SUBFIELDS OF $K(2^n)$ OF GENUS 0

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. The conjecture has been proven if n is prime to $2 \cdot 3 \cdot 5$ or is a power of 3 or 5 [5, 1]. In this paper we show that the conjecture is true if n is a power of 2.

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 $LF(2, n) = SL(2, n)/ \pm \mathrm{Id}$. 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 H equals 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 $\pm (a, b, c, d)$.

$$I = \pm (1, 0, 0, 1); \qquad T = \pm (0, -1, 1, 0);$$

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

T and S generate $LF(2, 2^n)$ and $R = TS$. H will be a subgroup of $LF(2, 2^n)$; $g(H) =$ 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. φ_r^n will denote the natural homomorphism from $LF(2, 2^n)$ to $LF(2, 2^r)$, $1 \leq r \leq n$,

Received April 29, 1970.

obtained by reducing all the entries in a matrix in $LF(2, 2^n)$ mod 2^r. K_r^n is the kernel of φ_r^n and so is a normal subgroup of $LF(2, 2^n)$.
$|LF(2, 2^n)| = 3\cdot 2^{3n-3}$ and $|K_r^n| = 2^{3(n-r)}$ if $r \neq 1$ and 2^{3n-4} if $r = 1$.

Our main result is

THEOREM 1. *Let H be a subgroup of $LF(2,2^n)$ with $|H \cap K_{n-1}^n| \leq 4$. If $g(H) = 0$, then $n < 8$.*

To compute $g(H)$ we use the following formula derived from McQuillan [5]: Let r, t and $s(2^r)$ be the number of distinct cyclic subgroups of H generated by a conjugate in $LF(2, 2^n)$ of R, T and S^{2^r} respectively where $1 \leq 2^r \leq 2^n$. Then

$$(1.1)\quad \begin{aligned} &g(H)\\ &= 1 + \{(2^n - 6)\cdot 3\cdot 2^{2n-2} - (8r\rho(2^n) + 6t\tau(2^n) + 6\cdot 2^{2n-2}W)\}/24h \end{aligned}$$

where $W = \sum s(2^r)$, $\rho(2^n) = 3\cdot 2^{n-1}$ and $\tau(2^n) = 2^n$.

One consequence of this is that if two groups are conjugate they have the same genus.

2. Some results on the structure of K_1^n

We first analyze K_{n-1}^n for $n > 2$ which has order 8 and in which every non-identity element has order two. It contains the center of

$$LF(2, 2^n) = [\pm (1 + 2^{n-1}, 0, 0, 1 + 2^{n-1})]$$

which will be denoted by $[Z_n]$. The other subgroups of K_{n-1}^n of order two in which we are interested are the three conjugates of $[S^{2^{n-1}}]$, namely

$$[S^{2^{n-1}}],\quad [\pm (1, 0, 2^{n-1}, 1)] \quad \text{and} \quad [\pm (1 + 2^{n-1}, 2^{n-1}, 2^{n-1}, 1 + 2^{n-1})].$$

The subgroups of K_{n-1}^n of order four are divided into three different conjugacy classes: (1) three groups containing Z_n and one conjugate of $S^{2^{n-1}}$ such as

$$D = \{I, Z_n, S^{2^{n-1}}, \pm (1 + 2^{n-1}, 2^{n-1}, 0, 1 + 2^{n-1})\};$$

(2) three groups containing two conjugates of $S^{2^{n-1}}$ such as

$$\begin{aligned} C = \{I, S^{2^{n-1}}, &\pm (1 + 2^{n-1}, 0, 2^{n-1}, 1 + 2^{n-1}),\\ &\pm (1 + 2^{n-1}, 2^{n-1}, 2^{n-1}, 1 + 2^{n-1})\}; \end{aligned}$$

$$(3)\quad \begin{aligned} B = \{I, \pm (1 + 2^{n-1}, 2^{n-1}, 0, 1 + 2^{n-1}), &\pm (1 + 2^{n-1}, 0, 2^{n-1}, 1 + 2^{n-1}),\\ &\pm (1, 2^{n-1}, 2^{n-1}, 1)\} \end{aligned}$$

which contains neither Z_n nor any conjugate of $S^{2^{n-1}}$ and is normal in $LF(2, 2^n)$.

We wish to prove for $LF(2, 2^n)$ two results for subgroups of K_1^n, which Gierster [2] has already done for $LF(2, p^n)$, $p > 2$. For $p > 2$, an element of K_r^n has the form

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

where $0 \leq \mu, \nu, \rho < 2^{n-r}$ and $u^2 \equiv 1 + p^{2r}(\mu^2 + \nu\rho) \pmod{p^n}$ which has two solutions for u. Gierster fixed the choice of u by further assuming $u \equiv 1 \pmod{p}$ so that μ, ν, ρ determine a unique element of K_r^n. For $p = 2$,

$$u^2 \equiv 1 + 2^r(\mu^2 + \nu\rho) \pmod{2^n}$$

has four solutions for $n \geq 3$. We can restrict the choices for u to two by assuming $u \equiv 1 \pmod 4$ but the representation of an element of K_r^n depends on the choice of u as well as μ, ν and ρ. In fact,

$$\{\mu, \nu, \rho, u\} \quad \text{and} \quad \{\mu + 2^{n-r-1}, \nu, \rho, u + 2^{n-1}\}$$

determine the same element of K_r^n. For an element of K_1^n, $n \geq 3$, we also require that $\mu^2 + \nu\rho$ be even since $u^2 \equiv 1 + 4(\mu^2 + \nu\rho) \pmod{2^n}$ has a solution if and only if $1 + 4(\mu^2 + \nu\rho) \equiv 1 \pmod 8$. Further note that if U is an element of K_r^n, then U^2 is in K_{r+1}^n and so an element in $K_r^n - K_{r+1}^n$ has order exactly 2^{n-r}.

The proofs of the propositions require the following two lemmas.

LEMMA 2.1. *Suppose U_1 and U_2 are elements of K_r^n. Then $U_1^2 = U_2^2$ if and only if $U_1 = U_2 \cdot k_{n-1}$ where k_{n-1} is an element of K_{n-1}^n.*

Proof. Since $K_r^n = U_2 \cdot K_r^n$, $U_1 = U_2 \cdot k_r$ for some k_r in K_r^n. If k_r is in K_{n-1}^n, then, since K_{n-1}^n is in the center of K_1^n [4],

$$U_1^2 = U_2 k_r U_2 k_r = U_2 k_r^2 U_2 = U_2^2 .$$

Conversely suppose $U_2 k_r U_2 k_r = U_2^2$. Then $U_2 k_r = k_r^{-1} U_2$. Let

$$U_2 = \pm\, (u' + 2^r\mu', 2^r\nu', 2^r\rho', u' - 2^r\mu')$$

and

$$k_r = \pm (u + 2^t\mu, 2^t\nu, 2^t\rho, u - 2^t\mu).$$

We may assume not all of μ, ν and ρ are divisible by two since we could then factor out two and change t to $t + 1$. To show $t = n - 1$, we assume $t < n - 1$ and prove that then two divides each of μ, ν and ρ.

Since $U_2 \cdot k_r = k_r^{-1} \cdot U_2$, we have by multiplying and comparing terms:

$$(2.1) \qquad 2^t u'\mu + 2^{r+t}\mu'\mu + 2^{r+t}\nu'\rho \equiv -2^t u'\mu - 2^{t+r}\mu'\mu - 2^{t+r}\rho'\nu$$

$$(2.2) \qquad 2^t u'\rho \equiv -2^t u'\rho \qquad \pmod{2^n}$$

$$(2.3) \qquad 2^t u'\nu \equiv -2^t u'\nu$$

Congruences (2.2) and (2.3) imply that

$$2^t u'\rho \equiv 0 \pmod{2^{n-1}} \quad \text{and} \quad 2^t u'\nu \equiv 0 \pmod{2^{n-1}}$$

so that 2 divides ρ and ν since u' is odd and $t < n - 1$. Replacing ν and ρ by $2\nu_0$ and $2\rho_0$ in congruence (2.1), we have

$$2^t u'\mu + 2^{r+t}\mu'\mu + 2^{r+t}\rho'\nu_0 + 2^{r+t}\rho_0\nu' \equiv 0 \pmod{2^{n-1}}$$

or $-2^t u'\mu = 2^{r+t}\mu'\mu + 2^{r+t}\rho'\nu_0 + 2^{r+t}\nu'\rho_0 + 2^{n-1}w$ for some w. Now the right hand side of the equation is divisible by a power of two higher than t so that two divides μ which gives our contradiction.

COROLLARY 2.1. *Each element in K_r^n has 8 square roots if it has any and, by induction, has at most 2^{3t} 2^t-th roots.*

LEMMA 2.2. *Suppose U and U_1 belong to K_{n-r}^n. Then for $s \leq r - 1$, $U^{2^s} = U_1^{2^s}$ if and only if $U_1 = U \cdot k_{n-s}$ where k_{n-s} is an element of K_{n-s}^n.*

Proof. By induction on s with the case $s = 1$ being Lemma 2.1. Assume for $t < s$, $U^{2^t} = U_1^{2^t}$ if and only if $U_1 = Uk_{n-t}$. Let $U_1 = k_{n-s}U$. Then $U_1^{2^s} = (k_{n-s}U)^{2^s}$. Since K_{n-s}^n is a normal subgroup, $k_{n-s}U = Uk'_{n-s}$ for some k'_{n-s} in K_{n-s}^n. Since k_{n-s} and k'_{n-s} are conjugate, they have the same order, $2^l \leq 2^s$. Then

$$U^{-1}(k_{n-s})^{2^{l-1}}U = (k'_{n-s})^{2^{l-1}}(k_{n-s})^{2^{l-1}}$$

belongs to K_{n-1}^n which is in the center of K_{n-r}^n [4] so that $(k_{n-s})^{2^{l-1}} = (k'_{n-s})^{2^{l-1}}$. Hence by induction $k_{n-s} = k'_{n-s}k_{n-t}$ for some k_{n-t} in K_{n-t}^n where $t < s$. But then

$$k'_{n-s}k_{n-s} = (k'_{n-s})^2(k'_{n-s})^{-1}k_{n-s} = (k'_{n-s})^2 k_{n-t} = k_{n-s+1}$$

where k_{n-s+1} is in K_{n-s+1}^n. Hence

$$U_1^{2^s} = (k_{n-s}U)^{2^s} = U(k'_{n-s}k_{n-s}U^2)^{2^{s-1}}U^{-1} = U(k_{n-s+1}U^2)^{2^{s-1}}U^{-1}.$$

But by induction $(k_{n-s+1}U^2)^{2^{s-1}} = (U^2)^{2^{s-1}} = U^{2^s}$. So if $U_1 = k_{n-s}U$, $U_1^{2^s} = U^{2^s}$. On the other hand, by Corollary 2.1, U^{2^s} has at most 2^{3s} 2^s-*th* roots and there are 2^{3s} elements in $U \cdot K_{n-s}^n$; so if $U_1^{2^s} = U^{2^s}$, U_1 belongs to $U \cdot K_{n-s}^n$.

COROLLARY 2.2. *Suppose U is an element of $H \cap K_{n-r}^n$. Then U_1 is an element of $H \cap K_{n-r}^n$ and $U^{2^s} = U_1^{2^s}$, if and only if $U_1 = U \cdot k_{n-s}$ where k_{n-s} is an element of $H \cap K_{n-s}^n$.*

PROPOSITION 2.1. *If $|H \cap K_{n-1}^n| = 2$, then $H \cap K_r^n$ is cyclic of the form*

$$\{U^i\}_{i=1}^{2^s} = \{\pm\ (u_i + 2^r\xi_i\mu, 2^r\xi_i\nu, 2^r\xi_i\rho, u_i - 2^r\xi_i\mu)\}$$

where $s \leq n - r$, $U = \pm\ (u + 2^r\mu, 2^r\nu, 2^r\rho, u - 2^r\mu)$ and u_i and ξ_i are given inductively by the formulas

$$u_i \equiv u_{i-1}u + \xi_{i-1}(u^2 - 1) \quad and \quad \xi_i \equiv \xi_{i-1}u + u_{i-1}$$

both mod 2^n *with $u_1 = u$ and $\xi_1 = 1$.*

Proof. We prove $H \cap K_r^n$ is cyclic by induction. Since $H \cap K_{n-1}^n$ is cyclic, we suppose $H \cap K_{s+1}^n$ is cyclic and show $H \cap K_s^n$ is cyclic for $s \geq r$. Let $H \cap K_{s+1}^n = [U_0]$ and let U be a fixed element of $(H \cap K_s^n) - (H \cap K_{s+1}^n)$. If there are no such elements we are done as then $H \cap K_r^n = [U_0]$. Let U_1 be any other element in $(H \cap K_s^n) - (H \cap K_{s+1}^n)$. Both U^2 and U_1^2 belong to $H \cap K_{s+1}^n$ so $[U_0] = [U^2] = [U_1^2]$. So $U_1^2 = (U^2)^j = (U^j)^2$ which, by Corollary 2.2, implies that $U_1 = k_{n-1} \cdot U^j$ where k_{n-1} belongs to $H \cap K_{n-1}^n$. Also $U_0 = (U^2)^m$ for some m. Therefore $U_1 = k_{n-1} \cdot U^j = U_0^l U^j = U^{2ml} \cdot U^j$. So U_1 is in $[U]$. Clearly any element of $H \cap K_{s+1}^n$ is in $[U]$ since U_0 is. So $H \cap K_s^n = [U]$ which has order less than or equal to 2^{n-s}.

Finally suppose we fix a representation of

$$U = \pm (u + 2^r\mu, 2^r\nu, 2^r\rho, u - 2^r\mu)$$

and suppose $U^i = \pm (u_i + 2^r\xi_i\mu, 2^r\xi_i\nu, 2^r\xi_i\rho, u - 2^r\xi_i\mu)$. Then

$$U^{i+1} = U^iU = \pm (u_iu + \xi_i(u^2 - 1) + 2^r(\xi_iu + u_i)\mu, 2^r\nu(u_i + \xi_iu),$$
$$2^r\rho(u_i + \xi_iu), u_iu + \xi_i(u^2 - 1) - 2^r(\xi_iu + u_i)\mu)$$

and we are done.

PROPOSITION 2.2. *If $|H \cap K_{n-1}^n| = 4$, then $H \cap K_r^n$ is generated by two elements U_1 and U_2 of orders 2^{n-t} and 2^{n-s} respectively where $s \geq t \geq r$. Further*

$$H \cap K_{n-r}^n = \{U_1{}^iU_2{}^j\}, \quad 1 \leq i \leq 2^{n-t}, \quad 1 \leq j \leq 2^{n-s},$$

so that $|H \cap K_{n-r}^n| = 2^{2n-t-s} \leq 2^{2n-2r}$.

Proof. We first show that $|H \cap K_r^n| \leq 2^{2n-2r}$. This is true for $r = n - 1$ so we assume that, for $x > r$, $|H \cap K_x^n| \leq 2^{2n-2x}$ and show that $|H \cap K_{x-1}^n| \leq 2^{2n-2x+2}$. By Lemma 2.1 and the fact that $|H \cap K_{n-1}^n| = 4$, if U is an element of $H \cap K_{x-1}^n$, there are four elements in $H \cap K_{x-1}^n$ which square to U^2. Since $|H \cap K_x^n| \leq 2^{2n-2x}$, there are at most 2^{2n-2x} possibilities for U^2. Hence there are at most $4 \cdot 2^{2n-2x} = 2^{2n-2x+2}$ elements in $H \cap K_{x-1}^n$.

Let 2^{n-t} be the maximum of the orders of elements in $H \cap K_r^n$, let U_1 be an element of order 2^{n-t} in $H \cap K_r^n$ and note that $t \geq r$. Then $H_1 = H \cap K_r^n$ is contained in K_t^n and so $|H_1| \leq 2^{2n-2t}$. $U_1^{2^{n-t-1}}$ is an element of $H \cap K_{n-1}^n$. Let $V = \{U' \mid U'$ is in $H \cap K_r^n$ and $U'^m = U_1^{2^{n-t-1}}$ for some $m\}$. Then $H_1 - V$ is non-empty since $|H \cap K_{n-1}^n| = 4$ and so $(H_1 - V) \cap (H \cap K_{n-1}^n)$ has two elements in it. Let 2^{n-s} be the maximum of the orders of elements in $H_1 - V$, let U_2 be an element of order 2^{n-s} in $H_1 - V$ and note that $s \geq t \geq r$. Since $U_1^i \neq U_2^j$ for $1 \leq i \leq 2^{n-t}, 1 \leq j \leq 2^{n-s}$, the set $\{U_1^iU_2^j\}$ has 2^{2n-t-s} elements in it and is contained in H_1. On the other hand, $V \cup (H \cap K_s^n)$ is all of H_1. By the first part of the proof $|H \cap K_s^n| \leq 2^{2n-2s}$. But the set $\{U_1^{li}U_2^j\}$ where $l = 2^{s-t}$, $1 \leq i, j \leq 2^{n-s}$, contains 2^{2n-2s} elements all belonging to $H \cap K_s^n$. So $|H \cap K_s^n| = 2^{2n-2s}$. By Corollary 2.2 and choice of s,

$$V \cap (K_{s-1}^n - K_s^n) = U_1^{2s-t-1} \cdot (H \cap K_s^n)$$

which has order 2^{2n-2s}. So $|H \cap K_{s-1}^n| = 2^{2n-2s} + 2^{2n-2s}$. In general,

$$V \cap (K_{s-q}^n - K_{s-(q-1)}^n) = U_1^{2^{s-t-q}} \cdot (H \cap K_{s-(q-1)}^n)$$

which has order $= | H \cap K^n_{s-(q-1)} |$. Hence

$$| H | = | K^n_s | + | V \cap (K^n_t - K^n_s) | = 2^{2n-2s} + 2^{2n-2s}\left(\textstyle\sum_{i=0}^{s-t-1} 2^i\right) = 2^{2n-s-t}$$

which is the order of $\{ U_1^i U_2^j \}$. So $H = \{ U_1^i U_2^j \}$.

3. Conjugates of S, T, and R

Unless otherwise indicated, by a conjugate of S, T, or R we mean aSa^{-1}, aTa^{-1} or aRa^{-1} where a is in $LF(2, 2^n)$. To calculate W for a given H, we are interested in how many groups conjugate to S^{2^r} belong to H. A conjugate of $\pm(1, 2^r, 0, 1)$ has the form

$$\pm(a, \ b, \ c, \ d)\cdot\pm(1, \ 2^r, \ 0, \ 1)\cdot\pm(d, \ -b, \ -c, \ a)$$
$$= \pm(1 - 2^r ac, 2^r a^2, -2^r c^2, 1 + 2^r ac).$$

Since $ad - bc \equiv 1 \pmod{2^n}$ both a and c cannot be even. The group generated by $\pm(1 - 2^r ac, 2^r a^2, -2^r c^2, 1 + 2^r ac)$ is

$$\{\pm(1 - 2^r tac, 2^r ta^2, -2^r tc^2, 1 + 2^r tac), 0 \le t \le 2^r - 1\}.$$

Thus if a is odd, any other conjugate of S^{2^r} generating the same group also has a odd. From [1], to obtain the number of subgroups of H conjugate to S^{2^r} for which a is odd, it is sufficient to count the number of elements in H of the form

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

i.e. we set $a = 1$. For each r, there are 2^{n-r} such elements and so there are $\sum_{r=0}^{n-1} 2^{n-r} = 2^{n+1} - 2$ such elements in $LF(2, 2^n)$. Similarly if a is even, c has to be odd and to count the number of groups conjugate to S^{2^r} generated by such elements we can set $c = 1$. For each r, there are 2^{n-r-1} such elements and so $\sum_{r=0}^{n-1} 2^{n-r-1} = 2^n - 1$ such elements are in $LF(2, 2^n)$. So for $LF(2, 2^n)$,

$$W = 2^{n+1} - 2 + 2^n - 1 = 3(2^n - 1).$$

Note that if U is conjugate to S^{2^r}, then U^2 is conjugate to $S^{2^{r+1}}$.

LEMMA 3.1. *Suppose U is conjugate to S^{2^r}. Then U_1 is conjugate to S^{2^r} and $U_1^2 = U^2$ if and only if $U_1 = Z_n \cdot U$.*

Proof. Suppose $U = \pm(1 - 2^r ac, 2^r a^2, -2^r c^2, 1 + 2^r ac)$. Then

$$U\cdot Z_n = \pm(1 - 2^r ac + 2^{n-1}, 2^r a^2, -2^r c^2, 1 + 2^r ac + 2^{n-1}).$$

If a is odd, set $\alpha = a$ and $\gamma = c + 2^{n-r-1}$; if a is even, c is odd and set $\gamma = c$ and $\alpha = a + 2^{n-r-1}$. In either case we see that

$$U\cdot Z_n = \pm(1 - 2^r \alpha\gamma, 2^r \alpha^2, -2^r \gamma^2, 1 + 2^r \alpha\gamma)$$

and is conjugate to S^{2^r}. Further $U^2 = U_1^2$ since Z_n is in the center of

$LF(2, 2^n)$. On the other hand, if

$$A = \pm(1 - 2^{r+1}ac, 2^{r+1}a^2, -2^{r+1}c^2, 1 + 2^{r+1}ac)$$

is conjugate to $S^{2^{r+1}}$, then $U = \pm(1 - 2^r ac, 2^r a^2, -2^r c^2, 1 + 2^r ac)$ is conjugate to S^{2^r} and $U^2 = A$. But then $U \cdot Z_n$ is also conjugate to S^{2^r} and $(U \cdot Z_n)^2 = A$. So each conjugate of $S^{2^{r+1}}$, $r \geq 0$, has at least two square roots conjugate to S^{2^r}. Since K^n_{n-1} has three conjugates of $S^{2^{n-1}}$, if any conjugate of $S^{2^{r+1}}$ had more than two square roots conjugate to S^{2^r}, W would be greater than $3(2^n - 1)$, a contradiction.

COROLLARY 3.1. *$s(2^r)$ = the number of groups conjugate to $S^{2^r} = 3 \cdot 2^{n-r-1}$.*

Next we calculate t = number of conjugates of T and $\tau(n)$ for $LF(2, 2^n)$ and obtain some information about conjugates of T. Let $E' = K^n_1 \cdot [T]$ which is one of the three conjugate Sylow 2-groups in $LF(2, 2^n)$. So $t = 3t'$ where t' is the number of conjugates of T in E'. Note that a conjugate of T has the form

$$\pm\ (ac + bd, -b^2 - a^2, c^2 + d^2, -ac - bd)$$

and so has trace 0.

LEMMA 3.2. *In $LF(2, 2^n)$, $t = 3 \cdot 2^{2n-3}$ and $\tau(2^n) = 2^n$.*

Proof. Since E' contains K^n_1,

$$0 = g(E') = 1 + [2^{2n-3}(2^n - 6) - t'\tau(n) - 2^{2n-2}(3 \cdot (2^{n-1} - 1) + 2^{n-1})]/4 \cdot 2^{3n-3}$$

so that $t'\tau(n) = 2^{3n-3}$. By writing down the elements one sees that, in $LF(2, 4)$, E' has two conjugates of T. Let

$$\varphi\colon LF(2, 2^n) \to LF(2, 2^{n-1})$$

be the natural homomorphism with kernel K^n_{n-1}. If T in $LF(2, 2^{n-1})$ has precisely four pre-images under φ which are conjugate to T in $LF(2, 2^n)$, then any conjugate of T in $LF(2, 2^{n-1})$ has precisely four pre-images conjugate to T in $LF(2, 2^n)$. Using the fact conjugates of T have the form

$$\pm\ (ac + bd, -b^2 - a^2, c^2 + d^2, -ac - bd),$$

we calculate that T in $LF(2, 4)$ has precisely four pre-images in $LF(2, 8)$ so that $t' = 8 = 2^{2n-3}$ for $LF(2, 8)$. In general, for $n \geq 4$, the kernel of

$$\varphi = \{\pm\ (1 + 2^{n-1}\alpha, 2^{n-1}\beta, 2^{n-1}\gamma, 1 + 2^{n-1}\alpha), 0 \leq \alpha, \beta, \gamma \leq 1\}.$$

Then the elements U in $LF(2, 2^n)$ such that $\varphi(U) = T$ in $LF(2, 2^{n-1})$ are given by

$$K^n_{n-1} \cdot T = \{\pm\ (2^{n-1}\beta, -1 + 2^{n-1}\alpha, 1 + 2^{n-1}\alpha, 2^{n-1}\gamma)\}.$$

Since conjugates of T have trace 0, for an element of $K^n_{n-1} \cdot T$ to be conjugate to T, it is necessary that $\beta = \gamma$. To see that the four elements of $K_{n-1}^n \cdot T$ with $\beta = \gamma$ are actually conjugate to T we need a, b, c and d which simultaneously satisfy

$$c^2 + d^2 \equiv 1 + 2^{n-1}\alpha, \tag{3.1}$$

$$a^2 + b^2 \equiv 1 + 2^{n-1}\alpha, \tag{3.2}$$

$$ac + bd \equiv 2^{n-1}\beta, \tag{3.3}$$

$$ad - bc \equiv 1, \tag{3.4}$$

all mod 2^n. Since $n \geq 4$, let u be a solution to

$$x^2 \equiv 1 + 2^{n-1} \pmod{2^n}.$$

If $\alpha = \beta = 0$, let $c = b = 0$, and $a = d = 1$; if $\alpha = 0$, $\beta = 1$, let $a = 2^{n-1}$, $c = -1$, $b = 1$, $d = 0$; if $\alpha = 1$, $\beta = 0$, let $c = b = 0$, $a = u$ and $d = u + 2^{n-1}$; if $\alpha = \beta = 1$, let $b = 0$, $c = 2^{n-1}$, $d = u$ and $a = u + 2^{n-1}$. We then see that T has four conjugates in $LF(2, 2^n)$ which reduce to T in $LF(2, 2^{n-1})$. Hence, by induction, $t' = 4 \cdot 2^{2(n-1)-3} = 2^{2n-3}$ in $LF(2, 2^n)$. So $t = 3 \cdot t' = 3 \cdot 2^{2n-3}$ and $\tau(n) = 2^{3n-3}/t' = 2^n$.

LEMMA 3.3. *For $n \geq 2$, an element of E' or any of its conjugates has trace 0 if and only if it is conjugate to T.*

Proof. We have seen that a conjugate of T has trace 0. An element of K_1^n has trace $2u \not\equiv 0$ since u is odd. So the only elements with trace 0 in E' are in the set

$$K_1^n \cdot T = \{\pm\ (-2\nu, u + 2\mu, -\ (u - 2\mu), 2\rho)\}.$$

So an element in E' has trace 0 if and only if $\nu = \rho$ which implies there are $2^{n-1} \cdot 2^{n-1}/2 = 2^{2n-3}$ such elements. But E' contains 2^{2n-3} conjugates of T all of which have trace 0 and hence these are the only elements of E' with trace 0. If A, an element of one of the conjugates of E', has trace 0, then since conjugation preserves traces, A is conjugate to an element in E' with trace 0 and so is conjugate to T.

From the proof of this lemma, we see that, if

$$U = \pm\ (u + 2\mu, 2\nu, 2\rho, u - 2\mu),$$

then $U \cdot T$ has order two if and only if $\nu = \rho$. Furthermore, by multiplying and comparing entries, we see first that if U has $\nu = \rho$ so does U^2 and second that if U has $\nu = \rho$ so does $d \cdot U$ where d is in

$$\{I, Z_n, \pm\ (1, 2^{n-1}, 2^{n-1}, 1), \pm\ (1 + 2^{n-1}, 2^{n-1}, 2^{n-1}, 1 + 2^{n-1})\} = D'$$

which is conjugate to D. Finally $(d \cdot U)^2 = U^2$ so that, if an element of K_1^n has one square root with $\nu = \rho$, it has precisely four.

Finally we obtain some information about conjugates of R in $LF(2, 2^n)$ and calculate $r =$ the number of conjugates of R and $\rho(n)$ for $LF(2, 2^n)$.

LEMMA 3.4. *An element of $LF(2, 2^n)$ is conjugate to R if and only if it has order 3 if and only if it has trace 1.*

Proof. R has order three and all elements of $LF(2, 2^n)$ of order three are conjugate by Sylow. Since R has trace 1 and conjugation preserves traces, all conjugates of R have trace 1. On the other hand, if an element has trace 1, it has the form $\pm\ (a, b, c, 1 - a)$ where $a - a^2 - bc \equiv 1 \pmod{2^n}$ which has order three and hence is conjugate to R.

LEMMA 3.5. $\rho(n) = 3\cdot 2^{n-1}$ *and* $r = 2^{2n-2}$ *for* $LF(2, 2^n)$.

Proof. Let $H = K_1^n\cdot[R]$ which is normal in $LF(2, 2^n)$ and so contains all the conjugates of R.

$$0 = g(H) = 1 + [3(2^n - 6)\cdot 2^{2n-5} - 9\cdot 2^{2n-4}(2^{n-1} - 1) - \rho(n)\cdot r]/9\cdot 2^{3n-4}$$

so that $\rho(n)\cdot r = 3\cdot 2^{3n-3}$. Arguing as in Lemma 3.2, there are eight elements of trace 1 in $LF(2, 4)$ and R, in $LF(2, 2^s)$, $s < n$, has four pre-images in $LF(2, 2^{s+1})$ which have trace 1 and which are given by $B\cdot R$ in $LF(2, 2^{s+1})$. So we see that $LF(2, 2^n)$ contains 2^{2n-1} elements of trace 1 and therefore $r = 2^{2n-2}$. This implies that $\rho(n) = 3\cdot 2^{n-1}$.

4. Subgroups of genus 0

Since $LF(2, 4)$ has genus 0 [3], we can restrict our attention to $LF(2, 2^n)$ for $n \geq 3$.

PROPOSITION 4.1. *Suppose* $|H \cap K_{n-1}^n| = 1$ *and* $n \geq 4$. *Then* $g(H) > 0$.

Proof. Since $|H \cap K_1^n| = 1$, $|H| \leq 6$ and $W = 0$. So

$$g(H) \geq 1 + (2^{3n-2} - 3\cdot 2^{2n-1} - 2^{n+2} - 3\cdot 2^{n+1})/48 > 0$$

for $n \geq 4$.

LEMMA 4.1. (a) *If* $|H \cap K_{n-1}^n| = 2$, *then* $r \leq 2^{n-1}$.
(b) *If* $|H \cap K_{n-1}^n| = 4$ *and* $H \cap K_{n-1}^n \neq B$ *then* $r = 0$.

Proof. Suppose $r \neq 0$ and conjugate H so that R is an element of H.
(a) Any element of order three in $LF(2, 2^n)$ is in $K_1^n\cdot[R]$. Thus any element of order three in H is in $(H \cap K_1^n)\cdot[R]$.
But $|H \cap K_1^n| \leq 2^{n-1}$ and so the number of groups of order three is bounded by 2^{n-1}.
(b) Let

$$S_1 = S^{2^{n-1}}, \qquad S_2 = \pm\ (1 + 2^{n-1}, 2^{n-1}, 2^{n-1}, 1 + 2^{n-1}),$$

$$S_3 = \pm\ (1, 0, 2^{n-1}, 1)$$

denote the three conjugates of $S^{2^{n-1}}$ in K_{n-1}^n. Then $S_1\cdot R = R\cdot S_2$, $S_3\cdot R = R\cdot S_1$ and $S_2\cdot R = R\cdot S_3$. Since $|H \cap K_{n-1}^n| = 4$ and $H \cap K_{n-1}^n \neq B$, at least one of S_1, S_2 and S_3 is in H. But then since R is in H, the above equalities show that S_1, S_2 and S_3 all are in H and so $H \cap K_{n-1}^n = K_{n-1}^n$ which is a contradiction. Therefore $r = 0$.

COROLLARY 4.1. *If* $|H \cap K_{n-1}^n| = 4$ *and* $H \cap K_{n-1}^n \neq B$, *then* $|H| = 2^l$ *for some* l.

Proof. Since $r = 0$, there are no elements of order 3 in H and so 3 does not divide $|H|$.

Suppose $|H| = 3 \cdot 2^l$ and that P_1, P_2 and P_3 are the three Sylow 2-groups of $LF(2, 2^n)$. If $|H \cap K_1^n| = 2^{l-1}$, then $|H \cap P_i|, i = 1, 2, 3, = 2^l$. This can be seen by observing that

$$H = (\cup_{i=1}^3 (H \cap P_i)) \cup (H \cap E)$$

where $E = K_1^n \cdot [R]$ and then counting elements. So H has three Sylow groups, $H \cap P_i$, $i = 1, 2, 3$, which are conjugate in H. Each of these contains the same number of conjugates in $LF(2, 2^n)$ of T since $T' = bTb^{-1}$ for b in $LF(2, 2^n)$ if and only if trace $T' = 0$. But conjugation, whether by elements of H or $LF(2, 2^n)$, preserves traces. So if $T_1, \cdots, T_m$ are the conjugates in $LF(2, 2^n)$ of T which are in $H \cap P_1$ and $a(H \cap P_1)a^{-1} = H \cap P_2$ where a is in H, then aT_ia^{-1} are precisely the elements of $H \cap P_2$ of trace 0, i.e. the conjugates in $LF(2, 2^n)$ of T which are in $H \cap P_2$. Similarly for $H \cap P_3$.

LEMMA 4.2. *Suppose* $|H \cap K_{n-1}^n| = 2$. *If* 3 *does not divide* $|H|$, $t \leq 2^{n-1}$; *if* 3 *divides* $|H|$, $t \leq 3 \cdot 2^{n-1}$.

Proof. If $t \neq 0$, conjugate H so that T is in H. Since $|H \cap K_{n-1}^n| = 2$, $H \cap K_1^n$ is cyclic of order bounded by 2^{n-1} and the set $(H \cap K_1^n) \cdot T$ also has order bounded by 2^{n-1}. Now if $|H| = 2^k$, then $H = (H \cap K_1^n) \cdot [T]$ and since no conjugate of T belongs to K_1^n, all the conjugates of T in H are in $(H \cap K_1^n) \cdot T$. So $t \leq 2^{n-1}$. If $|H| = 3.2^k$, then H has three conjugate subgroups of order 2^k each containing the same number of conjugates of T. So $t \leq 3 \cdot 2^{n-1}$.

PROPOSITION 4.2. *Suppose T is an element of H and* $|H \cap K_{n-1}^n| = 4$. *Suppose* $|H| = 2^k$. *If* $H \cap K_{n-1}^n \neq D'$, *then* $t \leq 2^{n-1}$; *if* $H \cap K_1^n = D'$, *then*

$$t \leq 2^{n-1} + 2^n(n - s - r + 1)$$

where $|H \cap K_1^n| = 2^{2n-s-r}$. *Suppose* $|H| = 3 \cdot 2^k$. *Then* $t \leq 3 \cdot 2^{n-1}$ *or* $3 \cdot (2^{n-1} + 2^n(n - s - r + 1))$ *depending on whether* $H \cap K_{n-1}^n \neq D'$ *or* $= D'$.

Proof. If $|H| = 3 \cdot 2^k$, it contains three conjugate subgroups of order 2^k all containing the same number of elements conjugate to T. So we only have to consider H with order 2^k containing T.

By the remark following Lemma 3.3, to compute t, it is sufficient to count the number of elements U in $H \cap K_1^n$ with $\nu = \rho$. If $H \cap K_1^n \neq D'$, then $H \cap K_{n-1}^n$ has at most one non-identity element with $\nu = \rho$ and so, again by the remarks after Lemma 3.3, $H \cap K^n_{n-r}$ has at most 2^r elements with $\nu = \rho$. So $t \leq 2^{n-1}$.

Suppose now that $H \cap K^n_{n-1} = D'$ and that r is the smallest number such that $H \cap K^n_r$ contains an element with $\nu = \rho$. By Propositions 2.1 and 2.2, $H \cap K^n_r$ has the form

$$\begin{aligned}\{U_1^i U_2^j\} = \{\pm(&u_i u_j' + 2^r \xi_i \mu u_j' + 2^s \xi_j \mu' u_i + 2^{r+s} \xi_i \xi_j (\mu\mu' + \nu\rho'),\\ &2^s \xi_j \nu' u_i + 2^r \xi_i \nu u_j' + 2^{r+s} \xi_i \xi_j (\mu\nu' - \mu'\nu),\\ &2^r \xi_i \rho u_j' + 2^s \xi_j \rho' u_i + 2^{r+s} \xi_i \xi_j (\rho\mu' - \rho'\mu),\\ &u_i u_j' - 2^r \xi_i \mu u_j' - 2^s \xi_j \mu' u_i + 2^{r+s} \xi_i \xi_j (\mu\mu' + \nu'\rho))\}\end{aligned}$$

where

$U_1 = \pm(u + 2^r\mu, 2^r\nu, 2^r\rho, u - 2^r\mu)$, $U_2 = \pm(u' + 2^s\mu', 2^s\nu', 2^s\rho', u' - 2^s\mu')$,

$s > r$, $1 \leq \xi_i \leq 2^{n-r}$, $1 \leq \xi_j \leq 2^{n-s}$ and $2^{n-r-x-1}$ of the ξ_i and $2^{n-s-x-1}$ of the ξ_j are divisible by precisely 2^x since the ξ_i and ξ_j determine which K^n_l U_1^i and U_2^j belong to. By the choice of r, to calculate t, it is sufficient to consider $H \cap K^n_r$ rather than $H \cap K^n_1$.

Suppose both U_1 and U_2 have $\nu = \rho$. We want the number of elements in $\{U_1^i U_2^j\}$ such that

$$\begin{aligned}&2^r \xi_i \nu u_j' + 2^s \xi_j \nu' u_i + 2^{r+s} \xi_i \xi_j (\nu\mu' - \nu'\mu)\\ &\qquad \equiv 2^s \xi_j \nu' u_i + 2^r \xi_i \nu u_j' + 2^{r+s} \xi_i \xi_j (\mu\nu' - \mu'\nu) \pmod{2^n}\end{aligned}$$

which is satisfied if and only if $\xi_i \xi_j (\nu\mu') \equiv \xi_i \xi_j (\mu\nu') \pmod{2^{n-r-s-1}}$. Now using the fact that $\rho = \nu$ and $\rho' = \nu'$ and the observation that if $\mu \equiv \mu'$, $\nu \equiv \nu'$ and $\rho \equiv \rho'$ all mod 2, then $U_1^{2^{n-r-1}} = U_2^{2^{n-s-1}}$, one calculates that $\nu\mu' \not\equiv \mu\nu' \pmod 2$. So

$$\xi_i \xi_j (\nu\mu' - \mu\nu') \equiv 0 \pmod{2^{n-r-s-1}}$$

if and only if $\xi_i \xi_j \equiv 0 \pmod{2^{n-r-s-1}}$. If $2^{n-r-x} \| \xi_i$ where $0 \leq x \leq s - 1$, there are 2^{x-1} choices for ξ_i if $x > 0$ and one choice if $x = 0$. Then ξ_j can be chosen arbitrarily so there are 2^{n-s} choices for ξ_j. If $2^{n-r-x} \| \xi_i$ where $s \leq x \leq n - r$, there are 2^{x-1} choices for ξ_i and 2^{n-x+1} choices for ξ_j since 2^{x-s-1} has to divide ξ_j. So

$$t = 2^{n-s} + 2^{n-s} \textstyle\sum_{i=1}^{s-1} 2^{i-1} + \sum_{i=s}^{n-r} 2^n = 2^{n-1} + 2^n(n - r - s + 1).$$

Suppose U_2 does not have $\nu = \rho$. We want the number of elements such that

$$2^s \xi_j \nu' u_i + 2^{r+s} \xi_i \xi_j (\mu\nu' - \nu\mu') \equiv 2^s \xi_j \rho' u_i + 2^{r+s} \xi_i \xi_j (\nu\mu' - \rho'\mu) \pmod{2^n}$$

which holds if and only if

$$2^s \xi_j u_i (\nu' - \rho') + 2^{r+s}(\xi_i \xi_j)\zeta \equiv 0 \pmod{2^n}$$

where $\zeta = \mu(\nu' + \rho') = 2\mu'\nu$. Let $2^x \| \nu' - \rho'$. If $x = 0$, there are no solutions unless 2^{n-s} divides ξ_j in which case there are at most 2^{n-r} such elements; if $x = 1$, there are no solutions unless 2^{n-s-1} divides ξ_j in which case there are at most 2^{n-r+1} such elements. Suppose $x \geq 2$. If ν', ρ' and μ are even and μ' and ν are odd, then 4 divides $\mu(\nu' + \rho')$ and 2 precisely divides $2\nu\mu'$ so that $2 \,\|\, \zeta$. Considering the other possible combinations for μ, ν, μ', ν' and ρ' in the same way we see that if $x \geq 2$, $2 \,\|\, \zeta$. So, if $x \geq 2$, we want the number of elements such that

$$2^{s+x}\xi_j u_i y + 2^{r+s+1}\xi_i \xi_j \zeta' \equiv 0 \pmod{2^n} \tag{4.1}$$

where y, ζ' are odd. Clearly $x \leq n - s$. We can assume that $r + s < n$ since otherwise the number of elements in $\{U_1^i U_2^j\}$ is bounded by 2^n so that $t \leq 2^n$. If $x < r + 1$, then 2^{n-s-x} has to divide ξ_j and so one has less than or equal to $2^x \cdot 2^{n-r} \leq 2^n$ elements of the type desired. So we can assume $r + 1 \leq x \leq n - s$. Let $2^l \,\|\, \xi_j$ where $0 \leq l \leq n - s$. For each l, $0 \leq l < n - s - r - 1$, there are at most 2^n elements of the type desired since there are at most $2^{n-s-l-1}$ choices for ξ_j and for each choice of ξ_j there are

$$2^{n-r-(n-r-s-l-1)} = 2^{s+l+1}$$

choices for ξ_i because in these cases congruence (4.1) becomes

$$2^{x-r-1}y' + \xi_i'\zeta'' \equiv 0 \pmod{2^{n-s-l-r-1}}$$

with y' and ζ'' odd. For each l, $n - s - r - 1 \leq l \leq n - s - 1$, there are $2^{n-s-1-l}$ choices for ξ_j and 2^{n-r} choices for ξ_i for each ξ_j. Finally for $l = n - s$, there is one choice for ξ_j and 2^{n-r} choices for ξ_i. So the total number of elements of the type desired is bounded by

$$\begin{aligned}(n - s - r - 1)2^n + 2^{n-r} + \textstyle\sum_{l=n-s-r-1}^{n-s-1} 2^{2n-s-r-1-l} \\ &= (n - s - r - 1)2^n + 2^{n-r} + 2^{\,n-r-1} \textstyle\sum_{i=1}^{r+1} 2^i \\ &= 2^n(n - s - r + 1).\end{aligned}$$

LEMMA 4.3. *If* $|H \cap K_{n-1}^n| = 2$, $W \leq n$.

Proof. By Proposition 2.1, $H \cap K_{n-r}^n$ is cyclic. So for $n - r \neq 0$, $s(2^{n-r}) \leq 1$ and therefore $W \leq n - 1 + s(1)$. If Z_n is not an element of H then, from Lemma 3.1 and the fact that $H \cap K_1^n$ is cyclic, there can be at most one group conjugate to S in H. If Z_n is in H, $W = 0$. So, in any case, $W \leq n$.

LEMMA 4.4. *If* $H \cap K_{n-1}^n$ *is conjugate to* C, *then* $W \leq 2n$.

Proof. Note that Z_n does not belong to H. Hence given U in H conjugate to $S^{2^{n-r+1}}$, Lemma 3.1 implies that at most one of its square roots which are conjugate to $S^{2^{n-r}}$ belongs to H. So, arguing by induction, we see that, in passing from conjugates of $[S^{2^{n-r+1}}]$ to conjugates of $[S^{2^{n-r}}]$ we add at most two conjugates of $[S^{2^{n-r}}]$. So $W \leq 2n$.

PROPOSITION 4.3. *If $H \cap K_{n-1}^n$ is conjugate to D,*

$$W \leq 2^{(n+1)/3} + 2^{2n/3+5/3} - 3.$$

Proof. Recall that a conjugate of S^{2^r} has the form

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

and that for computing $s(2^r)$ the relevant conjugates of S^{2^r} are the ones with $a = 1$; so we restrict our attention to these conjugates of S^{2^r}. By conjugating H, assume that $H \cap K_{n-1}^n = D$ and that $H \cap K_1^n$ has as many conjugates of S^{2^r}, $1 \leq r \leq n-1$, with zero in the lower left corner as possible. If H can be conjugated so that all the conjugates of S^{2^r}, $1 \leq r \leq n-1$, have this form, then if n is even,

$$W \leq 1 + 2^{(n/2)+1} + 2\sum_{i=1}^{(n/2)-1} 2^i = 2^{(n/2)+2} - 3;$$

if n is odd,

$$W \leq 1 + 2^{(n+1)/2} + 2\sum_{i=1}^{(n-1)/2} 2^i = 3 \cdot 2^{(n+1)/2} - 3.$$

Since $n \geq 2$, $W < 2^{(n+1)/3} + 2^{2n/3+5/3} - 3$.

If not, let m be the smallest integer such that $2^{n-m}c_0^2 \not\equiv 0 \pmod{2^n}$ for some c_0 and suppose $m \leq 2n/3 - 1/3$. Since m has the property that

$$2^{n-m}c_0^2 \not\equiv 0 \pmod{2^n} \quad \text{and} \quad 2^{n-(m-1)}c_0^2 \equiv 0 \pmod{2^n},$$

$c_0^2 \equiv 0 \pmod{2^{m-1}}$ and $c_0^2 \not\equiv 0 \pmod{2^m}$ so that $2^{m-1} \| c_0^2$ implying that m is odd. Now

$$\begin{aligned}
&\pm(1 + 2^{n-m}c_0, 2^{n-m}, -2^{n-m}c_0^2, 1 - 2^{n-m}c_0)^{2^{m-1}-1} \\
&= \pm(1 - 2^{n-m}c_0, 2^{n-1} - 2^{n-m}, 2^{n-m}c_0^2, 1 + 2^{n-m}c_0) \\
&= S'
\end{aligned}$$

is in H. By the second statement of the proof, we may assume that H contains $S^{2^{n-m}}$. So H contains

$$\begin{aligned}
S' \cdot S^{2^{n-m}} &= \pm(1 - 2^{n-m}c_0, -2^{2n-2m}c_0 + 2^{n-1}, 2^{n-m}c_0^2, 1 + 2^{2n-2m}c_0^2 + 2^{n-m}c_0) \\
&= \pm(1 - 2^{n-s}x, 2^{n-1}, 2^{n-1}, 1 + 2^{n-s}x)
\end{aligned}$$

where x is odd and $1 \leq s = (m+1)/2 \leq n/3 + 1/3$. The last equality is obtained by factoring the highest power of two out of c_0 and c_0^2 and observing that $m \leq 2n/3 - 1/3$ implies that $2n - 2m + (m-1)/2 \geq n$. Taking powers of

$$\pm(1 - 2^{n-s}x, 2^{n-1}, 2^{n-1}, 1 + 2^{n-s}x),$$

we get $U' = \pm(1 - 2^{n-s}, 2^{n-1}, 2^{n-1}, 1 + 2^{n-s})$ is in H.

Now suppose U and V are conjugates of $S^{2^{n-r}}$ such that $U^{2^s} = V^{2^s}$ and s is the smallest integer for which this is true. Then

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

and

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

with $\gamma = c - 2^{r-s}$. Let

$$\tfrac{2}{3}n - \tfrac{1}{3} \geq r \geq m + 1 > (m + 1)/2 = s.$$

If U and V belong to H, so does

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

Further note that $2^{s-1} = 2^{(m-1)/2}$ divides c since if not, let $2^t \| c$ with $t < (m - 1)/2$ and let $x = r - (m - 1)$. Since U is conjugate to $S^{2^{n-r}}$, U^{2^x} is conjugate to $S^{2^{n-r+x}}$ and the lower left corner of

$$U^{2^x} = -2^{n-(m-1)}c^2 \equiv 2^{n-(m-1)+2t}y \not\equiv 0 \pmod{2^n}$$

where y is odd. But this contradicts the choice of m. Set $k = 2^{r-1} - 1$. Then

$$\begin{aligned} &2^{n-r}(c + k\gamma) + 2^{2n-2r}k\gamma(c - \gamma) \\ &\quad\equiv 2^{n-r}(c + 2^{r-1}c - c + 2^{r+s}) + 2^{2n-2r}(2^{r-1} - 1)(c - 2^{r-s})2^{r-s} \\ &\quad\equiv 2^{n-s} \pmod{2^n} \end{aligned}$$

since $r \leq \frac{2}{3}n - \frac{1}{3}$, $s < r/2$ and 2 divides c.

$$\begin{aligned} &-2^{n-r}(c^2 + k\gamma^2) - 2^{2n-2r}kc\gamma(c - \gamma) \\ &\quad\equiv -2^{n-r}(c^2 + (2^{r-1} - 1)(c - 2^{r-s})^2) - 2^{2n-2r}(2^{r-1} - 1)(c^2 - 2^{r-s}c)2^{r-s} \\ &\quad\equiv 0 \pmod{2^n} \end{aligned}$$

since $r \leq \frac{2}{3}n - \frac{1}{3}$, $s < r/2$ and 2^{s-1} divides c.

$$2^{n-r}(k + 1) + 2^{2n-2r}k(c - \gamma) \equiv 2^{n-1} \pmod{2^n}.$$

So $U\cdot V^k = \pm(1 + 2^{n-s}, 2^{n-1}, 0, 1 - 2^{n-s})$. But then

$$U'\cdot U\cdot V^k = \pm(1, 0, 2^{n-1}, 1)$$

is in H contradicting the fact that $H \cap K^n_{n-1} = D$. So any two conjugates of $S^{2^{n-r}}$ where $\frac{2}{3}n - \frac{1}{3} \geq r \geq m$ whose 2^s-*th* powers are the smallest powers which are equal can not both belong to H.

For the rest of the proof, the phrase "at the *r-th* level" will mean in $K^n_{n-r} - K^n_{n-(r-1)}$. At the $(m - 1)$-*th* level, all conjugates of $S^{2^{n-(m-1)}}$ have zero in the lower left corner so that there are at most 2^{s-1} conjugates of $S^{2^{n-(m-1)}}$ in H. At the *m-th* level, there are at most 2^s conjugates of $S^{2^{n-m}}$ since each conjugate of $S^{2^{n-(m-1)}}$ has at most two square roots which are conjugate to $S^{2^{n-m}}$. For each of these 2^{s-1} divides c and all 2^s powers are equal. At the $(m+1)$-*th* level, there are at most $2\cdot 2^s$ conjugates of $S^{2^{n-(m+1)}}$, 2^{s-1} divides c and all 2^{s+1} powers are equal. So there are at most two elements in the set of 2^s powers and each has at most 2^s 2^s-*th* roots from the $(m+1)$-*th* level. From each of these two disjoint collections of 2^s-*th* roots, whose union is all the conjugates of $S^{2^{n-(m+1)}}$, at most 2^{s-1} 2^s-*th* roots can be in H since, if U given by c is in H, U' given by $c - 2^{r-s}$ can not be in H. So the $(m+1)$-*th* level has at most 2^s conjugates of $S^{2^{n-(m+1)}}$.

Now each of the two sets of 2^s-*th* roots at the $(m+1)$-*th* level can give at most one 2^{s-1} power since otherwise H will contain elements whose 2^s-*th* powers are the first ones equal. So there are at most two elements in the set of 2^{s-1} powers of conjugates of $S^{2^{n-(m+1)}}$ from the $(m+1)$-*th* level and hence the set of 2^s powers of conjugates of $S^{2^{n-(m+2)}}$ from the $(m+2)$-*th* level has at most two elements in it. Furthermore there are at most $2\cdot 2^s$ conjugates of $S^{2^{n-(m+2)}}$ in H. Repeat the above argument and continue inductively to see that each level from m to t contains at most 2^s conjugates of powers of S where t is the greatest integer less than or equal to $\frac{2}{3}n - \frac{1}{3}$. By Lemma 3.1, for $r > t$, the number of conjugates of $S^{2^{n-r}}$ in H is at most twice the number of conjugates of $S^{2^{n-r+1}}$ in H. So if t is even,

$$W \leq 1 + 2\sum_{i=1}^{t/2} 2^i + 2^{t/2}\sum_{i=1}^{n-t} 2^i = 2^{(t/2)+1} + 2^{n+1-t/2} - 3;$$

if t is odd,

$$W \leq 1 + 2\sum_{i=1}^{(t-1)/2} 2^i + 2^{(t-1)/2}\sum_{i=1}^{n-t} 2^i = 2^{(t+1)/2} + 2^{n+1-(t+1)/2} - 3.$$

Since in either case, $\frac{1}{3}(n+1) \geq \frac{1}{2}(t+1) > \frac{1}{2}t > \frac{1}{3}(n-2)$,

$$W \leq 2^{(n+1)/3} + 2^{2n/3+5/3} - 3.$$

PROPOSITION 4.4. *Suppose* $n \geq 6$. *Then if* $|H \cap K_{n-1}^n| = 2$ *or* $H \cap K_{n-1}^n$ *is conjugate to* C, $g(H) > 0$.

Proof. By Lemma 4.1, $r \leq 2^{n-1}$. If $|H \cap K_{n-1}^n| = 2$, $W \leq n$ by Lemma 4.3 and $t \leq 3\cdot 2^{n-1}$ by Lemma 4.2 and so

$$g(H) \geq 1 + (2^{3n-5} - (3\cdot 2^{2n-4} + 2^{n-1}\cdot 2^{n-1} + 3\cdot 2^{n-1}\cdot 2^{n-2} + 2^{2n-4}n))/h$$
$$\geq 1 + 2^{2n-4}(2^{n-1} - 13 - n)/h.$$

But $2^{n-1} - 13 - n > 0$ if $n \geq 6$. If $H \cap K_{n-1}^n$ is conjugate to C, $W \leq 2n$ by Lemma 4.4 and $t \leq 3\cdot 2^{n-1}$ by Proposition 4.2 and so

$$g(H) \geq 1 + 2^{2n-4}(2^{n-1} - 13 - 2n)/h$$

and $2^{n-1} - 13 - 2n > 0$ if $n \geq 6$.

LEMMA 4.5. *Suppose* $H \cap K_{n-1}^n = B$ *and* $n \geq 5$. *Then* $r = 2^{2l}$ *with* $2l \leq 2n - 6$.

Proof. By Sylow, r is an even power of 2 so that $r = 2^{2l}$. Since any subgroup of order three has the form $[U\cdot R]$ where U is in K_1^n, $r = 2^{2l} \leq 2^{2n-(t+s)}$ where $|H \cap K_1^n| = 2^{2n-(t+s)}$ with $s \geq t$. Since $H \cap K_{n-1}^n = B$ and any element in K_1^n has its 2^{n-2}-*th* power in $K_{n-1}^n - B$, $t \neq 1$ and so $2l \leq 2n-4$. Finally consider the case $t+s = 4$ and $2l = 2n-4$. Then $[U\cdot R]$ is a group of order three for any U in K_2^n. So suppose

$$U = \pm(u+4\mu, 4\nu, 4\rho, u-4\mu)$$

is in $K_2^n - K_3^n$ and $U\cdot R$ has order 3. Now

$$u^2 \equiv 1 + 16(\mu^2+\nu\rho) \pmod{2^n}$$

and, since $U^{2^{n-3}}$ is in B, exactly two of μ, ν and ρ are odd. So $\mu^2+\nu\rho$ is odd and $2^4 \,\|\, 1-u^2$. Since $U\cdot R$ has order 3 and so trace 1, $4(\nu-\rho-\mu) \equiv 1-u \pmod{2^n}$. $\nu-\rho-\mu$ is even exactly two of them are odd and so 2^3 divides $(1-u)$. But $2^3 \,\|\, (1-u)$ since 2 divides $1+u$ and $2^4 \,\|\, (1-u^2) = (1+u)(1-u)$. Therefore $2 \,\|\, (\nu-\rho-\mu)$. Now consider

$$U^2 = \pm(u^2+8\mu u+16(\mu^2+\nu\rho), 8\nu u, 8\rho u, u^2-8\mu u+16(\mu^2+\nu\rho)).$$

$U^2\cdot R$ has order 3 so that

$$8u(\nu-\rho-\mu)+16(\mu^2+\nu\rho) \equiv 1-u^2 \pmod{2^n}.$$

But $2^4 \,\|\, (1-u^2)$ and, since $\mu^2+\nu\rho$ is odd, $2 \,\|\, (\nu-\rho-\mu)$ and $n \geq 5$, then 2^5 divides $8u(\nu-\rho-\mu)+16(\mu^2+\nu\rho)$ which is a contradiction. So $2l \neq 2n-4$ which implies that $2l \leq 2n-6$.

PROPOSITION 4.5. *Suppose $H \cap K_{n-1}^n$ is B and $n \geq 5$. Then $g(H) > 0$.*

Proof. Since $H \cap K_{n-1}^n$ is B, $W = 0$. By Proposition 4.2, $t \leq 3\cdot 2^{n-1}$ and by Lemma 4.5, $r \leq 2^{2n-6}$. So

$$g(H) \geq 1 + (2^{3n-5} - 3\cdot 2^{2n-4} - 3\cdot 2^{n-1}\cdot 2^{n-2} - 2^{n-1}\cdot 2^{2n-6})/h$$
$$= 1 + 2^{2n-4}(2^{n-1} - (3+6+2^{n-3}))/h > 0$$

if $n \geq 5$.

PROPOSITION 4.6. *Suppose $H \cap K_{n-1}^n$ is conjugate to D. Then $g(H) > 0$ if $n \geq 8$.*

Proof. By Lemma 4.1 and Corollary 4.1, $r = 0$ and $|H| = 2^l$. By Proposition 4.2, $t \leq 2^{n-1} + 2^n(n-s-r+1)$ and by Proposition 4.3,

$$W \leq 2^{(n+1)/3} + 2^{2n/3+5/3} - 3.$$

So $g(H) \geq 1 + 2^{2n-4}(2^{n-1} - (3+2+4(n-2)+W))/h$. But if $n \geq 11$,

$$2^{n-1} - (5+4(n-2)+2^{(n+1)/3}+2^{2n/3+5/3}-3) > 0$$

and so $g(H) > 0$. From the proof of Proposition 4.3, we see that for $n = 10$, $W \leq 269$; for $n = 9$, $W \leq 133$; for $n = 8$, $W \leq 69$. Therefore for $n = 10$,

$$g(H) \geq 1 + 2^{16}(512 - (37 + 269))/h;$$

for $n = 9$,

$$g(H) \geq 1 + 2^{14}(256 - (33 + 133))/h;$$

for $n = 8$,

$$g(H) \geq 1 + 2^{12}(128 - (29 + 69))/h.$$

So for $n = 8$, 9 and 10, $g\ (H) > 0$.

The proof of Theorem 1 now follows from Propositions 4.1, 4.4, 4.5 and 4.6.

Bibliography

1. J. Dennin, *Fields of modular functions of Genus* 0, Illinois J. Math.
2. J. Gierster, *Über die Galois'sche Gruppe Modulargleichungen, wenn der Transformationsgrad Potenz einer Primzahl > 2 ist*, Math. Ann., vol. 26 (1886), pp. 309–368.
3. R. C. Gunning, *Lectures on modular forms*, Princeton, 1962.
4. D. McQuillan, *Classification of normal congruence subgroups of the modular group*, Amer. J. Math., vol. 87 (1965), pp. 285–296.
5. ———, *On the genus of fields of elliptic modular functions*, Illinois J. Math., vol. 10 (1966), pp. 479–487.

University of Connecticut
Storrs, Connecticut