SOME RESULTS ON THE LINEAR FRACTIONAL GROUP

BY

DONALD L. MCQUILLAN

1. Introduction

Let Γ denote the 2×2 modular group, that is the group of 2×2 rational integral matrices of 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 modulo n to $\pm I$ where I is the identity matrix. The factor-group $\Gamma/\Gamma(n)$ plays a central role in the theory of elliptic modular functions of level n in the sense of Klein [6] and Igusa [5]. If $SL(2, n)$ denotes the group of 2×2 matrices of determinant 1 over the ring of integers modulo n then the linear fractional group $LF(2, n)$ is defined to be $LF(2, n) = SL(2, n)/\pm I$ where I is the identity matrix, and it is well known [3] that $\Gamma/\Gamma(n) \cong LF(2, n)$. Since

$$SL(2, nm) \cong SL(2, n) \times SL(2, m)$$

when $(n, m) = 1$ it follows that the study of the linear fractional groups reduces essentially to the study of those which are of prime power level. In this paper we consider $LF(2, p^n)$ where p is an odd prime (cf. [1], [2]) and $n \geq 1$. The main results obtained are Theorems 1 and 2 of Section 3 which give, respectively, a set of defining relations for this group and the structure of the automorphism group. In Section 2 explicit representatives of the conjugacy classes are obtained and a simple demonstration of the normal subgroup structure is given (cf. [7]).

For brevity we set $H_n = LF(2, p^n)$, $n = 1, 2, \cdots$, and denote a typical element by $A = \pm\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ or $\pm (a, b, c, d)$. We set $s = \operatorname{tr}(A) = \pm(a + d)$, and use h_n for the order of H_n. It is well known that

$$h_n = \tfrac{1}{2}p^n\phi(p^n)\psi(p^n)$$

where ϕ is the Euler function and $\psi(p^n) = p^{n-1}(p + 1)$. The homomorphism from H_n to H_r $(n \geq r)$ defined by

$$\pm \begin{pmatrix} a & b \\ c & d \end{pmatrix} (\operatorname{mod} p^n) \quad \rightarrow \quad \pm \begin{pmatrix} a & b \\ c & d \end{pmatrix} (\operatorname{mod} p^r)$$

will be denoted by f_r^n. This homomorphism is surjective and the kernel K_r^n has order $p^{3(n-r)}$. In particular K_{n-1}^n $(n > 1)$ consists of all elements of H_n of the form

$$\pm \begin{pmatrix} 1 + xp^{n-1} & yp^{n-1} \\ zp^{n-1} & 1 - xp^{n-1} \end{pmatrix}$$

and so is easily seen to be abelian of type (p, p, p) (cf. [2, p. 310]).

Received June 22, 1964.

We shall often use $a = b$ instead of $a \equiv b \pmod{p^n}$ where there is no danger of confusion.

Finally we shall write $m > 0$ when $(m|p) = 1$ and $m < 0$ when $(m|p) = -1$ where $(m|p)$ is the Legendre symbol.

2. Normal subgroups and conjugacy classes

Proposition 1 (i) and Proposition 2 of this section are straight generalizations of results of Gierster [1] for H_1. In [2] necessary and sufficient conditions were obtained for two elements of H_n to be conjugate but explicit representatives of the conjugacy classes were not given.

The following result will be useful.

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

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

where A, B, C, D are rational integers and $D \not\equiv 0 \pmod{p}$. Then $N_r = p^{r-1}N_1$.

The elementary proof by induction is omitted.

PROPOSITION 1. (i) *If $s^2 - 4 > 0$ then A is conjugate to a diagonal element;*

(ii) *If $s^2 - 4 < 0$ then A is conjugate to $\pm(0, -1, 1, s)$.*

Proof. (i) Since $(a - d)^2 + 4bc = s^2 - 4$ is a quadratic residue modulo p, there exists one or two solutions of the congruence

$$cx^2 + (a - d)x - b \equiv 0 \pmod{p^n}$$

according as $c \equiv 0$ or $c \not\equiv 0 \pmod{p}$. Let x be a solution and

$$X = \pm(0, -1, 1, x).$$

Then

$$XAX^{-1} = \pm(d_1, -c, 0, a_1)$$

where $d_1 = d - cx$ and $a_1 = a + cx$. Since $s^2 - 4 = (a_1 - d_1)^2$ it follows that $a_1 - d_1$ is a unit mod p^n and setting $B = \pm(0, -1, 1, -c(d_1 - a_1)^{-1})$ we find $B(d_1, -c, 0, a_1) \cdot B^{-1} = \pm(a_1, 0, 0, d_1)$.

(ii) It is required to find $B = \pm(u, v, w, x)$ in H_n such that

$$BA = \pm(0, -1, 1, s)B.$$

For this it is sufficient to solve the congruences

$$w \equiv -ua - vc \pmod{p^n}, \quad x \equiv -ub - vd \pmod{p^n}, \quad 1 \equiv ux - vw \pmod{p^n}.$$

We must therefore find u and v satisfying

$$cv^2 + (a - d)uv - bu^2 \equiv 1 \pmod{p^n}.$$

Since the norm mapping from $GF(p)(\sqrt{(s^2 - 4)})^*$ to $GF(p)^*$ is surjective (here K^* denotes the multiplicative group of the field K) there are $\psi(p)$

solutions of this congruence mod p and so by Lemma 1 there are $\psi(p^n)$ solutions mod p^n. This completes the proof of the proposition.

We set

$$D(a) = \pm\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, \qquad E(s) = \pm\begin{pmatrix} 0 & -1 \\ 1 & s \end{pmatrix}.$$

It is clear that there are $\frac{1}{2}\phi(p^n) - p^{n-1}$ diagonal elements $D(a)$ with the property that $s^2 - 4 > 0$, and that $D(a)$ and $D(b)$ are conjugate if and only if either $a = \pm b$ or $\pm b^{-1}$. Furthermore $D(a) = D(a^{-1})$ if and only if $a^2 = -1$, i.e., $(-1|p) = 1$. It follows easily that the elements of H_n for which $s^2 - 4 > 0$ split into $\frac{1}{4}[(p-3)p^{n-1} + 1 + (-1/p)]$ complete classes of conjugate elements. Furthermore the normalizer of such a $D(a)$ consists of all diagonal elements in H_n and so has order $\frac{1}{2}\phi(p^n)$; however if $(-1/p) = 1$ then $D(\sqrt{-1})$ is exceptional since its normalizer contains $\frac{1}{2}\phi(p^n)$ additional elements of the form $\pm(0, b, -b^{-1}, 0)$. In a similar fashion, one sees that the elements of H_n for which $s^2 - 4 < 0$ split into $\frac{1}{4}[\phi(p^n) + 1 - (-1/p)]$ complete classes of conjugate elements. The proof of the proposition also shows that when $s \not\equiv 0$ the normaliser of $E(s)$ has order $\frac{1}{2}\psi(p^n)$; however when $s = 0$, so that $(-1/p) = -1$, there are $\frac{1}{2}\psi(p^n)$ additional elements of the form $\pm(a, b, -b, a)$ in the normalizer.

Now let u be a fixed quadratic non-residue modulo p and let

$$R(t) = \pm\begin{pmatrix} 1 & 1 \\ t & 1+t \end{pmatrix}, \qquad N(t) = \pm\begin{pmatrix} 1 & u \\ t & 1+ut \end{pmatrix}$$

where $t = 0, p, 2p, \cdots, (p^{n-1}-1)p$. These elements have the property that $s^2 - 4 \equiv 0 \pmod p$, but they do not belong to K_1^n. Furthermore, no two of them are conjugate in H_n—this is clear from consideration of the traces and from the fact that $f_1^n(R(t))$ and $f_1^n(N(\tau))$ are not conjugate in H_1 [1]. Now let C denote the totality of elements A in H_n with the property that $s^2 - 4 \equiv 0 \pmod p$ but $A \notin K_1^n$. We note that if $A = \pm(a, b, c, d)$ is an arbitrary member of C, then, by transforming first with $\pm(0, -1, 1, 0)$ if necessary, we may assume that $b \not\equiv 0 \pmod p$.

PROPOSITION 2. *If A belongs to C then A is conjugate in H_n to $R(s-2)$ or $N((s-2)/u)$ according as $b > 0$ or $b < 0$.*

Proof. It is required to find $B = \pm(y, v, w, x)$ in H_n such that $BA \equiv \pm(1, r, t, 1+rt)B$ where $r = 1$ or u and $t = (s-2)/r$. This yields the congruences

$$w \equiv r^{-1}[y(a-1) + vc] \pmod{p^n}$$

$$x \equiv r^{-1}[v(d-1) + yb] \pmod{p^n}$$

$$1 \equiv yx - vw \pmod{p^n}$$

which in turn give

$$by^2 + (d-a)yv - cv^2 \equiv r \pmod{p^n}.$$

A solution of this is $v \equiv 0$, $y \equiv \sqrt{(rb^{-1})} \pmod{p^n}$. This completes the proof of the proposition.

The proof shows that the order of the normalizer of $\pm(1, r, t, 1 + rt)$ is half the number of solutions of

$$ry^2 + rtyv - tv^2 \equiv r \pmod{p^n}.$$

By Lemma 1 this order is therefore p^n and consequently C splits into $2p^{n-1}$ complete classes of conjugate elements, each class containing $\frac{1}{2}\phi(p^n)\psi(p^n)$ elements.

It only remains to determine representatives of the conjugacy classes in K_1^n. Since K_r^n is normal in H_n and $K_{r+1}^n \subset K_r^n$, $1 \leq r \leq n - 1$, the set-theoretic difference $K_r^n - K_{r+1}^n$ splits in H_n into complete classes of conjugate elements. The following matrices belong to this set:

$$M(w, r) = \pm(1, wp^r, wup^r, 1 + w^2up^{2r})$$
$$D(1 + wp^r) = \pm(1 + wp^r, 0, 0, (1 + wp^r)^{-1})$$

where $1 < w = p^{n-r}$ and $(w, p) = 1$,

$$P(m, r) = \pm(1, p^{r+1}, mp^{r+1}, 1 + mp^{2r+2})(1, p^r, 0, 1)$$
$$Q(m, r) = \pm(1, p^{r+1}, mp^{r+1}, 1 + mp^{2r+2})(1, up^r, 0, 1)$$

where $1 \leq m \leq p^{n-r-1}$.

In these expressions, u is, as before, a fixed quadratic non-residue mod p. We note that $\pm(1, p^r, 0, 1)$ and $\pm(1, up^r, 0, 1)$ are not conjugate in H_{r+1} and therefore no $P(m, r)$ is conjugate in H_n to a $Q(m, r)$. In the following proposition $[A]$ denotes the conjugacy class represented by A.

PROPOSITION 3. (a) $[M(w, r)] = [M(w_1, r)]$ *if and only if*

$$w \equiv \pm w_1 \pmod{p^{n-r}};$$

$[M(w, r)]$ *contains* $\phi(p^{2n-2r})$ *elements.*

(b) $[P(m, r)] = [P(m_1, r)]$ *if and only if* $m \equiv m_1 \pmod{p^{n-r-1}}$; $[P(m, r)]$ *contains* $\frac{1}{2}\phi(p^{n-r})\psi(p^{n-r})$ *elements. An identical statement holds with* P *replaced by* Q.

(c) $[D(1 + wp^r)] = [D(1 + w_1p^r)]$ *if and only if* $D(1 + wp^r) = D(1 + w_1p^r)$ *or* $D(1 + w_1p^r)^{-1}$; $[D(1 + wp^r)]$ *contains* $\psi(p^{n-2r})$ *elements.*

Proof. (a) If $\pm(a, b, c, d)M(w, r) = \pm M(w_1, r)(a, b, c, d)$, then

(i) $bwu \equiv cw_1 \pmod{p^{n-r}}$
(ii) $d(w^2 - w_1^2)up^r \equiv bw_1u - cw \pmod{p^{n-r}}$
(iii) $dw^2up^r \equiv dw_1 - aw \pmod{p^{n-r}}$
(iv) $cw_1^2p^r \equiv dw - aw_1 \pmod{p^{n-r}}$.

Combining (i) and (ii) gives

$$dw_1(w^2 - w_1^2)p^r \equiv b(w_1^2 - w^2) \pmod{p^{n-r}}$$

and therefore if $w^2 - w_1^2 \not\equiv 0 \pmod{p^{n-r}}$ then $b \equiv 0 \pmod{p}$. Combining (i) and (iv) gives

$$bw^2up^r \equiv dw^2w_1^{-1} - aw \pmod{p^{n-r}}$$

and using (iii) we get

$$d(w^2 - w_1^2) \equiv 0 \pmod{p^{n-r}}.$$

Consequently if $w^2 - w_1^2 \equiv 0 \pmod{p^{n-r}}$ then $d \equiv 0 \pmod{p^{n-r}}$; but $b \equiv d \equiv 0 \pmod{p}$ is impossible and so $w^2 \equiv w_1^2 \pmod{p^{n-r}}$. Since w and w_1 are relatively prime to p this implies that $w \equiv \pm w_1 \pmod{p^{n-r}}$. Now using the above four congruences with $w = w_1$ it is clear that $\pm(a, b, c, d) \in H_n$ is in the normalizer of $M(w, r)$ if and only if $c \equiv bu$, $d \equiv a + bwup^r \pmod{p^{n-r}}$ and $a^2 + wup^rab - ub^2 \equiv 1 \pmod{p^{n-r}}$. By Lemma 1 this congruence has $\psi(p^{n-r})$ solutions and using the fact that K_{n-r}^n has order p^{3r} it is seen that the normaliser of $M(w, r)$ has order $\frac{1}{2}\psi(p^{n+2r})$. This proves (a).

(b) If $\pm(a, b, c, d)P(m, r) = \pm P(m_1, r)(a, b, c, d)$ then

$$\begin{aligned}
&\text{(i)} && bmp \equiv c(1 + p) && \pmod{p^{n-r}}\\
&\text{(ii)} && bmp^{r+1} \equiv d - a && \pmod{p^{n-r}}\\
&\text{(iii)} && (dm - am_1)p \equiv cm_1(1 + p)p^{r+1} && \pmod{p^{n-r}}\\
&\text{(iv)} && bm_1 p \equiv c(1 + p) + d(1 + p)(m - m_1)p^{r+1} && \pmod{p^{n-r}}.
\end{aligned}$$

Combining (i) and (iii) gives

$$d(1 + p)(m - m_1)p^{r+1} \equiv bp(m_1 - m) \pmod{p^{n-r}}$$

and therefore if $m - m_1 \not\equiv 0 \pmod{p^{n-r-1}}$ then $b \equiv 0 \pmod{p}$. Combining (ii) and (iii) gives

$$pa(m - m_1) \equiv bm^2p^{r+2} - cm_1(1 + p)p^{r+1} \pmod{p^{n-r}}$$

and using (i) we get

$$pa(m - m_1) \equiv c(1 + p)p^{r+1}(m - m_1) \pmod{p^{n-r}}.$$

If $m - m_1 \not\equiv 0 \pmod{p^{n-r-1}}$ then $a \equiv 0(p)$. But $a \equiv b \equiv 0 \pmod{p}$ is impossible.

Using the above four congruences with $m = m_1$ shows that $\pm(a, b, c, d) \in H_n$ is in the normalizer of $P(m, r)$ if and only if

$$c \equiv bmp(1 + p)^{-1} \pmod{p^{n-r}}, \qquad d \equiv a + bmp^{r+1} \pmod{p^{n-r}}$$

and

$$a^2 + mp^{r+1}ab - mp(1 + p)^{-1}b^2 \equiv 1 \pmod{p^{n-r}}.$$

By Lemma 1 there are $2p^{n-r}$ solutions of this congruence. The rest of the argument proceeds as in (a).

The proof of (c) is similar and is omitted.

A simple computation gives $p^{3(n-r)} - p^{3(n-r-1)}$ elements in the conjugacy classes represented by the non-conjugate $M(w, r)$, $D(1 + wp^r)$, $P(m, r)$,

$Q(w, r)$. But this is exactly the number of elements in the set $K_r^n - K_{r+1}^n$. This completes the discussion of representatives of the conjugacy classes of H_n.

It has already been remarked (see Section 1), that K_{n-1}^n is abelian of type (p, p, p) from which it follows by an easy induction argument, that the order of any element of K_r^n is a divisor of p^{n-r}; we shall make use of the fact that $\pm(1, p^r, 0, 1)$ belongs to K_r^n and has precisely the order p^{n-r}. On the other hand if A does not belong to K_1^n and m is the order of $f_1^n(A)$ then (cf. [1]) $m = p$ if $s^2 - 4 \equiv 0 \pmod p$, $m \mid (p-1)/2$ if $s^2 - 4 > 0$ and $m \mid (p+1)/2$ if $m < 0$. It follows that the order of A divides p^n or $\frac{1}{2}\phi(p^n)$ or $\frac{1}{2}\psi(p^n)$. More precise information concerning the order of elements in the set C is given by the following lemma, which is stated without proof since it is a special case of a result proved in [2, pp. 316–7].

LEMMA 2. *If $p > 3$ then $R(t)$ has order p^n and*

$$R(t)^{p^{n-1}} = \pm(1, p^{n-1}, 0, 1).$$

If $p = 3$, then $R(t)$ has order 3^n if and only if $t/3 \equiv 0$ or $1 \pmod 3$ and then

$$R(t)^{3^{n-1}} = \pm(1, (1 + t/3)3^{n-1}, 0, 1).$$

As a corollary to this lemma and the preceding remarks we can state

LEMMA 3. *Elements in H_n which have order p^n belong to C.*

When $p > 3$ the group H_1 is simple [1] so that K_1^n is a maximal normal subgroup of H_n. However, when $p = 3$, H is just the alternating group of four letters, and hence the elements of order 2, namely

$$\pm\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \pm\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \quad \pm\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$$

together with the identity form a normal subgroup of order 4, say V_4. Therefore the inverse image of V_4 under f_1^n is a maximal normal subgroup of H_n of order 4.3^{3n-3} and will be denoted by M_n.

LEMMA 4. *K_{n-1}^n is the center of K_1^n. No proper subgroup of K_{n-1}^n is normal in H_n.*

Proof. The group K_1^n consists of all elements in H_n of the form

$$A = \pm(1 + ap, bp, cp, 1 + dp)$$

where

$$a, b, c \equiv 0, 1, 2, \cdots, p^{n-1} - 1 \pmod{p^{n-1}}$$

and

$$d \equiv (-a + bcp)(1 + ap)^{-1} \pmod{p^{n-1}}.$$

It is easily verified that K_{n-1}^n is in the center of K_1^n. On the other hand, if A is in the center then A commutes with $\pm(1, p, 0, 1)$ and $\pm(1, 0, p, 1)$. These conditions give

$$b \equiv c \equiv 0 \pmod{p^{n-2}} \quad \text{and} \quad a \equiv d \pmod{p^{n-2}}.$$

But since $d \equiv (-a + bcp)(1 + ap)^{-1} \pmod{p^{n-2}}$ it follows that

$$a(2 + ap) \equiv 0 \pmod{p^{n-2}}$$

and so

$$a \equiv d \equiv 0 \pmod{p^{n-2}}.$$

Therefore A belongs to K_{n-1}^n. Now if N is a proper subgroup of K_{n-1}^n which is normal in H_n then the order of N is either p or p^2 and it splits in H_n into complete conjugacy classes. It is easy to see from Proposition 3, with $r = n - 1$, that this is impossible.

PROPOSITION 4. *The set $\{K_r^n\}_{r=0}^n$ gives all normal subgroups of H_n when $p > 3$. When $p = 3$, there is one other, namely M_n. In particular, every normal subgroup is a characteristic subgroup.*

Proof. Let N be normal in H_n and suppose first that $f_1^n(H_n) = \{1\}$ so that $N \subset K_1^n$. We prove by induction that $N = K_r^n$ for some r, $1 \leq r \leq n$; the case $n = 1$ is known. Now if $n > 1$ and $f_{n-1}^n(N) = \{1\}$ then $N = K_n^n$ or K_{n-1}^n by the preceding lemma. Otherwise by the induction hypothesis, $f_{n-1}^n(N) = K_r^{n-1}$, $1 \leq r \leq n - 2$, and therefore $N \subset K_r^n$ and

$$N/N \cap K_{n-1}^n \cong K_r^{n-1}.$$

We show that $N \cap K_{n-1}^n = \{1\}$ brings a contradiction. In that case by considering orders it follows that $N \cdot K_{n-1}^n = K_r^n$ and $N \cong K_r^{n-1}$. However this is impossible since by Lemma 4 and a previous remark the maximum order of elements in $N \cdot K_{n-1}^n$ is p^{n-r-1} while K_r^n contains elements of order p^{n-r}. If $p = 3$ and $f_1^n(N) = V_4$ then $N \subset M_n$ and we prove by inductino that $N = M_n$. Again the case $n = 1$ is known. When $n > 1$ then $f_{n-1}^n(N) = M_{n-1}$ by the induction hypothesis and if $N \cap K_1^n \supset K_{n-1}^n$ it follows that $N = M_n$. Otherwise by the preceding part of the proof $N \cap K_1^n = \{1\}$ so that $N \cong M_{n-1}$. By comparing orders it is clear that $N \cdot K_1^n = M_n$, $n = 2$ and hence $N \cong V_4$. However the remarks following Proposition 1 concerning normalizers show that this is impossible.

There remains only the possibility that $f_1^n(N) = H_1$. In that case it is easy to see by induction that $N = H_n$. Indeed the case $n = 1$ is trivial; if $n > 1$ then $f_{n-1}^n(N) = H_{n-1}$ by the induction hypothesis and if $N \supset K_{n-1}^n$ then $N = H_n$. Otherwise, by the preceding parts of the proof, $N \cap K_1^n = \{1\}$ and $N \cap M_n = \{1\}$ ($p = 3$), and therefore $N \cong H_{n-1}$. If $p \neq 3$ this is impossible since $R(t) \in N$ for some t and this element has order p^n. If $p = 3$ then clearly $N \cdot M = H_n$ and the order of N is 3 by one of the isomorphism theorems. This is a contradiction. The proof is complete.

3. The automorphisms of H_n

It is well known that the elements

$$S_0 = \pm(1, 1, 0, 1) \quad \text{and} \quad T_0 = \pm(0, -1, 1, 0)$$

generate H_n. The orders of these elements are p^n and 2 respectively while $T_0 S_0 = \pm(0, -1, 1, 1)$ has order 3. The following theorem is analogous to a result for $LF(2, GF(p^n))$; we use the notation Z_n for the ring of integers modulo p^n.

THEOREM 1. *Let the group G be generated by the elements S and T, which are subject to the sole defining relations*

$$\text{(i)} \qquad S^{p^n} = 1, \qquad T^2 = 1,$$

$$\text{(ii)} \qquad M\left(\frac{r-1}{rs-1}\right) M(1-rs) M\left(\frac{s-1}{rs-1}\right) M(r) M(s) = 1$$

where $M(a) = TS^a$ *and* $rs - 1$ *is a unit in* Z_n,

$$\text{(iii)} \qquad M(r)M(s)M(u)M\left(\frac{rs}{rsu - r - u}\right) \cdot M(rsu - r - u)M\left(\frac{su}{rsu - r - u}\right) = 1$$

where $rs \equiv su \equiv 1 \pmod p$ *but* $r \equiv u \equiv s^{-1} \pmod{p^n}$ *is excluded.*

Then H_n *is isomorphic to G under the map which sends* S_0 *and* T_0 *to S and T respectively.*

Proof. Taking $T = T_0$, $S = S_0$ it is easily verified that the above relations are consistent. From this it also follows that the theorem is proved if we show that the order of G is not greater than the order of H_n. For clarity in printing we shall write $S(a)$ for S^a. We first show that the excluded case in (iii) above follows from (ii). The relation to be verified is

$$TS(r^{-1})TS(r)TS(r^{-1}) = S(r)TS(r^{-1})TS(r)T$$

or equivalently (by rearrangement)

$$S(-r)TS(r^{-1})TS(r)T = TS(r^{-1})TS(r)TS(-r^{-1}).$$

Putting $s = -r^{-1}$ in (ii) we obtain

$$M\left(\frac{1-r}{2}\right) M(2) M\left(\frac{1-r^{-1}}{2}\right) TM(r^{-1})M(r)M(-r^{-1}) = 1$$

and so our relation is verified if

$$M\left(\frac{1-r}{2}\right) M(2) M\left(\frac{1-r^{-1}}{2}\right) TS(-r)TS(r^{-1})TS(r)T = 1.$$

However this is verified if we replace r by $-r$ and s by r^{-1} in (ii).

We consider now the following subsets of G:

$$A = \{TS(x)TS(y)TS(z)\} \quad \text{and} \quad B = \{S(x)TS(y)TS(z)\}$$

where x, y, z run through all members of Z_n with the restrictions that y is a unit and, in the set B, $xy \equiv 1 \pmod p$. It will be shown that $A \cup B$ contains all members of G by proving that A and B are permuted among themselves in multiplying on the left by T and each $S(u)$. Now TB is contained in A. A typical member of TA has the form $S(x)TS(y)TS(z)$ and if $xy \equiv 1 \pmod p$ this belongs to B. If $xy - 1$ is a unit in Z_n then take $r = -x$ $s = -y$ in (ii), solve for $S(x)TS(y)TS(z)$ and obtain this element in the form of an element of A. Next multiply on the left by $S(u)$, $u \neq 0$. The argument used on TA now applies to $S(u)B$. Finally consider $S(u)A$, which consists of elements of the form

$$R = S(u)TS(x)TS(y)TS(z).$$

If $xy - 1$ is a unit in Z_n put $r = 1 - xy$ and $s = (1 - y)/(1 - xy)$ in (ii) and get

$$R = S\left(u - \frac{1-y}{1-xy}\right) TS(xy - 1)TS\left(\frac{x + z - 1 - xyz}{1 - xy}\right).$$

Again the argument used on TA shows that R belongs to $A \cup B$. Suppose now that $xy - 1$ is a non-unit but that $ux - 1$ is a unit. Then from (ii) we obtain

$$TR = S\left(\frac{1-x}{ux-1}\right) TS(ux - 1)TS\left(\frac{1-u}{ux-1} + y\right) TS(z).$$

Now

$$(ux - 1)\left(\frac{1-u}{ux-1} + y\right) - 1 \equiv -y \pmod p$$

and is therefore a unit in Z_n so that making use of (ii) once more we obtain

$$TR = S(a)TS(b)TS(c) \qquad \text{for some } a, b, c \text{ with } b \equiv y \pmod p$$

and hence is a unit. It follows that R is in A. Finally suppose that $ux \equiv xy \equiv 1 \pmod p$. Then from (iii) we obtain

$$R = TS(a)TS(b)TS(c)$$

where a is a unit. Hence R is in A.

We have therefore shown that $G = A \cup B$. The number of elements in this union is $p^{2n}\phi(p^n) + p^{2n-1}\phi(p^n) = p^n\phi(p^n)\psi(p^n)$. The order of H_n is just half of this while the order of G is a multiple of that of H_n and is not greater than $p^n\phi(p^n)\psi(p^n)$. Hence G and H_n are isomorphic if two notationally distinct members of A, say, are equal. This is true of $(TS)^3$ and $(TS^{-1})^3$ which can be seen by taking $r = 1$, $s = 0$ in (ii). This completes the proof of the theorem.

Now the center of H_n reduces to the identity and therefore the group I_n of inner automorphisms has order h_n, $n = 1, 2, \cdots$. Let u be once more a fixed quadratic non-residue modulo p and let $U = \pm(u, 0, 0, 1)$. The element U does not belong to H_n and the map f from H_n to H_n defined by

$$f(A) = UAU^{-1}$$

is an outer automorphism with the property that f^2 belongs to I_n. It follows that

$$G_n = I_n \cup I_n f$$

is a group of automorphisms of order $2h_n$ (cf. [1]).

LEMMA 1. *If σ is an arbitrary automorphism of H_n then there is an automorphism τ in G_n such that*

$$\tau\sigma(S_0) = R(t)$$

$$\tau\sigma(T_0) = \pm \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix}$$

where $t \equiv 0 \pmod p$ and $c + bt \equiv \pm 1 \pmod{p^n}$.

Proof. Since $\sigma(S_0)$ has order p^n it belongs to C by Lemma 3 of Section 2 and hence by Proposition 2 there is an inner automorphism which sends it to $R(t)$ or $N(t)$. However $f(N(t)) = \pm(1, u^2, u^{-1}t, 1 + ut)$ and by Proposition 2 again there is an inner automorphism which sends this element to $R(ut)$. Consequently there is an automorphism ρ in G_n such that $\rho\sigma(S_0) = R(t)$ for some $t \equiv 0 \pmod p$. We now prove that there is an integer m with the property

$$R(t)^{-m}\rho\sigma(T_0)\cdot R(t)^m = \pm \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix}$$

where $c + bt \equiv \pm 1 \pmod{p^n}$. This is true by a lemma of Hecke [3] when $n = 1$ and so we proceed by induction. Since K_{n-1}^n is a characteristic subgroup of H_n the automorphism $\rho\sigma$ induces an automorphism $\overline{\rho\sigma}$ of H_{n-1} and

$$\overline{\rho\sigma} : S_0 \pmod{p^{n-1}} \to R(t) \bmod p^{n-1}.$$

If we now use the induction hypothesis, go back up to H_n and recall that an element of H_n of order 2 has trace zero, we get

$$R(t)^{-r}\cdot\rho\sigma(T_0)\cdot R(t)^r = \pm \begin{pmatrix} a & b \\ c & -a \end{pmatrix}$$

where $a \equiv 0 \ (p^{n-1})$, c is a unit mod p^n, and r is an integer. Now if v is an arbitrary integer then

$$R(t)^{vp^{n-1}} = \pm \begin{pmatrix} 1 & \varepsilon v p^{n-1} \\ 0 & 1 \end{pmatrix}$$

by Lemma 2 of Section 2, where $\epsilon = \pm 1$, and therefore

$$\pm R(t)^{-vp^{n-1}} \begin{pmatrix} a & b \\ c & -a \end{pmatrix} \cdot R(t)^{vp^{n-1}} = \begin{pmatrix} a - \varepsilon cvp^{n-1} & b \\ c & -a + \varepsilon cvp^{n-1} \end{pmatrix}.$$

We can clearly choose v so that $a \equiv \varepsilon cvp^{n-1}$. If then $m = r + vp^{n-1}$ and i is the inner automorphism induced by $R(t)^m$ we have

$$i\rho\sigma(S_0) = R(t), \qquad i\rho\sigma(T_0) = \pm \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix}.$$

The relation $c + bt \equiv \pm 1 \pmod{p^n}$ follows at once from the fact that $i\rho\sigma(S_0 \cdot T_0)$ has order 3 so that its trace is ± 1. Finally, setting $\tau = i\rho$, we obtain the statement in the lemma.

If $t \equiv 0 \pmod{p^n}$ then $\tau\sigma$ is identity and so σ belongs to G_n. Otherwise suppose $t \equiv 0 \pmod{p^v}$ but $t \not\equiv 0 \pmod{p^{v+1}}$ where $1 \leq v \leq n - 1$. We set $v(t) = v$ and make the following

DEFINITION. An automorphism ρ of H_n will be said to have weight v if $\rho(S_0) = R(t)$, $\rho(T_0) = \pm(0, b, c, 0)$ where $c + bt \equiv \pm 1 \pmod{p^n}$, and $v(t) = v$.

PROPOSITION. *When $p > 5$ there are no automorphisms of H_n of weight $n - 1$ $(n > 1)$. When $p = 3$ or 5 there are no automorphisms of H_n of weight $n - 2$ $(n > 2)$.*

Proof. Let ρ be an automorphisms of H_n of weight v. The element $A = T_0 S_0^r T_0 S_0^s$ has order 2 when $rs \equiv 2 \pmod{p^n}$ (cf. Theorem 1), and therefore $B = \rho(A)$ has trace zero. Since

$$R(t)^r \equiv \pm \begin{pmatrix} 1 + \binom{r}{2} t + \binom{r+1}{4} t^2 & r + \binom{r+1}{3} t + \binom{r+2}{s} t^2 \\ rt + \binom{r+1}{3} t^2 & 1 + \binom{r+1}{2} t + \binom{r+2}{4} t^2 \end{pmatrix} \pmod{t^3}$$

it follows easily that $\operatorname{tr}(B) \equiv \pm(a_1 t + a_2 t^2) \pmod{t^3}$ where

$$a_1 \equiv \frac{2(r^2 - 1)(r^2 - 4)}{3r^2} \pmod{p^n}$$

and

$$a_2 \equiv \frac{(r^2 - 1)^2(r^2 - 4)^2}{15r^4} + \frac{(r^2 - 1)(r^2 - 4)}{18r^4} \pmod{p^n}.$$

Now if $v(t) = n - 1$ $(n > 1)$ then $\operatorname{tr}(B) \equiv 0 \pmod{p^n}$ for all units $r \pmod{p^n}$ if and only if $p = 3$ or 5. If $v(t) = n - 2$ with $n \geq 4$, (so that $t^2 \equiv 0 \pmod{p^n}$)) there are always units $r \pmod{p^n}$ such that $\operatorname{tr}(B) \not\equiv 0 \pmod{p^n}$ no matter what the value of p. Finally when $n = 3$, $v(t) = 1$ and $p = 3$ or 5 we have $\operatorname{tr}(B) \equiv \pm pt \pmod{p^3}$. This completes the proof of the proposition.

COROLLARY 1. *When $p > 5$ there are no automorphisms of H_n of weight v where $1 \leq v \leq n - 1$ $(n > 1)$. When $p = 3$ or 5 there are no automorphisms of H_n* of weight v where $1 \leq v \leq n - 2$ $(n > 2)$.

Proof. Let ρ be an automorphism of H_n of weight v and suppose that $p > 5$. Then, since K_{v+1}^{n} is a characteristic subgroup of H_n, ρ induces an automorphism of H_{v+1} which has weight v. This contradicts the proposition. The statement concerning $p = 3$ or 5 is proved similarly.

COROLLARY 2. Aut $(H_n) = G_n$ *when $p > 5$.*

Proof. This is immediate from the previous corollary and Lemma 1. It only remains to consider the case $v(t) = n - 1$ when $p = 3$ or 5. The conditions $c + bt \equiv \pm 1 \pmod{p^n}$ and $bc \equiv -1 \pmod{p^n}$ imply now that $b = -1 + t$ and $c = 1 + t$. We therefore set

$$S = R(t) \quad \text{and} \quad T = \pm \begin{pmatrix} 0 & -1 + t \\ 1 + t & 0 \end{pmatrix}$$

and verify that the assignment $S_0 \to S$, $T_0 \to T$ induces an automorphism of H_n. For this it is sufficient to verify the relations of Theorem 1. The following remark will simplify the calculations. We write

$$M(r) = TS^r = M_0(r) + tA(r);$$

here

$$M_0(r) = T_0 S_0^r \quad \text{and} \quad A(r) = \pm \begin{pmatrix} -r & b(r) \\ c(r) & d(r) \end{pmatrix}$$

where $b(r) = 1 - \frac{1}{2}r(r + 1)$, $c(r) = 1 + \frac{1}{2}r(r - 1)$ and $d(r) = \frac{1}{6}r(r^2 + 5)$. It is clear from this that the terms involving t in $M(r)$ depend only on the value of r modulo p, except that when $p = 3$ the term $td(r)$ depends on the value of r modulo 3^2. Let now $F(r, s)$ and $L(r, s, u)$ denote the expressions on the left in relations (ii) and (iii) respectively of Theorem 1, and $F_0(r, s)$, $L_0(r, s, u)$ the same expressions with S and T replaced by S_0 and T_0.

LEMMA 2. *Let $w \equiv r$, $x \equiv s$, and $y \equiv u \pmod{p}$. Then*

(i) $F(w, x) = \pm I$ *implies* $F(r, s) = \pm I$

(ii) $L(w, x, y) = \pm I$ *implies* $L(r, s, u) = \pm I$.

Proof. (i) Let $w_1 = (w - 1)/(wu - 1)$, $w_2 = 1 - wx$, $w_3 = (u - 1)/(wu - 1)$, $w_4 = w$, $w_5 = u$ and define r_i similarly in terms of r and s, $i = 1, 2, \cdots, 5$. Since

$$\prod_{i=1}^{5} M_0(w_i) = \prod_{i=1}^{5} M_0(r_i) = \pm I$$

it follows from the remark preceding the lemma that, when $p = 5$

$$\begin{aligned}\prod_{i=1}^{5} M(r_i) &= \prod_{i=1}^{5} [M_0(r_i) + tA(w_i)] \\ &= \prod_{i=1}^{5} [M_0(w_i) + tA(w_i)] \\ &= \pm I.\end{aligned}$$

When $p = 3$ we can write

$$\prod_{i=1}^{5} M(r_i) = \prod_{i=1}^{5} \left[M_0(r_i) + tA(w_i) \pm t\left(0, 0, 0, \frac{r_i - w_i}{3}\right)\right]$$

since

$$d(r_i) - d(w_i) \equiv (r_i - w_i)/3 \pmod 3.$$

Using the fact that $\prod_{i=1}^{5} M_0(r_i) = \prod_{i=1}^{5} M_0(w_i) = \prod_{i=1}^{5} M(w_i) = \pm I$ we get

$$\begin{aligned}\prod_{i=1}^{5} M(r_i) &= \prod_{i=1}^{5} \left[M_0(w_i) + tA(w_i) \pm t\left(0, 0, 0, \frac{r_i - w_i}{3}\right)\right] \\ &= \prod_{i=1}^{5} \left[M(w_i) \pm t\left(0, 0, 0, \frac{r_i - w_i}{3}\right)\right] \\ &= \prod_{i=1}^{5} \left[M_0(w_i) \pm t\left(0, 0, 0, \frac{r_i - w_i}{3}\right)\right] \\ &= \prod_{i=1}^{5} M_0\left(w_i + t\,\frac{r_i - w_i}{3}\right)] \\ &= F_0\left(w_4 + t\,\frac{r_4 - w_4}{3}, \qquad w_s + t\,\frac{r_5 - w_5}{3}\right) \\ &= \pm I.\end{aligned}$$

The proof of (ii) is similar.

Now if r, s, u satisfy $rs \equiv su \equiv 1 \pmod p$ one can choose w, x, y congruent respectively to r, s, $u \pmod p$ and satisfying $w \equiv y \equiv x^{-1} \pmod{p^n}$. It follows from the preceding lemma and the remark made at the beginning of the proof of Theorem 1 that relation (iii) of that theorem follows from relation (ii) in the present special case. Now in relation (ii) let $rs \equiv d \pmod p$ $0 \leq d \leq p - 1$, $d \not\equiv 1$. One can choose w, x congruent respectively to r, $s \pmod p$ and satisfying $wx \equiv d \pmod{p^n}$, and then $F(w, x) = \pm I$ will imply $F(r, s) = \pm I$. When $d = 2$ the proof of Lemma 1 shows that $F(w, x) = \pm I$. When $d = 0$ the relation to be verified is

$$TS^w \cdot TS^x = S^x TS^w T, \qquad wx \equiv 0 \pmod{p^n}.$$

However, an easy calculation shows that $TS^w \cdot TS^x = (TS^{-w} \cdot TS^{-x})^{-1}$ and this gives the required relation.

It therefore only remains to verify relation (ii) for $d = 3$ or 4 when $p = 5$. Putting $k^{-1} \equiv 1 - wu \pmod{5^n}$ the relation can be written

$$M(k(1 - w))M(k - 1) = [M(k(1 - u))M(w)M(u)]^{-1}.$$

A straightforward calculation yields the following congruences:

$$(w^2 + u^2)(3k^2 - 2k - 1) \equiv 0$$

$$w^3(1 - k^2) \equiv 2uk^{-1}(k^3 + k^2 - k - 1) \pmod 5$$

$$w^3k(k^2 - 1) + 2w^2(k - 1)(k^2 + k + 1)$$
$$\equiv -2u(k^2 - 1)(k + 1) - u^2k(k + 3)(k - 1).$$

Bearing in mind that $k \equiv 2$ or $3 \pmod 5$ and $w \equiv (1 - k^{-1})u^{-1}$ it is a simple matter to verify that these congruences are satisfied.

Finally, relation (i) is satisfied when $p = 5$ but when $p = 3$ we have the condition $t/3 \equiv 0$ or $1 \pmod 3$ from Lemma 2 of Section 2. We have proved the

PROPOSITION. *When $p = 3$ or 5, and $v(t) = n - 1$ there is an automorphism of H_n which sends*

$$S_0 \text{ to } \pm \begin{pmatrix} 1 & 1 \\ t & 1 + t \end{pmatrix} \quad \text{and} \quad T_0 \text{ to } \pm \begin{pmatrix} 0 & -1 + t \\ 1 + t & 0 \end{pmatrix},$$

with the condition that $t/3 \equiv 0$ or $1 \pmod 3$ when $p = 3$.

Now if ρ and μ are automorphisms of weight $n - 1$ the cosets $G_n\,\rho$ and $G_n\,\mu$ are distinct. We can therefore collect our results in

THEOREM 2. *The order of* Aut (H_n) *is $d_n h_n$ where h_n is the order of H_n, $d_1 = 2$, and, when $n > 1$,*

$$\begin{aligned} d_n &= 2, && \text{if } p > 5, \\ &= 10, && \text{if } p = 5, \\ &= 6, && \text{if } p = 3,\ n > 2, \\ &= 4, && \text{if } p = 3,\ n = 2. \end{aligned}$$

REFERENCES

1. G. GIERSTER, *Die Untergruppen der galois'schen Gruppe der Modulargleichungen für den Fall eines primzahligen Transformationsgrades*, Math. Ann., vol 18 (1881), pp. 319–365.
2. ———, *Über die galois'sche Gruppe der Modulargleichungen, wenn der Transformationsgrad die Potenz einer Primzahl > 2 ist*, Math. Ann., vol. 26 (1886), pp. 309–368.
3. E. HECKE, *Die eindeutige Bestimmung der Modulfunktionen q-ter Stufe durch algebraische Eigenschaften*, Math. Ann., vol. 111 (1935), pp. 293–301.

4. R. C. GUNNING, *Lectures on Modular Forms*, Princeton, Princeton University Press, 1962.
5. J. I. IGUSA, *Fibre systems of Jacobian varieties, III: Fibre systems of elliptic curves*, Amer. J. Math., vol. 81 (1959), pp. 453–476.
6. F. KLEIN, *Zur Theorie der Elliptischen Modulfunktionen*, Collected Works, vol. 3 (1923), pp. 169–178.
7. D. MCQUILLAN, *Some structure theorems for* $SL(2, n)$, Abstracts, International Congress of Mathematicians, Stockholm, 1962.

UNIVERSITY OF WISCONSIN
MADISON, WISCONSIN