Tôhoku Math. J.
42 (1990), 149–161

GALOIS EXTENSIONS OF ALGEBRAIC FUNCTION FIELDS

Dedicated to Professor Ichiro Satake on his sixtieth birthday

HISASHI KOJIMA

(Received December 27, 1988, revised October 23, 1989)

Introduction. Let K be an algebraic function field of one variable of genus g over the complex number field $\boldsymbol{C}$. Let $\mathfrak{P}_1, \cdots, \mathfrak{P}_n$ and $m_1, \cdots, m_n$ be any given distinct prime divisors of K over $\boldsymbol{C}$ and any given elements of $\boldsymbol{N} \cup \{\infty\}$ satisfying $2g-2+\sum_{i=1}^{n}(1-1/m_i)>0$, respectively, where $\boldsymbol{N}$ means the set of natural numbers. Set $\Delta=\{i \mid 1 \leqq i \leqq n, m_i=\infty\}$ and $\Delta'=\{1, 2, \cdots, n\}-\Delta$. We consider all Galois extensions L of K in a fixed algebraic closure $\bar{K}$ of K such that the divisors $\mathfrak{D}(L/K)'$ divide $\sum_{i=1}^{n}(m_i-1)\mathfrak{P}_i$ and that the ramification indices $e_{\mathfrak{P}_i}$ $(1 \leqq i \leqq n)$ of divisors of L over $\mathfrak{P}_i$ divide m_i, where $\mathfrak{D}(L/K)'=\mathfrak{D}(L/K)-\sum_{i \in \Delta} v_{\mathfrak{P}_i}\mathfrak{P}_i$ and $\mathfrak{D}(L/K)=\sum_{\mathfrak{P}} v_{\mathfrak{P}}\mathfrak{P}$ is the ramification divisor of L over K. It is well known that the Galois group of the composite field of all these Galois extensions of K is isomorphic to the profinite completion of a Fuchsian group Γ_0 with signature $(m_1, \cdots, m_n: g)$ (cf. Eichler [2] and Weil [9]). We fix an odd prime number p and denote by F_p the finite field with p elements.

In this paper, we shall study the number of Galois extensions L (resp. $\tilde{L}$) of K in $\bar{K}$ with $SL_2(F_p)$ (resp. $PSL_2(F_p)$) as their Galois groups such that $\mathfrak{D}(L/K)' \mid \sum_{i=1}^{n}(m_i-1)\mathfrak{P}_i$, $e_{\mathfrak{P}_i} \mid m_i$ $(i \in \Delta')$ and $e_{\mathfrak{P}_1}=m_1$. This number is independent of $\mathfrak{P}_1, \cdots, \mathfrak{P}_n$. So we denote by $N(m_1, \cdots, m_n: g)$ (resp. $\tilde{N}(m_1, \cdots, m_n: g)$) the number of such Galois extensions. Throughout this paper, for technical reasons, we confine ourselves to the case where $m_1=p$. This assumption is essential to our arguments. In Theorem 1, we shall obtain formulas for $N(m_1, \cdots, m_n: g)$ and $\tilde{N}(m_1, \cdots, m_n: g)$. In particular, $N(k)=N(p, \infty, k: 0)$ $(k=1, \cdots, 7$ or k is a prime), $N(p, \overbrace{\infty, \cdots, \infty}^{n-1}: g)$ and $\tilde{N}(p, \overbrace{\infty, \cdots, \infty}^{n-1}: g)$ $(p \neq 2)$ can be determined explicitly as follows:

$$N(1)=N(2)=0,\ N(4)=(p-1),\ N(6)=2(p-1)$$

$$N(q)=\begin{cases}(p-1)(q-1)/2 & q \mid (p^2-1)\\ p-1 & q=p\\ 0 & \text{otherwise}\end{cases}$$

for every odd prime q. Furthermore,

Partly supported by the Grants-in-Aid for Encouragement of Young Scientists, The Ministry of Education, Science and Culture, Japan (1988).

$$N(p, \overbrace{\infty, \cdots, \infty}^{n-2} : g) = p^{2g+n-3}(p-1)^{2g+n-2}((p+1)^{2g+n-2}-1)$$

and

$$\tilde{N}(p, \overbrace{\infty, \cdots, \infty}^{n-1} : g) = (1/2)^{2g+n-2} N(p, \overbrace{\infty, \cdots, \infty}^{n-1} : g) .$$

In a preparatory Section 1, we shall discuss elementary properties of the uniformization theorem of Riemann surfaces and Fuchsian groups. Using Galois theory of algebraic function fields of one variable, we can verify that $N(p, m_2, \cdots, m_n: g)$ (resp. $\tilde{N}(p, m_2, \cdots, m_n: g)$) equals the number of normal subgroups Γ of Γ_0 such that $\Gamma_0/\Gamma \cong SL_2(\boldsymbol{F}_p)$ (resp. $PSL_2(\boldsymbol{F}_p)$) and $\gamma_1 \notin \Gamma$, where γ_1 is an element of Γ_0 defined in Section 1. In Section 2, we reduce the computation to that of the number of $GL_2(\boldsymbol{F}_p)$-equivalence classes of ordered systems of generators of $SL_2(\boldsymbol{F}_p)$ (resp. $PSL_2(\boldsymbol{F}_p)$) satisfying certain conditions. In Section 3, applying the method used in §1 and §2, we shall calculate $\tilde{N}_1(p, m_2, \cdots, m_n: g)$ (resp. $\tilde{N}_2(p, m_2, \cdots, m_n: g)$) which is the number of Galois extensions L of K in $\bar{K}$ such that $\mathrm{Gal}(L/K) \cong PSL_2(\boldsymbol{F}_p)$ and $\mathfrak{D}(L/K)' = \sum_{i \in \Delta}(m_i - 1)\mathfrak{P}_i$ (resp. isomorphism classes of $PSL_2(\boldsymbol{F}_p)$-Galois extensions L of K in $\bar{K}$ of type $(p, m_2, \cdots, m_n: g)$) (See §3 for definition).

We note that Hecke [3] essentially obtained a formula for $\tilde{N}_1(p, 3, 2: 0)$ in the study of elliptic modular function fields of level p (cf. Shih [7]).

After having written down the first draft of this paper, Professor Y. Morita informed the author that Professor Y. Ihara obtained results closely relative to ours. H. Katsurada gave an upper bound of the number of étale-$SL_2(\boldsymbol{F}_p)$ Galois covering of algebraic curves of genus 2 of positive characteristic p (cf. [5]). To compare a gap between the number of étale-$SL_2(\boldsymbol{F}_p)$ Galois covering of algebraic curves of characteristic 0 and p, Y. Ihara obtained explicit formulas for unramified $SL_2(\boldsymbol{F}_p)$ Galois extensions of algebraic function fields over $\boldsymbol{C}$ (cf. [5]). His result does not overlap with ours: The motives and the method are different. Thanks are due to Professor Y. Ihara for valuable suggestions, interest in this work and warm encouragement.

Finally, the author is indebted to the referee for suggesting some revisions of the original version of this paper and showing a simple proof of Corollary 1.

NOTATION. We denote by $\boldsymbol{C}$ and $\boldsymbol{Z}$, the complex number field and the ring of rational integers, respectively. The complex upper half plane is denoted by H. $\#S$ denotes the cardinality of a set S. $\mathrm{Gal}(L/K)$ means the Galois group of a Galois extension L over a field K.

1. Galois extensions of algebraic function fields of one variable. If Γ is a finitely generated Fuchsian group of the first kind, the quotient spaces $\Gamma\backslash H$ and $\Gamma\backslash H^*$ become Riemann surfaces, where $H^* = H \cup \{\text{cusps of } \Gamma\}$. $\Gamma\backslash H^*$ is well-known to be compact. We denote by $K(R)$ the field consisting of rational functions on a compact Riemann surface R. Let K be an algebraic function field of one variable of genus g

over C, i.e. K is a finite algebraic extension of a rational function field $C(z)$. Denote by $R(K)$ the set of all prime divisors of K over C. Then $R(K)$ has a structure of a compact Riemann surface. We fix a finite number of distinct prime divisors $\mathfrak{P}_1, \cdots, \mathfrak{P}_n$ of K over C and fix a finite set of elements $m_1, \cdots, m_n$ of $N \cup \{\infty\}$ satisfying $2g-2+\sum_{i=1}^{n}(1-1/m_i)>0$. Moreover, we fix an algebraic closure $\bar{K}$ of K and consider all fields here to be subfields of $\bar{K}$. We further fix an odd prime number p. Hereafter we assume that $m_1=p$. Now we consider Galois extensions L (resp. $\tilde{L}$) of K in $\bar{K}$ satisfying the following conditions:

(1.1) Every prime divisor $\mathfrak{P}$ of K over C except the prime divisors $\mathfrak{P}_i$ $(1 \leqq i \leqq n)$ is unramified in L, and the ramification indices $e_{\mathfrak{P}_i}$ $(1 \leqq i \leqq n)$ relative to $\mathfrak{P}_i$ of the divisors of L over $\mathfrak{P}_i$ divide m_i.

(1.2) (resp. (1.2)′) The Galois group $\mathrm{Gal}(L/K)$ (resp. $\mathrm{Gal}(L/K)$) is isomorphic to the special linear group $SL_2(\boldsymbol{F}_p)$ (resp. projective special linear group $PSL_2(\boldsymbol{F}_p)$) over the finite field with p elements.

(1.3) The index $e_{\mathfrak{P}_1}$ is equal to m_1.

When $g=0, n=3$, the condition (1.3) is automatically satisfied because there exist no non-abelian Galois extensions of $C(z)$ ramified only at two prime divisors of $C(z)$. We denote by $N(p, m_2, \cdots, m_n; g)$ (resp. $\tilde{N}(p, m_2, \cdots, m_n; g)$) the number of Galois extensions L (resp. $\tilde{L}$) of K in $\bar{K}$ satisfying the conditions (1.1), (1.2) (resp. (1.2)′) and (1.3).

Let L be a Galois extension of K in $\bar{K}$ satisfying (1.1). Then the projection $f: R(L) \to R(K)$ is a surjective holomorphic mapping and the ramification index of f at every point in $f^{-1}(\mathfrak{P}_i)$ equals $e_{\mathfrak{P}_i}$. Conversely, for any surjective holomorphic mapping $f: R \to R(K)$ of compact Riemann surfaces such that the ramification index of f at every point in $f^{-1}(\mathfrak{P}_i)$ divides m_i, $K(R)$ is a finite algebraic extension of $K(R(K))$ $(=K)$ and all ramification indices of K over $\mathfrak{P}_i$ divide m_i. By the uniformization theorem of compact Riemann surfaces, we have a suitable Fuchsian group Γ_0 $(\subset PSL_2(\boldsymbol{R}))$ of the first kind and a biholomorphic mapping $h_0: R(K) \to \Gamma_0 \backslash H^*$ satisfying the following condition: If $f: R \to R(K)$ is any surjective holomorphic mapping of compact Riemann surfaces such that all ramification indices of f at $f^{-1}(\mathfrak{P}_i)$ divide m_i, then there exists a subgroup Γ of Γ_0 of finite index and a biholomorphic mapping $h: R \to \Gamma \backslash H^*$ such that the diagram

(1.4)
$$\begin{array}{ccc} R & \xrightarrow{h} & \Gamma \backslash H^* \\ {\scriptstyle f}\downarrow & & \downarrow \\ R(K) & \xrightarrow{h_0} & \Gamma_0 \backslash H^* \end{array}$$

is commutative.

It is known that Γ_0 has a system of generators $\alpha_1, \beta_1, \cdots, \alpha_g, \beta_g, \gamma_1, \cdots, \gamma_n$ with the following fundamental relations

$$[\alpha_1, \beta_1] \cdots [\alpha_g, \beta_g] \gamma_1 \cdots \gamma_n = \gamma_i^{m_i} = 1 \qquad (i \in \Delta')$$

(cf. Eichler [2] and Weil [9]).

Let $\mathfrak{G} = \mathrm{Aut}(\tilde{K})$ be the group of automorphisms of the field $\tilde{K}$ of all meromorphic functions on H which are meromorphic at every cusp of Γ_0. Consider the injective mapping Φ of Γ_0 into $\mathfrak{G}$ defined by $\Phi(\gamma)(u)(t) = u(\gamma^{-1}(t))$ for every $\gamma \in \Gamma_0$, $u \in \tilde{K}$ and $t \in H$. We put $\mathfrak{G}_0 = \Phi(\Gamma_0)$ and $\Psi = \Phi^{-1}$ (the inverse mapping of Φ).

For any subgroup $\mathfrak{H}$ of $\mathfrak{G}_0$ of finite index, we put $K(\mathfrak{H}) = K(\Psi(\mathfrak{H})\backslash H^*)$. For any $u \in K(\Psi(\mathfrak{H})\backslash H^*)$, we define a function $\tilde{u}$ on H by $\tilde{u}(t) = u(\pi_{\mathfrak{H}}(t))$ for any $t \in H$ with the natural projection $\pi_{\mathfrak{H}}$ of H onto $\Psi(\mathfrak{H}\backslash H)$. It is well known that the set $\{\tilde{u} \mid u \in K(\Psi(\mathfrak{H})\backslash H^*)\}$ coincides with the field of automorphic functions with respect to $\Psi(\mathfrak{H})$. Therefore, we can regard $K(\Psi(\mathfrak{H})\backslash H^*)$ as a subfield of $\tilde{K}$. By (1.4), we have a natural isomorphisms

$$K(\mathfrak{G}_0) = K(\Gamma_0\backslash H^*) \cong K(R(K)) \cong K$$

of fields. Hence in what follows, we identify $\Gamma_0\backslash H^*$ and $K(\mathfrak{G}_0)$ with $R(K)$ and K, respectively.

Let L be an algebraic extension of K in $\bar{K}$ satisfying the condition (1.1). By (1.4), there exists a subgroup $\Gamma = \Gamma(L)$ of Γ_0 such that

$$K(\Psi^{-1}(\Gamma))/K \cong L/K \ (K\text{-isomorphism}) .$$

Hence, to study such finite algebraic extensions L in $\bar{K}$, *it is* sufficient to study $K(\Gamma\backslash H^*)$ instead of L. Since, by (1.4),

$$L \cong K(\Gamma(L)\backslash H^*) \subset \tilde{K} ,$$

$\mathfrak{G}_0$ acts on L. For $\gamma \in \mathfrak{G}_0$ and $u' \in L$, we write this action as $\gamma(u')$. Put $\mathfrak{G}(L) = \{\gamma \in \mathfrak{G}_0 \mid \gamma(u') = u' \text{ for any } u' \in L\}$. Following the methods in Iwasawa [4], we can easily prove the following in parallel with Galois theory:

PROPOSITION 1.1. (1) *If $n = [\mathfrak{G}_0 : \mathfrak{H}]$ is finite, then $K(\mathfrak{H})$ is an algebraic extension of K of degree n satisfying the condition* (1.1) *and $\mathfrak{G}(K(\mathfrak{H})) = \mathfrak{H}$.*

(2) *If L satisfies the condition* (1.1) *and $n = [L : K]$, then $\mathfrak{G}(L)$* is a subgroup of $\mathfrak{G}_0$ *of index n and $K(\mathfrak{G}(L)) = L$.*

(3) *L is a Galois extension of K if and only if $\mathfrak{G}(L)$ is a normal subgroup of $\mathfrak{G}_0$. Furthermore, in this case, there exist isomorphisms*

$$\mathrm{Gal}(L/K) \cong \mathfrak{G}_0/\mathfrak{G}(L) \cong \Gamma_0/\Gamma(L) .$$

We identify the profinite completion $\hat{\Gamma}_0$ with the Galois group of the maximum

Galois extension of K in $\bar{K}$ satisfying (1.1) via an isomorphism in such a way γ_i $(1 \leqq i \leqq n)$ generate inertia groups above $\mathfrak{P}_i$. Fix this isomorphism. Then we have the following proposition.

PROPOSITION 1.2. *Let the notation be as above. There exists a one-to-one correspondence between the set of Galois extensions L (resp. $\tilde{L}$) of K in $\bar{K}$ satisfying* (1.1), (1.2) (*resp.* (1.2)'), (1.3) *and the set of normal subgroups of Γ_0 of finite index such that Γ_0/Γ is isomorphic to $SL_2(\boldsymbol{F}_p)$ (resp. $PSL_2(\boldsymbol{F}_p)$) and $\gamma_1 \notin \Gamma$.*

2. Calculation of the number of Galois extensions. In this section, we calculate $N(p, m_2, \cdots, m_n; g)$ only. $\tilde{N}(p, m_2, \cdots, m_n; g)$ can be calculated similarly. In this section, we assume that p is an odd prime number. By Proposition 1.2, we obtain

$$N(p, m_2, \cdots, m_n; g)$$
$$= \#\{\Gamma \mid \Gamma \text{ is a normal subgroup of } \Gamma_0 \text{ such that } \gamma_1 \notin \Gamma \text{ and } \Gamma_0/\Gamma \cong SL_2(\boldsymbol{F}_p)\}.$$

Let $GL_2(\boldsymbol{F}_p)$ denote the general linear group over the finite field $\boldsymbol{F}_p$. By Steinberg [8], we can easily show the following lemma.

LEMMA 2.1. *Let σ be an automorphism of $SL_2(\boldsymbol{F}_p)$. Then there exists an element g of $GL_2(\boldsymbol{F}_p)$ such that*

$$\sigma(x) = gxg^{-1} \text{ for every } x \in SL_2(\boldsymbol{F}_p).$$

We put $M = \{\phi \mid \phi \text{ is a surjective homomorphism of } \Gamma_0 \text{ to } SL_2(\boldsymbol{F}_p) \text{ and the order of } \phi(\gamma_1) \text{ is } p\}$. For elements ϕ and ϕ' of M, suppose $\Gamma = \mathrm{Ker}\,\phi = \mathrm{Ker}\,\phi'$ induce natural surjective isomorphisms:

$$\bar{\phi}: \Gamma_0/\Gamma \longrightarrow SL_2(\boldsymbol{F}_p) \text{ and } \bar{\phi}': \Gamma_0/\Gamma \longrightarrow SL_2(\boldsymbol{F}_p).$$

Since $\bar{\phi} \circ (\bar{\phi}')^{-1}$ is an automorphism of $SL_2(\boldsymbol{F}_p)$, by Lemma 2.1, there exists an element g in $GL_2(\mathbf{F}_p)$ such that

$$\bar{\phi} \circ (\bar{\phi}')^{-1}(x) = g^{-1}xg \text{ for every } x \in SL_2(\boldsymbol{F}_p).$$

Therefore we conclude

$$\phi(\gamma) = \bar{\phi}(\gamma\Gamma) = \bar{\phi} \circ (\bar{\phi}')^{-1}(\bar{\phi}'(\gamma\Gamma)) = g^{-1}\phi'(\gamma\Gamma)g = g^{-1}\phi'(\gamma)g$$

for every $\gamma \in \Gamma_0$. If ϕ and ϕ' of M satisfy this condition, we say that ϕ and ϕ' are $GL_2(\boldsymbol{F}_p)$-equivalent to each other and denote $\phi' \sim \phi$. When there is no fear of confusion, we simply write $\phi' \sim \phi$. Consequently, we have

$$N(p, m_2, \cdots, m_n; g) = \#(M/G), \tag{2.1}$$

where M/G denotes the set of $GL_2(\boldsymbol{F}_p)$-equivalence classes of M. We define a subset $\Lambda = \{x = (x_0, x_1, \cdots, x_{2g+n-2})\}$ (resp. $\tilde{\Lambda} = \{(x_0, x_1, \cdots, x_{2g+n-2})\}$) of $SL_2(\boldsymbol{F}_p)^{2g+n-1}$

(resp, $PSL_2(\boldsymbol{F}_p)^{2g+n-1}$) by the following conditions:

(2.2) The order of x_0 is equal to p.

(2.3) If $n \geqq 3$, $(x_{n-i+1})^{m_i} = 1$ for every $i \in \{3, 4, \cdots, n\} - \Delta$.

(2.4) If m_2 is not equal to ∞, then

$$(x_0^{-1}[x_{n-1}, x_n]^{-1}[x_{n+1}, x_{n+2}]^{-1} \cdots [x_{2g+n-3}, x_{2g+n-2}]^{-1} x_{n-2}^{-1} \cdots x_1^{-1})^{m_2} = 1 .$$

For $x = (x_i)$ and $y = (y_i)$ of Λ, we write $x \sim y$ if there is a $g \in GL_2(\boldsymbol{F}_p)$ satisfying $x_i = g y_i g^{-1}$ for every i $(0 \leqq i \leqq 2g+n-2)$. For every set S $(\subset \Lambda)$, we denote by S/G the set of all $GL_2(\boldsymbol{F}_p)$-equivalence classes of S. For every $\phi \in M$, put $x_0 = \phi(\gamma_1)$, $x_1 = \phi(\gamma_3)$, $\cdots$, $x_{n-2} = \phi(\gamma_n)$, $x_{n-1} = \phi(\alpha_g)$, $x_n = \phi(\beta_g)$, $\cdots$, $x_{2g+n-3} = \phi(\alpha_1)$, $x_{2g+n-2} = \phi(\beta_1)$. Then we conclude that $x = (x_0, x_1, \cdots, x_{2g+n-2})$ belongs to Λ. Furthermore, this mapping induces a bijection of M/G to

$$\{x = (x_0, x_1, \cdots, x_{2g+n-2}) \in \Lambda \mid \langle x_0, x_1, \cdots, x_{2g+n-2} \rangle = SL_2(\boldsymbol{F}_p)\}/G .$$

It follows that

$$\begin{aligned} &N(p, m_2, \cdots, m_n; g) = \#(M/G) \\ &= \#(\{x = (x_0, x_1, \cdots, x_{2g+n-2}) \in \Lambda \mid \langle x_0, x_1, \cdots, x_{2g+n-2} \rangle = SL_2(\boldsymbol{F}_p)\}/G) . \end{aligned} \tag{2.5}$$

To express $N(p, m_2, \cdots, m_n; g)$ in a clearer form, we need the following well known lemma (cf. Serre [6] and Burnside [1, p. 325]).

LEMMA 2.2. *Let G be a subgroup of $SL_2(\boldsymbol{F}_p)$ such that $p \mid \#(G)$ and $G \nsubseteqq SL_2(\boldsymbol{F}_p)$. Then there exists an element g of $SL_2(\boldsymbol{F}_p)$ satisfying*

$$gGg^{-1} \subset \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \middle| a \in \boldsymbol{F}_p^{\times}, b \in \boldsymbol{F}_p \right\} .$$

For every k $(1 \leqq k \leqq 2g+n-1)$, we put

$$\Lambda_k = \left\{ x = (x_0, x_1, \cdots, x_{2g+n-2}) \in \Lambda \middle| x_0 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \right.$$

$$\left. x_i \in B \ (0 \leqq i \leqq k-1), \quad x_k \notin B \right\} \quad (1 \leqq k \leqq 2g+n-2) \quad \text{and}$$

$$\Lambda_{2g+n-1} = \left\{ x = (x_0, x_1, \cdots, x_{2g+n-2}) \in \Lambda \middle| x_0 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \right.$$

$$\left. x_i \in B \ (1 \leqq i \leqq 2g+n-2) \right\},$$

where

$$B=\left\{\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \middle| a\in \boldsymbol{F}_p^{\times}, b\in \boldsymbol{F}_p\right\}.$$

The following lemma can be easily shown.

LEMMA 2.3. *Let the notation be as above. Then the following assertions hold.*

(1) *Any element x of Λ is $GL_2(\boldsymbol{F}_p)$-equivalent to a suitable element of Λ_k for some k.*

(2) *If $x=(x_0, \cdots, x_{2g+n-2})$ and $y=(y_0, \cdots, y_{2g+n-2})$ of Λ_k satisfy $x_i=gy_ig^{-1}$ $(0\leqq i\leqq 2g+n-2)$ for some $g\in GL_2(\boldsymbol{F}_p)$, then g is of the form*

$$\begin{pmatrix} \alpha & \beta \\ 0 & \alpha \end{pmatrix}.$$

(3) *If $k\neq k'$, then any elements $x\in\Lambda_k$ and $y\in\Lambda_k'$ are not $GL_2(\boldsymbol{F}_p)$-equivalent to each other.*

PROOF. First we prove the assertion (1). Let $x=(x_0, x_1, \cdots, x_{2g+n-2})$ be an element of Λ. By Lemma 2.2, there exist g of $SL_2(\boldsymbol{F}_p)$ and $b\in\boldsymbol{F}_p^{\times}$ such that

$$gx_0g^{-1}=\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}.$$

Since the order of x_0 is p, we have $a=1$. A computation yields that

$$\left\{\begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix}g\right\}x_0\left\{\begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix}g\right\}^{-1}=\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Hence we obtain the assertion (1).

To verify the assertion (2) and (3), it is sufficient to use the following property: If

$$g^{-1}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}g=\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \tag{2.6}$$

for some $g\in GL_2(\boldsymbol{F}_p)$, then

$$g=\begin{pmatrix} \alpha & \beta \\ 0 & \alpha \end{pmatrix}.$$

We put

$$\Lambda_0=\{x=(x_0, \cdots, x_{2g+n-2})\in\Lambda \mid \langle x_0, \cdots, x_{2g+n-2}\rangle\neq SL_2(\boldsymbol{F}_p)\}.$$

By Lemma 2.2, for every $x=(\cdots, x_i, \cdots)$ of Λ, there is an element g of $SL_2(\boldsymbol{F}_p)$ such that

$$g^{-1}x_ig=\begin{pmatrix} a_i & b_i \\ 0 & d_i \end{pmatrix} \quad \text{for each} \quad i\ (0\leqq i\leqq 2g+n-2).$$

Since the order of x_0 is p, we have

$$g^{-1}x_0g=\begin{pmatrix}1 & b_0\\ 0 & 1\end{pmatrix}.$$

Hence x_0 and x_i can be written in the form

$$x_0=g\begin{pmatrix}1 & 0\\ 0 & b_0\end{pmatrix}^{-1}\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & b_0\end{pmatrix}g^{-1}$$

and

$$x_i=g\begin{pmatrix}a_i & b_i\\ 0 & d_i\end{pmatrix}g^{-1}=g\begin{pmatrix}1 & 0\\ 0 & b_0\end{pmatrix}^{-1}\begin{pmatrix}a_i & b_i'\\ 0 & d_i'\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & b_0\end{pmatrix}g^{-1}$$

for some b_i' and $d_i'\in \boldsymbol{F}_p^{\times}$. This implies that

$$\#(\Lambda_0/G)=\#(\Lambda_{2g+n-1}/G)\,. \tag{2.7}$$

Now, by (2.5),

$$N(p, m_2, \cdots, m_n; g)=\#(\Lambda/G)-\#(\Lambda_0/G)\,. \tag{2.8}$$

By Lemma 2.3, we conclude that

$$\#(\Lambda/G)=\sum_{k=1}^{2g+n-1}\#(\Lambda_k/G)\,. \tag{2.9}$$

Now we can prove the following lemma.

LEMMA 2.4. *The following assertions hold.*

(1) *Any element*

$$\begin{pmatrix}a & b\\ c & d\end{pmatrix}(c\neq 0)$$

of $GL_2(\boldsymbol{F}_p)$ *can be expressed in the form*

$$\begin{pmatrix}a & b\\ c & d\end{pmatrix}=\begin{pmatrix}1 & k\\ 0 & 1\end{pmatrix}\begin{pmatrix}0 & b'\\ c' & d'\end{pmatrix}\begin{pmatrix}1 & k\\ 0 & 1\end{pmatrix}^{-1}$$

for some k, b', c' *and* d' *of* $\boldsymbol{F}_p$.

(2) *If*

$$\begin{pmatrix}0 & -c^{-1}\\ c & d\end{pmatrix}=\begin{pmatrix}1 & k\\ 0 & 1\end{pmatrix}\begin{pmatrix}0 & -c'^{-1}\\ c' & d'\end{pmatrix}\begin{pmatrix}1 & k\\ 0 & 1\end{pmatrix}^{-1}$$

for some k, d *and* $d'\in \boldsymbol{F}_p$ *and* c *and* $c'\in \boldsymbol{F}_p^{\times}$, *then* $k=0$.

PROOF. First, we prove the assertion (1). A direct computation yields that

$$\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}^{-1}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}=\begin{pmatrix} a-kc & k(a-kc)+b-kd \\ c & ck+d \end{pmatrix}.$$

Since $c\neq 0$, we can choose $k\in \boldsymbol{F}_p$ satisfying $a-kc=0$. Put $c'=c$, $d'=ck+d$ and $b'=b-kd$. Then we obtain (1). To verify (2), we put

$$\begin{pmatrix} 0 & -c^{-1} \\ c & d \end{pmatrix}=\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & -c'^{-1} \\ c' & d' \end{pmatrix}\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}^{-1}$$

for some c and $c'\in \boldsymbol{F}_p^{\times}$ and d, d' and $k\in \boldsymbol{F}_p$. Then

$$\begin{pmatrix} 0 & -c^{-1} \\ c & d \end{pmatrix}\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}=\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & -c'^{-1} \\ c' & d' \end{pmatrix}.$$

Hence

$$\begin{pmatrix} 0 & -c^{-1} \\ c & ck+d \end{pmatrix}=\begin{pmatrix} kc' & -c'^{-1}+kd' \\ c' & d' \end{pmatrix}.$$

Since $c'\neq 0$, we see that $k=0$, so the lemma is proved.

For any k $(1\leqq k\leqq 2g+n-2)$, we put

$$\tilde{\Lambda}_k=\left\{x=(x_0, x_1, \cdots, x_{2g+n-2})\in\tilde{\Lambda}\,\middle|\, x_0=\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},\ x_i\in\tilde{B}\ (0\leqq i\leqq k-1)\ x_k\notin\tilde{B}\right\},$$

where

$$\tilde{B}=\left\{g=\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in PSL_2(\boldsymbol{F}_p)\,\middle|\, c=0\right\}.$$

From the properties (2.*l*) ($l=7$, 8 and 9), (2) of Lemma 2.3 and Lemma 2.4, we have the following theorem.

THEOREM 1. *Let the notation be as above. Suppose that $p\neq 2$. Then the following equalities hold.*

$$N(p, m_2, \cdots, m_n; g)=\sum_{k=1}^{2g+n-2}\#\left\{x\in\Lambda_k\,\middle|\, x=(\cdots, x_k, \cdots), x_k=\begin{pmatrix} 0 & -c_k^{-1} \\ c_k & d_k \end{pmatrix}\right\}$$

and

$$\tilde{N}(p, m_2, \cdots, m_n; g)=\sum_{k=1}^{2g+n-2}\#\left\{x\in\tilde{\Lambda}_k\,\middle|\, x=(\cdots, x_k, \cdots), x_k=\begin{pmatrix} 0 & -c_k^{-1} \\ c_k & d_k \end{pmatrix}\right\}.$$

We put $N(k)=N(p, \infty, k:0)$ and $\tilde{N}(k)=\tilde{N}(p, \infty, k:0)$. By Theorem 1, we can prove the following corollary.

COROLLARY 1. *The notation being as above. Suppose that* $p\neq 2$. *Then*

$$N(1)=N(2)=0,\ N(4)=(p-1),\ N(6)=2(p-1),$$

$$N(q)=\begin{cases}(p-1)(q-1)/2 & q\,|\,(p^2-1)\\ p-1 & q=p\\ 0 & \textit{otherwise,}\end{cases}$$

for every odd prime q, $\tilde{N}(1)=0$, $\tilde{N}(2)=(p-1)/2$, $\tilde{N}(4)=(p-1)\left(\left(\frac{2}{p}\right)+2\right)$,

$$\tilde{N}(6)=\begin{cases}(p-1)\left(\left(\frac{3}{p}\right)+4\right)\Big/2 & (p\neq 3)\\ 4 & (p=3),\end{cases}$$

and $\tilde{N}(q)=N(q)$ *for every odd prime* q.

Furthermore

$$N(p, \overbrace{\infty, \cdots, \infty}^{n-1}: g)=p^{2g+n-3}(p-1)^{2g+n-2}((p+1)^{2g+n-2}-1)$$

and

$$\tilde{N}(p, \overbrace{\infty, \cdots, \infty}^{n-1}: g)=(1/2)^{2g+n-2}N(p, \overbrace{\infty, \cdots, \infty}^{n-1}: g).$$

PROOF. For a natural number k, we put

$$\mathcal{M}(k)=\left\{A=\begin{pmatrix}0 & -c^{-1}\\ c & d\end{pmatrix}\,\middle|\, A\in SL_2(\boldsymbol{F}_p) \quad \text{and} \quad A^k=1\right\}.$$

By Theorem 1, $N(k)$ is equal to $\#(\mathcal{M}(k))$.

First we treat the case where k is an odd prime number q satisfying $q\,|\,(p^2-1)$. Put

$$J(q)=\{(\beta, x)\in \boldsymbol{F}_p^{\times}\times \bar{\boldsymbol{F}}_p^{\times}\,|\, x^q=1 \quad \text{and} \quad x\neq 1\}.$$

Then we easily see that $x+x^{-1}\in \boldsymbol{F}_p$ for every $(\beta, x)\in J(q)$. Hence we may define a mapping $\Phi: J(q)\to SL_2(\boldsymbol{F}_p)$ by

$$\Phi((\beta, x))=\begin{pmatrix}0 & -\beta^{-1}\\ \beta & x+x^{-1}\end{pmatrix} \qquad \text{for every} \quad (\beta, x)\in J(q).$$

We put $\Phi((\beta, x))=A$ for every (β, x) of $J(q)$. Since x and x^{-1} are distinct eigenvalues

of A and $x^q=1$, we have

$$A\in\mathcal{M}(q)\,.$$

It follows that Φ induces a mapping of $J(q)$ to $\mathcal{M}(q)$. We easily see that Φ is a two-to-one and surjective mapping. Consequently, we obtain

$$N(q)=\#(\mathcal{M}(q))=\#(J(q))/2=(p-1)(q-1)/2\,.$$

Secondly, we shall caluculate $N(p)$. We define a mapping Ψ: $\boldsymbol{F}_p^\times\to\mathcal{M}(p)$ by

$$\Psi(\beta)=\begin{pmatrix}0 & -\beta^{-1}\\ \beta & 2\end{pmatrix}\qquad\text{for every}\quad \beta\in\boldsymbol{F}_p^\times\,.$$

Then this mapping yields a bijective mapping between $\boldsymbol{F}_p^\times$ and $\mathcal{M}(p)$. Consequently, we have

$$N(p)=\#(\mathcal{M}(p))=(p-1)\,.$$

By our definition, we easily obtain $N(q)=0$ for every odd prime q satisfying $q\neq p$ and $q\nmid(p^2-1)$. In a similar manner, we can show that $\tilde{N}(q)=N(q)$ for every odd prime q.

Thirdly, we shall compute $N(p,\overbrace{\infty,\cdots,\infty}^{n-1}:g)$. When $(m_2,m_3,\cdots,m_n)=(\infty,\overbrace{\infty,\cdots,\infty}^{n-1})$, we have

$$\#\left\{x\in\Lambda_k\,\middle|\,x=(\cdots,x_k,\cdots),\ x_k=\begin{pmatrix}0 & -c_k^{-1}\\ c_k & d_k\end{pmatrix}\right\}=(p(p^2-1))^{2g+n-2}(p+1)^{-k}$$

for every k $(1\leqq k\leqq 2g+n-2)$. By Theorem 1, we have

$$N(p,\overbrace{\infty,\cdots,\infty}^{n-1}:g)=p^{2g+n-3}(p-1)^{2g+n-2}((p+1)^{2g+n-2}-1)\,.$$

Since we can also verify the remainders, we may omit the details.

3. Isomorphism classes of Galois extensions of algebraic function fields. The details for our argument in this section can be found in Shih [7]. Though he studied Galois coverings in the category of algebraic curves, we rewrite his definitions and terminology in terms of field extensions. In this section, we suppose that p is an odd prime number.

We consider Galois extensions L of K in $\bar{K}$ with $PSL_2(\boldsymbol{F}_p)$ as their Galois groups such that $\mathfrak{D}(L/K)'=\sum_{i\in\Delta}(m_i-1)\mathfrak{P}_i(m_1=p)$. We denote by $\tilde{N}_1(p,m_2,\cdots,m_n:g)$ the number of such Galois extensions. Let us consider a pair $\{L,\phi\}$ consisting of a Galois extension L of K in $\bar{K}$ satisfying $\mathfrak{D}(L/K)'=\sum_{i\in\Delta'}(m_i-1)\mathfrak{P}_i$ and an isomorphism ϕ of $PSL_2(\boldsymbol{F}_p)$ onto Gal (L/K). We call a pair $\{L,\phi\}$ a $PSL_2(\boldsymbol{F}_p)$-Galois extension of K of type $(p,m_2,\cdots,m_n:g)$. We say that $PSL_2(\boldsymbol{F}_p)$-Galois extensions $\{L,\phi\}$, $\{L',\phi'\}$ of type $(p,m_2,\cdots,m_n:g)$ are $PSL_2(\boldsymbol{F}_p)$-isomorphic if there is a K-isomorphism f of $\bar{K}$ such that $L'=f(L)$ and $f\circ\phi(g)=\phi'(g)\circ f$ for every $g\in PSL_2(\boldsymbol{F}_p)$. We also denote by

$\tilde{N}_2(p, m_2, \cdots, m_n; g)$ the number of the isomorphism classes of $PSL_2(\boldsymbol{F}_p)$-Galois extensions of K of type $(p, m_2, \cdots, m_n; g)$.

Let α_0 be an element of $\boldsymbol{F}_p$ such that $\left(\frac{\alpha_0}{p}\right)=-1$. Define a subset $\tilde{\Lambda}'=\{x=(x_0, x_1, \cdots, x_{2g+n-2})\}$ of $PSL_2(\boldsymbol{F}_p)^{2g+n-1}$ by the following conditions:

(3.1) The order of x_0 id p.

(3.2) If $n\geqq 3$, the order of x_{n-i+1} is m_i for every $i\in\{3, 4, \cdots, n\}-\Delta$.

(3.3) If m_2 is not ∞, then the order of

$$x_0^{-1}[x_{n-1}, x_n]^{-1}[x_{n+1}, x_{n+2}]^{-1}\cdots[x_{2g+n-3}, x_{2g+n-2}]^{-1}\cdot x_{n-1}^{-1}\cdots x_1^{-1} \quad \text{is } m_2.$$

We put

$$\tilde{\Lambda}'_1(\text{resp. } \tilde{\Lambda}'_2)=\{x=(x_0, x_1, \cdots, x_{2g+n-2})\in\tilde{\Lambda}'\}$$

with

$$x_0=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\left(\text{resp.}\begin{pmatrix}1 & \alpha_0\\ 0 & 1\end{pmatrix}\right).$$

Furthermore, for every k $(1\leqq k\leqq 2g+n-2)$, we put

$$\tilde{\Lambda}'_{1,k}=\{x=(x_0, x_1, \cdots, x_{2g+n-2})\in\tilde{\Lambda}'_1 \,|\, x_1, \cdots, x_{k-1}\in\tilde{B} \text{ and } x_k\notin\tilde{B}\}$$

and

$$\tilde{\Lambda}'_{2,k}=\{x=(x_0, x_1, \cdots, x_{2g+n-2})\in\tilde{\Lambda}'_2 \,|\, x_1, \cdots, x_{k-1}\in\tilde{B} \text{ and } x_k\notin\tilde{B}\},$$

where

$$\tilde{B}=\left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix}\notin PSL_2(\boldsymbol{F}_p)\,\middle|\, c=0\right\}.$$

By the same method as in §2 and Proposition 1, we can verify the following theorem:

THEOREM 2. *Let the notation be as above. Suppose that $p\neq 2$. Then we have*

$$\tilde{N}_1(p, m_2, \cdots, m_n; g)=\sum_{k=1}^{2g+n-2}\#\left\{x=(\cdots, x_k, \cdots)\in\tilde{\Lambda}'_{1,k}\,\middle|\, x_k=\begin{pmatrix}0 & -c_k^{-1}\\ c_k & d_k\end{pmatrix}\right\}$$

and

$$\tilde{N}_2(p, m_2, \cdots, m_n; g)=\sum_{k=1}^{2g+n-2}\left(\#\left\{x=(\cdots, x_k, \cdots)\in\tilde{\Lambda}'_{1,k}\,\middle|\, x_k=\begin{pmatrix}0 & -c_k^{-1}\\ c_k & d_k\end{pmatrix}\right\}\right.$$
$$\left.+\#\left\{x=(\cdots, x_k, \cdots)\in\tilde{\Lambda}'_{2,k}\,\middle|\, x_k=\begin{pmatrix}0 & -c_k^{-1}\\ c_k & d_k\end{pmatrix}\right\}\right).$$

In particular, we have

$$\tilde{N}_1(p, 3, 2:0)=1 \quad \textit{and} \quad \tilde{N}_2(p, 3, 2:0)=2\,.$$

REFERENCES

[1] W. BURNSIDE, Theory of groups of finite order (2nd ed.). Cambridge Univ. Press, 1911.
[2] M. EICHLER, Eine Verallgemeinerung der Abelschen Integrale, Math. Z. 67 (1957), 267–298.
[3] E. HECKE, Die eindeutige Bestimmung der Modulfunktionen q-ter Stufe durch algebraische Eigenschaften, Math. Ann. 111 (1935), 293–301 (Math. Werke, 568–576, Göttingen, Vandenhoeck und Ruprecht 1970).
[4] K. IWASAWA, The theory of Algebraic Functions (in Japanese), Iwanami Shoten, Tokyo, 1952.
[5] H. KATSURADA, On étale SL_2 (F_p)-covering of algebraic curves of genus 2, J. Math. Soc. Japan 39 (1987), 397–434.
[6] J.-P. SERRE, Propriétés galoisiennes de points d'order fini des courbes elliptietes, Invent. Math. 15 (1972), 259–331.
[7] K. Y. SHIH, On the construction of Galois extensions of function fields and number fields. Math. Ann. 207 (1974), 99–120.
[8] R. STEINBERG, Automorphisms of finite linear groups. Canad. J. Math. 10 (1960), 606–615.
[9] A. WEIL, Généralisation des fonctions abéliennes. J. de Math. pure et appl. 17 (1938), 47–87.

DEPARTMENT OF MATHEMATICS
THE UNIVERSITY OF ELECTRO-COMMUNICATION
CHOFU-SHI, TOKYO 182
JAPAN