 \to \mathrm{Gal}(X/Z) \to \mathrm{Gal}(X/W) \to \mathrm{Gal}(Z/W) \to 1$ splits, and hence such τ exists.) Then τ acts on $M = \mathcal{L}(dP_1 + P_2)$ because it fixes P_1 and P_2. The action of τ on M is semisimple because $(p, E) = 1$, i.e. M is spanned over k by eigenvectors of τ (one of them is a constant function). Namely, we have $M = k \oplus ku$, where $u \in M$ satisfies $\tau \cdot u = \zeta u$ for some $\zeta \in k^\times$ $(\zeta^E = 1)$. We denote by $(u)_0$ and $(u)_\infty$ the zero-divisor and the pole-divisor of u, respectively ($(u) = (u)_0 - (u)_\infty$ holds). Then we have

$$(u)_\infty = dP_1 + P_2. \tag{4.10}$$

(By the minimality of d, $\mathrm{ord}_{P_1}(u) = -d$. Hence Lemma 6(i) and (4.9) show (4.10).)

For $\sigma \in H$, put $\chi(\sigma) = \sigma \cdot u - u$. Then $\mathrm{ord}_{P_1}(\chi(\sigma)) \geq -d+1$ because $\sigma \in H = H_1(P_1)$. Hence $\chi(\sigma) \in k$ by the minimality of d. It is easy to verify that χ is a group homomorphism from H to k, i.e. $\chi \in \mathrm{Hom}(H, k)$. Further we see that χ is injective. For, if $\chi(\sigma_0) = 0$ for some $\sigma_0 \in H$, $\sigma_0 \neq 1$, then u belongs to the fixed field of σ_0, which is impossible because $\mathrm{ord}_{P_2}(u) = -1$ (P_2 is totally ramified in $X \to Z$). We define a polynomial $f(U) \in k[U]$ by

$$f(U) = \prod_{\sigma \in H} (U - \chi(\sigma)).$$

Then $f(U)$ is an additive polynomial of degree q (cf. [**9**, Chapter V, §5]). Further, it is separable because χ is injective. Putting $U = u$, we have $f(u) \in k(X)$. Since, by definition, $\sigma \cdot f(u) = f(u)$ holds for all $\sigma \in H$, we see that $f(u) \in k(Z)$. On the other hand, there exists an element $t \in k(Z)$ whose divisor in Z coincides with $\pi_{X/Z}(P_2) - \pi_{X/Z}(P_1)$, since $g_Z = 0$. Then we have $k(Z) = k(t)$, and so $f(u)$ is a rational function of t. Examining the poles of $f(u)$ (see (4.10)), we obtain a precise form

$$f(u) = g(t) + at^{-1} + b, \tag{4.11}$$

where $a \in k^\times$, $b \in k$ and $g(T) \in k[T]$ is a polynomial of degree d satisfying $g(0) = 0$. The following lemma holds by virtue of the assumption that X is ordinary.

LEMMA 7. *$g(T)$ is an additive polynomial. In particular, $d = \deg g(T)$ is a power of p.*

PROOF. Let $f(U) = \sum_{i=0}^{n} c_i U^{p^{n-i}}$, where $q = p^n$ and $c_0 = 1$, and take $\alpha \in k$ which satisfies

$$\sum_{i=0}^{n} (c_i \alpha)^{p^i} = 0. \tag{4.12}$$

Then we see easily that there exists an additive polynomial $h_\alpha(U)$ which satisfies

$$h_\alpha(U)^p - h_\alpha(U) = \alpha f(U). \tag{4.13}$$

(We put $h_\alpha(U) = \sum_{i=1}^{n} b_i U^{p^{n-i}}$ and try to solve (4.13). The solvability condition is just (4.12).) Next we decompose $g(T)$ into the form

$$g(T) = \sum_{(p,m)=1} g_m(T^m),$$

where each $g_m(T)$ is an additive polynomial and m runs over all natural numbers satisfying $(p, m) = 1$. (Such a decomposition is possible since $g(0) = 0$.) Then, for $\alpha \in k$ satisfying (4.12), we have from (4.11) and (4.13),

$$h_\alpha(u)^p - h_\alpha(u) = \sum_{(p,m)=1} \alpha g_m(t^m) + \alpha a t^{-1} + \alpha b.$$

Here we take suitable $r_\alpha(t) \in k[t]$, for which the following holds: When we put $v_\alpha = h_\alpha(u) + r_\alpha(t)$, it satisfies

$$v_\alpha^p - v_\alpha = \sum_{(p,m)=1} \tilde{g}_m(\alpha) t^m + \alpha a t^{-1} + \alpha b, \tag{4.14}$$

where $\tilde{g}_m(\alpha) = \sum_i (\alpha a_i)^{p^{-i}} \in k$ when $g_m(T) = \sum_i a_i T^{p^i}$. (Such $r_\alpha(t)$ is obtained by repeating the transformation $at^{pl} = \{(a^{p^{-1}}t^l)^p - a^{p^{-1}}t^l\} + a^{p^{-1}}t^l$; cf. [**1**].) Let m_0 be the largest m for which $g_m(T) \neq 0$ holds. Then there exists $\alpha = \alpha_0$ satisfying (4.12) and $\tilde{g}_{m_0}(\alpha_0) \neq 0$. For, we have $\deg g_{m_0}(T) \leq \deg g(T) = d < q$ (see (4.9)), and (4.12) has q different solutions ($c_0, c_n \neq 0$ since $f(U)$ is a separable polynomial of degree q). We fix such α_0. Let V be the curve satisfying $k(V) = k(t, v_{\alpha_0})$. Then $V \to Z$ is a cyclic covering of degree p (it is defined by (4.14) for $\alpha = \alpha_0$), and $D = \mathrm{Gal}(V/Z)$ is a quotient group of $H = \mathrm{Gal}(X/Z)$. Putting $T_1 = \pi_{X/V}(P_1)$, we try to determine the ramification groups $D_i(T_1)$ ($i \geq 1$). First we apply Herbrand's theorem [**9**, p. 82, Lemme 5] to D and H. Then we obtain $D_1(T_1) = D$ and $D_2(T_1) = \{1\}$ since we know $H_1(P_1) = H$ and $H_2(P_1) = \{1\}$ (cf. Theorem 2(i)). On the other hand, we can determine $D_i(T_1)$ from the equation (4.14) for $\alpha = \alpha_0$. By the choice of m_0 and α_0, the result is $D_{m_0}(T_1) = D$ and $D_{m_0+1}(T_1) = \{1\}$. (For the method of computation, see [**1**] and [**11**, Teil II, Satz 1].) Therefore we obtain $m_0 = 1$, which shows that $g(T)$ itself is additive.

By $\tau \cdot u = \varsigma u$ ($\varsigma \in k^\times$), the zero-divisor $(u)_0$ of u is invariant under τ. The fixed points of τ are only P_1 and P_2, and $(u)_0$ does not contain them because of (4.10). Hence E, the order of τ, divides $\deg(u)_0$. On the other hand, $\deg(u)_0 = \deg(u)_\infty = d + 1$ (see (4.10)). So we have

$$E \text{ divides } d + 1. \tag{4.15}$$

(An alternative proof of (4.15) is as follows: It is easy to see that $\tau \cdot t = \omega t$ for a primitive Eth root of unity ω. Then applying τ to (4.11) (recall $\tau \cdot u = \varsigma u$) and comparing coefficients, we obtain (4.15). Further, this argument gives more accurate information about $f(U)$ and $g(T)$, although we do not need it here.) By Proposition 1 and Theorem 2(i), E divides $q - 1$. Combined with (4.15), this shows that E divides $q + d$. From Lemma 7 and (4.9), we see that d is a divisor of q. Hence we obtain

$$E \text{ divides } qd^{-1} + 1, \tag{4.16}$$

recalling $(p, E) = 1$. Clearly, we have $d \leq \sqrt{q}$ or $qd^{-1} \leq \sqrt{q}$. In either case, the equality $E \leq \sqrt{q} + 1$ is true in view of (4.15) and (4.16). Consequently, (4.8) shows $E \leq \sqrt{g_X + 1} + 1$. (This estimate of E cannot be improved as the example in the Remark after Theorem 3 shows.) By an easy computation we obtain $E^2 \leq (\sqrt{g_X + 1} + 1)^2 \leq 4g_X$ ($g_X \geq 2$). Therefore the inequality (4.1) holds by virtue of (4.5). Thus the proof of Theorem 3 is completed.

REFERENCES

1. H. Hasse, *Theorie der relativ-zyklischen algebraischen Funktionenkörper, insbesondere bei endlichem Konstantenkörper*, J. Reine Angew. Math. **172** (1934), 37–54 = Math. Abh. Band 2, 133–150.
2. H. Hasse and E. Witt, *Zyklische unverzweigte Erweiterungskörper von Primzahlgrad p über einem algebraischen Funktionenkörper der charakteristik p*, Monatsh. Math. Phys. **43** (1936), 477–492=Math. Abh. Band 2, 202–217.
3. H.-W. Henn, *Funktionenkörper mit grosser Automorphismengruppe*, J. Reine Angew. Math. **302** (1978), 96–115.
4. M. L. Madan, *On a theorem of M. Deuring and I. R. Šafarevič*, Manuscripta Math. **23** (1977), 91–102.

5. D. J. Madden and R. C. Valentini, *The group of automorphisms of algebraic function fields*, J. Reine Angew. Math. **343** (1983), 162–168.
6. S. Nakajima, *Equivariant form of the Deuring-Šafarevič formula for Hasse-Witt invariants*, Math. Z. **190** (1985), 559–566.
7. P. Roquette, *Abschätzung der Automorphismenanzahl von Funktionenkörpern bei Primzahlcharakteristik*, Math. Z. **117** (1970), 157–163.
8. I. R. Šafarevič, *On p-extensions*, Amer. Math. Soc. Transl. (2) 4 (1954), 59–72.
9. J-P. Serre, *Corps locaux*, Hermann, Paris, 1968.
10. B. Singh, *On the group of automorphisms of a function field of genus at least two*, J. Pure Appl. Algebra **4** (1974), 205–229.
11. H. Stichtenoth, *Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik*, I, II, Arch. Math. **24** (1973), 527–544, 615–631.
12. D. Subrao, *The p-rank of Artin-Schreier curves*, Manuscripta Math. **16** (1975), 169–193.
13. F. J. Sullivan, *p-torsion in the class group of curves with too many automorphisms*, Arch. Math. **26** (1975), 253–261.
14. A. Wiman, *Über die hyperelliptischen Curven und diejenigen von Geschlechte $P = 3$ welche eindeutigen Transformationen in sich zulassen*, Bihang Till. Kongl. Svenska Vetenskaps-Akademiens Hadlingar **21** (1895–96), 1–23.

DEPARTMENT OF MATHEMATICS, COLLEGE OF ARTS AND SCIENCES, UNIVERISTY OF TOKYO, KOMABA, MEGURO, TOKYO 153, JAPAN