98. On Unramified $SL_2(F_p)$ Extensions of an Algebraic Function Field of Genus 2

By Hidenori KATSURADA
Department of Mathematics, Muroran Institute of Technology

(Communicated by Shokichi IYANAGA, M. J. A., Oct. 12, 1981)

Let k be an algebraically closed field of characteristic p. Let K be an algebraic function field over k. In [1], we calculated the number of unramified $SL_2(F_4)$ extensions of some algebraic function field of characteristic 2. In this note, we obtain the best possible estimation of the number of unramified Galois extensions of K whose Galois groups are isomorphic to $SL_2(F_p)$ when $p \geqq 5$ and the genus of K is 2. Detailed accounts will be published elsewhere.

Definition 1. For any system $(m_1, \cdots, m_r; n_1, \cdots, n_s)$ of integers such that $m_1 = n_1$, we define the number $N(m_1, \cdots, m_r; n_1, \cdots, n_s)$ inductively as follows:

(1) When $r=s$, we define

$$N(m_1, \cdots, m_r; n_1, \cdots, n_r) = \sum_{i=1}^{r} m_i + \sum_{i=1}^{r} n_i - r m_1.$$

(2) When $r<s$, first we define

$$N(m_1, n_1, \cdots, n_s) = n_1 \cdots n_s.$$

Assume that for $(m_1, \cdots, m_r; n_1, \cdots, n_{s-1})$ and $(m_1, \cdots, m_{r-1}; n_1, \cdots, n_{s-1})$ the number $N(\cdots)$ is defined. Then we define

$$N(m_1, \cdots, m_r; n_1, \cdots, n_s) = (m_r + n_s - m_1) N(m_1, \cdots, m_r; n_1, \cdots, n_{s-1}) + N(m_1, \cdots, m_{r-1}; n_1, \cdots, n_{s-1}).$$

(3) When $r>s$, we define

$$N(m_1, \cdots, m_r; n_1, \cdots, n_s) = N(n_1, \cdots, n_s; m_1, \cdots, m_r).$$

Let K be the maximum unramified Galois extension of K. We put $q = p^m$, where m is a natural number. We denote by $\mathrm{Irr}(\mathrm{Gal}(\tilde{K}/K), SL_2(F_q))$ the set of $GL_2(k)$ equivalence classes of 2-dimensional irreducible representations of $\mathrm{Gal}(\tilde{K}/K)$ whose images are isomorphic to subgroups of $SL_2(F_q)$. Let ρ be a representative of an element of $\mathrm{Irr}(\mathrm{Gal}(\tilde{K}/K), SL_2(F_p))$. Then we note that the order $\sharp\rho(\mathrm{Gal}(\tilde{K}/K))$ is prime to p if $\rho(\mathrm{Gal}(\tilde{K}/K)) \subsetneqq SL_2(F_p)$. Hence to estimate the number of unramified $SL_2(F_p)$ extensions of K, it suffices to estimate

$$\sharp \mathrm{Irr}(\mathrm{Gal}(\tilde{K}/K), SL_2(F_p)).$$

Theorem 1. *We put*

$$A = N(p+\overbrace{1, \cdots, p}^{p+2}+1, \overbrace{p, \cdots, p}^{p-3}; p+\overbrace{1, \cdots, p}^{p}+1, \overbrace{p, \cdots, p}^{p+1})$$

$$B=N(p+\overbrace{1,\cdots,p}^{p-1}+1,\ \overbrace{p,\cdots,p}^{p};\ p+\overbrace{1,\cdots,p}^{p+3}+1,\ \overbrace{p,\cdots,p}^{p-2})$$
$$C=N(p+\overbrace{1,\cdots,p}^{(p+3)/2}+1,\ \overbrace{p,\cdots,p}^{(p-5)/2};\ p+\overbrace{1,\cdots,p}^{(p-1)/2}+1,\ \overbrace{p,\cdots,p}^{(p+3)/2})$$
$$D=N(p+\overbrace{1,\cdots,p}^{(p-3)/2}+1,\ \overbrace{p,\cdots,p}^{(p+1)/2};\ p+\overbrace{1,\cdots,p}^{(p+5)/2}+1,\ \overbrace{p,\cdots,p}^{(p-3)/2}).$$

We assume that $p\geqq 5$. *Then we have*

$$(*)\qquad \sharp\mathrm{Irr}\,(\mathrm{Gal}\,(\tilde{K}/K), SL_2(F_p)) \leqq (A+B-6C-6D)/2-((p+1)^4+(p-1)^4)/2.$$

Next we look for a condition under which the equality holds in (*) of Theorem 1.

Let P_∞ be a Weierstrass point of K. Let $\{u_i\}$ be a basis of $L(P_\infty^{p-1})=\{u\in K\,;\,(u)\geqq P_\infty^{1-p}\}$. Let K_A be the adele ring of K. We put for any divisor Q,

$K_A(Q)=\{b\in K_A$ such that $\nu_P(b)\geqq -\nu_P(Q)$ for any prime P of $K\}$.

Let $\{y_i\}_{1\leqq i\leqq 3}$ (resp. $\{z_i\}_{1\leqq i\leqq p+2}$) be a set of elements of K_A such that

$$\{y_i \bmod K_A(P_\infty^{-2})+K\}\qquad (\text{resp. } \{z_i \bmod K_A(P_\infty^{-p-1})+K\})$$

be a basis of $H^1(P_\infty^{-2})=K_A/(K_A(P_\infty^{-2})+K)$ (resp. $H^1(P_\infty^{-p-1})$).

Then for $i=1,2,3$, there is a $(p-2, p+2)$ matrix (c_{ijk}) of $M_{p-2,p+2}(k)$ such that

$$u_j y_i^p=\sum_{k=1}^{p+2} c_{ijk} z_k \qquad \bmod K_A(P_\infty^{-p-1})+K.$$

We put $a_{jk}=\sum_{i=1}^{3} c_{ijk}X_i^p$, where X_i are indeterminates. We put $F=(a_{jk})$. For any element $(x_1, x_2, x_3)\in k^3$, we denote by $F(x_1, x_2, x_3)$ the $(p-2, p+2)$ matrix of $M_{p-2,p+2}(k)$ substituting x_i for X_i in F. Then

$$\mathcal{F}=\{(x_1, x_2, x_3)\in P^2(k)\,;\,\mathrm{rank}_k\, F(x_1, x_2, x_3)\leqq p-3\}$$

defines a 0-dimensional closed subset of $P^2(k)$.

We note that $\mathcal{F}$ is uniquely determined (up to isomorphism of $P^2(k)$) only by K. Then

Theorem 2. *In* (*) *of Theorem* 1, *the equality holds if and only if* $\mathcal{F}$ *is an empty set.*

Remark. The geometrical meaning of the condition that $\mathcal{F}$ is empty is as follows.

Let C be a complete nonsingular model of K over k. Let L_∞^{-1} be the line bundle of C of degree 1 which corresponds to a divisor P_∞^{-1}. Let f be a Frobenius map of C. Then "$\mathcal{F}$ is empty" means that for any stable vector bundle V of rank 2 such that

$$0\longrightarrow L_\infty^{-1}\longrightarrow V\longrightarrow L_\infty\longrightarrow 0,$$

f^*V is always stable.

Reference

[1] H. Katsurada: On unramified $SL_2(F_4)$ extensions of an algebraic function field. Proc. Japan Acad., **56A**, 36–39 (1980).