THE AUTOMORPHISMS AND CONJUGACY CLASSES OF $LF(2, 2^n)$

BY

JOSEPH B. DENNIN, JR.

1. Introduction

Let Γ denote the 2×2 modular group; that is, the group of 2×2 matrices with integer entries and determinant 1 in which a matrix is identified with its negative. Let $\Gamma(n)$ denote the principal congruence subgroup of level n; that is, the subgroup of Γ consisting of all matrices congruent mod n to $\pm I$ where I is the identity matrix. A subgroup G of Γ is called a congruence subgroup of level n if G contains $\Gamma(n)$ and n is the smallest such integer. Let $LF(2, n) = SL(2, n)/\pm I$ where $SL(2, n)$ is the special linear group of degree two with coefficients in Z_n, the integers mod n. Then $LF(2, n)$ is isomorphic to $\Gamma/\Gamma(n)$. The congruence subgroups of Γ and hence the groups $LF(2, n)$ play an important role in the study of elliptic modular functions and so the structure of both Γ and $LF(2, n)$ have been studied in some detail (cf. the bibliography for some examples). In particular, in [5] D. McQuillan determined the automorphisms of and explicit representatives for the conjugacy classes of $LF(2, p^n)$, p an odd prime. In this paper, we determine explicit representatives for the conjugacy classes of $LF(2, 2^n)$ in Section 2 and determine the automorphisms of $LF(2, 2^n)$ in Section 3.

The following notation will be standard. $H_n = LF(2, 2^n)$. An element A in H_n will be written $\pm(a, b, c, d)$. ϕ_r^n will denote the natural homomorphism from H_n to H_r, $1 \le r \le n$, defined by reducing all the entries in a matrix in H_n mod 2^r. K_r^n will denote the kernel of ϕ_r^n and it is well known that the order of $K_r^n = 2^{3(n-r)}$ if $r \neq 1$ and 2^{3n-4} if $r = 1$. Let X be a set of representatives, including 1, for V/V^2 where V is the set of units in Z_{2^n}. u will denote an arbitrary element in X.

2. The conjugacy classes

$LF(2, 2)$ has order 6 and $LF(2, 4)$ has order 24 and the representatives of the conjugacy classes in these groups are easily obtained by listing the elements and calculating. For $LF(2, 2)$, one has $\pm I$, $\pm(0, -1, 1, 1)$, $\pm(0, 1, -1, 0)$; for $LF(2, 4)$, one has $\pm I$, $\pm(1, 2, 0, 1)$, $\pm(0, 1, -1, 0)$, $\pm(1, 1, 0, 1)$, $\pm(0, -1, 1, 1)$. So we consider H_n, $n \geq 3$. The following result, analogous to Lemma 1 in [5] will be useful.

LEMMA 1. *Let N_r be the number of solutions of the congruence*

$$Ax^2 + Bxy + Cy^2 \equiv D \pmod{2^r} \tag{1}$$

where A, B, C, D are integers, $D \not\equiv 0 \pmod 2$ and $r \geq 3$. Then $N_r = 2^{r-3}N_3$.

Received October 28, 1974.

Proof. The proof is by induction on r with the case $r = 3$ obvious. Suppose $r > 3$ and (a, b) is a solution to (1) mod 2^{r-1}. If $B \not\equiv 0 \pmod 2$, then (a, b) generates two solutions to (1) mod 2^r. To see this, consider

$$A(a + 2^{r-1}t)^2 + B(a + 2^{r-1}t)(b + 2^{r-1}s) + C(b + 2^{r-1}s)^2 \equiv D \pmod{2^r}$$

and observe there are precisely two solutions for (t, s) since at least one of a and b is odd. So $N_r = 2 \cdot N_{r-1}$. If $B \equiv 0 \pmod 2$, then (a, b) generates eight solutions to (1) mod 2^r. To see this, consider

$$A(a + 2^{r-2}t)^2 + B(a + 2^{r-2}t)(b + 2^{r-2}s) + C(b + 2^{r-2}s)^2 \equiv D \pmod{2^r}$$

which has two solutions for (t, s). The eight solutions are then given by

$$(a + 2^{r-2}t + 2^{r-1}\varepsilon, b + 2^{r-2}s + 2^{r-1}\varepsilon')$$

where $\varepsilon, \varepsilon'$ are in $\{0, 1\}$. However, these same eight solutions to (1) mod 2^r are also generated by the solutions

$$(a + 2^{r-2}, b), (a, b + 2^{r-2}) \quad \text{and} \quad (a + 2^{r-2}, b + 2^{r-2})$$

to (1) mod 2^{r-1} and by no other pair (c, d) which is a solution to (1) mod 2^{r-1}. So $N_r = 2 \cdot N_{r-1}$.

First we will classify the elements of $H_n - K_1^n$. Note that if $A = \pm(a, b, c, d)$ is in $H_n - K_1^n$, then, by conjugating by $\pm(0, -1, 1, 0)$ if necessary, we may assume that $b \not\equiv 0 \pmod{2^n}$. Let

$$s = \text{trace of } \pm(a, b, c, d) = \pm(a + d).$$

Let $N(t, u) = \pm(1, u, t, 1 + ut)$ where 2 divides t.

THEOREM 1. *Suppose $A = \pm(a, b, c, d)$ is in H_n, $n \geq 3$, A is not in K_1^n, $b \not\equiv 0 \pmod{2^n}$ and 2 divides $s^2 - 4$. Then A is conjugate to $N(t, u)$ where u is chosen such that $b^{-1}u$ is a quadratic residue and t is chosen such that*

$$tu \equiv s - 2 \pmod{2^n}.$$

Proof. We need $B = \pm(y, v, w, x)$ such that $BA = N(t, u)B$. This leads to the following congruences (mod 2^n):

$$w \equiv u^{-1}(y(a - 1) + cv) \tag{1}$$

$$x \equiv u^{-1}(v(d - 1) + by) \tag{2}$$

$$aw + cx \equiv ty + w + tuw \tag{3}$$

$$bw + dx \equiv tv + x + tux \tag{4}$$

$$1 \equiv yx - vw. \tag{5}$$

(1), (2), and (5) in turn give

$$by^2 + (d - a)yv - cv^2 \equiv u \pmod{2^n}. \tag{6}$$

Pick the u such that $b^{-1}u$ is a quadratic residue mod 2^n. Then $v \equiv 0$ and $y \equiv (b^{-1}u)^{1/2} \pmod{2^n}$ is a solution to (6) and with t chosen such that $tu \equiv s - 2$, the y, v, w, and x from (1), (2), and (5) also satisfy (3) and (4).

COROLLARY 1. *If* $2 \parallel s$, *then* A *is conjugate to exactly one element in* $N_1 = \{N(t, u) \colon 8 \mid t\}$ *and the conjugacy class of* A *has order* $3 \cdot 2^{2n-4}$.

Proof. By selecting the proper sign, we may assume $s - 2$ and hence t is divisible by 8 since exactly one of $s - 2$ or $-s - 2$ is. By Theorem 1, A is conjugate to some element in N_1. If $N(t, u)$ is conjugate to $N(t', u')$, then by comparing traces either $tu \equiv t'u' \pmod{2^n}$ or $tu + 2 \equiv -t'u' - 2 \pmod{2^n}$. In the second case, $-4 \equiv t'u' + tu \pmod{2^n}$ which is impossible since 8 divides t and t'. In the first case, reducing mod 8, we see that $\pm(1, u, 0, 1)$ is conjugate to $\pm(1, u', 0, 1)$ in H_3 which implies that $u = u'$. But then $t \equiv t' \pmod{2^n}$. So $N(t, u)$ is conjugate to $N(t', u')$ if and only if $t = t'$ and $u = u'$. So A is conjugate to exactly one element in N_1. To find the elements $\pm(y, v, w, x)$ in the normalizer of $N(t, u)$, use the argument of Theorem 1 and solve $y^2 + yvt + v^2ut \equiv 1 \pmod{2^n}$. This has 2^5 solutions mod 8 and so by Lemma 1, 2^{n+2} solutions mod 2^n. So there are 2^{n+1} elements in the normalizer of $N(t, u)$ and $3 \cdot 2^{2n-4}$ elements in its conjugacy class.

Since there are $2^{n-1}N(t, u)$ in $N_1(2^{n-3}$ choices for t and 4 choices for u), this accounts for $3 \cdot 2^{3n-5}$ elements in H_n.

COROLLARY 2. *If* $4 \mid s$, *then* A *is conjugate to exactly one element in* $N_2 = \{N(t, 1) \colon 2 \parallel t\}$ *and the conjugacy class of* A *has order* $3 \cdot 2^{2n-3}$.

Proof. Applying Theorem 1 and its proof, we see that with $2 \parallel t$ and t', $N(t, u)$ is conjugate to $N(t', u')$ if and only if $uu' \equiv 1$ or $5 \pmod 8$ and $tu \equiv t'u' \pmod{2^n}$ or $uu' \equiv 3$ or $7 \pmod 8$ and $tu + t'u' \equiv -4 \pmod{2^n}$. By Theorem 1, A is conjugate to $N(t, u)$ for some t, u with $2 \parallel t$ and by the previous comment u can be chosen to be 1. For the normalizer of $N(t, u)$, we must solve $y^2 + yvt + v^2t \equiv 1 \pmod{2^n}$ which has 2^{n+1} solutions. So there are 2^n elements in the normalizer of $N(t, u)$ and $3 \cdot 2^{2n-3}$ elements in its conjugacy class.

Since there are 2^{n-2} elements in N_2, there are 2^{n-2} distinct conjugacy classes represented here accounting for $3 \cdot 2^{3n-5}$ elements of H_n.

THEOREM 2. *Suppose* $A = \pm(a, b, c, d)$ *has* $s^2 - 4 \equiv 5 \pmod 8$. *Then* A *is conjugate to* $\pm(0, -1, 1, s)$ *and the conjugacy class of* A *has* 2^{2n-1} *elements in it.* $\pm(0, -1, 1, s)$ *is conjugate to* $\pm(0, -1, 1, s')$ *if and only if* $s' = \pm s$.

Proof. We need to find $B = \pm(y, v, w, x)$ such that $BA = \pm(0, -1, 1, s) \cdot B$. It is sufficient to solve $w \equiv -ay - cv$, $x \equiv -by - dv$, $yx - vw \equiv 1$ all mod 2^n which yield

$$cv^2 + (a - d)yv - b^2 \equiv 1 \pmod{2^n}.$$

Since $(a - d)^2 + 4bc = s^2 - 4 \equiv 5 \pmod 8$, b, c, and $(a - d)$ have to be odd. Then $cv^2 + (a - d)yv - by^2 \equiv 1$ is solvable mod 8 and so is solvable mod 2^n. For the normalizer of $\pm(0, -1, 1, s)$, we must solve $y^2 - yvs + v^2 \equiv 1 \pmod{2^n}$ which has $4 \cdot 3$ solutions mod 8 and so, by Lemma 1, $3 \cdot 2^{n-1}$ solutions mod 2^n. So there are 2^{2n-1} elements in its conjugacy class. The usual calculations show that $\pm(0, -1, 1, s)$ is conjugate to $\pm(0, -1, 1, s')$ if and only if $s' = \pm s$.

Since s is odd, there are 2^{n-2} distinct conjugacy classes with representatives $\pm(0, -1, 1, s)$ accounting for 2^{3n-3} elements in H_n. Any element in $H_n - K_1^n$ is conjugate to one of $N(t, u)$ with 8 dividing t or $2 \parallel t$ or to one of $\pm(0, -1, 1, s)$ since the number of elements in their conjugacy classes is

$$3 \cdot 2^{3n-5} + 3 \cdot 2^{3n-5} + 2^{3n-3} = 5 \cdot 2^{3n-4}$$

which is the order of $H_n - K_1^n$.

Now we must determine representatives for the conjugacy classes in K_1^n. Since K_r^n is normal in H_n and $K_{r+1}^n \subseteq K_r^n$, $1 \le r \le n - 1$, $K_r^n - K_{r+1}^n$ splits in H_n into complete classes of conjugate elements. K_{n-1}^n has four conjugacy classes represented by

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

Now consider the following sets of matrices in $K_r^n - K_{r+1}^n$ for $2 \le r \le n - 2$:

(1) $P(m, r, u) = \pm(1, 2^r u + 2^{r+1}, 2^{r+1}m, 1 + 2^{2r+2}m + 2^{2r+1}mu)$ where $1 \le m \le 2^{n-r-1}$;

(2) $M(w, r, u) = \pm(1, 2^r w, 2^r wu, 1 + 2^{2r}w^2u)$ where $1 \le w \le 2^{n-r}$ and $(w, 2) = 1$;

(3) $Q(a, r) = \pm(1 + 2^r + 2^{r+2}a, 2^{r+1}, 2^{r+1}, 1 - 2^r + 2^{r+2}d)$ where $1 \le a \le 2^{n-r-2}$ and d is chosen so that the determinant is ± 1;

(4) $D(x) = \pm(x, 0, 0, x^{-1})$ where $1 \le x \le 2^n$ and $x \equiv 1 \pmod{2^r}$, $x \not\equiv 1 \pmod{2^{r+1}}$.

To see that an element in one of these sets is not conjugate to any element in a different set, reduce mod 2^{r+2} and observe that in $K_r^{r+2} - K_{r+1}^{r+2}$, their images belong to the sets corresponding to the original sets. Then a straightforward calculation shows that these images are not conjugate and so the original elements could not be conjugate.

PROPOSITION 1.

element		*order of conjugacy class*
(i) $D(x)$	$3 \cdot 2^{2n-2r-3}$	
(ii) $Q(a, r)$	$2^{2n-2r-3}$	
(iii) $P(m, r, u)$	$3 \cdot 2^{2n-2r-3}$	*if* $m \equiv 1$ *or* $2 \pmod 4$
	$3 \cdot 2^{2n-2r-4}$	*if* $m \equiv 0 \pmod 4$
(iv) $M(w, r, u)$	$3 \cdot 2^{2n-2r-2}$	*if* $u \equiv 1$ *or* $5 \pmod 8$ *and* $w \equiv 1 \pmod 8$
	$3 \cdot 2^{2n-2r-3}$	*if* $u \equiv 3$ *or* $7 \pmod 8$ *and* $w \equiv 1$ *or* $3 \pmod 8$

Proof. (i) $\pm(a, b, c, d)$ is in the normalizer of $D(x)$ if and only if $bx \equiv bx^{-1}$ and $cx \equiv cx^{-1} \pmod{2^n}$. Since $D(x)$ is in $K_r^n - K_{r+1}^n$, $D(x)$ can be written

$$\pm(u + 2^r\mu, 0, 0, u - 2^r\mu)$$

where 2 does not divide μ and $u^2 - 2^{2r}\mu^2 \equiv 1 \pmod{2^n}$. So $x - x^{-1} \equiv 2^{r+1}\mu \pmod{2^n}$ and $\pm(a, b, c, d)$ is in the normalizer if and only if 2^{n-r-1} divides both b and c. Since b and c are both even and $ad - bc \equiv 1 \pmod{2^n}$, a has to be odd and $d \equiv a^{-1}(1 + bc) \pmod{2^n}$. So there are 2^{n+2r} elements in the normalizer of $D(x)$ and $3 \cdot 2^{2n-2r-3}$ elements in its conjugacy class.

(ii) $\pm(x, y, w, z)$ is in the normalizer of $Q(a, r)$ if and only if

$$2^{r+1}y \equiv 2^{r+1}w \tag{1}$$

$$2^{r+1}x + 2^{r+2}dy \equiv 2^{r+1}y + 2^{r+2}ay + 2^{r+1}z \pmod{2^n} \tag{2}$$

$$xz - yw \equiv 1. \tag{3}$$

(1) implies that $w \equiv y \pmod{2^{n-r-1}}$ and then (2) implies that

$$x \equiv y(1 + 2a - 2d) + z \pmod{2^{n-r-1}}.$$

Now solving (3) mod 8 and using Lemma 1, one obtains $3 \cdot 2^{n+2r}$ elements in the normalizer of $Q(a, r)$ and $2^{2n-2r-3}$ elements in its conjugacy class.

The proofs of (iii) and (iv) are similar.

THEOREM 3. *A complete set of representatives for the conjugacy classes in* $K_r^n - K_{r+1}^n$, $2 \le r \le n - 2$, *is given by:*

(i) $\{D(x) \mid x \neq \pm y^{-1}$ *for any two* $D(x), D(y)\}$;

(ii) $\{Q(a, r)\}$;

(iii) $\{P(m, r, u)$: *if* $m \equiv 0$ *or* $1 \pmod 4$, *then* u *is arbitrary*; *if* $m \equiv 2 \pmod 4$ *then* $u \equiv 1$ *or* $3 \pmod 8\}$;

(iv) $\{M(w, r, u)$: *if* $u \equiv 1$ *or* $5 \pmod 8$, *then* $w \equiv 1 \pmod 8$; *if* $u \equiv 3$ *or*, $7 \pmod 8$, *then* $w \equiv 1$ *or* $3 \pmod 8\}$.

Proof. (i) A conjugate of $D(x)$ has the form

$$\pm(cdx - bcx^{-1}, ab(x^{-1} - x), cd(x - x^{-1}), -bcx + adx^{-1})$$

and so $D(x)$ is conjugate to $D(y)$ if and only if $x \equiv x^{-1} \pmod{2^n}$ or ab and $cd \equiv 0 \pmod{2^n}$. In the second case, one has $y = -x^{-1}$ since $ad - bc \equiv 1 \pmod{2^n}$. So $D(x)$ is conjugate to $D(y)$ if and only if $y = \pm x^{-1}$.

(ii) We show that $Q(a, r)$ is not conjugate to $Q(a', r)$, $a \neq a'$, by induction on $n - r$ where $r = n - (n - r)$. If $n - r = 2$, there is only one value for a. For $n - r > 2$, if $Q(a, r)$ is conjugate to $Q(a', r)$, their images mod 2^{n-1} are conjugate and so by the induction hypothesis, they reduce to the same element. So $a' = a + 2^{n-r-3}$. But then

$$\pm(x, y, w, z) \cdot Q(a, r) = Q(a', r) \cdot \pm(x, y, w, z)$$

if and only if

$$y \equiv w + 2^{n-r-2}x \tag{1}$$

$$z \equiv x + yt \tag{2}$$

$$z \equiv x + wt \tag{3}$$

$$w \equiv y + 2^{n-r-2}z \tag{4}$$

all mod 2^{n-r-1}, where t is odd. Then (1) and (4) imply $z \equiv x \pmod 2$. If x and z are even, then w and y are even which contradicts $xz - yw \equiv 1 \pmod{2^n}$; if x and z are odd, (1) implies that $y \equiv w + 2^{n-r-2} \pmod{2^{n-r-1}}$ and (2) and (3) imply that $y \equiv w \pmod{2^{n-r-1}}$ which is a contradiction. So $Q(a, r)$ is not conjugate to $Q(a', r)$.

(iii) Direct calculation shows that distinct representatives for conjugacy classes with representatives of the form $P(m, r, u)$ are given by $P(1, n-2, 1)$, $P(2, n-2, 1)$, and $P(2, n-2, 3)$ in $K^n_{n-2} - K^n_{n-1}$ and by $P(1, n-3, u)$ and $P(4, n-3, u)$ with $u = 1, 3, 5$, or 7 and $P(2, n-3, u)$ with $u = 1$ or 3 in $K^n_{n-3} - K^n_{n-2}$. Assume $r \leq n - 4$. For a fixed u,

$$\pm(a, b, c, d)P(m, r, u) = P(m', r, u) \cdot \pm(a, b, c, d)$$

if and only if

$$2bm \equiv (2 + u)c \tag{1}$$

$$(2 + u)a + 2^{r+1}bm(u + 2) \equiv (u + 2)d \tag{2}$$

$$2dm \equiv 2m'a + 2^{r+1}m'c(u + 2) \tag{3}$$

$$(2 + u)c + 2^{r+1}dm(u + 2) \equiv 2bm' + 2dm'(u + 2), \tag{4}$$

all mod 2^{n-r}. Suppose $m - m' \not\equiv 0 \pmod{2^{n-r-1}}$. Then (1) and (4) imply that $b \equiv 0 \pmod{2^r}$ and (2) and (3) imply that $a \equiv 0 \pmod{2^r}$. Therefore $ad - bc \equiv 0 \pmod{2^r}$, a contradiction. Assume that if m (respectively m') $\equiv 0$ or $1 \pmod 4$, then $u(u')$ is arbitrary and if $m(m') \equiv 2 \pmod 4$, then $u(u') \equiv 1$ or $3 \pmod 8$. If $P(m, r, u)$ is conjugate to $P(m', r, u')$, then their images under ϕ^n_{r+3} are conjugate in H_{r+3} and so $u \equiv u' \pmod{2^{r+3}}$. Therefore $u \equiv u' \pmod 8$ and so $u = u'$. Therefore, by the first part of the argument, $m = m'$.

(iv) One argues as in (iii) showing that if $M(w, r, u)$ is conjugate to $M(w', r, u')$, then $w^2u \equiv w'^2u' \pmod{2^{n-r}}$ and then applying ϕ^n_{r+2} to see that these elements are conjugate if and only if they are equal.

Now since all these conjugacy classes are distinct, one uses Proposition 1 to show that the number of elements contained in the union of these classes equals the order of $K^n_r - K^n_{r+1}$ which is $7 \cdot 2^{3n-3r-3}$. $\{Q(a, r)\}$, $\{D(x)\}$, $\{P(m, r, u)$: $m \equiv 2 \pmod 4\}$, and $\{P(m, r, u)$: $m \equiv 0 \pmod 4\}$ each contribute $3 \cdot 2^{3n-3r-5}$ elements; $\{M(w, r, u)$: $u \equiv 1$ or $5 \pmod 8\}$, $\{M(w, r, u)$: $u \equiv 3$ or $7 \pmod 8\}$, and $\{P(m, r, u)$: $m \equiv 1 \pmod 4\}$ each contribute $3 \cdot 2^{3n-3r-4}$ elements. Adding, one gets $7 \cdot 3^{3n-3r-3}$ elements as desired.

Finally we give representatives for conjugacy classes in $K^n_1 - K^n_2$.

Proposition 2. *In $K_1^n - K_2^n$, a complete set of representatives for the distinct conjugacy classes is* $\{P(m, 1, u)$: *if* $m \equiv 0$ *or* 1 (mod 4), *then u is arbitrary*; *if* $m \equiv 2$ (mod 4), *then* $u \equiv 1$ *or* 3 (mod 8)$\}$.

Proof. The order of $K_1^n - K_2^n$ is $3 \cdot 2^{3n-6}$ and calculating as in Proposition 1 and Theorem 3, we see that the number of elements obtained from conjugacy classes represented by the $P(m, 1, u)$ is $3 \cdot 2^{3n-6}$ and that these classes are distinct.

Note that there are no $Q(a, r)$ and $D(x)$ elements in $K_1^n - K_2^n$ and that the $M(w, 1, u)$ give the same classes as the $P(m, 1, u)$.

3. The automorphisms

The elements $S = \pm(1, 1, 0, 1)$ of order 2^n and $T = \pm(0, -1, 1, 0)$ of order 2 generate H_n and $ST = \pm(1, -1, 1, 0)$ has order 3. Aut $(H_1) \cong H_1$ since H_1 is isomorphic to S_3. Suppose $n \geq 2$. The center of H_n is

$$\{\pm(1 + 2^{n-1}, 0, 0, 1 + 2^{n-1}), \pm I\}$$

and so the group I_n of inner automorphisms has order $\frac{1}{2}|H_n|$. Let $U_i = \pm(u_i, 0, 0, 1)$ for $u_i \in X$, $u_i \neq 1$. Then $f_i(B) = U_i B U_i^{-1}$ is an automorphism of H_n, not an inner automorphism, and f_i^2 is in I_n since f_i^2 is the inner automorphism given by $\pm(u_i, 0, 0, u_i^{-1})$. For $n = 2$, let $G_2 = I_2 \cup f_1 I_2$. The following will show $G_2 =$ Aut (H_2). For $n \geq 3$, let $G_n = I_n \cup f_1 I_n \cup f_2 I_n \cup f_3 I_n$. Then G_n is a subgroup of Aut (H_n) of order $2|H_n|$. This follows from the facts that I_n is a normal subgroup of Aut (H_n) and so is normal in G_n and that $(f_i f_j)(B) = A \cdot f_k(B) \cdot A^{-1}$ where $u_i u_j = u_k a^2$ and $A = \pm(a, 0, 0, a^{-1})$.

Lemma 2. *If σ is an arbitrary automorphism of H_n, $n \geq 2$, there is an automorphism τ in G_n such that*

$$\tau\sigma(S) = N(t, 1), \quad \tau\sigma(T) = \pm(0, b, c, 0)$$

where $t \equiv 0$ (mod 4) *and* $c + bt \equiv \pm 1$. *If* $n \geq 3$, *then* $t \equiv 0$ (mod 8).

Proof. Since $\sigma(S)$ has order 2^n, there exists an inner automorphism which sends $\sigma(S)$ to $N(t, u_i)$ for some t, u_i where $4 \mid t$ since $\{N(t, u): 4 \mid t\}$ is a complete set of representatives for conjugacy classes of elements of order 2^n. If $n \geq 3$, by Corollary 1, t can be chosen so that $8 \mid t$. But then

$$f_i(N(t, u_i)) = \pm(1, u_i^2, tu_i^{-1}, 1 + tu_i)$$

which is conjugate to $\pm(1, 1, tu_i, 1 + tu_i)$. So there is an element ρ in G_n such that $\rho\sigma(S) = \pm(1, 1, t, 1 + t)$ for some t. Now $\rho\sigma(ST)$ has order 3 and so trace 1 while $\rho\sigma(T)$ has order 2, is not in K_1^n, and so has trace 0. Let $\rho\sigma(T) = \pm(a, b, c, -a)$. Then the trace of $\rho\sigma(S)\rho\sigma(T)$ is $c + (b - a)t \equiv \pm 1$ (mod 2^n) so that c is odd. By a simple calculation for $LF(2, 4)$, there exists an m such that

$$N(t, 1)^{-m}\rho\sigma(T)N(t, 1)^m = \pm(0, b, c, 0) \quad \text{for some } b, c.$$

Now K^n_{n-1} is a characteristic subgroup of H_n since it is the only normal subgroup of H_n of order 8 so the proof can proceed by induction on n. Since $\rho\sigma$ induces an automorphism on H_{n-1}, one uses the induction hypothesis and then comes back up to H_n to get

$$N(t, 1)^{-r}\rho\sigma(T)N(t, 1)^r = \pm(a, b, c, -a)$$

where $a \equiv 0 \pmod{2^{n-1}}$. If $a \equiv 0 \pmod{2^n}$, we are done. If $a \not\equiv 0 \pmod{2^n}$, then conjugate by $N(t, 1)^{2^{n-1}} = \pm(1, 2^{n-1}, 0, 1)$ to get

$$\begin{aligned} N(t, 1)^{-r-2^{n-1}}\rho\sigma(T)N(t, 1)^{r+2^{n-1}} &= \pm(a + 2^{n-1}c, b, c, -a + 2^{n-1}c) \\ &= \pm(0, b, c, 0) \end{aligned}$$

since c is odd. As seen earlier in the proof, since the image of ST has trace 1, $c + bt \equiv \pm 1 \pmod{2^n}$.

If $t \equiv 0 \pmod{2^n}$, then $\tau\sigma$ is the identity and so $\sigma \in G_n$. Suppose $t \equiv 0 \pmod{2^v}$ but $t \not\equiv 0 \pmod{2^{v+1}}$ where $3 \leq v \leq n - 1$. We set $v(t) = v$ and make the following definition.

DEFINITION. A mapping ρ of H_n has weight v if $\rho(S) = N(t, 1)$, $\rho(T) = \pm(0, b, c, 0)$ where $c + bt \equiv \pm 1 \pmod{2^n}$ and $v(t) = v$.

To determine the automorphisms of H_n we use the following unpublished fact communicated to us by J. G. Sunday.

LEMMA 3. *A presentation of H_n is given by generators A, B and relations $A^{2^n} = B^2 = (AB)^3 = (A^qBA^{10}B)^2 = 1$ where $5q \equiv 1 \pmod{2^n}$.*

Reduced mod 4, $N(t, 1)$ and $\pm(0, b, c, 0)$ with $c + bt \equiv \pm 1 \pmod{2^n}$ and $8 \mid t$ generate H_2. Therefore, using Theorem 8 of [1], one sees that they generate H_n. With $A = N(t, 1)$ and $B = \pm(0, b, c, 0)$, the relations $A^{2^n} = B^2 = (AB)^3 = 1$ are easily seen to be satisfied. So ρ is an automorphism of weight v if and only if $(A^qBA^{10}B)^2 = 1$.

THEOREM 4. *For $n \geq 7$, there are no automorphisms of weight $\leq n - 5$ and all mappings ρ of weight $\geq n - 4$ are automorphisms. For $n = 6, 5,$ or 4, all mappings of weight $\geq n - 3$, $n - 2$, or $n - 1$, respectively are automorphisms.*

We do the proof for $n \geq 10$ and indicate the necessary modifications in the calculations for the cases of smaller n. First we find b and c specifically.

LEMMA 4. *For $n \geq 10$ and mappings of weight $\geq n - 5$, for $n = 8$ or 9 and weight $\geq n - 4$, for $n = 6$ or 7 and weight $\geq n - 3$ and for $n = 4$ or 5 and weight $\geq n - 2$, $b = \pm(t - 1)$ and $c = \pm(t + 1)$. For $n = 9$ and weight $= n - 5$ and for $n = 7$ and weight $= n - 4$, $b = \pm(t - 1)$ and $c + \pm(1 + t - t^2)$. For $n = 8$ and weight $= n - 5$, $b = \pm(t - 1 + 2^{n-1})$ and $c = \pm(1 + t - t^2)$.*

Proof. Consider

$$c + bt \equiv \pm 1 \pmod{2^n} \quad \text{and} \quad bc \equiv -1 \pmod{2^n}.$$

Then $\pm b - b^2 t \equiv -1 \pmod{2^n}$. Let $b = 2r + 1$ and $t = 2^{n-5}x$ for some r, x. Then one has

$$\pm 2r \pm 1 - 2^{n-3}r^2 x - 2^{n-3}rx - 2^{n-r}x + 1 \equiv 0 \pmod{2^n}.$$

Consider the plus value and note that if $n \geq 10$, then $8 \mid (r + 1)$. So one has

$$2(r + 1) - 2^{n-5}x \equiv 0 \pmod{2^n}.$$

So $r \equiv 2^{n-6}x - 1 \pmod{2^{n-1}}$ which implies that $b \equiv 2^{n-5}x - 1 \equiv t - 1 \pmod{2^n}$. Then $c \equiv 1 + t \pmod{2^n}$. Similarly for the minus value, one gets

$$b \equiv -(t - 1) \pmod{2^n} \quad \text{and} \quad c \equiv -(1 + t) \pmod{2^n}.$$

So the proof is done for $n \geq 10$ and mappings of weight $\geq n - 5$. By appropriately modifying the form of t, the other cases are done in an analogous fashion.

As in [5],

$$N(t, 1)^r \equiv \pm\left(1 + \binom{r}{2}t + \binom{r+1}{4}t^2, r + \binom{r+1}{3}t + \binom{r+2}{5}t^2,\right.$$
$$\left. rt + \binom{r+1}{3}t^2, 1 + \binom{r+1}{2}t + \binom{r+2}{4}t^2\right) \pmod{t^3}.$$

THEOREM 5. *If $n \geq 8$, there are no automorphisms of weight $n - 5$ and any mapping of weight $\geq n - 4$ is an automorphism. For $n = 4, 5, 6, 7$, any mapping of weight ≥ 3 is an automorphism.*

Proof. Suppose $2^n \mid t^2$ and $B = \pm(0, t - 1, t + 1, 0)$. This is the situation unless $n = 8$ or 9 and weight $= n - 5$ or $n = 7$ and weight $= n - 4$. Now

$$(A^q B A^{10} B) = \pm\left(10q - 1 + \left[20q + \binom{11}{3}q + 10\binom{q+1}{3} + \binom{11}{2} - \binom{q}{2}\right]t,\right.$$
$$-q + \left[10 - q\binom{10}{2} - \binom{q+1}{3}\right]t,$$
$$10 + \left[20 + \binom{11}{3} + \binom{q+1}{2} - q\right]t,$$
$$\left. -1 - \left[\binom{10}{2} + \binom{q+1}{2}\right]t\right)$$

which is not in K_1^n so that it has order 2 if and only if its trace is 0. But $5q \equiv 1 \pmod{2^n}$ and so q can be written as

$$1 - 2^2 + 2^4 - \cdots + 2^{2t} \pmod{2^n}$$

so that the trace of $(A^qBA^{10}B)$ is

$$(-63 - 1/3(2q^2 - 1))t \equiv 16(t)(-17)/3 \pmod{2^n}$$

For $n \geq 10$ this is congruent to 0 if and only if $2^{n-4} \mid t$. For smaller values of n, the trace is easily calculated from this formula. For the special cases $n = 9$ and 8, weight $= n - 5$ and $n = 7$, weight $= n - 4$, one uses the form for B given in Lemma 4 and retains the t^2 term in A to get that:

$$\text{for } n = 9, \text{ trace } (A^qBA^{10}B) \equiv 2^8 \pmod{2^9};$$

$$\text{for } n = 8, \text{ trace } (A^qBA^{10}B) \equiv 2^7 \pmod{2^8};$$

$$\text{for } n = 7, \text{ trace } (A^qBA^{10}B) \equiv 0 \pmod{2^7}.$$

COROLLARY 1. *There are no automorphisms of weight* $\leq n - 5$.

Proof. Since $8 \mid t$, we may assume $n \geq 8$ and for $n = 8$, the corollary is true by Theorem 5. If σ is an automorphism of weight x on H_n, $n > 8$, $3 \leq x \leq n - 5$, then σ induces an automorphism of weight $x = (x + 5) - 5$ on H_{x+5} which contradicts Theorem 5.

The proof of Theorem 4 is now complete. Using Lemma 2, Theorem 4 and the following Proposition, one obtains Aut (H_n).

PROPOSITION 2. *Suppose* ρ, σ *are automorphisms of* H_n *of weight* v_1 *and* v_2 *respectively* (v_1 *may equal* v_2). *Then* $G_n\rho \neq G_n\sigma$.

Proof. If $G_n\rho = G_n\sigma$, then $\rho = \tau f_i \sigma$ for some τ an inner automorphism, $f_i = \pm(u_i, 0, 0, 1)$. Let $\rho(S) = N(t, 1)$ and $\sigma(S) = N(t', 1)$ with $t \neq t'$. Then

$$f_i\sigma(S) = \pm(1, u_i, t'u_i^{-1}, 1 + t')$$

which is conjugate to $\pm(1, u_i, t'', 1 + t'')$ where $t''u \equiv t' \pmod{2^n}$. But by Corollary 1 to Theorem 1, $N(t, 1)$ is not conjugate to $N(t'', u_i)$ and so is not conjugate to $f_i\sigma(S)$. Therefore there is no inner automorphism τ such that $\rho = \tau f_i \sigma$.

THEOREM 6. Aut $(H_n) = \bigcup_\rho G_n\rho$, ρ *an automorphism of* H_n *of weight* $\geq n - 4$.

BIBLIOGRAPHY

1. J. DENNIN, *Subgroups of LF*(2, 2ⁿ), to appear.
2. J. GIERSTER, *Die Untergruppen der galois'schen Gruppe der Modulargleichungen fur den Fall eines primzahligen Transformationsgrades*, Math. Ann., vol. 18 (1881), pp. 319–365.
3. ———, *Uber die galois'sche Gruppe der Modulargleichungen, wenn der Transformationsgrad die Potenz einer Primzahl* >2 *ist*, Math. Ann., vol. 26 (1886), pp. 309–368.

4. D. McQuillan, *Classification of normal congruence subgroups of the modular groups*, American J. Math., vol. 87 (1965), pp. 285–296.
5. ———, *Some results on the linear fractional group*, Illinois J. Math., vol. 10 (1966), pp. 24–38.
6. M. Newman, *The structure of some subgroups of the modular group*, Illinois J. Math., vol. 6 (1962), pp. 480–487.
7. ———, *Normal congruence subgroups of the modular group*, American J. Math., vol. 85 (1963), pp. 419–427.
8. ———, *Classification of normal subgroups of the modular group*, Trans. Amer. Math. Soc., vol. 126 (1967), pp. 267–277.

University of Connecticut
Storrs, Connecticut