THE GENUS OF SUBFIELDS OF $K(p^n)$

BY
JOSEPH B. DENNIN, JR.

1. Introduction

Let Γ be the group of linear fractional transformations

$$w \to (aw + b)/(cw + d)$$

of the upper half plane into itself with integer coefficients and determinant 1. Γ is isomorphic to the 2×2 modular group; i.e., the group of 2×2 matrices with integer entries and determinant 1 in which a matrix is identified with its negative. Let $\Gamma(n)$, the principal congruence subgroup of level n, be the subgroup of Γ consisting of those elements for which $a \equiv d \equiv 1 \pmod{n}$ and $b \equiv c \equiv 0 \pmod{n}$. G is called a congruence subgroup of level n if G contains $\Gamma(n)$ and n is the smallest such integer. G has a fundamental domain in the upper half plane which can be compactified to a Riemann surface and then the genus of G can be defined to be the genus of the Riemann surface. H. Rademacher has conjectured that the number of congruence subgroups of genus 0 is finite. D. McQuillan [7] has shown that the conjecture is true if n is relatively prime to $2 \cdot 3 \cdot 5$ and J. Dennin [1, 2] has shown that the conjecture is true if $n = 2^m$, 3^m or 5^m. In this paper we show that the number of subgroups of prime power level of genus g is finite for any g. We may assume $g \neq 0$ since the case $g = 0$ is done.

2. Preliminary results and definitions

Consider $M_{\Gamma(n)}$, the Riemann surface associated with $\Gamma(n)$. The field of meromorphic functions on $M_{\Gamma(n)}$ is called the field of modular functions of level n and is denoted by $K(n)$. If j is the absolute Weierstrass invariant, $K(n)$ is a finite Galois extension of $C(j)$ with $\Gamma/\Gamma(n)$ for Galois group. Let $SL(2, n)$ be the special linear group of degree two with coefficients in Z/nZ and let $LF(2, n) = SL(2, n)/\pm I$. Then $\Gamma/\Gamma(n)$ is isomorphic to $LF(2, n)$. If $\Gamma(n) \subset G \subset \Gamma$ and H is the corresponding subgroup of $LF(2, n)$, then by Galois theory H corresponds to a subfield F of $K(n)$ and the genus of F equals the genus of G.

The following notation will be standard. A matrix

$$\pm \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

will be written $\pm(a, b, c, d)$.

$$T = \pm(0, -1, 1, 0); \quad S = \pm(1, 1, 0, 1); \quad R = \pm(0, -1, 1, 1).$$

Received August 1, 1972.

T and S generate $LF(2, n)$ and $R = TS$. F will be a subfield of $K(n)$ containing $C(j)$ and H the corresponding subgroup of $LF(2, n)$. $g(H) =$ the genus of H and h or $|H| =$ the order of H. $[A]$ or $[\pm(a, b, c, d)]$ will denote the group generated by A or $\pm(a, b, c, d)$ respectively.

We now concentrate on $LF(2, p^n)$, $p > 2$, whose order is $p^{3n-2}(p^2 - 1)/2$. The case $p = 2$ will be considered in the last section. McQuillan [7] obtained the following formula for the genus of H.

Let r, t and $s(p^r)$ be the number of distinct cyclic subgroups of H generated by a conjugate in $LF(2, p^n)$ of R, T and S^{p^r} respectively where $1 \leq p^r < p^n$. Then

$$(2.1)\quad \begin{aligned} g(H) = 1 + p^{2n-2}(p^2 - 1)(p^n - 6)/24h - p^{n-1}(p - \\ (-3/p))\ r/3h - p^{n-1}(p - (-1/p))t/4h - p^{2n-2}(p - 1)^2W/4h \end{aligned}$$

where $W = \sum s(p^r)$. One immediate consequence of this is that if two groups are conjugate, they have the same genus.

We now collect some basic facts about subgroups of $LF(2, p^n)$ and conjugates of S^{p^r}, R and T which we will use later. First we have three propositions which are found in Gierster [4]. Let f_r^n be the natural homomorphism from $LF(2, p^n)$ to $LF(2, p^r)$, $0 < r < n$, given by reducing an element mod p^r. The kernel of this homomorphism is denoted by K_r^n and has order $p^{3(n-r)}$.

PROPOSITION 2.1. *If $H \cap K_{n-1}^n$ is the identity, $H \cap K_r^n$ is the identity for $r = 1, \cdots, n - 2$.*

PROPOSITION 2.2. *If $|H \cap K_{n-1}^n| = p$, then $H \cap K_1^n$ is cyclic and*

$$|H \cap K_1^n| \leq p^{n-1}.$$

PROPOSITION 2.3. *If $|H \cap K_{n-1}^n| = p^2$, then $H \cap K_1^n$ is generated by two transformations U_1 and U_2 of order p^{n-r} and p^{n-s} respectively and*

$$|H \cap K_1^n| = p^{2n-r-s} \leq p^{2n-2}.$$

In Proposition 2.2, $H \cap K_1^n = [U]$ where

$$U = \pm(u + p^r\mu, p^r\nu, p^r\rho, u - p^r\mu)$$

with not all of $\mu, \nu, \rho \equiv 0 \pmod p$ and $u^2 + p^{2r}(\mu^2 + \nu\rho) \equiv 1 \pmod{p^n}$. Following Gierster, we make the selection of u unique by choosing $u \equiv 1 \pmod p$ and we write $U = \phi(\mu, \nu, \rho)_r$. The order of U is then p^{n-r} and

$$[U] = \{U^i = \phi(\mu\xi_i, \nu\xi_i, \rho\xi_i)\}$$

where u_i and ξ_i are given inductively by the formulas

$$(2.2)\qquad u_i \equiv u_{i-1}u + \xi_{i-1}(u^2 - 1), \quad \xi_i \equiv \xi_{i-1}u + u_{i-1} \qquad \pmod{p^n}$$

where $u_1 = u$ and $\xi_1 = 1$ [2]. From Proposition 2.3, let

$$U_1 = \phi(\mu, \nu, \rho)_r \quad \text{and} \quad U_2 = \phi(\mu', \nu', \rho')_s.$$

Then $[U_1] \cap [U_2] = \{I\}$ and

$$\begin{aligned} H \cap K_1^n &= \{U_1^i U_2^j\} \\ &= \{\pm(u_i u_j' + p^r \xi_i \mu u_j' + p^s \xi_j \mu' u_i + p^{r+s} \xi_i \xi_j (\mu\mu' + \nu\rho'), \\ &\quad \rho^s \xi_j \nu' u_i + p^r \xi_i \nu u_j' + p^{r+s} \xi_i \xi_j (\mu\nu' - \mu'\nu), \\ &\quad p^r \xi_i \rho u_j' + p^s \xi_j \rho' u_i + p^{r+s} \xi_i \xi_j (\rho\mu' - \rho'\mu), \\ &\quad u_i u_j' - p^r \xi_i \mu u_j' - p^s \xi_j \mu' u_i + p^{r+s} \xi_i \xi_j (\mu\mu' + \nu'\rho))\} \end{aligned}$$

where $1 \leq \xi_i \leq p^{n-r}$ and $1 \leq \xi_j \leq p^{n-s}$. The power of p dividing ξ_i and ξ_j determines to which K_l^n U_1^i and U_2^j belong.

We use the groups K_r^n to define the concept of level for H. H is of level r if H contains K_r^n and does not contain K_{r-1}^n. Similarly we say a subfield F of $K(p^n)$ is of level r if F is a subfield of $K(p^r)$ and not a subfield of $K(p^{r-1})$. Note that F is of level r if and only if its Galois group is of level r. Similarly we will use the phrase "at the r-th level" to mean in $K_{n-r}^n - K_{n-(r-1)}^n$.

A conjugate of S^{p^r} has the form $\pm(1 - p^r ac, p^r a^2, -p^r c^2, 1 + p^r ac)$. The following proposition simplifies the task of counting groups conjugate to $[S^{p^r}]$ [1].

PROPOSITION 2.4. *Any group A conjugate to $[S^{p^r}]$, where*

$$\pm(1 - p^r ac, p^r a^2, -p^r c^2, 1 + p^r ac)$$

is an element of A and $(a, p^n) = 1$, contains one and only one element of the form $\pm(x, p^r, y, z)$ and it is conjugate to S^{p^r}.

So under the proper conditions, to calculate $s(p^r)$ for H, it is sufficient to count the number of elements of the form $\pm(1 - p^r c, p^r, -p^r c^2, 1 + p^r c)$ in H. Unless otherwise indicated, the phrase "a conjugate of S^{p^r}" will mean one in this form. If $U = \pm(1 - p^{r-1}c, p^{r-1}, -p^{r-1}c^2, 1 + p^{r-1}c)$ is a conjugate of $S^{p^{r-1}}$ and V is a conjugate of $S^{p^{r-1}}$ such that $U^p = V^p$, then

$$V = \pm(1 - p^{r-1}(c + xp^{n-r}), p^{r-1}, -p^{r-1}(c^2 + 2cxp^{n-r}), 1 + p^{r-1}(c + xp^{n-r}))$$

where $0 \leq x < p$.

The following proposition simplifies the calculation of the number of conjugates of T and R in H.

PROPOSITION 2.5. *Let H be a subgroup of $LF(2, p^n)$ and $\bar{H}$ be its image in $LF(2, p)$. If $\bar{T}$ (respectively $\bar{R}$) in $\bar{H}$ has k pre-images in H conjugate to $T(R)$, then each conjugate of $\bar{T}(\bar{R})$ in $\bar{H}$ has 0 or k pre-images conjugate to $T(R)$ in H.*

Proof. Suppose $\bar{T}$ in $\bar{H}$ has $U_1 T U_1^{-1} = T$, $U_2 T U_2^{-1}, \cdots, U_k T U_k^{-1}$ as its pre-images in H conjugate to T. Suppose $\bar{T}_1$ is conjugate to $\bar{T}$ in $\bar{H}$ and that $\bar{T}_1$ has at least one pre-image conjugate to T so that we may assume T_1 is conjugate to T. Then there is a B in $LF(2, p^n)$ such that $BTB^{-1} = T_1$ in H

and so $\bar{B}\bar{T}\bar{B}^{-1} = \bar{T}_1$ in $\bar{H}$. Then, for $i = 1, \cdots, k$,

$$(B(U_i T U_i^{-1})B^{-1})^- = \bar{T}_1$$

so that $\bar{T}_1$ has at least k pre-images conjugate to T in H. Suppose

$$(UTU^{-1})^- = \bar{T}_1 \quad \text{and} \quad UTU^{-1} \neq B(U_i TU_i^{-1})B^{-1} \text{ for any } i = 1, \cdots, k.$$

Then $B^{-1}(UTU^{-1})B \neq U_i TU_i^{-1}$ for any i and yet $(B^{-1}(UTU^{-1})B)^- = \bar{T}$ in $\bar{H}$ which is a contradiction. Therefore $\bar{T}_1$ has at most k pre-images in H conjugate to T. A similar argument works for R and $\bar{R}$.

By conjugating H, we may assume that T is an element of H. By Proposition 2.5, it is sufficient to count the number of elements in H conjugate to T which are in $(H \cap K_1^n) \cdot T$. By Gierster [4], for $p > 2$, T_1 in $LF(2, p^n)$ is conjugate to T if and only if the trace of T_1 is congruent to 0 mod p^n. Let $U = \phi(\mu, \nu, \rho)_r$. Then

$$U \cdot T = \pm(p^r\nu, -u - p^r\mu, u - p^r\mu, -p^r\rho)$$

which has trace 0 if and only if $p^r(\nu - \rho) \equiv 0 \pmod{p^n}$ if and only if $\nu \equiv \rho \pmod{p^{n-r}}$ where $1 \leq \nu, \rho \leq p^{n-r}$.

DEFINITION 2.1. $U = \phi(\mu, \nu, \rho)_r$ has property A if and only if $\nu \equiv \rho \pmod{p^{n-r}}$.

We will want to calculate the number of elements in H with property A.

Similarly, by conjugating H, we may assume that R is an element of H and again by Proposition 2.5, it is sufficient to count the number of elements in H conjugate to R which are in $(H \cap K_1^n) \cdot R$. By Gierster [4], for $p > 3$, R_1 in $LF(2, p^n)$ is conjugate to R if and only if the trace of R_1 is congruent to ± 1 mod p^n.

$$U \cdot R = \pm(p^r\nu, \quad -u - p^r\mu + p^r\nu, \quad u - p^r\mu, \quad u - p^r\mu - p^r\rho)$$

which has trace congruent to $u + p^r(\nu - \mu - \rho)$ mod p^n.

DEFINITION 2.2. $U = \phi(\mu, \nu, \rho)_r$ has property B if and only if

$$u + p^r(\nu - \mu - \rho) \equiv 1 \pmod{p^n}.$$

It it sufficient to count the U with property B in H since the previous assumption that $u \equiv 1 \pmod p$ implies that p divides $1 - u$. But if

$$u + p^r(\nu - \mu - \rho) \equiv -1 \pmod{p^n},$$

then p divides $-(1 + u)$ so that p divides $(1 - u) + (1 + u) = 2$, a contradiction. Here we have used the $+$ sign in front of the matrix; using the $-$ sign would have given all the relevant matrices trace -1.

First we are going to show that it is enough to consider $LF(2, p^n)$ for a fixed p. In doing this and later in applying Proposition 1.5, it is necessary to have a list of subgroups of $LF(2, p)$. The possibilities are [3, 7]:

(1) a cyclic group C_m of order m where $m = p$, m divides $(p-1)/2$ or $(p+1)/2$;
(2) a dihedral group D_{2n} of order $2n$ where n divides $p-1$ or $p+1$;
(3) a metacyclic group M_{pu} of order pu where u divides $(p-1)/2$;
(4) a tetrahedral group $\mathfrak{T}$ for each p, an octahedral group $\mathfrak{O}$ if $p \equiv \pm 1 \pmod 8$ or an icosahedral group $\mathfrak{J}$ if $p \equiv \pm 1 \pmod 5$.

PROPOSITION 2.6. *Fix $g > 0$. There exists a p_0 such that if $p \geq p_0$, then $K(p)$ has no subfields of genus g.*

Proof. D. McQuillan has formulas for the genus of subgroups of $LF(2, p)$, $p > 5$ [7]. Using them we see that

(1) $g(I) = 1 + (p-6)(p^2-1)/24$,
(2) $g(\mathfrak{T}) \geq 1 + (p^3 - 6p^2 - p + 6)/288 - (p+1)/9 - (p+1)/16$,
(3) $g(\mathfrak{O}) \geq 1 + (p^3 - 6p^2 - p + 6)/576 - (p+1)/18 - 3(p+1)/32$,
(4) $g(C_p) = (p^2 - 12p + 35)/24$,
(5) $g(C_m) \geq 1 + (p+\epsilon)((p-6)(p-\epsilon)/12 - 7/6)/2m$,
(6) $g(D_{2n}) \geq 1 + (p+\epsilon)((p-6)(p-\epsilon)/48 - 1/6 - (p+1)/4)/n$,
(7) $g(M_{pu}) \geq 1 + (p-11)/12 - 7/6$,
(8) $g(\mathfrak{J}) \geq 1 + (p^3 - 6p^2 - p + 6)/1440 - (p+1)/18 - (p+1)/16$,

where $\epsilon = \pm 1$. So $\lim_{p\to\infty} g(H) = \infty$ where H is a proper subgroup of $LF(2, p)$. Further $g(LF(2, p)) = 0$. So for p sufficiently large, $LF(2, p)$ contains no subgroups of genus g and hence $K(p)$ has no subfields of genus g.

To show that the same result is true for $K(p^n)$, $n \geq 2$, we need the following fact.

LEMMA 2.7. *If F is a subfield of L, then $g(F) \leq g(L)$.*

Proof. By the relative genus formula,

$$2\,g(L) - 2 = (2\,g(F) - 2)[L:F] + d(D_{L/F})$$

where $d(D_{L/F})$ is the degree of the discriminant of L over F. But $[L:F] \geq 1$ and $d(D_{L/F}) \geq 0$ so that $2\,g(L) - 2 \geq 2\,g(F) - 2$ which implies that $g(L) \geq g(F)$.

THEOREM 1. *Fix $g > 0$. There exists a p_0 such that if $p \geq p_0$, then $K(p^n)$ has no subfields of genus g.*

Proof. We proceed by induction on n. By Proposition 2.6, there is a p_0 such that if $p \geq p_0$, $K(p)$ has no subfields of genus less than or equal to g except for $C(j)$ which has genus 0. Suppose F is a subfield of $K(p^n)$ of genus g. Then by Lemma 2.7, $F_1 = F \cap K(p^{n-1})$ which is a subfield of F has genus $g_1 \leq g$. By the induction hypothesis, $K(p^{n-1})$ has no subfield of genus less than or equal to g except $C(j)$ so that $F_1 = C(j)$. Let $H = G(K(p^n)/F)$.

Then $H \pmod{p^{n-1}} = G(K(p^{n-1})/F_1) = LF(2, p^{n-1})$ since $F_1 = C(j)$. So H contains K_{m-1}^m [7] implying that $F \subseteq K(p^{n-1})$. So by induction, $F = C(j)$ and $g(F) = 0 \neq g$, a contradiction.

3. $LF(2, p^n), p > 3$

By Theorem 1, we may assume that p is a fixed prime and we continue to assume that $p > 2$. Fix $g > 0$. We will show that

$$\{F \mid F \subseteq K(p^n) \text{ for some } n, g(F) = g\}$$

is finite by showing that there is an r_0 such that for $r \geq r_0$ there are no fields of level r and genus g in $K(p^n)$, $n > r$. So we must show that any subfield of $K(p^n)$ of genus g is already a subfield of $K(p^{r_0})$. Therefore it is enough to assume that F is a subfield of $K(p^n)$ and is not a subfield of $K(p^{n-1})$ and show that $g(F) > g$. In terms of the associated subgroup H of $LF(2, p^n)$, this means there are three cases to consider:

$$(1)\ H \cap K_{n-1}^n = \{I\}, \quad (2)\ |H \cap K_{n-1}^n| = p, \quad (3)\ |H \cap K_{n-1}^n| = p^2$$

since if $|H \cap K_{n-1}^n| = p^3$, then $K_{n-1}^n \subseteq H$ and so $F \subseteq K(p^{n-1})$.

The first case is easy and is done in the following proposition.

PROPOSITION 3.1. *There exists an n_1 such that if $n \geq n_1$ and $H \cap K_{n-1}^n = \{I\}$, then $g(H) > g$.*

Proof. Suppose $H \cap K_{n-1}^n = \{I\}$. By Proposition 2.1, $H \cap K_1^n = \{I\}$. Then $t \leq 15$, $r \leq 10$ and $h \leq (p^2 - 1)/2 \leq p^2$. To see this, apply f_1^n, whose kernel is K_1^n, to H and then count the appropriate elements in the image of H in $LF(2, p)$. Further $W = 0$ since any conjugate of a power of S raised to some power is in K_1^n. Therefore, by formula (2.1),

$$\begin{aligned} g(H) &\geq 1 + \{p^{3n-2}(p^2 - 1) - (6p^{2n-2} + 80p^{n-1}(p + 1) \\ &\qquad + 90p^{n-1}(p + 1))\}/24p^2 \\ &= 1 + f(n) \end{aligned}$$

where $\lim_{n\to\infty} f(n) = \infty$. So there is an n_1 such that for $n \geq n_1$, $g(H) > g$.

For the second case we use the bounds on r, t and W given in the following lemma.

LEMMA 3.2. *Suppose $|H \cap K_{n-1}^n| = p$. Then $W \leq n$, $t \leq 15p^{n+1}$ and $r \leq 20p^n$.*

Proof. Since $|H \cap K_{n-1}^n| = p$, by Proposition 2.2, $H \cap K_1^n$ is cyclic with $|H \cap K_1^n| \leq p^{n-1}$. If $W \neq 0$, conjugate H so that $S^{p^{n-1}}$ is in H. Then $W \leq n - 1 + s(1)$. Suppose U and V are conjugates of S such that $U^p = V^p$. Then

$$U = \pm(1 - c, 1, -c^2, 1 + c)$$

and

$$V = \pm(1 - (c + xp^{n-1}), 1, -(c^2 + 2cxp^{n-1}), 1 + (c + xp^{n-1}))$$

where $1 \leq x < p$ and p divides c since $U^{p^{n-1}} = S^{p^{n-1}}$. Then

$$U^{-1}V = \pm(1 - xp^{n-1}, -xp^{n-1}, 0, 1 + xp^{n-1})$$

is in $H \cap K_{n-1}^n$. But $H \cap K_{n-1}^n = \{\pm(1, yp^{n-1}, 0, 1) \mid 0 \leq y \leq p^{n-1}\}$. So $s(1) \leq 1$ and $W \leq n$. To calculate t and r we use Proposition 2.5. From McQuillan [7], we see that in $LF(2, p)$ $t \leq 15(p + 2)$ and $r \leq 20p$. Since $|H \cap K_1^n| \leq p^{n-1}$,

$$t \leq 15(p + 2)p^{n-1} \leq 15p^{n+1} \quad \text{and} \quad r \leq 20p^n.$$

PROPOSITION 3.3. *There exists an n_2 such that if $n \geq n_2$ and $|H \cap K_{n-1}^n| = p$, then $g(H) > g$.*

Proof. By Lemma 3.2, $W \leq n$, $t \leq 15p^{n+1}$ and $r \leq 20p^n$. Since

$$|LF(2, p)| = p(p^2 - 1)/2 \leq p^3 \quad \text{and} \quad |H \cap K_1^n| \leq p^{n-1},$$

$h \leq p^{n+2}$. So by formula (2.1),

$$\begin{aligned} g(H) \geq 1 + \{&p^{3n-2}(p^2 - 1) - (6(p^2 - 1)p^{2n-2} + 160p^{2n-1}(p + 1) \\ &+ 90p^{2n}(p + 1) + 6np^{2n-2}(p - 1)^2)\}/24p^{n+2} \\ = 1 + &f(n) \end{aligned}$$

where $f(n) = p^{n-4}(ap^n - bn - c)$ with $a > 0$, b and c constants. But $\lim_{n\to\infty} f(n) = \infty$ so that there is an n_2 such that for $n \geq n_2$, $g(H) > g$.

In the case $|H \cap K_{n-1}^n| = p^2$, we will use the following notation from Gierster [4]. Let $U = \phi(\mu, \nu, \rho)$ and set $\pi = \mu^2 + \nu\rho$. Then K_{n-1}^n contains 3 different conjugacy classes of groups of order p:

(1) $(p + 1)G_p(I)$ determined by $\pi \equiv 0 \pmod p$, e.g. $[\pm(1, p^{n-1}, 0, 1)]$,
(2) $p(p + 1)/2\ G_p(II)$ determined by $(\pi/p) = 1$, e.g. $[\pm(1 + p^{n-1}, 0, 0, 1 - p^{n-1})]$,
(3) $p(p - 1)/2\ G_p(III)$ determined by $(\pi/p) = -1$, e.g. $[\pm(1, p^{n-1}\nu, p^{n-1}, 1)]$ where $(\nu/p) = -1$.

Similarly the subgroups of order p^2 in K_{n-1}^n divide into 3 conjugacy classes:

(1) $(p + 1)G_{p^2}\ (I)$ containing $1G_p$ (I) and $pG_p\ (II)$,
(2) $p(p + 1)/2\ G_{p^2}\ (II)$ containing $2\ G_p\ (I)$, $(p - 1)/2\ G_p\ (II)$ and $(p - 1)/2\ G_p\ (III)$,
(3) $p(p - 1)/2\ G_{p^2}\ (III)$ containing $(p + 1)/2\ G_p\ (II)$ and $(p + 1)/2\ G_p\ (III)$.

We now give a series of propositions which give bounds on W, t and r in the case $|H \cap K_{n-1}^n| = p^2$.

PROPOSITION 3.4. *Suppose $H \cap K^n_{n-1}$ is conjugate to G_{p^2} (II). Then*

$$W \leq 2(n + p - 1).$$

Proof. By conjugating H, we can assume the G_{p^2} (II) is generated by $S^{p^{n-1}} = \pm(1, p^{n-1}, 0, 1)$ and $S_1 = \pm(1 - p^{n-1}, p^{n-1}, -p^{n-1}, 1 + p^{n-1})$ and so a typical element in G_{p^2} (II) is

$$\pm(1 - ip^{n-1}, p^{n-1}(i + j), -ip^{n-1}, 1 + ip^{n-1}).$$

Suppose $U = \pm(1 - p^r c, p^r, -p^r c^2, 1 + p^r c)$ and V are conjugates of S^{p^r}, $r \geq 1$, $U^p = V^p$ and U is in H. Then

$$V = \pm(1 - p^r(c + xp^{n-r-1}), p^r, -p^r(c^2 + 2cxp^{n-r-1}), 1 + p^r(c + xp^{n-r-1}))$$

with $(p, x) = 1$. If V is in H, then

$$U^{-1}V = \pm(1 - xp^{n-1}, 0, -2cxp^{n-1}, 1 + xp^{n-1})$$

is in $H \cap K^n_{n-1}$. But the only elements in $H \cap K^n_{n-1}$ with 0 in the upper right corner are

$$\pm(1 - ip^{n-1}, 0, -ip^{n-1}, 1 + ip^{n-1}).$$

So $2cx \equiv x \pmod p$ which implies that $1 \equiv 2c \pmod p$. But $U^{p^{n-r-1}} = S^{p^{n-1}}$ or S_1 so that $c \equiv 0$ or $1 \pmod p$ and hence $1 \not\equiv 2c \pmod p$. So each level from 1 to $n - 1$ has at most two groups conjugate to S^{p^r} and so

$$W \leq 2(n - 1) + s(1).$$

But $s(1) \leq 2p$ since each of the two conjugates to S^p has at most p p-*th* roots conjugate to S and so $W \leq 2(n - 1) + 2p$.

LEMMA 3.5. *Suppose $H \cap K^n_{n-1}$ is generated by*

$$S^{p^{n-1}} \quad \textit{and} \quad \pm(1 + p^{n-1}, 0, 0, 1 - p^{n-1}).$$

Consider all the conjugates of powers of S in H and let m be the smallest integer such that there is a c_0 with $p^{n-m}c_0^2 \not\equiv 0 \pmod{p^n}$. Suppose $m < \frac{2}{3}n - \frac{1}{3}$ and let $s = (m + 1)/2$ and r be such that $m + 1 \leq r \leq \frac{2}{3}n - \frac{1}{3}$. Consider $\{U_t\}$, a set of conjugates of S^{p^r}, such that the p^s-th powers of any two are the smallest powers which are equal. Then at most two of the U_t are in H.

Proof. A typical element in $H \cap K^n_{n-1}$ is $\pm(1 + ip^{n-1}, jp^{n-1}, 0, 1 - ip^{n-1})$ where $0 \leq i, j \leq p - 1$. m is odd since $p^{m-1} \| c_0^2$. U, a conjugate of S^{p^r} in H, has p dividing c since $U^{p^{r-1}}$ has 0 in the lower left corner. Conjugate H so that S^{p^r} is in H for each r for which S^{p^r} has some conjugate in H. Then

$$S' = \pm(1 + p^{n-m}c_0, p^{n-m}, -p^{n-m}c_0^2, 1 - p^{n-m}c_0)^{p^{m-1}-1},$$

which equals $\pm(1 - p^{n-m}c_0, p^{n-1} - p^{n-m}, p^{n-m}c_0^2, 1 + p^{n-m}c_0)$ since p divides

c_0, is in H. Then

$$S'\cdot S^{p^{n-m}} = \pm(1 - p^{n-s}x^{-1}, p^{n-1}, p^{n-1}y, 1 + p^{n-s}x^{-1})$$

where $(x^{-1}, p) = (y, p) = 1$ is in H and so

$$(S'\cdot S^{p^r})^x = U' = \pm(1 - p^{n-s}, p^{n-1}x, p^{n-1}xy, 1 + p^{n-s})$$

with $(xy, p) = 1$ is in H. Let

$$U = \pm(1 + p^{n-r}c, p^{n-r}, -p^{n-r}c^2, 1 - p^{n-r}c)$$

be in H and suppose

$$V = \pm(1 + p^{n-r}\gamma, p^{n-r}, -p^{n-r}\gamma^2, 1 - p^{n-r}\gamma)$$

with $m + 1 \leq r \leq \frac{2}{3}n - \frac{1}{3}$. Then $U^{p^s} = V^{p^s}$ if and only if $\gamma \equiv c \pmod{p^{r-s}}$ and the p^s*-th* powers of U and V are the smallest which are equal if and only if $\gamma = c - tp^{r-s}$ where $(t, p) = 1$. $\{U_t\}$ in the hypothesis is a subset of $\{U$ and V's in H obtained by different choices of $\gamma\}$. Then

$$\begin{aligned} U\cdot V^k = \pm(&1 + p^{n-r}(c + k\gamma) + p^{2n-2r}k\gamma(c - \gamma),\\ &p^{n-r}(k + 1) + p^{2n-2r}k(c - \gamma),\\ &-p^{n-r}(c^2 + k\gamma^2) - p^{2n-2r}ck\gamma(c - \gamma),\\ &1 - p^{n-r}(c + k\gamma) - p^{2n-2r}kc(c - \gamma)).\end{aligned}$$

Suppose $p^l \parallel c$ and let $a = r - (m - 1)$. Then U^{p^a} has lower left corner equal to

$$-p^{n-r+r-(m-1)}c^2 \equiv -p^{n-(m-1)+2l}y \equiv 0 \pmod{p^n}$$

if and only if $2l \geq m - 1$. But by choice of m, $-p^{n-(m-1)}c^2 \equiv 0 \pmod{p^n}$ so that $l \geq (m - 1)/2 = s - 1$. So p^{s-l} divides c. Let $k = p^{n-1} - 1$ so that

$$U\cdot V^k = \pm(1 + tp^{n-s}, p^{n-1}, 2p^{n-1}tc^*, 1 - tp^{n-s})$$

since p^{s-1} divides c, $r \leq \frac{2}{3}n - \frac{1}{3}$ and $s \leq r/2$. Now if V is in H, then

$$U'\cdot U\cdot V^k = \pm(1, p^{n-1}(1 + x), p^{n-1}xy + 2c^*t, 1)$$

is in $H \cap K^n_{n-1}$ and so $xy + 2c^*t \equiv 0 \pmod p$. If p divides c^*, i.e. if p^s divides c, then $xy + 2c^*t \equiv xy \not\equiv 0 \pmod p$ so that V is not in H. If p does not divide c^*, then $t \equiv -(xy)(2c^*)^{-1} \pmod p$ and so there is exactly one choice for γ for which V belongs to H. So at most two from the set $\{U_t\}$ are in H.

PROPOSITION 3.6. *Suppose* $H \cap K^n_{n-1}$ *is a* G_{p^2} *(I). Then* $W \leq p^{7n/9+4}$ *for* $n \geq 9$.

Proof. Conjugate H so that $H \cap K^n_{n-1}$ is generated by

$$S^{p^{n-1}} \quad\text{and}\quad \pm(1 + p^{n-1}, 0, 0, 1 - p^{n-1}).$$

If H can be conjugated so that all the conjugates of S^{p^r} have 0 in the lower left corner, then each conjugate of $S^{p^{n-r}}$ in H has p^r dividing c^2 and so

$$W \leq 1 + 2\sum_{i=1}^{n/2-1} p^i + p^{n/2} = 1 + 2p(p^{n/2-1} - 1)/(p-1) + p^{n/2}$$

if n is even and

$$W \leq 1 + 2p(p^{(n-1)/2} - 1)/(p-1)$$

if n is odd both of which are less than $p^{7n/9+4}$ for $n \geq 9$.

If H can not be so conjugated, let m be the smallest integer such that

$$p^{n-m}c_0^2 \not\equiv 0 \pmod{p^n}$$

for some c_0 and suppose $m \leq \frac{2}{3}n - \frac{1}{3}$. Now if U in H is conjugate to S^{p^r} and V in H is a conjugate of $S^{p^{r-1}}$ such that $V^p = U$, then there are p conjugates V_i of $S^{p^{r-1}}$ in H such that $V_i^p = U$ and these are given by

$$V_i = V \cdot \pm(1 - ip^{n-1}, 0, 0, 1 + ip^{n-1})$$

since p divides the c for V. At the $(m-1)$-*st* level, since p^{m-1} divides c^2 there are at most $p^{(m-1)/2}$ conjugates of $S^{p^{n-(m-1)}}$ in H so that at the m-*th* level there are at most p^s conjugates of $S^{p^{n-m}}$ in H and at the $(m+1)$-*st* level, there are at most p^{s+1} conjugates of $S^{p^{n-(m+1)}}$ in H. These p^{s+1} conjugates can be partitioned into p^s sets of p elements each where if c determines one element in a set, then $c - kp^{r-s}$ where $(k, p) = 1$ determine the others. By Lemma 3.5, H contains at most two elements from each of these sets and so $s(p^{n-(m+1)}) \leq 2p^s$. Continuing this argument, one sees that

$$s(p^{n-(m+i)}) \leq 2^i p^s \text{ for } m + i \leq \tfrac{2}{3}n - \tfrac{1}{3}.$$

Let x be the greatest integer less than or equal to $\frac{2}{3}n - \frac{1}{3}$. Then for $r > x$,

$$s(p^{n-r}) \leq p \cdot s(p^{n-r+1}).$$

So

$$\begin{aligned} W &\leq 1 + 2\sum_{i=1}^{s} p^i + p^s \sum_{i=1}^{x-m} 2^i + 2^{x-s}p^s \sum_{i=1}^{n-x} p^i \\ &\leq 1 + 2p(p^s - 1)/(p-1) + p^s(2^{x-m+1} - 2) \\ &\qquad + 2^{x-s}p^{s+1}(p^{n-x} - 1)/(p-1) \\ &\leq 1 + p^{n/3+1} + p^{n/3-2/3} \cdot 2^{2n/3-s+1} + 2^{2n/3-s}p^{s+1}p^{n/3+1} \end{aligned}$$

since $1 \leq s = (m+1)/2 \leq n/3 - \frac{2}{3}$. But $2^{2n/3} = (2^6)^{n/9} < (3^4)^{n/9} \leq p^{4n/9}$ so that

$$W \leq 1 + p^{n/3+1} + p^{3n/9-2/3}p^{4n/9} + p^{4n/9+1}p^{3n/9+1} \leq p^{7n/9+4}.$$

LEMMA 3.7. *Suppose $U = \phi(\mu, \nu, \rho)_r$ has property A, $U' = \phi(\mu', \nu', \rho')_s$ does not have property A and $[U] \cap [U'] = \{I\}$. Then if $U^{p^{n-r-1}}$ and $U'^{p^{n-s-1}}$ have property A, p does not divide $(\mu(\nu' + \rho') - 2\mu'\nu)$.*

Proof. Since $U'^{p^{n-s-1}}$ has property A, $\nu' \equiv \rho' \pmod{p}$. Recall we are assuming that not all of μ, ν and ρ (and μ', ν' and ρ') are divisible by p. There are four cases to consider. Suppose p does not divide ν. Then, by taking an appropriate power of U, we can assume that

$$\nu \equiv \rho \equiv 1 \pmod{p^{n-s}}.$$

(1) If p divides ν', then p divides ρ' and so p does not divide μ'. So p does not divide $2\mu'\nu$ and divides $\mu(\nu' + \rho')$ so that p does not divide the sum. (2) If p does not divide ν', then p does not divide ρ' and we may assume $\nu' \equiv \rho' \equiv 1 \pmod p$. Since $[U] \cap [U'] = \{I\}$, it is false that

$$\mu \equiv c\mu', \quad \nu \equiv c\nu', \quad \rho \equiv c\rho' \qquad \pmod p$$

for any c. So

$$\mu \not\equiv \mu' \pmod p \quad \text{and} \quad \mu(\nu' + \rho') - 2\mu'\nu \equiv 2(\mu - \mu') \not\equiv 0 \pmod p.$$

Suppose p divides ν and ρ. Then p does not divide μ. (3) If p divides ν' and ρ', then p does not divide μ'. So for some $c \not\equiv 0 \pmod p$

$$\mu \equiv c\mu', \quad \nu \equiv c\nu' \equiv 0, \quad \rho \equiv c\rho' \equiv 0 \qquad \pmod p$$

which is a contradiction. (4) If p does not divide ν' and ρ', then

$$\mu(\nu' + \rho') - 2\mu'\nu \equiv 2\mu\nu' \not\equiv 0 \pmod p$$

since $\nu' \equiv \rho' \pmod p$.

PROPOSITION 3.8. *Suppose* $|H \cap K_{n-1}^n| = p^2$. *The number of elements in* $H \cap K_r^n$ *with property* A *is bounded by* $(n+1)p^{n+3}$.

Proof. Let a denote the number of elements with property A in $H \cap K_1^n$. Suppose r is the smallest number such that $H \cap K_r^n$ contains an element with property A. Let $U_1 = \phi(\mu, \nu, \rho)_r$ and $U_2 = \phi(\mu', \nu', \rho')_s$ be generators of $H \cap K_1^n$ with $s \geq r$ and U_1 having property A. Then $[U_1] \cap [U_2] = \{I\}$ and $\{U_1^i U_2^j\}$ is as described in Section 2. Now $p^{n-r-x-1}(p-1)$ of the ξ_i and $p^{n-s-x-1}(p-1)$ of the ξ_j are divisible by precisely p^x since ξ_i and ξ_j determine which K_l^n, U_1^i and U_2^j belong to. Suppose U_2 also has property A. We want the number of elements in $\{U_1^i U_2^j\}$ such that

$$\begin{aligned} p^r\xi_i\nu u_j' + p^s\xi_j\nu' u_i + p^{r+s}\xi_i\xi_j(\nu\mu' - \nu'\mu) \\ \equiv p^s\xi_j\nu' u_i + p^r\xi_i\nu u_j' + p^{r+s}\xi_i\xi_j(\mu\nu' - \mu'\nu) \quad \pmod{p^n} \end{aligned} \tag{3.1}$$

which is true if and only if

$$2\,\xi_i\xi_j(\nu\mu' - \mu\nu') \equiv 0 \pmod{p^{n-r-s}}. \tag{3.2}$$

We claim that $\nu\mu' \not\equiv \mu\nu' \pmod p$. Since U_1 and U_2 have property A, $\nu \equiv \rho$ and $\nu' \equiv \rho' \pmod p$. There are 3 cases to consider: (1) Suppose p does not divide ν, ρ, ν' and ρ'. Then, as in Lemma 3.7, we can assume $\nu \equiv \rho \equiv \nu' \equiv \rho' \equiv 1 \pmod p$. But then $\mu' \not\equiv \mu \pmod p$ since there is no c such that

$$\nu \equiv c\nu', \quad \rho \equiv c\rho', \quad \mu \equiv c\mu' \qquad \pmod p$$

so $\nu\mu' \equiv \mu' \not\equiv \mu \equiv \mu\nu' \pmod p$. (2) Suppose p divides all of ν, ρ, ν' and ρ'. Then $U_1^{\xi_i} = U_2^{\xi_j}$ for some ξ_i, ξ_j divisible by p^{n-r-1} and p^{n-s-1} respectively which is a contradiction to $[U_1] \cap [U_2] = \{I\}$. (3) Suppose $\nu \equiv \rho \equiv 1 \pmod p$ and p divides ν' and ρ'. Then p does not divide μ' and so $\mu'\nu \not\equiv 0 \equiv \mu\nu'$ $\pmod p$. Therefore the solutions (ξ_i, ξ_j) to (3.2) are the same as the solutions to

$$\xi_i \xi_j \equiv 0 \pmod{p^{n-r-s}}. \tag{3.3}$$

If p^{n-r} divides ξ_i, there is one choice for ξ_i and p^{n-s} choices for ξ_j since ξ_j can be chosen arbitrarily. If $p^{n-r-x} \parallel \xi_i$ where $1 \le x \le s$, there exist $p^{x-1}(p-1)$ choices for ξ_i and p^{n-s} choices for ξ_j since ξ_j can be chosen arbitrarily. If $p^{n-r-x} \parallel \xi_i$ where $s+1 \le x \le n-r$, there exist $p^{x-1}(p-1)$ choices for ξ_i and p^{n-x} choices for ξ_j since p^{x-s} has to divide ξ_j. So

$$\begin{aligned} a &\le p^{n-s} + p^{n-s}\left(\textstyle\sum_{i=1}^{s} p^{i-1}(p-1)\right) + \textstyle\sum_{i=s+1}^{n-r} p^{n-1}(p-1) \\ &= p^{n-s} + (p-1)\left(p^{n-s}(p^s-1)/(p-1) + (n-r-s-1)p^{n-1}\right) \\ &< p^{n+3} + np^{n-1} < (n+1)p^{n+3}. \end{aligned}$$

Now suppose U_2 does not have property A. We want the number of elements such that

$$\begin{aligned} &p^s\xi_j\,\nu' u_i + p^{r+s}\xi_i\xi_j(\mu\nu' - \nu\mu') \\ &\qquad \equiv p^s\xi_j\,\rho' u_i + p^{r+s}\xi_i\xi_j(\nu\mu' - \rho'\mu) \pmod{p^n} \end{aligned} \tag{3.4}$$

which is true if and only if

$$p^s\xi_j\,u_i(\nu' - \rho') + p^{r+s}\xi_i\xi_j\,\zeta \equiv 0 \pmod{p^n} \tag{3.5}$$

where $\zeta = \mu(\nu' + \rho') - 2\mu'\nu$. However by Lemma 3.7, p does not divide ζ. Let $p^x \parallel (\nu' - \rho')$. Then $x \ge 1$ since $\nu' \equiv \rho' \pmod p$. Now $x \le n - s$ since $1 \le \nu', \rho' \le p^{n-s}$ and we may assume $r + s < n$ since otherwise the number of elements in $\{U_1^i\, U_2^j\}$ is bounded by p^n and so $a \le p^n$. Equation (3.5) becomes

$$p^{x+s}\xi_j\,u_i\,y + p^{r+s}\xi_i\,\xi_j\,\zeta \equiv 0 \pmod{p^n} \tag{3.6}$$

where $(y, p) = (\zeta, p) = 1$. Now if $x < r$, then p^{n-s-x} has to divide ξ_j and so a is bounded by $p^x \cdot p^{n-r} \le p^n$. So assume $r \le x \le n - s$ and let $p^l \parallel \xi_j$ where $0 \le l \le n - s$. There are $p^{n-s-l-1}(p-1)$ choices for ξ_j. Suppose $0 \le l \le n - s - r$. Then equation (3.6) becomes

$$p^{x-r}y' + \zeta''\xi_i \equiv 0 \pmod{p^{n-r-s-l}} \tag{3.7}$$

where $(y', p) = (\zeta'', p) = 1$. So, mod $p^{n-r-s-l}$, there is a unique solution for ξ_i and so there are $p^{n-r-(n-r-s-l)} = p^{s+l}$ choices for ξ_i which gives

$$p^{n-s-l-1}p^{s+l}(p-1) = p^{n-1}(p-1)$$

elements with property A. Suppose $n - s - r \leq l \leq n - s - 1$. Then there are $p^{n-s-l-1}(p-1)$ choices for ξ_j and p^{n-r} choices for ξ_i since ξ_i can be chosen arbitrarily. For $l = n - s$, there is one choice for ξ_j and p^{n-r} choices for ξ_i. So

$$\begin{aligned} a &\leq p^{n-r} + p^{n-r} \textstyle\sum_{l=n-s-r}^{n-s-1} p^{n-s-l-1}(p-1) + (n-s-r)p^{n-1}(p-1) \\ &\leq p^{n-r} + p^{n-r}(p^r - 1)(p-1) + (n-s-r)p^{n-1}(p-1) \\ &< (n-s-r+2)p^{n+1} < (n+1)p^{n+3}. \end{aligned}$$

LEMMA 3.9. *Let $p > 3$. Suppose $U = \phi(\mu, \nu, \rho)_r$ and $U' = \phi(\mu', \nu', \rho')_s$ with $r \leq s < n/2$ and $[U] \cap [U'] = \{I\}$. Then if U and U' both have property* B, *U and U' can not generate a group of order p^{2n-r-s}.*

Proof. Since $[U] \cap [U'] = \{I\}$, there is no c such that

$$\mu \equiv c\mu', \quad \nu \equiv c\nu' \quad \text{and} \quad \rho \equiv c\rho' \qquad (\text{mod } p).$$

We know that

$$u^2 - p^{2r}(\mu^2 + \nu\rho) \equiv 1 \quad \text{and} \quad u'^2 - p^{2s}(\mu'^2 + \nu'\rho') \equiv 1 \quad (\text{mod } p^n) \tag{3.8}$$

with $u, u' \equiv 1 \pmod p$. Since U and U' have property B,

$$u + p^r(\nu - \rho - \mu) \equiv 1 \quad \text{and} \quad u' + p^s(\nu' - \rho' - \mu') \equiv 1 \quad (\text{mod } p^n). \tag{3.9}$$

So by (3.8), p^{2r} divides $1 - u$ and p^{2s} divides $1 - u'$. Together with (3.9), this implies p^r divides $\nu - \rho - \mu$ and p^s divides $\nu' - \rho' - \mu'$. Hence

$$\nu \equiv \rho + \mu \pmod p \quad \text{and} \quad \nu' \equiv \rho' + \mu' \pmod p.$$

If U and U' generate a group of order p^{2n-r-s}, then

$$\mu''^2 + \nu''\rho'' \equiv 0 \quad (\text{mod } p^{n-r-s})$$

where $\mu'' = (\nu\rho' - \nu'\rho)/2$, $\nu'' = \mu\nu' - \mu'\nu$ and $\rho'' = \rho\mu' - \rho'\mu$ [4]. So

$$\mu''^2 + \nu''\rho'' \equiv 0 \quad (\text{mod } p)$$

since $r + s < n$. Now $\mu'' \equiv ((\rho + \mu)\rho' - (\rho' + \mu')\rho)/2 \equiv -\rho''/2 \pmod p$. Similarly $\nu'' \equiv -\rho'' \pmod p$. So $0 \equiv -3\rho''^2/4 \pmod p$ which implies that $\rho'' \equiv 0 \pmod p$. So $\rho\mu' \equiv \rho'\mu \pmod p$. Suppose p divides ρ. Then p divides ρ' or μ. If p divides μ, then $0 \equiv \mu + \rho \equiv \nu \pmod p$ so that p also divides ν. Hence p divides all of μ, ν and ρ, a contradiction. If p divides ρ', then $\rho \equiv c\rho' \pmod p$ for any c. Pick c so that $\mu \equiv c\mu' \pmod p$. Then

$$\nu \equiv \mu + \rho \equiv c\mu' + c\rho' \equiv c(\mu' + \rho') \equiv c\nu' \quad (\text{mod } p).$$

So we have $\mu \equiv c\mu'$, $\nu \equiv c\nu'$ and $\rho \equiv c\rho' \pmod p$, a contradiction. Suppose p does not divide ρ. Then $\mu' \equiv (\rho^{-1}\rho')\mu \pmod p$. Certainly $\rho' \equiv (\rho^{-1}\rho')\rho$ $(\text{mod } p)$. Finally

$$\nu' \equiv \mu' + \rho' \equiv (\rho^{-1}\rho')(\mu + \rho) \equiv (\rho^{-1}\rho')\nu \quad (\text{mod } p).$$

So again there is a c such that $\mu \equiv c\mu'$, $\nu \equiv c\nu'$ and $\rho \equiv c\rho' \pmod p$, a contradiction.

PROPOSITION 3.10. *Suppose $p > 3$ and $|H \cap K_{n-1}^n| = p^2$. The number of elements in $H \cap K_1^n$ with property* B *is less than p^{2n-3}.*

Proof. Suppose n is even. Since $|H \cap K_r^n| \leq 2n - 2r$, then if $r = n/2$, the number of elements in $H \cap K_r^n$ with property B is at most n. Suppose $r < n/2$. The $p^{2n-2(r+1)}(p^2 - 1)$ elements at the $(n - r)$-*th* level can be partitioned into $p^2 - 1$ sets of $p^{2n-2(r+1)}$ elements each where U and U' are in the same set if and only if $U^{p^{n-r-1}} = U'^{p^{n-r-1}}$. By Lemma 3.9, if U has property B, then any other element V with property B has to be such that $[V^{p^{n-r-1}}] = [U^{p^{n-r-1}}]$ so that $[U] \cap [V] \neq \{I\}$. So, at the $(n - r)$-*th* level, there are at most $(p - 1)\, p^{2n-2(r+1)}$ elements with property B. Therefore the number of elements in $H \cap K_1^n$ with property B is bounded by

$$p^n + (p - 1) \sum_{i=0}^{n/2-2} p^{2n-(n-2i)} = (p^{2n-2} + p^{n+1})/(p + 1) < p^{2n-3}.$$

A similar argument in the case where n is odd yields the bound

$$p^{n+1} + (p - 1) \sum_{i=1}^{(n-3)/2} p^{n+(2i-1)} = (p^{2n-2} + p^{n+2})/(p + 1) < p^{2n-3}.$$

PROPOSITION 3.11. *Suppose $p > 3$. There exists an n_3 such that if $n \geq n_3$ and $|H \cap K_{n-1}^n| = p^2$, then $g(H) > g$.*

Proof. If $H \cap K_{n-1}^n$ is a G_{p^2} (III), then $W = 0$. Otherwise by Propositions 3.4 and 3.6, for $n \geq 9$, $W \leq p^{7n/9+4}$. By Proposition 2.5, to calculate t we need to know the number of elements in $H \cap K_1^n$ with property A and the number of elements of order 2 in $H \bmod p$. By Proposition 3.8, the number of elements in $H \cap K_1^n$ with property A is at most $(n + 1)p^{n+3}$. By McQuillan [7], the number of elements of order 2 in $H \bmod p$ is bounded by $p + 2$ if $p \geq 15$ or 15 if $p < 15$. So $t \leq (p + 2)(n + 1)p^{n+3}$ or $15(n + 1)p^{n+3}$. Similarly we calculate r. By Proposition 3.10, the number of elements in $H \cap K_1^n$ with property B is less than p^{2n-3}. By McQuillan [7], the number of distinct groups in $H \bmod p$ generated by a conjugate of R is bounded by $2p$. So $r \leq 2p^{2n-2}$. Finally $h \leq p^{2n-1}(p^2 - 1)$. So

$$\begin{aligned} g(H) \geq 1 + \{p^{2n-2}(p^2 - 1)(p^n - 6) - 8p^{n-1}(p + 1)2p^{2n-2} \\ - 6p^{n-1}(p + 2)(n + 1)p^{n+4} \\ - 6p^{2n-2}(p - 1)^2 p^{7n/9+4}\}/24p^{2n-1}(p^2 - 1). \end{aligned}$$

For $n \geq 9$, $p^3(n + 1)(p + 2) \leq p^{7n/9+4}$. So

$$g(H) \geq 1 + a(dp^{n-1} - (b + 1)p^{7n/9+4} - c)$$

where $a = 1/24(p^3 - p)$, $b = 6(p - 1)^2$, $c = 6p^2 + 6(p - 1)^2$ and $d = p^3 - 17p - 16 > 0$ since $p \geq 5$. But

$$\lim_{n\to\infty} 1 + a(dp^{n-1} - (b + 1)p^{7n/9+4} - c) = \infty$$

and therefore there is an n_3 such that if $n \geq n_3$, $g(H) > g$. For $p < 15$, the only adjustment in the calculation is that the term $p^3(n+1)(p+2)$ becomes $15p^3(n+1)$. But $15p^3(n+1)$ is still less than $p^{7n/9+4}$ for $n \geq 9$.

THEOREM 2. *Suppose $p > 3$. Then there exists an n_4 such that if $n \geq n_4$ and H is of level n, then $g(H) > g$.*

Proof. $n_4 = \max\{n_1, n_2, n_3\}$ where n_1, n_2, n_3 are as in Propositions 3.1, 3.3 and 3.11 respectively works.

4. $LF(2, 3^n)$ and $LF(2, 2^n)$

Finally we must consider the cases $p = 2$ and 3. We first consider $p = 3$. The propositions leading to bounds for t and W are valid for $p = 3$ so we only have to obtain bounds for r. For $p = 3$, it is still true that if R_1 is conjugate to R, then R_1 has trace $= \pm 1$. Therefore an upper bound on the number of elements of trace ± 1 still yields an upper bound on the number of conjugates of R. So as before we wish to calculate the number of elements in $H \cap K_1^n$ with property B.

LEMMA 4.1. *Suppose the number of elements in $H \cap K_{n-1}^n$ with property* B *is bounded by* 3. *Then, if $n \geq 4$, there are less than 3^{2n-4} elements with property* B *in $H \cap K_1^n$.*

Proof. Suppose $U = \phi(\mu, \nu, \rho)_r$ has property B. Then $U \cdot V$ has property B where

$$V = \phi(\mu', \nu', \rho')_{n-1}$$

if and only if V has property B since

$$U \cdot V = \pm(u + 3^r\mu + 3^{n-1}\mu' u, 3^{n-1}\nu' u + 3^r\nu, 3^r\rho + 3^{n-1}\rho' u, u - 3^r\mu - 3^{n-1}\mu' u)$$

and

$$u + 3^r(\nu - \mu - \rho) + 3^{n-1}u(\nu' - \mu' - \rho') \equiv 1 \pmod{3^n}$$

if and only if 3 divides $\nu' - \mu' - \rho'$ since $u + 3^r(\nu - \mu - \rho) \equiv 1 \pmod{3^n}$. Suppose

$$U^x = \phi(\xi\mu, \xi\nu, \xi\rho)$$

is in K_{n-1}^n. Then U^x has property B since

$$u_x + 3^r\xi(\nu - \mu - \rho) \equiv 1 + 3^r \cdot 3^{n-r-1} \cdot 3y \equiv 1 \pmod{3^n}$$

since 3^{n-r-1} divides ξ, 3 divides $\nu - \mu - \rho$ and $u_x = 1$.

$|H \cap K_1^n| \leq 3^{2n-2}$ and $H \cap K_1^n$ can be partitioned into one set of at most 9 elements consisting of $H \cap K_{n-1}^n$ and 8 sets of at most $(3^{2n-2} - 9)/8$ elements each as follows: Suppose U and U_1, not in K_{n-1}^n, are such that U^{3^w} and $U_1^{3^{w_1}}$ are in K_{n-1}^n. Then U and U_1 are in the same set in the partition if and only if $U^{3^w} = U_1^{3^{w_1}}$. By the second observation, only 2 of these sets contain elements with property B. Consider one of these sets and call it M. M can be partitioned into $(3^{2n-2} - 9)/8\cdot 9$ sets of at most 9 elements each where the other elements in the set containing an element U are $U\cdot V$ where V is in $H \cap K^n_{n-1}$. By the first observation, at most 3 of these elements can have property B. So the total number of elements in $H \cap K^n_1$ with property B is bounded by

$$2\cdot 3\cdot (3^{2n-2} - 9)/8\cdot 9 + 9 < 3^{2n-4}$$

for $n \geq 4$.

LEMMA 4.2. *Suppose $U = \phi(\mu, \nu, \rho)_1$ has property* B, $9 \parallel 1 - u$ *and* $n \geq 4$. *Then $U' = \phi(\xi\mu, \xi\nu, \xi\rho)_r$ with 3 not dividing ξ has property* B *only if* $\xi \equiv 1 \pmod 9$.

Proof. Suppose $u' + 3\xi(\nu - \rho - \mu) \equiv 1 \pmod{3^n}$. Then

$$1 - u' \equiv \xi 3(\nu - \rho - \mu) \equiv \xi(1 - u) \pmod{3^n}.$$

Also $(u' - 1) \equiv 9\xi^2(\mu^2 + \nu\rho)/(u' + 1) \pmod{3^n}$. So

$$(u' + 1)(1 - u)\xi \equiv \xi^2(-9(\mu^2 + \nu\rho)) \pmod{3^n}.$$

Therefore

$$(u' + 1)(1 - u)\xi \equiv (1 - u)(1 + u)\xi^2 \pmod{3^n}. \tag{4.1}$$

Since 3 does not divide ξ and $9 \parallel (1 - u)$, congruence (4.1) becomes

$$(u' + 1) \equiv \xi(u + 1) \pmod{3^{n-2}}.$$

But since both u and u' are congruent to 1 mod 9, $u' + 1 \equiv u + 1 \pmod 9$ and since $n - 2 \geq 2$, this gives $1 \equiv \xi \pmod 9$.

Now K^n_{n-1} has 9 elements with property B and the elements with property B in $H \cap K^n_{n-1}$ form a subgroup of $H \cap K^n_{n-1}$ so that if $H \cap K^n_{n-1}$ has more than 3 elements with property B, then

$$H \cap K^n_{n-1} = \{\pm(1 + 3^{n-1}\mu, 3^{n-1}\nu, 3^{n-1}\rho, 1 - 3^{n-1}\mu)\}$$

with $(\nu - \mu - \rho) \equiv 0 \pmod{3^n}$ which contains only $1G_p(I)$, namely

$$[\pm(1 - 3^{n-1}, 3^{n-1}, -3^{n-1}, 1 + 3^{n-1})].$$

Suppose $U = \phi(\mu, \nu, \rho)_1$ is in $H \cap K^n_1$. Then $U^x = \phi(\xi\mu, \xi\nu, \xi\rho)$ is in $H \cap K^n_{n-1}$ for some x and if 3 divides $\mu^2 + \nu\rho$, then U^x is in the $G_p(I)$ since $(\mu^2 + \nu\rho) \equiv 0 \pmod 3$ implies that U^x generates a $G_p(I)$ [4].

LEMMA 4.3. *Suppose $H \cap K^n_{n-1}$ contains* 9 *elements with property* B. *Then $H \cap K^n_1$ has at most $3^{2n-3} + 3^{2n-4}$ elements with property* B.

Proof. If $|H \cap K^n_1| \leq 3^{2n-3}$, we are done so that we may assume

$$|H \cap K^n_1| = 3^{2n-2}.$$

Consider

$$M = \{U \mid U \text{ is in } K^n_1 - K^n_2 \text{ and } U^{3^{n-2}} \text{ is not in the } G_p(I)\}.$$

$|M| = 3^{2n-2} - 3^{2n-3}$ and each element in M has order 3^{n-1}. So there are

$$3^{2n-3}(2)/3^{n-2}(2) = 3^{n-1}$$

distinct cyclic groups of order 3^{n-1} whose generators are in M. Let

$$[U = \phi(\mu, \nu, \rho)_1]$$

be such a cyclic group and, if possible, select U with property B. Then by the assumptions on M, 3 does not divide $\mu^2 + \nu\rho$ so that $9 \parallel \nu - \rho - \mu$. Then, by Lemma 4.2, the other elements in $M \cap [U]$ with property B have $\xi \equiv 1 \pmod 9$ where $1 \leq \xi \leq 3^{n-1}$. So the number of such elements is at most 3^{n-3}. So the number of elements in $H \cap K_1^n$ with property B is bounded by

$$3^{n-3}(3^{n-1}) + 3^{2n-4} + 2\cdot 3^{2n-4} = 3^{2n-4} + 3^{2n-3}.$$

LEMMA 4.4. *Suppose $H \pmod 3 = \mathfrak{T}$, the tetrahedral group, and that H contains R. Then $r \leq 4\cdot 3^{2n-4}$.*

Proof. The elements generating groups conjugate to $[R]$ in $LF(2, 3) = \mathfrak{T}$ are R,

$$R_1 = \pm(0, 1, -1, 1), \quad R_2 = \pm(-1, 1, 0, -1), \quad R_3 = \pm(-1, 0, 1, -1).$$

Consider a fixed R_i. There is an A in $LF(2, 3)$ such that $ARA^{-1} = R_i$ and since $H \bmod p = LF(2, 3)$, there is an A_1 in H such that $\bar{A}_1 = A$. Then $(A_1 R A_1^{-1})^- = R_i$ and $A_1 R A_1^{-1}$ is conjugate to R in H. So each conjugate of R in $LF(2, 3)$ has a pre-image in H which is conjugate to R. If $H \cap K_{n-1}^n$ contains at most 3 elements with property B, then we are done by Lemma 4.1 and Proposition 2.4. Suppose $H \cap K_{n-1}^n$ has 9 elements with property B. Consider R' in H such that R' is conjugate to R and $\bar{R}' = R_1$. Then

$$\begin{aligned} R' &= U\cdot \pm(0, 1, -1, 1) \\ &= \pm(-3^r\nu, u + 3^r\mu + 3^r\nu, -u + 3^r\mu, u + 3^r\rho - 3^r\mu) \end{aligned}$$

where $U = \phi(\mu, \nu, \rho)_r$ is some fixed element of K_1^n such that

$$u + 3^r(\rho - \mu - \nu) \equiv 1 \pmod{3^n}.$$

Consider $U'\cdot R'$ where $U' = \phi(\mu', \nu', \rho')_s$. This will be conjugate to R' if and only if

$$\begin{aligned} 1 &\equiv -u'3^r\nu - 3^{r+s}\mu'\nu - 3^s\nu'u + 3^{r+s}\mu\nu' + 3^s\rho'u + 3^{r+s}\mu\rho' + 3^{r+s}\nu\rho' \\ &\quad + u'u + u'3^r\rho - u'3^r\mu - 3^{r+s}\mu'\rho - 3^s\mu'u + 3^{r+s}\mu'\mu \\ &\equiv u' + 3^s u(\rho' - \nu' - \mu') + 3^{r+s}(\mu\nu' - \mu'\nu - \mu'\rho + \mu\rho' + \nu\rho' + \mu'\mu) \\ &\qquad \pmod{3^n} \end{aligned} \tag{4.2}$$

since $u + 3^r(\rho - \mu - \nu) \equiv 1 \pmod{3^n}$. If U' satisfies congruence (4.2), we say U' has property C. Suppose $V = \phi(x, y, z)$ is in K_{n-1}^n. Then $V\cdot U'$ has property C if and only if V does since

$$u' + u3^s(\rho' - \nu' - \mu' + 3^{n-s-1}u'(z - x - y)) \\ + 3^{r+s}(\mu\nu' - \mu'\nu - \mu'\rho + \mu\rho' + \nu\rho' + \mu'\mu) \\ + 3^{n-s-1}u'(\mu y - \nu x - x\rho + \mu z + \nu z + x\mu) \\ \equiv 1 \pmod{3^n}$$

if and only if 3 divides $(z - x - y)$ if and only if V has property C. Also if U' has property C and $U'^x = \phi(\mu'\xi, \nu'\xi, \rho'\xi)$ is in K_{n-1}^n, then U'^x has property C. Since all the elements in $H \cap K_{n-1}^n$ have property B, at most 3 elements in $H \cap K_{n-1}^n$ have property C. Arguing as in Lemma 4.1, we see that R_1 has at most 3^{2n-4} pre-images in H conjugate to R and so by Proposition 2.5, each of R, R_1, R_2 and R_3 has at most 3^{2n-4} such pre-images. Hence $r \leq 4 \cdot 3^{2n-4}$.

THEOREM 3. *There exists an n_5 such that if $n \geq n_5$ and H is of level n in $LF(2, 3^m)$, $m \geq n$, then $g(H) > g$.*

Proof. From Lemma 3.2 and Propositions 3.4 and 3.6, $W < 3^{7n/9+4}$ for $n \geq 9$; from Proposition 3.8, the number of elements with property A is at most $(n + 1)3^{n+3}$. Now if $H \bmod 3 = \mathfrak{I}$, then $r \leq 4 \cdot 3^{2n-4}$ and $t \leq 3 \cdot (n + 1)3^{n+3}$. So

$$\begin{aligned} g(H) &\geq 1 + 3^{2n-2}\{3^{n+2} + 6 - (3^n + 54 + 32 \cdot 3^{n-2} + 24 \cdot (n + 1) \cdot 3^5 \\ &\qquad + 24 \cdot 3^{7n/9+4}\}/12 \cdot 3^{2n-1} \\ &= 1 + a\{3^{n-2}(81 - 9 - 32) - b(n + 1) - c \cdot 3^{7n/9+4} - d\} \\ &= 1 + f(n) \end{aligned}$$

where a, b, c and d are constants. But $\lim_{n\to\infty} f(n) = \infty$. If $H \bmod 3 \neq \mathfrak{I}$, then $r \leq 3^{2n-3} + 3^{2n-4}$ and $t \leq (n + 1)^2 3^{n+3}$ so that

$$\begin{aligned} g(H) &\geq 1 + 3^{2n-2}\{3^{n+2} - 6 - (3^n + 54 + 8 \cdot 3^{n-1} + 8 \cdot 3^{n-2} \\ &\qquad + 24(n + 1)^2 3^5 + 24 \cdot 3^{7n/9+4}\}/12 \cdot 3^{2n-1} \\ &= 1 + a\{3^{n-2}(81 - 9 - 24 - 8) - b(n + 1)^2 - c \cdot 3^{7n/9+4} - d\} \\ &= 1 + f_1(n) \end{aligned}$$

where a, b, c and d are constants. But $\lim_{n\to\infty} f_1(n) = \infty$. So in either case, there is an n_5 such that for $n \geq n_5$ and H of level n, $g(H) > g$.

For the case $p = 2$, refer to the lower bounds for $g(H)$ given in Propositions 4.1, 4.4, 4.5 and 4.6 in [2]. Observe that in each case, the lower bound on $g(H) \to \infty$ as $n \to \infty$. Hence we have the following theorem which completes our proof that the number of fields of a fixed genus in $K(p^n)$, all p and n, is finite.

THEOREM 4. *There exists an* n_6 *such that if* $n \geq n_6$ *and* H *is of level* n *in* $LF(2, 2^m)$, $m \geq n$, *then* $g(H) > g$.

BIBLIOGRAPHY

1. J. DENNIN, *Fields of modular functions of genus* 0, Illinois J. Math., vol. 15 (1971), pp. 442–455.
2. ———, *Subfields of* $K(2^n)$ *of genus* 0, Illinois J. Math., vol 16 (1972), pp. 502–518.
3. J. GIERSTER, *Die Untergruppen der Galois' schen Gruppe der Modular-Gleichungen für den Fall eines primzahlen Transformation-grades*, Math. Ann., vol. 18 (1881), pp. 319–365.
4. ———, *Über die Galois' sche Gruppe der Modulargleichungen wenn der Transformationsgrad die Potenz einer Primzahl* > 2 *ist*, Math. Ann., vol. 26 (1886), pp. 309–368.
5. R. C. GUNNING, *Lectures on modular forms*, Princeton, 1962.
6. D. L. MCQUILLAN, *Some results on the linear fractional group*, Illinois J. Math., vol. 10 (1966), pp. 24–38.
7. ———, *On the genus of fields of elliptic modular functions*, Illinois J. Math., vol. 10 (1966), pp. 479–487.

UNIVERSITY OF CONNECTICUT
STORRS, CONNECTICUT