ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 15, Number 1, Winter 1985

THE GENERA OF PSL(F_q)-LÜROTH COVERINGS

ARTHUR K. WAYMAN

1. Introduction. In [3] H. Hasse studies the ramification theory of Kummer and Artin-Schreier cyclic coverings of an algebraic function field in one variable. These cyclic extensions are special cases of a wider class of function fields which we will entitle Lüroth coverings. In this paper we will study in detail the ramification theory of PSL($\mathbf{F}_q$)-Lüroth coverings. We will classify all genus zero and genus one PSL($\mathbf{F}_q$)-Lüroth coverings of a rational function field and construct bases for the spaces of differentials of the first kind for coverings with genus $\geqq 2$.

For notation, definitions, and standard theorems used here, the reader may consult the bibliography.

2. Lüroth coverings. Let k be a field and Y an indeterminate over k. Denote by PGL(k) the group of k-automorphisms of the rational function field $k(Y)$. For each element $\sigma \in \mathrm{PGL}(k)$ there are elements a_σ, b_σ, c_σ, $d_\sigma \in k$ with $a_\sigma d_\sigma - b_\sigma c_\sigma \neq 0$ satisfying $\sigma(f) = f((a_\sigma Y + b_\sigma)/(c_\sigma Y + d_\sigma))$ for all $f \in k(Y)$. We recall that two substitutions

$$Y \rightarrow \frac{aY + b}{cY + d} \text{ and } Y \rightarrow \frac{a'Y + b'}{c'Y + d'}$$

induce the same k-automorphism of $k(Y)$ if and only if $(a', b', c', d') = (\lambda a, \lambda b, \lambda c, \lambda d)$ for some $\lambda \in k^x = k - \{0\}$.

Let $\mathscr{G}$ be a finite non-trivial subgroup of PGL(k). If $k(Y)^{\mathscr{G}}$ is the subfield of $k(Y)$ left invariant by the action of $\mathscr{G}$, then $k(Y)^{\mathscr{G}}$ contains k and from galois theory we have $[k(Y)\colon k(Y)^{\mathscr{G}}] = |\mathscr{G}|$, where $|\mathscr{G}|$ denotes the cardinality of $\mathscr{G}$. By Lüroth's theorem (see van der Waerden [5]) there is an element $Z_{\mathscr{G}}$ in $k(Y)$ such that $k(Y)^{\mathscr{G}} = k(Z_{\mathscr{G}})$. We can write $Z_{\mathscr{G}} = U_{\mathscr{G}}/V_{\mathscr{G}}$ for some $U_{\mathscr{G}}$, $V_{\mathscr{G}} \in k[Y]$ with $(U_{\mathscr{G}}, V_{\mathscr{G}}) = 1$. Moreover,

$$\deg_Y Z_{\mathscr{G}} = \max\{\deg_Y U_{\mathscr{G}}, \deg_Y V_{\mathscr{G}}\} = |\mathscr{G}|.$$

We remark that any other generator of $k(Y)^{\mathscr{G}}$ is of the form $(aZ_{\mathscr{G}} + b)/(cZ_{\mathscr{G}} + d)$ where $a, b, c, d \in k$ and $ad - bc \neq 0$.

Let K be an algebraic function field in one variable over the algebraically

Received by the editors on December 20, 1982 and in revised form on September 27, 1983.

closed field k. For the group $\mathscr{G}$ set $Z = Z_{\mathscr{G}}$ and let z be a nonconstant element of K. The polynomial

$$L_Z(\mathscr{G}, z)(Y) = U_{\mathscr{G}}(Y) - zV_{\mathscr{G}}(Y)$$

is called a Lüroth polynomial. If $L_Z(\mathscr{G}, z)$ is irreducible over K, then the extension $L = K(y)$ where $L_Z(\mathscr{G}, z)(y) = 0$ is called a Lüroth covering of K. Observe that if $L|K$ is a Lüroth covering defined by $L_Z(\mathscr{G}, z)$, then $[L: K] = \deg_Y L_Z(\mathscr{G}, z) = |\mathscr{G}|$.

PROPOSITION 1. *Let L be a Lüroth covering of K defined by the irreducible polynomial $L_Z(\mathscr{G}, z)$. Then the extension $L|K$ is galois and* $\mathrm{Gal}(L|K) = \mathscr{G}$.

PROOF. The field $L = K(y)$ where $L_Z(\mathscr{G}, z)(y) = 0$. Since $U_{\mathscr{G}}/V_{\mathscr{G}}$ is invariant under substitutions of the form $Y \to (a_\sigma Y + b_\sigma)/(c_\sigma Y + d_\sigma)$, $\sigma \in \mathscr{G}$, we conclude that each conjugate of y is of the form $(a_\sigma y + b_\sigma)/(c_\sigma y + c_\sigma)$, $\sigma \in \mathscr{G}$. Since $a_\sigma, b_\sigma, c_\sigma, d_\sigma \in k$, each conjugate of y is in L. Furthermore, since y is transcendental over k, if $\sigma, \phi \in \mathscr{G}$ and $\sigma \neq \phi$, then $(a_\sigma y_\sigma + b_\sigma)/(c_\sigma y_\sigma + d_\sigma) \neq (a_\phi y_\phi + b_\phi)/(c_\phi y_\phi + d_\phi)$. We conclude that $L|K$ is galois and $\mathrm{Gal}(L|K) = \mathscr{G}$.

PROPOSITION 2. *Let $L_Z(\mathscr{G}, z)$ be a (possibly reducible) Lüroth polynomial. If $L_Z(\mathscr{G}, z)$ has no root in K, then its splitting field is a Lüroth covering of K defined by a Lüroth polynomial of the form $L_{Z_{\mathscr{H}}}(\mathscr{H}, z')$ where $\mathscr{H}$ is a subgroup of $\mathscr{G}$ and z' is a non-constant in K.*

PROOF. The proof of Proposition 1 shows that if L is an extension of K containing one root of $L_Z(\mathscr{G}, z)$, then L contains all roots of $L_Z(\mathscr{G}, z)$. Proposition 2 follows if $L_Z(\mathscr{G}, z)$ is irreducible; so assume that $L_Z(\mathscr{G}, z)$ factors over K and write $L_Z(\mathscr{G}, z) = GH$ for some $G, H \in K[Y]$ with $\deg_Y G$ and $\deg_Y H \geqq 1$. We may and do assume that G is irreducible and monic. Let y be a root of G and set $L = K(y)$. Then L contains all of the roots of $L_Z(\mathscr{G}, z)$ and is therefore the splitting field of $L_Z(\mathscr{G}, z)$ over K. The argument in Proposition 1 also shows that the roots of G are distinct and hence $L|K$ is galois. Each conjugate of y has the form $(a_\sigma y_\sigma + b_\sigma)/(c_\sigma y_\sigma + d_\sigma)$ for some $\sigma \in \mathscr{G}$ (with $a_\sigma, b_\sigma, c_\sigma, d_\sigma \in k$). Let

$$\mathscr{H} = \left\{\sigma \in \mathscr{G} | G\left(\frac{a_\sigma y + b_\sigma}{c_\sigma y + d_\sigma}\right) = 0\right\}.$$

Observe that $|\mathscr{H}| = \deg_Y G$. An element $\tau \in \mathrm{Gal}(L|K)$ is determined by its value at y; in particular, for each $\tau \in \mathrm{Gal}(L|K)$, there exists a $\tau \in \mathscr{H}$ satisfying $\tau(y) = (a_\sigma y_\sigma + b_\sigma)/(c_\sigma y_\sigma + d_\sigma)$. Let τ_σ denote the element of $\mathrm{Gal}(L|K)$ corresponding to $\sigma \in \mathscr{H}$. It is easy to see that the correspondence $\tau_\sigma \to \sigma$ of $\mathrm{Gal}(L|K)$ into $\mathscr{G}$ is a group homomorphism. Hence $\mathscr{H}$ is a subgroup of $\mathscr{G}$ canonically isomorphic to $\mathrm{Gal}(L|K)$. Let $Z_{\mathscr{H}} = U_{\mathscr{H}}/V_{\mathscr{H}}$ be a generator of $k(Y)^{\mathscr{H}}$ where $U_{\mathscr{H}}, V_{\mathscr{H}} \in k[Y]$ and $(U_{\mathscr{H}}, V_{\mathscr{H}}) = 1$. Write

$$\text{(A)} \qquad G(Y) = \prod_{\sigma \in \mathscr{H}} \left(Y - \frac{a_\sigma y_\sigma + b_\sigma}{c_\sigma y_\sigma + d_\sigma} \right).$$

Let $h = |\mathscr{H}|$ and expand the right side of equation (A) to obtain

$$\text{(B)} \qquad G(Y) = y^h + \sum_{i=1}^{h} \frac{A_i}{B_i} Y^{h-i}$$

where A_i, $B_i \in k[y]$ with $(A_i, B_i) = 1$. An easy calculation shows that $\deg_y A_i \leqq h$ and $\deg_y B_i \leqq h$. The action of $\mathscr{H}$ on $k(y)$ is induced by the action of $\mathscr{H}$ on $k(Y)$ and hence all of the coefficients of G lie in $k(y)^{\mathscr{H}}$. The degree constraint on A_i and B_i shows that $A_i/B_i = (a_i Z_{\mathscr{H}}(y) + b_i)/(c_i Z_{\mathscr{H}}(y) + d_i)$ for some $a_i, b_i, c_i, d_i \in k$. Since y is transcendental over k and $G(y) = 0$, at least one coefficient of G must satisfy $a_i d_i - b_i c_i \neq 0$. Write this coefficients as $(aZ_{\mathscr{H}} + b)/(cZ_{\mathscr{H}} + d)$. Since all coefficients of G lie in k we conclude that

$$\text{(C)} \qquad \frac{aZ_{\mathscr{H}} + b}{cZ_{\mathscr{H}} + d} = z_0 \in K - k.$$

Inverting equation (C), we obtain

$$Z_{\mathscr{H}} = \frac{dz_0 - b}{-cz_0 + a}.$$

Hence $L|K$ is a Lüroth covering defined by $L_{Z_{\mathscr{H}}}(\mathscr{H}, z') = U_{\mathscr{H}} - z'V_{\mathscr{H}}$ where $z' = (dz_0 - b)/(-cz_0 + a)$.

COROLLARY 1. *Any Lüroth polynomial $L_Z(\mathscr{G}, z)$ either splits completely over K or decomposes into the product of irreducible Lüroth polynomials associated with isomorphic subgroups of $\mathscr{G}$.*

COROLLARY 2. *If $M|K$ is a Lüroth extension and L is an intermediate field, then $M|L$ is a Lüroth extension.*

PROPOSITION 3. *Let $Z = U/V$ be a generator of $k(Y)^{\mathscr{G}}$ and suppose that $L_Z(\mathscr{G}, z) = U - zV$ is irreducible. Let $Z^* = U^*/V^*$ be another generator of $k(Y)^{\mathscr{G}}$ and write $Z^* = (aZ + b)/(cZ + d)$ with $a, b, c, d \in k$, $ad - bc \neq 0$. Then $L_{Z^*}(\mathscr{G}, (az + b)/(cz + d))$ is irreducible.*

PROOF. The proof is immediate from the observation that $L_{Z^*} = (ad - bc)/(cz + d)L_Z$.

3. The group PSL($\mathbf{F}_q$). Let p be an odd prime number and let $\mathbf{F}_q$ be the finite field containing $q = p^N$ elements for some $N \in \mathbf{Z}^+$. The projective special linear group, PSL($\mathbf{F}_q$), is the subgroup of all $\sigma \in$ PGL($\mathbf{F}_q$) satisfying $a_\sigma d_\sigma - b_\sigma c_\sigma \in (\mathbf{F}_q^\times)^2 = \{a^2 | a \in \mathbf{F}_q^\times\}$. Let k be an algebraically closed field with char $k = p$. Then k contains $\mathbf{F}_q$ and PSL($\mathbf{F}_q$) is a group of k-automorphisms of the rational function field $k(Y)$ if Y is an indeterminate over

k. The field of $\mathrm{PSL}(\mathbf{F}_q)$-invariants in $k(Y)$ is the rational function field $k(Z)$ where

$$Z = \frac{(Y^{(q-1)q} + Y^{(q-1)(q-1)} + Y^{(q-1)(q-2)} + \cdots + Y^{q-1} + 1)^{(q-1)/2}}{(Y^q - Y)^{(q^2-q)/2}}$$

4. $\mathrm{PSL}(\mathbf{F}_q)$-Lüroth coverings. Let k be an algebraically closed field with char $k = p > 2$, let $\mathscr{G} = \mathrm{PSL}(\mathbf{F}_q)$, and let K be an algebraic function field in one variable over k. Assume that the Lüroth polynomial

$$L_Z(\mathscr{G}, z)(Y) = (G(Y))^{(q+1)/2} - z(J(Y))^{(q^2-q)/2}$$

is irreducible over K where $z \in K - k$ and

$$G(Y) = Y^{(q-1)q} + \cdots + Y^{q-1} + 1 = \prod_{\alpha \in \mathbf{F}_{q^2} - \mathbf{F}_q} (Y - \alpha),$$
$$J(Y) = Y^q - y = \prod_{\beta \in \mathbf{F}_q} (Y - \beta).$$

Assume further that $p \nmid \mathrm{ord}_{\mathfrak{p}}^K z$ for any pole $\mathfrak{p}$ of z in K. Let $L = K(y)$ where $L_Z(\mathscr{G}, z)(y) = 0$. Then the extension $L|K$ is a $\mathrm{PSL}(\mathbf{F}_q)$-Lüroth covering and we have $\mathrm{Gal}(L|K) = \mathscr{G}$.

5. The different $\mathscr{D}_{L\backslash K}$. We will calculate the different $\mathscr{D}_{L|K}$ of the $\mathrm{PSL}(\mathbf{F}_q)$-Lüroth covering L of K. We shall employ the following notation:

$$\mathrm{div}_K^0(z) = \text{divisor of zeros of } z,$$
$$\mathrm{div}_K^\infty(z) = \text{divisor of poles of } z,$$
$$\mathrm{div}_K(z) = \frac{\mathrm{div}_K^0(z)}{\mathrm{div}_k^\infty(z)}.$$

Let $\mathfrak{p}$ be a place of K with places $\mathscr{P}$ and $\mathscr{P}'$ in L lying over $\mathfrak{p}$. Then, since $L|K$ is galois, the ramification indices $e_{\mathscr{P}}$ and $e_{\mathscr{P}'}$ satisfy $e_{\mathscr{P}} = e_{\mathscr{P}'}$; we denote this common index by $e_{\mathfrak{p}}$. Let $\mathscr{D}_{L|K}$ denote the different of the extension $L|K$. Then $\deg_L \mathscr{D}_{L|K}$ denotes its degree as a divisor. Recall that if $\mathrm{div}_K z = (\mathfrak{q}_1^{n_1} \cdots \mathfrak{q}_s^{n_s})/(\mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_r^{m_n})$, then

$$\sum_{i-1}^{r} m_i = \sum_{j=1}^{s} n_j = [K: k(z)].$$

PROPOSITION 4. *Assume that $\mathscr{P}$ is a place of L which is neither a zero nor pole of $y - \alpha$ for any $\alpha \in \mathbf{F}_{q^2}$. Then $\mathscr{P}$ is unramified in $L|K$.*

PROOF. It suffices to show that $\mathscr{P}$ is not a fixed point for any $\sigma \in \mathscr{G}\backslash\{\mathrm{id}\}$. Assume that $\sigma(\mathscr{P}) = \mathscr{P}$. We will show that $\sigma = \mathrm{id}$. By acsumption, $\mathscr{P}$ is neither a zero nor a pole of y, so $y(\mathscr{P}) \in k^x$ (where $y \equiv y(\mathscr{P}) \bmod \mathscr{P}$). Since $\sigma(\mathscr{P}) = \mathscr{P}$ we have $(a_\sigma y_\sigma + b_\sigma)/(c_\sigma y_\sigma + d_\sigma) \equiv y(\mathscr{P}) \bmod \mathscr{P}$. If $c_\sigma = 0$, then $a_\sigma y(\mathscr{P}) + b_\sigma = d_\sigma y(\mathscr{P})$, i.e., $\mathscr{P}$ is a zero of the function $y + b_\sigma/(a_\sigma - d_\sigma)$ if $a_\sigma - d_\sigma \neq 0$. We conclude that $a_\sigma - d_\sigma = b_\sigma = 0$ and hence $\sigma = \mathrm{id}$. If $c_\sigma \neq 0$, $\mathscr{P}$ is neither a zero nor a pole of $c_\sigma y(\mathscr{P}) + d_\sigma$. Therefore $a_\sigma y(\mathscr{P}) + b_\sigma = c_\sigma y^2(\mathscr{P}) + d_\sigma y(\mathscr{P})$, and we conclude that $y(\mathscr{P}) \in \mathbf{F}_{q^2}$. But this contradicts the assumption that $\mathscr{P}$ is not a zero of $y - \alpha$ for any $\alpha \in \mathbf{F}_{q^2}$. We conclude that $\sigma = \mathrm{id}$.

If $\mathscr{P}$ is a place of L and $\mathfrak{p}$ the place of K lying below $\mathscr{P}$, then the equation $L_Z(\mathscr{G}, z)(y) = 0$ implies

$$\text{(D)} \qquad \frac{q+1}{2}\operatorname{ord}^L_{\mathscr{P}} G(y) = e_\mathfrak{p} \operatorname{ord}^K_\mathfrak{p} z + \frac{q^2-q}{2}\operatorname{ord}^L_{\mathscr{P}} J(y).$$

Let $\mathfrak{p}$ be a zero of z in K. Since y is integral over $k[z]$, we have $\operatorname{ord}^L_{\mathscr{P}}(y) \geqq 0$, and hence $\operatorname{ord}^L_{\mathscr{P}} J(y) \geqq 0$. Therefore equation (D) implies the inequality

$$\text{(E)} \qquad \frac{q+1}{2}\operatorname{ord}^L_{\mathscr{P}} G(y) > \frac{(q-1)q}{2}\operatorname{ord}^L_{\mathscr{P}} J(y) \geqq 0.$$

Hence $\mathscr{P}$ is a zero of $G(y)$, and therefore $y(\mathscr{P}) \in \mathbf{F}_{q^2} - \mathbf{F}_q$. Conversely, if $\mathscr{P}$ is a zero of $G(y)$ in L, then $\operatorname{ord}^L_{\mathscr{P}} J(y) = 0$ since $(G(Y), J(Y)) = 1$. Equation (D) therefore implies

$$\text{(F)} \qquad \frac{q+1}{2}\operatorname{ord}^L_{\mathscr{P}} G(y) = e_\mathfrak{p} \operatorname{ord}^K_\mathfrak{p} z.$$

THEOREM 1. *Let $\mathscr{P}$ be a zero of z in L, $\mathfrak{p}$ the place of K lying below $\mathscr{P}$ and $d_\mathfrak{p} = ((q+1)/2, \operatorname{ord}^K_\mathfrak{p} z)$. Then $e_\mathfrak{p} = (q+1)/(2d_\mathfrak{p})$.*

PROOF. By equation (F) we have $((q+1)/(2d_\mathfrak{p})) | e_\mathfrak{p}$. To show that $e_\mathfrak{p} = (q+1)/(2d_\mathfrak{p})$, it suffices to show that

$$\text{(G)} \qquad |\mathscr{G}(\mathscr{P})| \leqq \frac{q+1}{2d_\mathfrak{p}},$$

where $\mathscr{G}(\mathscr{P}) = \{\sigma \in \mathscr{G} | \sigma(\mathscr{P}) = \mathscr{P}\}$ is the decomposition group of $\mathscr{P}$ over K. For if inequality (G) holds, then for $\operatorname{orb}_\mathscr{G}(\mathscr{P}) = \{\sigma(\mathscr{P}) | \sigma \in \mathscr{G}\}$ we have

$$\begin{aligned}\frac{q^3-q}{2} = |\mathscr{G}| &= |\operatorname{orb}_\mathscr{G}(\mathscr{P})|\,|\mathscr{G}(\mathscr{P})| \\ &\leqq |\operatorname{orb}_\mathscr{G}(\mathscr{P})| \frac{q+1}{2d_\mathfrak{p}} \\ &\geqq |\operatorname{orb}_\mathscr{G}(\mathscr{P})|\, e_\mathfrak{p} \\ &= \frac{q^3-q}{2},\end{aligned}$$

and hence equality must hold at every stage. We now prove inequality (G). If $\sigma \in \mathscr{G}$, then either $\sigma = \sigma_{b,c}$ or $\sigma = \sigma_{b,c}\sigma_a$, where $\sigma_{b,c}(Y) = bY + c$ and $\sigma_a = (aY+1)/(-Y)$ with $a, b, c \in \mathbf{F}_q$ and $b \in (\mathbf{F}_q^\times)^2$. The latter factorization of σ follows from the fact that the set $\{\phi \in \mathrm{PSL}(\mathbf{F}_q) | \phi = \mathrm{id}$ or

$\psi = \sigma_a (a \in \mathbf{F}_q)\}$ represents the right cosets of the group $\{\sigma_{b,c} | c \in \mathbf{F}_q, b \in (\mathbf{F}_q^\times)^2\}$ in $\mathscr{G}$. Let $\sigma \in \mathscr{G}(\mathscr{P})$ and set $\alpha = y(\mathscr{P})$. Then equation (F) shows that $\alpha \in \mathbf{F}_{q^2} - \mathbf{F}_q$. Since $y \equiv \alpha \bmod \mathscr{P}$ and $\sigma(\mathscr{P}) = \mathscr{P}$, we conclude that $\sigma(y) \equiv \alpha \bmod \mathscr{P}$. If $\sigma = \sigma_{b,c}$, we assert that $\sigma = \mathrm{id}$, for $y \equiv \sigma_{b,c}(y) \equiv \alpha \bmod \mathscr{P}$ implies that $b\alpha + c = \alpha$. Thus $(b - 1)\alpha + c = 0$. But, since b, $c \in \mathbf{F}_q$ and $\alpha \in \mathbf{F}_{q^2} - \mathbf{F}_q$, we conclude that $b = 1$ and $c = 0$. Now suppose that $\sigma = \sigma_{b,c}\sigma_a$. Then $y \equiv \sigma_{b,c}\sigma_a(y) \equiv \alpha \bmod \mathscr{P}$ and

$$\sigma_{b,c}\sigma_a(y) = \sigma_{b,c}\left(\frac{ay + 1}{-y}\right) = \frac{aby + ac + 1}{-(by + c)}.$$

We conclude

$$\text{(H)} \qquad \alpha^2 + (b^{-1}c + a)\alpha + b^{-1}(ac + 1) = 0.$$

Since, α is quadratic over $\mathbf{F}_q$, there is exactly one monic irreducible quadratic equation of which α is a root. Thus if we fix $a \in \mathbf{F}_q$ and let

$$\text{(I)} \qquad X^2 + AX + B = \mathrm{Irr}(\alpha, \mathbf{F}_q)(X),$$

then we have $b^{-1}c + a = A$ and $b^{-1}(ac + 1) = B$. So we consider the pair of equations

$$(A - a)b - c = 0,$$
$$Bb - ac = 1.$$

Taking b and c as unknowns, the determinant of the coefficients is $a^2 - Aa + B = \mathrm{Irr}(\alpha, \mathbf{F}_q)(-a) \neq 0$. Thus, given $a \in \mathbf{F}_q$, there is at most one $\sigma_{b,c}$ satisfying $\sigma_{b,c}\sigma_a(\mathscr{P}) = \mathscr{P}$. We note that $-A = \mathrm{Tr}\,\alpha$ and $b^{-1}c = -a - \mathrm{Tr}\,\alpha$ (where $\mathrm{Tr} = \mathrm{Tr}_{\mathbf{F}_{q^2}/\mathbf{F}_q}$). Easy computations establish that $\sigma_{b,c}(G(Y)) = G(Y)$ and $\sigma_a(G(Y)) = G(Y)/Y^{q^2-q}$. Let $t_{\mathfrak{p}} \in K$ be a local parameter at $\mathfrak{p}$ and set $n = \mathrm{ord}_{\mathfrak{p}}^K z$. Let

$$H(y) = \frac{(G(y))^{(q-1)/(2d_{\mathfrak{p}})}}{t_{\mathfrak{p}}^{(n)/d_{\mathfrak{p}}}}.$$

Then from the equation $L_Z(\mathscr{G}, z)\,(y) = 0$, we have

$$(H(y))^{d_{\mathfrak{p}}} = \frac{z}{t_{\mathfrak{p}}^n}(J(y))^{(q^2-q)/(2)}.$$

Since $((z)/t_{\mathfrak{p}}^n) \not\equiv 0 \bmod \mathscr{P}$ and the zeros of $G(y)$ and $J(y)$ are disjoint, we have $J(y) \not\equiv 0 \bmod \mathscr{P}$, and hence $H(y) \not\equiv 0 \bmod(\mathscr{P})$, i.e., $\beta = H(\alpha) \neq 0$. Thus $\sigma_{b,c}\sigma_a(\mathscr{P}) = \mathscr{P}$ implies $\sigma_{b,c}\sigma_a H(y) \equiv \beta \bmod \mathscr{P}$. Now we obtain

$$\text{(J)} \qquad \sigma_a H(y) = \frac{H(y)}{y^{(q^3-q)/(2d_{\mathfrak{p}})}},$$

and applying $\sigma_{b,c}$ to equation (J), we obtain

$$\text{(K)} \qquad \frac{H(y)}{(by + c)^{(q^3-q)/(2d_\mathfrak{p})}} \equiv \beta \bmod \mathscr{P}.$$

Since $y(\mathscr{P}) = \alpha$ and $b^{q-1} = 1$, equation (K) implies

$$(\alpha + b^{-1}c)^{(q^3-q)/(2d_\mathfrak{p})} = 1,$$

and hence

$$(\alpha - \operatorname{Tr} \alpha - a)^{(q^3-q)/(2d_\mathfrak{p})} = 1.$$

Therefore a is a root of the equation

$$(\alpha - \operatorname{Tr} \alpha - X)^{(q^3-q)/(2d_\mathfrak{p})} = 1.$$

LEMMA 1. *Fix $\gamma \in \mathbf{F}_{q^2} - \mathbf{F}_q$ and $d \in \mathbf{Z}^+$ with $d|(q+1)$. Then there are exactly $((q+1)/d) - 1$ roots of the polynomial $U^{(q-1)/d} - 1$ in the coset $\gamma + \mathbf{F}_q$.*

PROOF. Let ξ be a generator of $\mathbf{F}_q^\times$. Then the set $\{0\} \cup \{\xi^i\gamma | 0 \leqq i \leqq q-2\}$ represents $\mathbf{F}_{q^2}$ mod $\mathbf{F}_q$. If $\gamma + a$ is a root of $U^{(q^2-1)/d} - 1$ in $\gamma + \mathbf{F}_q$, then $\xi^i\gamma + \xi^i a$ is a root in $\xi^i + \mathbf{F}_q$. This correspondence is bijective, so the number of roots in each coset $\xi^i + \mathbf{F}_q$ (where $0 \leqq i \leqq q-2$) is the same. Now $\mathbf{F}_{q^2}^\times$ contains all roots of $U^{(q^2-1)/d} - 1$ and each element of $\mathbf{F}_q^\times$ is a root, so $\mathbf{F}_{q^2} - \mathbf{F}_q$ contains $(q^2-1)/d - (q-1) = (q-1)((q-1)/d) - 1$ roots. Thus each coset not equal to $\mathbf{F}_q$ contains $((q+1)/d) - 1$ roots.

It follows immediately from the lemma that there are at most $((q+1)/2d_\mathfrak{p}) - 1$ elements $a \in \mathbf{F}_q$ such that $\sigma_{b,c}\sigma_a(\mathscr{P}) = \mathscr{P}$ for some $\sigma_{b,c}$. Including $\sigma = \mathrm{id}$, we see that

$$|\mathscr{G}(\mathscr{P})| \leqq \frac{q+1}{2d_\mathfrak{p}},$$

and Theorem 1 is established.

COROLLARY 3. *Any zero $\mathfrak{p}$ of z in K is tamely ramified in L with decom position number $h_\mathfrak{p} = (q^2 - q)d_\mathfrak{p}$ and differential exponent $m_\mathfrak{p} = ((q+1)/2d_\mathfrak{p}) - 1$.*

We now consider the ramification propelties of the poles of z. Let $\mathscr{P}$ be a pole of z in L and $\mathfrak{p}$ the place of K lying below $\mathscr{P}$. From equation (D) we conclude that $\mathscr{P}$ is either a zero of $J(y)$ or a pole of y. If $\mathscr{P}$ is a zero of $J(y)$, then $\operatorname{ord}_\mathscr{P}^L G(y) = 0$ and we have

$$\text{(L)} \qquad \frac{q^2-q}{2} \operatorname{ord}_\mathscr{P}^L J(y) = -e_\mathfrak{p} \operatorname{ord}_\mathfrak{p}^K z;$$

if $\mathscr{P}$ is a pole of y, then

$$\text{(M)} \qquad \frac{q^2 - q}{2} \operatorname{ord}_{\mathscr{P}}^{L} y = e_{\mathfrak{p}} \operatorname{ord}_{\mathfrak{p}}^{K} z.$$

THEOREM 2. *Let $\mathscr{P}$ be a pole of z in L, $\mathfrak{p}$ the place of K lying below $\mathscr{P}$ and $d_{\mathfrak{p}} = ((q-1)/2, \operatorname{ord}_{\mathfrak{p}}^{K} z)$. Then $e_{\mathfrak{p}} = (q^2 - q)/2d_{\mathfrak{p}}$ and $h_{\mathfrak{p}} = (q+1)d_{\mathfrak{p}}$.*

PROOF. Since char $k = p \nmid \operatorname{ord}_{\mathfrak{p}}^{K} z$, equation (M) shows that $((q^2 - q)/2d_{\mathfrak{p}}) | e_{\mathfrak{p}}$. Let $\operatorname{orb}_{\mathscr{G}} \mathscr{P} = \{\sigma(\mathscr{P}) | \sigma \in \mathscr{G}\}$. To show that $e_{\mathfrak{p}} = (q^2 - q)/(2d_{\mathfrak{p}})$, it suffices to show that

$$\text{(N)} \qquad |\operatorname{orb}_{\mathscr{G}} \mathscr{P}| \geqq d_{\mathfrak{p}}(q+1).$$

For if equation (N) holds, then

$$\frac{q^3 - q}{2} = \frac{q^2 - q}{2d_{\mathfrak{p}}}(q+1)d_{\mathfrak{p}} \leqq e_{\mathfrak{p}} |\operatorname{orb}_{\mathscr{G}} \mathscr{P}| = \frac{q^3 - q}{2}$$

and hence equality holds throughout. Before proceeding we define $\tau_b = \sigma_{1,-b}$ and $\mu_a = \sigma_{a,0}$. Observe that $\sigma_{b,c} = \mu_b \tau_{-c}$. Easy computations show that $\tau_b J(Y) = J(Y)$ for all $b \in \mathbf{F}_q$, $\sigma_{b,c} J(Y) = bJ(Y)$ for all $\sigma_{b,c} \in \mathscr{G}$, $\sigma_a J(Y) = (J(Y))/Y^{q+1}$ for all $a \in \mathbf{F}_q$ and hence if $\sigma = \sigma_{b,c}\sigma_a$, then $\sigma J(Y) = (bJ(Y))/(bY + c)^{q+1}$. Now let $\mathscr{P}$ be a pole of z in L. If it is a pole of $J(y)$, then it is a pole of y. Thus $\sigma_0(\mathscr{P})$ is a zero of y and hence $\mathscr{P}$ is conjugate to a zero of y. Therefore we can assume without loss of generality that $y(\mathscr{P}) = 0$. This implies $G(y) \not\equiv 0 \bmod \mathscr{P}$, since $G(y) \equiv 1 \bmod \mathscr{Q}$ for any zero $\mathscr{Q}$ of $J(y)$. Let $\mathfrak{p}$ be the pole of z in K lying below $\mathscr{P}$ and let $t_{\mathfrak{p}} \in K$ be a local parameter at $\mathfrak{p}$. Set $n = \operatorname{ord}_{\mathfrak{p}}^{K} z$ and $d_{\mathfrak{p}} = ((q-1)/2, n)$. Let

$$F(y) = t^{(n)/d_{\mathfrak{p}}}(J(y))^{(q^2-q)/2d_{\mathfrak{p}}}.$$

Then

$$\text{(O)} \qquad (F(y))^{d_{\mathfrak{p}}} = \frac{t_{\mathfrak{p}}^{n}}{z} G(y))^{(q-1)/2}.$$

The right side of equation (O) is finite and $\not\equiv 0 \bmod \mathscr{P}$, i.e., $y = F(0) \neq 0$. We will need the following concept. If $(u, v) \in L \times L$ we write $(u, v)_{\mathscr{P}}$ whenever $u \equiv 0 \bmod \mathscr{P}$ and $v \equiv 0 \bmod \mathscr{P}$. We shall say that $(u, v)_{\mathscr{P}}$ is an admissible pair with respect to $\mathscr{P}$. If σ is a k-automorphism of L, then it is clear that $(u, v)_{\mathscr{P}}$ implies $(\sigma(u), \sigma(v))_{\sigma(\mathscr{P})}$; we shall write this implication as

$$(u, v)_{\mathscr{P}} \to (\sigma(u), \sigma(v))_{\sigma(\mathscr{P})}.$$

In general, if for a place $\mathscr{Q}$, the pair $(w, x)_{\mathscr{Q}}$ can be deduced from the pair $(u, v)_{\mathscr{P}}$, then we write $(u, v)_{\mathscr{P}} \to (w, x)_{\mathscr{Q}}$. Now consider the admissible pair $(y, F(y) - \gamma)_{\mathscr{P}}$. From this pair we obtain $d_{\mathfrak{p}}$ distinct pairs via the automorphism μ_a (where $a \in (\mathbf{F}^{x})^2$); namely,

$$(y, F(y) - \gamma)_{\mathscr{P}} \to (y, a^{(q^2-q)/2d_{\mathfrak{p}}}F(y) - \gamma)_{\mu_a(\mathscr{P})}.$$

Since

$$\operatorname{card}\{a^{(q^2-q)2d_{\mathfrak{p}}} | \, a \in (\mathbf{F}_q^x)^2\} = d_{\mathfrak{p}},$$

we see by comparing second coordinates in these pairs that $\operatorname{card}\{\mu_a(\mathscr{P}) | \, a \in (\mathbf{F}_q^x)^2\} = d_{\mathfrak{p}}$. Now to each of the pairs

$$(y, a^{(q^2-q)/2d_{\mathfrak{p}}}F(y) - \gamma)_{\mu_a(\mathscr{P})}$$

we apply τ_b, where $b \in \mathbf{F}_q$. Then we get

$$(y, a^{(q^2-q)/2d_{\mathfrak{p}}}F(y) - \gamma)_{\mu_a(\mathscr{P})} \to (y - b, a^{(q^2-q)/2d_{\mathfrak{p}}}F(y) - \gamma)_{\tau_b\mu_a(\mathscr{P})}.$$

We also obtain

$$(y, a^{(q^2-q)/2d_{\mathfrak{p}}}F(y) - \gamma)_{\mu_a(\mathscr{P})} \to \left(\frac{1}{y}, a^{(q^2-q)2d_{\mathfrak{p}}} \frac{F(y)}{y^{(q^3-q)/2d_{\mathfrak{p}}}} - \gamma\right)_{\sigma_0\mu_a(\mathscr{P})}.$$

By comparing first coordinates we see that each place $\mu_a(\mathscr{P})$ yields $q + 1$ distinct new places. We conclude that there are at least $d_{\mathfrak{p}}(q + 1)$ pairs, no two of which can belong to the same place. Therefore we have $|\operatorname{orb}_{\mathscr{G}}\mathscr{P}| \geqq d_{\mathfrak{p}}(q + 1)$, and Theorem 2 is established.

Since the poles of z are wildly ramified, the calculation of their differential exponents requires further consideration.

THEOREM 3. *Let $\mathscr{P}$ be a pole of z in L and $\mathfrak{p}$ the place of K lying below $\mathscr{P}$. Then the differential exponent of $\mathscr{P}$ over $\mathfrak{p}$ is*

$$m_{\mathfrak{p}} = \frac{q(q-1)}{2d_{\mathfrak{p}}} - \frac{q-1}{d_{\mathfrak{p}}} \operatorname{ord}_{\mathfrak{p}}^K z - 1.$$

PROOF. Since all conjugates of $\mathscr{P}$ have the same differential exponent, we can assume without loss of generality that $\mathscr{P}$ is chosen so that the pair $(y, F(y) - \gamma)_{\mathscr{P}}$ is admissible. Let $L_Z(\mathscr{P})$ be the decomposition field of $\mathscr{P}$. Then $[L: L_Z(\mathscr{P})] = |\mathscr{G}(\mathscr{P})| = e_{\mathfrak{p}}$. Let $\mathfrak{p} = L_Z(\mathscr{P}) \cap \mathscr{P}$. Then $\mathscr{P}$ is totally ramified over $L_Z(\mathscr{P})$, while $\mathfrak{p}$ is unamified over K. We will determine the elements of $\mathscr{G}(\mathscr{P})$ and apply Hilbert's formula for the computation of $m_{\mathfrak{p}}$. We saw in Theorem 2 that a necessary condition for $\sigma \in \mathscr{G}$ to be in $\mathscr{G}(\mathscr{P})$ is that

$$\text{(P)} \qquad (y, F(y) - \gamma)_{\mathscr{P}} \to (\sigma(y), \sigma F(y) - \gamma)_{\mathscr{P}}.$$

We know that no $\tau_b (b \in \mathbf{F}_q)$ can satisfy the implication in (P). And in Theorem 2 we saw that if $\mu_a(a \in (\mathbf{F}_q^x)^2)$ satisfies (P), then $a^{(q-1)/(2d_{\mathfrak{p}})} = 1$. If $\sigma = \mu_a\tau_b\sigma_0$, then $\sigma(y) = -1/(ay - b)$. Since $y \equiv 0 \bmod \mathscr{P}$ we have $\operatorname{ord}_{\mathscr{P}}^L\sigma(y) \leqq 0$. Hence $\sigma(\mathscr{P}) \neq \mathscr{P}$. Since the set $\{\mathrm{id}\} \cup \{\sigma_a | \, a \in \mathbf{F}_q\}$ represents the right cosets of the group $\{\sigma_{b,c} | c \in \mathbf{F}_q, b \in (\mathbf{F}_q^\times)^2\}$ in $\mathscr{G}$, so does the set $\{\sigma_0\} \cup \{\sigma_a\sigma_0 | a \in \mathbf{F}_q\}$. Now consider the elements of the form

$$\sigma = \mu_a \tau_b \sigma_c \sigma_0.$$

We have $\sigma(y) = (ay - b)/(acy - bc + 1)$. If $\sigma(\mathscr{P}) = \mathscr{P}$, then

$$\text{(Q)} \qquad \operatorname{ord}_{\mathscr{P}}^L \sigma(y) = \operatorname{ord}_{\mathscr{P}}^L y > 0.$$

If $bc = 1$, then $b \neq 0$ and we obtain

$$\begin{aligned} \operatorname{ord}_{\mathscr{P}}^L \sigma(y) &= \operatorname{ord}_{\mathscr{P}}^L(ay - b) - \operatorname{ord}_{\mathscr{P}}^L(acy - bc + 1) \\ &= -\operatorname{ord}_{\mathscr{P}}^L acy < 0, \text{ a contradiction.} \end{aligned}$$

We conclude that $bc \neq 1$, and hence $\operatorname{ord}_{\mathscr{P}}^L(acy - bc + 1) = 0$. So by equation (Q) we have $\operatorname{ord}_{\mathscr{P}}^L(ay - b) > 0$, and therefore $b = 0$. Thus $\mu_a\tau_b\sigma_c\sigma_0(\mathscr{P}) = \mathscr{P}$ implies that $b = 0$. Now suppose that $\mu_a\sigma_c\sigma_0(\mathscr{P}) = \mathscr{P}$. Given $c \in \mathbf{F}_q$ we want to determine the set $\{a \in (\mathbf{F}_q^\times)^2 \mid \mu_a\sigma_c\sigma_0 \in \mathscr{G}(\mathscr{P})\}$. If $\sigma = \mu_a\sigma_c\sigma_0$, then we obtain

$$\text{(R)} \qquad \sigma F(y) - \gamma = a^{(q^2-q)/2d_\mathfrak{p}} \frac{F(y)}{(acy + 1)^{(q^3-q)/2d_\mathfrak{p}}} - \gamma.$$

But $y(\mathscr{P}) = 0$, so $acy + 1 \equiv 1 \bmod \mathscr{P}$. Therefore, if $\sigma(\mathscr{P}) = \mathscr{P}$, then (P) and (R) imply that $a^{(q^2-q)/(2d_\mathfrak{p})} = 1$. We conclude that

$$\mathscr{G}(\mathscr{P}) \subset S = \{\sigma \in \mathscr{G} | \sigma = \mu_a\sigma_c\sigma_0, c \in \mathbf{F}_q, a \in (\mathbf{F}_q^\times)^2, a^{(q-1)/(2d_\mathfrak{p})} = 1\}.$$

The cardinality of S is $(q^2 - q)/(2d_\mathfrak{p}) = |\mathscr{G}(\mathscr{P})|$. Hence $\mathscr{G}(\mathscr{P}) = S$.

Let $t_\mathfrak{p} \in K$ be a local parameter at $\mathfrak{p}$. Since $\mathfrak{p}$ is unramified over K, $t_\mathfrak{p}$ is also a local parameter at $\mathfrak{p}$ in $L_Z(\mathscr{P})$. Since $y(\mathscr{P}) = 0$, equation (L) and Theorem 2 yield $\operatorname{ord}_{\mathscr{P}}^L y = -(\operatorname{ord}_\mathfrak{p}^K z)/d_\mathfrak{p}$. Therefore there are integers r and s satisfying $re_\mathfrak{p} + s \operatorname{ord}_\mathfrak{p}^K y = 1$; we may assume $s > 0$. Then the element $t = t_\mathfrak{p}^r y^s$ is a local parameter at $\mathscr{P}$. Furthermore the set $\{1, t, \ldots, t^{e_\mathfrak{p}-1}\}$ is an integral basis at $\mathscr{P}$ over $L_Z(\mathscr{P})$. Let $\mathscr{G}_\nu$ denote the νth ramification group at $\mathscr{P}$. We have $\mathscr{G}_1 = \mathscr{G}(\mathscr{P})$. Now we compute $\mathscr{G}_\nu$ for $\nu > 1$. If $\sigma = \mu_a$ where $a \in (\mathbf{F}_q^\times)^2$, $a^{(q-1)/(2d_\mathfrak{p})} = 1$ and $a \neq 1$, then

$$\begin{aligned} \sigma(t) - t &= t_\mathfrak{p}^r(a^s y^s - y^s) \\ &= (a^s - 1)t. \end{aligned}$$

But $(s, (q - 1)/(2d_\mathfrak{p})) = 1$, so $a^s - 1 \neq 0$. Therefore $\operatorname{ord}_{\mathscr{P}}^L(\sigma(t) - t) = 1$ and hence $\mu_a \notin \mathscr{G}_\nu$ for $\nu > 1$. If $\sigma = \mu_a\sigma_c\sigma_0$, where $c \in \mathbf{F}_q^\times$, $a \in (\mathbf{F}_q^\times)^2$, $a^{(q-1)/(2d_\mathfrak{p})} = 1$ and $a \neq 1$, then

$$\begin{aligned}\sigma(t) - t &= t_{\mathfrak{p}}^{r}\left(\left(\frac{cy}{y + a^{-1}c}\right)^{s} - y^{s}\right)\\ &= (y + a^{-1}c)^{-s} t_{\mathfrak{p}}^{r}(c^{s}y^{s} - (y + a^{-1}c)^{s}y^{s})\\ &= (y + a^{-1}c)^{-s} t_{\mathfrak{p}}^{r}[c^{s}(1 - a^{-s})y^{s} + \text{terms in } y \text{ of degree} > s].\end{aligned}$$

Again we have $a^{-s} - 1 \neq 0$ and $c^{s} \neq 0$. So $\sigma(t) - t = ut$ where u is a unit mod $\mathcal{P}$. Thus $\operatorname{ord}_{\mathcal{P}}^{L}(\sigma(t) - t) = 1$, so $\mu_a\sigma_c\sigma_0 \notin \mathcal{G}_\nu$ for $\nu > 1$.

If $\sigma = \sigma_c\sigma_0 (c \in \mathbf{F}_q^{\times})$, then

$$\begin{aligned}\sigma(t) - t &= t_{\mathfrak{p}}^{r}\left(\left(\frac{cy}{y + c}\right)^{s} - y^{s}\right)\\ &= (y + c)^{-s} t_{\mathfrak{p}}^{r}(c^{s}y^{s} - (y + c)^{s}y^{s})\\ &= -(y + c)^{-s}\left[y^{s} + c\binom{s}{1}y^{s-1} + \cdots + c^{s-1}\binom{s}{s-1}y\right]t_{\mathfrak{p}}^{r}y^{s}\\ &= -(y + c)^{-s}(y^{s-1} + csy^{s-2} + \cdots + c^{s-1}s)ty.\end{aligned}$$

Now $p \nmid s$ since $p \mid e_{\mathfrak{p}}$ and $(e_{\mathfrak{p}}, s) = 1$. Also $c \neq 0$, so the coefficient of ty is a unit mod $\mathcal{P}$. We conclude that

$$\operatorname{ord}_{\mathcal{P}}^{L}(\sigma(t) - t) = 1 + \operatorname{ord}_{\mathcal{P}}^{L} y = 1 - \frac{\operatorname{ord}_{\mathfrak{p}}^{K} z}{d_{\mathfrak{p}}}.$$

It follows from the above computationt that if $\nu > 1 - (\operatorname{ord}_{\mathfrak{p}}^{K} z)/d_{\mathfrak{p}}$, then $\mathcal{G}_\nu = \{\mathrm{id}\}$; if $\nu = 1$, $\mathcal{G}_1 = \mathcal{G}(\mathcal{P})$; and if $2 \leqq \nu \leqq 1 - (\operatorname{ord}_{\mathfrak{p}}^{K} z)/d_{\mathfrak{p}}$, then $\mathcal{G} = \{\sigma_c\sigma_0 \mid c \in \mathbf{F}_q\}$ and $|\mathcal{G}_\nu| = q$. The differential exponent $m_{\mathfrak{p}}$ of $\mathcal{P}$ over $\mathfrak{p}$ can now be calculated via Hilbert's formula as shown here.

$$\begin{aligned}m_{\mathfrak{p}} &= \sum_{\nu=1}^{\infty} (|\mathcal{G}_\nu| - 1)\\ &= \frac{q^{2} - q}{2d_{\mathfrak{p}}} - 1 - \frac{q - 1}{d_{\mathfrak{p}}} \operatorname{ord}_{\mathfrak{p}}^{K} z.\end{aligned}$$

The following corollary is immediate from Theorems 1, 2 and 3.

COROLLARY 4. *Let*

$$\operatorname{div}_K z = \frac{\mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_r^{m_r}}{\mathfrak{q}_1^{n_1} \cdots \mathfrak{q}_s^{n_s}},$$

where $m_i, n_j \in \mathbf{Z}^{+}$ *and* $(n_j, \text{char } k) = 1$. *Set* $d_{\mathfrak{p}_i} = ((q + 1/2, m_i)$ *and* $d_{\mathfrak{q}_j} = ((q - 1)/2, n_j)$. *Then*

$$\deg_L \mathcal{D}_{L/K} = (r + s)\frac{q^{3} - q}{2} - (q^{2} - q)\sum_{i=1}^{r} d_{\mathfrak{p}_i} - (q + 1)\sum_{j=1}^{s} d_{\mathfrak{q}_j} + (q^{2} - 1)[K: k(z)].$$

6. Genus zero and genus one coverings of k(x). Let x be an indeterminate over k and set $K = k(x)$. We will determine all genus zero and genus one $\mathrm{PSL}(\mathbf{F}_q)$-Lüroth coverings L of K. Assume that L is given by the irreducible Lüroth polynomial $L_Z(\mathcal{G}, z)(Y)$ where $z \in K - k$ satisfies

$$\operatorname{div}_K z = \frac{\mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_r^{m_r}}{\mathfrak{q}_1^{n_1} \cdots \mathfrak{q}_s^{n_s}}$$

$m_k, n_j \in \mathbf{Z}^+$ and $p \nmid n_j$.

THEOREM 4. *The genus* $\mathcal{G}_L = 0$ *if and only if* $\operatorname{div}_K z = \mathfrak{p}/\mathfrak{q}$, i.e., $z = (ax + b)/(cx + d)$ *for some* $a, b, c, d \in k$, $ad - bc \neq 0$.

PROOF. It is obvious that if $z = (ax + b)/(cx + d)$, then $\mathcal{G}_L = 0$. In order to establish the converse, we show that if $[k(x)\colon k(z)] \geqq 2$, then $\mathcal{G}_L \geqq 1$; so assume $[k(x)\colon k(z)] \geqq 2$. By Corollary 4 and the Riemann-Hurwitz formula we obtain

$$\text{(S)}\qquad \begin{aligned} 2\mathcal{G}_L - 2 = {} & (r + s - 2)\frac{q^3 - q}{2} + (q^2 - 1)[k(x)\colon k(z)] \\ & - (q^2 - q)\sum_{i=1}^{r} d_{\mathfrak{p}_i} - (q + 1)\sum_{j=1}^{s} d_{\mathfrak{q}_j} \end{aligned}$$

We have $d_{\mathfrak{p}_i} \leqq (q + 1)/2$, $d_{\mathfrak{q}_j} \leqq (q - 1)/2$ and $[k(x)\colon k(z)] \geqq s$. Therefore from equation (S) we obtain

$$\text{(T)}\qquad \begin{aligned} 2\mathcal{G}_L - 2 & \geqq (r+s-2)\frac{q^3-q}{2} + (q^2-1)[k(x)\colon k(z)] - r\frac{q^3-q}{2} - s\frac{q^2-1}{2} \\ & = \frac{q^2-1}{2}[(s - 2)q + 2[k(x)\colon k(z)] - s]. \end{aligned}$$

From inequality (T) we see that if $s \geqq 2$ or if $s = 1$ and $[k(x)\colon k(z)] \geqq q$, then $2\mathcal{G}_L - 2 > 0$, i.e., $\mathcal{G}_L > 1$. We consider the case $s = 1$ and $[k(x)\colon k(z)] < q$. From equation (S) we obtain

$$\text{(U)}\qquad \begin{aligned} 2\mathcal{G}_L - 2 & = (r-1)\frac{(q^3-q)}{2} + (q^2-1)[k(x)\colon k(z)] - (q^2-q)\sum_{i=1}^{r} d_{\mathfrak{p}_i} - (q+1)d_{\mathfrak{q}_1} \\ & \geqq (r-1)\frac{(q^3-q)}{2} + (q^2-1)[k(x)\colon k(z)] \\ & \quad - (q^2-q)[k(x)\colon k(z)] - (q+1)[k(x)\colon k(z)] \\ & = (r - 1)\frac{q^3 - q}{2} - 2[k(x)\colon k(z)] > (r - 1)\frac{q^3 - q}{2} - 2q. \end{aligned}$$

If $r \geqq 2$, then $(r - 1)((q^3 - q)/2) - 2q > 0$ since $q > 2$. Hence in this case $\mathcal{G}_L > 1$. To finish the proof of the theorem we consider the case $r = s = 1$ and $[k(x)\colon k(z)] < q$, i.e., $\operatorname{div}_K z = \mathfrak{p}^\mu/\mathfrak{q}^\mu$ where $\mu = [k(x)\colon k(z)]$ and $1 < \mu < q$. From equation (S) we obtain

(V) $$2\mathscr{G}_L - 2 = \mu(q^2 - 1) - (q^2 - q)\left(\frac{q+1}{2}, \mu\right) - (q+1)\left(\frac{q-1}{2}, \mu\right).$$

From equation (V) we see that $\mathscr{G}_L = 0$ only if

(W) $$-1 = \mu\frac{(q^2 - 1}{2} - \frac{q^2 - q}{2}\left(\frac{q+1}{2}, \mu\right) - \frac{q+1}{2}\left(\frac{q-1}{2}, \mu\right).$$

From equation (W) we conclude that $((q + 1)/2, \mu) = 1$. But then equation (V) implies

$$\begin{aligned} 2\mathscr{G}_L - 2 &= (q^2 - 1)\mu - (q^2 - q) - (q + 1)\left(\frac{q-1}{2}, \mu\right) \\ &\geqq (q^2 - 1)\mu - (q^2 - q) - (q + 1)\mu \\ &= (q^2 - q)(\mu - 1) - 2\mu. \end{aligned}$$

Hence $2\mathscr{G}_L \geqq (q^2 - q - 2)(\mu - 1) > 2$ since $q > 2$ and $\mu > 1$, a contradiction. Therefore $\mathscr{G}_L \geqq 1$.

A closer examination of the inequalities in the proof of Theorem 4 reveals that there is a unique family of PSL($\mathbf{F}_q$)-Lüroth coverings L of $k(x)$ with $\mathscr{G}_L = 1$; namely,

THEOREM 5. *The genus* $\mathscr{G}_L = 1$ *if and only if* $q = 3$ *and* $\operatorname{div}_K z = \mathfrak{p}^2/\mathfrak{q}^2$, i.e., $z = ((ax + b)/(cx + d))^2$ *where* $a, b, c, d\ k$ *and* $ad - bc \neq 0$.

7. Differentials of the first kind. In this section we will describe a k-basis for the space $\Omega(L)$ of differentials of the first kind of a particular type of PSL($\mathbf{F}_q$)-Lüroth covering L of $K(x)$. Let $L|K$ be a PSL($\mathbf{F}_q$)-Lüroth covering of $K = k(x)$ and assume that $\operatorname{div}_K z = (\mathfrak{p}_1 \cdots \mathfrak{p}_m)/\mathfrak{p}_\infty^m \quad (\mathfrak{p}_i \neq \mathfrak{p}_j$ if $i \neq j)$ with $(m, (q^2 - q)/2) = 1$ and $m > (q^2 - q)/2$. We have

$$\mathscr{D}_{L|K} = (\mathscr{P}_0\mathscr{P}_1 \cdots \mathscr{P}_q)^{m_{\mathfrak{p}_\infty}} \prod_{i=1}^{m} (\mathscr{P}_{i,1} \cdots \mathscr{P}_{i,q^2-q})^{q-1/2}$$

where $m_{\mathfrak{p}_\infty} = ((q^2 - q)/2) - 1 + m(q - 1)$, the $\mathscr{P}_r$ are the places of L lying over $\mathfrak{p}_\infty$ and the $\mathscr{P}_{i,j}$ are the places of L lying over $\mathfrak{p}_i$. Define integers s_μ and r_μ for $1 \leqq \mu \leqq (m - 1)$ by

(X) $$\mu\left(m - \frac{q^2 - q}{2}\right) = s_\mu m + r_\mu$$

where $1 \leqq r_\mu \leqq m$ (note that $r_\mu > 0$). If $\nu \in \mathbf{Z}$ satisfies $0 \leqq \nu \leqq (q + 1)\mu - (q + 1)s_\mu - 2$, then for each μ, $1 \leqq \mu \leqq (m - 1)$, set

$$\phi(\mu, \nu) = (q + 1)\mu - (q + 1)s_\mu - \nu - 2.$$

Then we have $\phi(\mu, \nu) \geqq 0$. The following theorem is easily established by calculating the orders of the differentials.

THEOREM 6. *For each pair of integers* (μ, ν) *define the differential*

$$\omega_{\mu,\nu} = x^{m-\mu-1}h^{\phi(\mu,\nu)} \frac{(J(y))^{t_\mu}}{(G(y))^{q-1/2}}\, dx$$

where $t_\mu = (1/2)(q^2 - 3q + 4 - 2s_\mu - 2\mu)$. *Then the set*

$$\{\omega_{\mu,\nu} \mid 1 \leqq \mu \leqq (m-1),\ 0 \leqq \nu \leqq (q+1)\mu - (q+1)s_\mu - 2\}$$

is a k-basis of $\Omega(L)$.

Note that using Theorem 6 we can show that m is a gap for infinitely many places of L, but that m is a non-gap for each $\mathscr{P}_r$, $0 \leqq r \leqq q$. Hence each $\mathscr{P}_r$ is a Weierstrass point.

REFERENCES

1. C. Chevalley, *Introduction to the theory of Algebraic Functions of One Variable*, Amer. Math. Soc., New York, 1951.
2. H. Boseck, *Zur Theorie der Weierstrasspunkte*, Math. Nachr. **19** (1958), 29–63.
3. H. Hasse, *Theorie der relativ-zyklishen algebraischen Funcktionenkörper*, *J.* reine angew. Math. **172** (1935), 37–54.
4. F.K. Schmidt, *Zur arithmetischen Theorie der algebraischen Funcktionen.* II. *Allgemeine Theorie der Weierstrasspunkte*, Math. Zeit. **45** (1933), 75–96.
5. B.L. van der Waerden, *Modern Algebra, Vol.* I, Ungar, New York, 1964.
6. H. Weber, *Lehrbuch der Algebra, Vol.* II, reprinted from second edition (1908), Chelsea, New York.

CALIFORNIA STATE UNIVERSITY, LONG BEACH