THE NORMALIZER OF $\Gamma_0(N)$ IN PSL$(2, \mathbb{R})$

by M. AKBAS and D. SINGERMAN

(Received 17 April, 1989)

1. The structure of the normalizer. Let Γ denote the modular group, consisting of the Möbius transformations

$$z \to \frac{az+b}{cz+d} \qquad a, b, c, d \in \mathbb{Z}, \qquad ad - bc = 1. \tag{1}$$

As usual we denote the above transformation by the matrix $V = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ remembering that V and $-V$ represent the same transformation. If N is a positive integer we let $\Gamma_0(N)$ denote the transformations for which $c \equiv 0 \bmod N$. Then $\Gamma_0(N)$ is a subgroup of index

$$N \prod_{p \mid N} \left(1 + \frac{1}{p}\right) \tag{2}$$

the product being taken over all prime divisors of N.

In this paper we are interested in the normalizer of $\Gamma_0(N)$ in the group PSL$(2, \mathbb{R})$ of all Möbius transformations with real coefficients and determinant one.

This normalizer has acquired significance because it is related to the Monster simple group [2]. It has also played an important role in work on Weierstrass points on the Riemann surfaces associated to $\Gamma_0(N)$, [5], on Modular forms [1] and on Ternary quadratic forms [6].

We denote the normalizer by $\Gamma_B(N)$ and define

$$B(N) = \Gamma_B(N)/\Gamma_0(N).$$

Our main result gives the structure of $B(N)$ for all integers $N \geq 2$. Such a result was given without proof in [1] but we have found several errors in their list, so it may be worthwhile to give a careful treatment. We use the description of the normalizer given by Conway and Norton [2]. No proof was given though a verification can be obtained by the accounts in [1], [5], [7]. The normalizer is given by the transformations corresponding to the matrices

$$\begin{pmatrix} ae & b/h \\ c\dfrac{N}{h} & de \end{pmatrix} \tag{3}$$

where all symbols represent integers, h is the largest divisor of 24 such that $h^2 \mid N$, $e > 0$ is an exact divisor of N/h^2 and the determinant of the matrix is e. (We say that e is an *exact divisor* of M if $e \mid M$ and $(e, M/e) = 1$.)

If $M = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ is the prime-power decomposition of M then M has 2^r exact divisors, all of the form $p_1^{\beta_1} p_2^{\beta_2} \ldots p_r^{\beta_r}$ where $\beta_i = 0$ or α_i for $i = 1, 2, \ldots, r$.

We denote the set of exact divisors of M by Ex(M). Our investigation into $B(N)$ and $\Gamma_B(N)$ is facilitated by the observation that Ex(M) is a group with respect to a suitable binary operation.

LEMMA 1. *If $l, m \in \mathrm{Ex}(M)$, define $*$ by $l*m = lm/(l, m)^2$. Then $*$ is a binary operation on $\mathrm{Ex}(M)$ and $(\mathrm{Ex}(M), *)$ is a group isomorphic to C_2^r, where r is the number of distinct prime factors of M.*

Proof. We note that 1 is the identity and $l*l = 1$ for all $l \in \mathrm{Ex}(M)$ so that every element is its own inverse. The only awkward part of the proof is the associative law. This is proved by observing that if P, Q are the sets of exact prime power divisors of l, m respectively then the symmetric difference $P \Delta Q = (P \cup Q) - (P \cap Q)$ is the set of exact prime power divisors of $l*m$ and that Δ is a group operation on subsets. Also, as the group is abelian of order 2^r, and every element has order 2, $\mathrm{Ex}(M) \cong C_2^r$.

The matrix (3) (of determinant $e > 0$) represent a Möbius transformation. We now show that the only other rational matrix of the form (3) which represents the same Möbius transformation is the negative of the matrix. Specifically we prove

LEMMA 2. *If*

$$k_1 \begin{pmatrix} a_1 e_1 & b_1/h \\ \dfrac{c_1 N}{h} & d_1 e_1 \end{pmatrix} = k_2 \begin{pmatrix} a_2 e_2 & b_2/h \\ \dfrac{c_2 N}{h} & d_2 e_2 \end{pmatrix}$$

where k_1, k_2 are non-zero integers with $(k_1, k_2) = 1$ and where the matrices have positive determinants e_1, e_2 respectively then k_1, $k_2 = \pm 1$ and $e_1 = e_2$.

Proof. $k_1 b_1 = k_2 b_2$, $k_1 c_1 = k_2 c_2$ so that $k_2 \mid b_1$, $k_2 \mid c_1$ and thus $k_2^2 \mid b_1 c_1$. Taking determinants, $k_1^2 e_1 = k_2^2 e_2$ so that $k_2^2 \mid e_1$.

As

$$a_1 d_1 e_1 - \frac{b_1 c_1 N}{h^2 e_1} = 1$$

and $h^2 e_1 \mid N$, $k_2^2 \mid 1$. Thus $k_2 = \pm 1$ and similarly $k_1 = \pm 1$. As e_1, e_2 are the positive determinants of the matrices, $e_1 = e_2$. Thus e is an invariant of the transformation V given by the matrix (3) and so we can define a function

$$E : \Gamma_B(N) \to \mathrm{Ex}(N/h^2) \quad \text{by} \quad E(V) = e.$$

DEFINITION. We call e the *eterminant* of the transformation V.

PROPOSITION 1. *E is an epimorphism.*

Proof.

$$\begin{pmatrix} a_1 e_1 & b_1/h \\ \dfrac{c_1 N}{h} & d_1 e_1 \end{pmatrix} \begin{pmatrix} a_2 e_2 & b_2/h \\ \dfrac{c_2 N}{h} & d_2 e_2 \end{pmatrix} = \begin{pmatrix} A & B/h \\ \dfrac{cN}{h} & D \end{pmatrix}$$

where A, B, C, D are all divisible by (e_1, e_2) and the final matrix has determinant $e_1 e_2$. Also, as $e_1, e_2 \in \mathrm{Ex}(N/h^2)$, we find that A and D are both divisible by the least common multiple of e_1 and e_2 which is $e_1 e_2/(e_1, e_2)$.

Thus final matrix is (e_1, e_2) times the matrix

$$\begin{pmatrix} a_3(e_1 * e_2) & b_3/h \\ c_3 N/h & d_3(e_1 * e_2) \end{pmatrix}$$

https://doi.org/10.1017/S001708950000940X Published online by Cambridge University Press

of determinant $e_1e_2/(e_1, e_2)^2 = e_1 * e_2$. Thus the eterminant of the product transformation is $e_1 * e_2$, so E is a homomorphism. That E is onto follows from the Conway–Norton descrption of the normalizer.

We also note the following properties of the eterminant which follows from the result, of Lemma 1, that $\mathrm{Ex}(M) \cong C_2^r$.

COROLLARY. (i) $E(V) = E(V^{-1})$

(ii) $E(V_1V_2) = 1$ *if and only if* $E(V_1) = E(V_2)$.

Thus the two matrices of $\Gamma_B(N)$ *which belong to the same* $\Gamma_0(N)$*-coset have the same eterminant (but not always conversely as we shall see). In fact if*

$$V_i = \begin{pmatrix} a_i e & b_i/h \\ c_i N/h & d_i e \end{pmatrix}, \qquad i = 1, 2$$

both have eterminant e then by calculating $V_1V_2^{-1}$ *we deduce the following result which will be useful later.*

LEMMA 3. V_1 *and* V_2 *belong to the same* $\Gamma_0(N)$*-coset if and only if* $a_1b_2 \equiv a_2b_1 \bmod h$, $c_1d_2 \equiv c_2d_1 \bmod h$.

DEFINITION. The transformations in $\Gamma_B(N)$ of eterminant one will be denoted by $\Gamma_C(N)$.

As $\Gamma_C(N)$ is the kernel of $E: \Gamma_B(N) \to \mathrm{Ex}(N/h^2)$ we see that $\Gamma_C(N)$ is a normal subgroup of $\Gamma_B(N)$ of index 2^ρ where ρ is the number of distinct prime factors of N/h^2. Also $\Gamma_0(N) \lhd \Gamma_C(N)$, as $\Gamma_C(N)$ belongs to the normalizer.

PROPOSITION 2. *The index* $|\Gamma_C(N) : \Gamma_0(N)| = h^2\tau$ *where* $\tau = (\frac{3}{2})^{\varepsilon_1}(\frac{4}{3})^{\varepsilon_2}$ *and where*

$$\varepsilon_1 = \begin{cases} 1 & \text{if } 2^2, 2^4, 2^6 \parallel N \\ 0 & \text{otherwise} \end{cases}, \qquad \varepsilon_2 = \begin{cases} 1 & \text{if } 9 \parallel N, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. As $\Gamma_C(N)$ is the set of transformations of the form $\begin{pmatrix} a & b/h \\ c(N/h) & d \end{pmatrix}$ of determinant 1, we have $\Gamma_C(N) = H^{-1}\Gamma_0(N/h^2)H$ where $H = \begin{pmatrix} h & 0 \\ 0 & 1 \end{pmatrix}$. Thus

$$\begin{aligned} |\Gamma_C(N) : \Gamma_0(N)| &= |\Gamma_0(N/h^2) : \Gamma_0(N)| \\ &= \frac{N \prod_{p \mid N} \left(1 + \frac{1}{p}\right)}{\frac{N}{h^2} \prod_{p \mid N/h^2} \left(1 + \frac{1}{p}\right)} \qquad \text{(using (2))} \\ &= h^2\tau \quad \text{where} \quad \tau = \frac{\prod_{p \mid N} \left(1 + \frac{1}{p}\right)}{\prod_{p \mid N/h^2} \left(1 + \frac{1}{p}\right)}. \end{aligned}$$

Now for each integer r, write $h(r)$ to be the largest divisor of 24 such that $(h(r))^2 \mid r$. Then by writing N as a product of prime powers, $N = 2^\alpha 3^\beta \ldots$ we see that $\tau \neq 1$ if and only if $2^\alpha = (h(2^\alpha))^2$ or $3^\beta = h(3^\beta))^2$. That is, if $\alpha = 2$, 4, 6 or $\beta = 1$. The expression for τ given in the theorem now follows.

https://doi.org/10.1017/S001708950000940X Published online by Cambridge University Press

COROLLARY. $|\Gamma_B(N):\Gamma_0(N)| = 2^\rho h^2\tau$, *where* ρ *is the number of distinct prime factors of* N/h^2.

REMARKS. (1) This formula coincides with the one stated by Ogg [7].

(2) Our group $\Gamma_C(N)$ is denoted by $\Gamma_0(n \mid h)$ in Conway–Norton [2]. We have $\Gamma_0(N) \lhd \Gamma_C(N) \lhd \Gamma_B(N)$. In order to understand the elements of $\Gamma_B(N)$ not contained in $\Gamma_C(N)$ we introduce the *Atkin–Lehner transformations*. Such a transformation is represented by the matrix

$$W_e = \begin{pmatrix} ae & b \\ cN & de \end{pmatrix} \qquad \text{where } e \parallel N \text{ and the determinant is } e$$

(All such transformations with a given e belong to the same $\Gamma_0(N)$-coset and we can use the notation W_e to represent any of them. For example, $W_N = \begin{pmatrix} 0 & 1 \\ -N & 0 \end{pmatrix}$, which is called the *Fricke transformation.*)

As we can write

$$W_e = \begin{pmatrix} ah(e)\dfrac{e}{(h(e))^2} & \dfrac{bh/h(e)}{h} \\ \dfrac{cNh/h(e)}{h} & dh(e)\dfrac{e}{(h(e))^2} \end{pmatrix}$$

we see that as this matrix has the form (3), so W_e is an element of $\Gamma_B(N)$ of eterminant $e/(h(e))^2$. Note that $\dfrac{e}{(h(e))^2} \Big\| \dfrac{N}{h^2}$. (The definition of $h(e)$ is given in the proof of Proposition 2.) As in Proposition 1 we see that $W_{e_1}W_{e_2} = W_{e_1 * e_2}$ and then we see that the Atkin–Lehner transformations form a group which we denote by $\Gamma_W(N)$. We then have an epimorphism $E' : \Gamma_W(N) \to \mathrm{Ex}(N)$ whose kernel is $\Gamma_0(N)$. The quotient group $\Gamma_W(N)/\Gamma_0(N) \cong C_2^r$, where r is the number of prime divisors of N, and so $W_e^2 \in \Gamma_0(N)$, for all Atkin–Lehner transformations W_e.

PROPOSITION 3. *Every element* V *of* $\Gamma_B(N)$ *can be written as a product* WT *where* $W \in \Gamma_W(N)$, $T \in \Gamma_C(N)$.

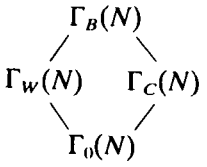
Proof. Suppose that $E(V) = e$ where $e \parallel N/h^2$. We look for an $f \in \mathrm{Ex}(N)$ such that $E(W_f) = e$. Let $N = 2^\alpha 3^\beta N_0$, $(N_0, 6) = 1$. If $h(2^\alpha) = 2^u$, $h(3^\beta) = 3^v$ then $N/h^2 = 2^{\alpha-2u} \cdot 3^{\beta-2v} \cdot N_0$. As $e \parallel N/h^2$ we have $e = 2^i 3^j N_1$ with $i = \alpha - 2u$ or 0, $j = \beta - 2v$ or 0 and $N_1 \parallel N$. Now let

$$f = \begin{cases} 2^\alpha 3^\beta N_1 & \text{if } i, j \neq 0, \\ 2^\alpha N_1 & \text{if } i \neq 0, j = 0, \\ 3^\beta N_1 & \text{if } i = 0, j \neq 0, \\ N_1 & \text{if } i = j = 0. \end{cases}$$

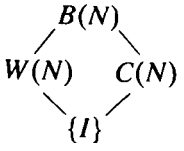
Then $E(W_f) = f/(h(f))^2 = e$. Thus $E(W_f) = E(V)$ so that $E(W_f^{-1}V) = 1$ and $W_f^{-1}V \in \Gamma_C(N)$. Therefore $V = WT$ where W is an Atkin–Lehner transformation and $T \in \Gamma_C(N)$.

As $\Gamma_C(N) \lhd \Gamma_B(N)$ we can write $\Gamma_B(N) = \Gamma_C(N)\Gamma_W(N)$ and we have a subgroup

diagram



or defining $B(N) = \Gamma_B(N)/\Gamma_0(N)$, $C(N) = \Gamma_C(N)/\Gamma_0(N)$, $W(N) = \Gamma_W(N)/\Gamma_0(N)$



From our work, in particular Proposition 2, we have $|C(N)| = h^2\tau$, $|B(N)| = 2^\rho h^2\tau$, $|W(N)| = 2^r$ and thus $|W(N) \cap C(N)| = 2^{r-\rho}$. Here r is the number of distinct prime factors of N and ρ is the number of distinct prime factors of N/h^2. Thus $|W(N) \cap C(N)| = 4$ if $3^2 \| N$ and $2^{2\delta} \| N$, $\delta = 1$, 2 or 3, $|W(N) \cap C(N)| = 2$ if $3^2 \| N$ or $2^{2\delta} \| N$ but not both, and $|W(N) \cap C(N)| = 1$ otherwise. (Thus only in the later case is $B(N)$ a semi-direct product of $W(N)$ and $C(N)$.)

As $W(N) \cong C_2^r$, the elements of $W(N) - \{I\}$ commute and all have order two. They are called *Atkin–Lehner involutions*. The above paragraph tells us that $C(N)$ contains Atkin–Lehner involutions if 2^2, 2^4, $2^6 \| N$ or $3^2 \| N$, and not otherwise.

2. The structure of $B(N)$. In this section we find the structure of the finite groups $B(N)$. Note that if N is not divisible by 4 or 9 then $h = 1$ and so $B(N) \cong C_2^r$. We are interested in the cases where $h > 1$. The basic idea is that $B(N)$ is "almost" a direct product of groups $B(p^\alpha)$ where $p^\alpha \| N$ (p prime) and that the subgroups $C(p^\alpha)$ are "almost" abelian; see Lemma 4, Proposition 6.

The elements of $B(N)$ are $\Gamma_0(N)$-cosets and as a matter of notation we shall use lower-case letters to represent $\Gamma_0(N)$-cosets while the corresponding capital letters denote the transformation in $\Gamma_B(N)$.

PROPOSITION 4. *$C(N)$ is generated by the $\Gamma_0(N)$-cosets*

$$r = \begin{pmatrix} 1 & 0 \\ N/h & 1 \end{pmatrix}, \qquad s = \begin{pmatrix} 1 & 1/h \\ 0 & 1 \end{pmatrix}.$$

Proof. We have $r^h = s^h = I$ and by Lemma 3, $\langle r \rangle \cap \langle s \rangle = \{I\}$. Thus $\{r^i s^j \mid 0 \le i < h, 0 \le j < h\}$ consists of h^2 elements so that if $|C(N)| = h^2$, the result follows. By Proposition 2 this occurs in all cases except when N is exactly divisible by 2^2, 2^4, 2^6, or 3^2. Thus we can assume that $N = 2^{2\alpha}3^{2\beta}N_1$ where $\alpha = 0$, 1, 2 or 3, $\beta = 0$ or 1 and $(N_1, 6) = 1$. Then $h = 2^\alpha 3^\beta$, $(h, N/h^2) = 1$ and therefore we can find integers $k, l \neq 0$ such that $1 + klN/h^2 \equiv 0 \bmod h$. Now

$$s^k r^l = \begin{pmatrix} 1 + klN/h^2 & k/h \\ lN/h & 1 \end{pmatrix}, \qquad r^i s^j = \begin{pmatrix} 1 & j/h \\ iN/h & 1 + ijN/h^2 \end{pmatrix}$$

https://doi.org/10.1017/S001708950000940X Published online by Cambridge University Press

so by Lemma 3, $s^k r^l \neq r^i s^j$ for any i, j. Thus $\langle r, s \rangle$, the group generated by r and s, has more than h^2 elements and as $|C(N)| \leq 2h^2$, by Proposition 2, we conclude that $\langle r, s \rangle = C(N)$.

The structure of $B(p^\alpha)$. From Proposition 2 we can calculate the order of $B(p^\alpha)$ for all prime powers p^α. We obtain the following table:

p^α	2	4	8	16	32	64	$2^\alpha(\alpha \geq 7)$	3	9	$3^\beta(\beta \geq 3)$	$p^\alpha(p \geq 5)$
$\lvert B(p^\alpha)\rvert$	2	6	8	24	32	96	128	2	12	18	2

Now in $B(p^\alpha)$ the only Atkin–Lehner involution is the Fricke involution w_{p^α} (the coset of the Fricke transformation W_{p^α}). This has eterminant $p^\alpha/(h(p^\alpha))^2$ which is equal to 1 if and only if $p^\alpha = 2^2, 2^4, 2^6$ or 3^2. We thus have

LEMMA 4. *$C(p^\alpha) = B(p^\alpha)$ if and only if $p^\alpha = 2^2, 2^4, 2^6$ or 3^2. In all other cases $C(p^\alpha)$ has index 2 in $B(p^\alpha)$.*

The following result, which follows directly from Proposition 4, is of interest.

PROPOSITION 5. *Each group $B(p^\alpha)$ is generated by two elements, one of which has order 2.*

Proof. The element of order 2 is $w = w_{p^\alpha}$. We have $wsw = r^{-1}$ and $\langle r, s \rangle = C(p^\alpha)$ which has index one or two in $B(p^\alpha)$. If it has index 2 then $w \notin C(p^\alpha)$, by Lemma 4 and the remark above it. Hence $\langle w, s \rangle = B(p^\alpha)$.

We now investigate the structure of $C(p^\alpha)$

PROPOSITION 6. *$C(N)$ is abelian if and only if $h^3 \mid N$. In these cases $C(N) \cong C_h \times C_h$.*

Proof. Direct computation shows that $RSR^{-1}S^{-1} \in \Gamma_0(N)$ if and only if $h^3 \mid N$. Therefore by Proposition 4.

$$C(N) \cong \langle r, s \mid r^h = s^h = I \mid rs = sr \rangle \cong C_h \times C_h.$$

This occurs only for the prime powers 2, 8, $2^\alpha(\alpha \geq 9)$, 3, $3^\beta(\beta \geq 3)$, $p^\alpha(p \geq 5)$.

COROLLARY. *For these prime powers $N = p^\alpha$, $B(N)$ has presentation*

$$\langle w, s \mid w^2 = s^h = I, (ws)^2 = (sw)^2 \rangle.$$

Proof. As $wsw = r^{-1}$ and r and s commute we obtain the relation $(ws)^2 = (sw)^2$. This presentation does define a group of order $2h^2$ as s and wsw generated an abelian subgroup of index 2 and of order h^2.

We now deal with the prime powers N for which $h^2 = N$, i.e. those of Lemma 4, namely $N = 2^2, 2^4, 3^2$ and 2^6. Direct computation gives the relations $w^2 = s^h = (ws)^3 = I$. In the first three cases $h = 2, 3, 4$ and as the orders of $B(N)$ are 6, 12 and 24 we obtain $B(4) \cong D_3$, $B(9) \cong A_4$, $B(16) \cong S_4$. If $n = 2^6$, $h = 2^3$, $|B(N)| = 96$ and $w^2 = s^8 = (ws)^3 = I$.

LEMMA 5. *$B(2^6)$ has presentation*

$$\langle w, s \mid w^2 = s^8 = (ws)^3 = (ws^{-1}ws)^3 = I \rangle.$$

Proof. Direct computation shows that $ws^{-1}ws$ does have order 3, so we just need to show that this presentation does define a group of order 96. This in fact is well-known

https://doi.org/10.1017/S001708950000940X Published online by Cambridge University Press

(see, e.g. [**10**]) but we outline a proof. Consider the subgroup generated by the elements of order 2, s^4 and ws^4w; we show that this is normal and we can deduce from the relations that their product has order 2. Thus the normal subgroup generated by s^4 has order 4 and if we factor out by this normal subgroup we get a group isomorphic to S_4 of order 24. Thus the above presentation does define a group of order $24 \times 4 = 96$.

The only prime powers not dealt with are 2^5, 2^7 and 2^8 and we take these in turn.

$N = 2^5$. Here $h = 2^5$ so if we let

$$w = \begin{pmatrix} 0 & -1 \\ 32 & 0 \end{pmatrix}, \qquad s = \begin{pmatrix} 1 & 1/4 \\ 0 & 1 \end{pmatrix}$$

then w and s generate $B(2^5)$ and we find $w^2 = s^4 = (ws)^4 = (ws^{-1}ws)^2 = I$. However, a group with the above generators and relations has order 32 ([**3**]) so that these relations do define the group.

$N = 2^7$. Here $h = 2^3$. We begin by finding $C(2^7)$ which has order 64. This is generated by

$$r = \begin{pmatrix} 1 & 0 \\ 16 & 1 \end{pmatrix}, \qquad s = \begin{pmatrix} 1 & 1/8 \\ 0 & 1 \end{pmatrix}.$$

We find by calculation that $r^2s^2 = s^2r^2$ and that $\langle r^2 \rangle \cap \langle s^2 \rangle = \{I\}$. Thus r^2 and s^2 generate an abelian subgroup N isomorphic to $C_4 \times C_4$ and of index 4. We further calculate that $r^{-1}s^2r = r^4s^2$ and $s^{-1}r^2s = r^2s^4$ so that N is normal. Clearly $C(2^7)/N \cong C_2 \times C_2$ so we can use a standard method (e.g. [**4**, p. 149]) to find the following presentation for $C(2^7)$.

$$\langle r, s \mid r^8 = s^8 = I,\ r^2s^2 = s^2r^2,\ r^{-1}s^2r = r^4s^2,\ s^{-1}r^2s = r^2s^4,\ r^{-1}s^{-1}rs = r^{-2}s^2 \rangle.$$

The last relation is found by calculation and is just the relation in the quotient group $C(2^7)/N$, saying that this group is abelian, pulled back to $C(2^7)$.

To find the presentation for $B(2^7)$ we just introduce the generator w and add the relations $w^2 = 1$ $wsw = r^{-1}$. We then obtain the following presentation for $B(2^7)$.

$$\langle w, s \mid w^2 = s^8 = I,\ (ws^2)^2 = (s^2w)^2,\ s^2ws^{-1}w = ws^3ws^2,\ ws^2ws = s^{-3}ws^2w,\ (ws)^4 = 1 \rangle,$$

and we see that the penultimate relation follows from the previous one.

$N = 2^8$. Again we start by finding $C(2^8)$. Its generators are

$$r = \begin{pmatrix} 1 & 0 \\ 32 & 1 \end{pmatrix}, \qquad s = \begin{pmatrix} 1 & 1/8 \\ 0 & 1 \end{pmatrix}$$

and we calculate that s commutes with r^2. As $r^8 = s^8 = I$, s and r^2 generate a subgroup isomorphic to $C_8 \times C_4$ of index 2. We compute that $r^{-1}sr = r^4s^5$ so $C(2^8)$ has presentation

$$\langle r, s \mid r^8 = s^8 = 1,\ r^2s = sr^2,\ r^{-1}sr = r^4s^5 \rangle$$

and so $B(2^8)$ has presentation

$$\langle w, s \mid w^2 = s^8 = I,\ ws^2ws = s^2wsw,\ sws^{-1}w = sw^3ws^{-3} \rangle.$$

We present our results in the following table. In the final column we describe $B(N)$, if possible, as a known abstract group. The notation $(l, m, n; q)$ denotes the group

$$\langle A, B \mid A^l = B^m = (AB)^n = (A^{-1}B^{-1}AB)^q = I \rangle;$$

the notation $C_h \sim C_2$ denotes the particular extension of $C_h \times C_h$ obtained by adjoining the automorphism which interchanges the generators of the factors.

https://doi.org/10.1017/S001708950000940X Published online by Cambridge University Press

The groups $B(N)$, $N = p^\alpha$, with generators

$$w = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}, \qquad s = \begin{pmatrix} 1 & 1/h \\ 0 & 1 \end{pmatrix}$$

N	h	Relations	$\lvert B(N)\rvert$	$B(N) \cong$
2	1	$w^2 = s = I$	2	C_2
4	2	$w^2 = s^2 = (ws)^3 = I$	6	D_3
8	2	$w^2 = s^2 = I, \quad (ws)^2 = (sw)^2$	8	D_4
16	4	$w^2 = s^4 = (ws)^3 = I$	24	S_4
32	4	$w^2 = s^4 = (ws)^4 = (ws^{-1}ws)^2 = I$	32	(2, 4, 4; 2)
64	8	$w^2 = s^8 = (ws)^3 = (ws^{-1}ws)^3 = I$	96	(2, 8, 3; 3)
128	8	$\left\{ \begin{array}{c} w^2 = s^8 = (ws)^4 = I, \\ (ws^2)^2 = (s^2w)^2, \\ s^2ws^{-1}w = ws^3ws^2, \end{array} \right\}$	128	
256	8	$w^2 = s^8 = I, \quad ws^2ws = s^2wsw,$ $sws^{-1}w = ws^3ws^{-3}$	128	
$2^\alpha (\alpha \geq 9)$	8	$w^2 = s^8 = I, \quad (ws)^2 = (sw)^2$	128	$C_8 \sim C_2$
3	1	$w^2 = s = I$	2	C_2
9	3	$w^2 = s^3 = (ws)^3 = I$	12	A_4
$3^\beta (\beta \geq 3)$	3	$w^2 = s^3 = I, \quad (ws)^2 = (sw)^2$	18	$C_3 \sim C_2$
$p^\alpha (p \geq s)$	1	$w^2 = s = I$	2	C_2

3. The product structure. In [1] it was claimed that $B(N)$ can always be expressed as a direct product $\otimes B(p^\alpha)$ over all exact prime power divisors p^α of N. This is not always the case. For an example we consider $N = 18$. By the corollary to Proposition 2, $|B(18)| = 24$. Also $B(N)$ contains

$$w = \begin{pmatrix} 0 & -1 \\ 18 & 0 \end{pmatrix} \quad \text{and} \quad s = \begin{pmatrix} 1 & 1/3 \\ 0 & 1 \end{pmatrix}.$$

As $w^2 = s^3 = (ws)^4 = I$ it is easy to see that $B(18) \cong S_4$ which can not be written as a direct product in a non-trivial way. In this section we investigate circumstances in which $B(N)$ is a direct product. We first show that if $M \parallel N$ then $B(N)$ contains a subgroup isomorphic to $B(M)$. We will then investigate when this subgroup is normal.

PROPOSITION 7. *Let $M \parallel N$. Then the elements of $B(N)$ of the form*

$$t = \begin{pmatrix} ae & b/h(M) \\ cN/h(M) & de \end{pmatrix}$$

where, as before, $h(M)$ is the largest divisor of 24 such that $(h(M))^2 \mid M$, where $e \parallel M/(h(M))^2$ and the determinant is e, form a subgroup of $B(N)$ which is isomorphic to $B(M)$.

Proof. Write $N = MK$ where $(M, K) = 1$. Then

$$t = \begin{pmatrix} ae & b\dfrac{h(K)}{h(N)} \\ \dfrac{cNh(K)}{h(N)} & de \end{pmatrix}$$

https://doi.org/10.1017/S001708950000940X Published online by Cambridge University Press

showing that $t \in B(N)$. It is easy to see that these elements form a subgroup which we denote by $B'(M)$. We also let $\Gamma_{B'}(M)$ denote the corresponding set of matrices in $\Gamma_B(N)$.

Now $t \in B(N)$ represents a coset $\Gamma_0(N)T$ where $T \in \Gamma_B(N)$ is the above matrix. The form of the matrix given in the proposition shows that $T \in \Gamma_B(M)$ as well, so we can define

$$F: B'(M) \to B(M) \quad \text{by} \quad F(\Gamma_0(N)T) = \Gamma_0(M)T,$$

and we note that this is well-defined as $\Gamma_0(N) \leq \Gamma_0(M)$. To show that F is one-to-one we prove the

LEMMA. $\Gamma_{B'}(M) \cap \Gamma_0(M) \leq \Gamma_0(N)$.

Proof. If

$$V_1 = \begin{pmatrix} \alpha e & \beta/h(M) \\ \gamma N/h(M) & \delta e \end{pmatrix} \in \Gamma_{B'}(M) \cap \Gamma_0(M)$$

then $h(M) \mid \beta$, $M \left| \frac{\gamma N}{h(M)} \right.$. Thus $M \left| \frac{\gamma MK}{h(M)} \right.$ so that $h(M) \mid \gamma K$. As $(h(M), K) = 1$, $h(M) \mid \gamma$ so that $N \left| \frac{\gamma N}{h(M)} \right.$ and therefore $V_1 \in \Gamma_0(N)$.

This lemma shows that the kernel of F is trivial so that F is one-to-one. We now show that F is onto. By Propositions 3 and 4 (and the equation $r = w_M s^{-1} w_M$) we see that $B(M)$ is generated by the Atkin–Lehner involutions in $B(M)$ together with the element $\begin{pmatrix} 1 & 1/h(M) \\ 0 & 1 \end{pmatrix}$. As remarked after their definition in §1, any two Atkin–Lehner transformations of $\Gamma_B(M)$ with a given e belong to the same $\Gamma_0(M)$-coset. Hence for each $e \parallel M$ there is a unique Atkin–Lehner involution $w_e \in B(M)$. The Atkin–Lehner involutions in $B'(M)$ have the form $\begin{pmatrix} ae & b \\ cN & de \end{pmatrix}$ where $e \parallel M$ so that these map, under F, to the Atkin–Lehner involutions in $B(M)$ $\left(\text{just write } N = \frac{N}{M} M\right)$. Also the coset of $\begin{pmatrix} 1 & 1/h(M) \\ 0 & 1 \end{pmatrix}$ in $B'(M)$ maps under F to the coset of this element in $B(M)$. Thus the generators of $B(M)$ lie in the image of F so that F is onto.

We use the same ideas to find the condition for $B'(M)$ to be a normal subgroup of $B(N)$, $N = MK$, $(M, K) = 1$. We note that if w_f is an Atkin–Lehner involution then w_f normalizes $B'(M)$; for every element of $B'(M)$ can be written as $w_e v'$ where $e \parallel M$ and $v' \in B'(M)$ has eterminant one. Now $w_f(w_e v')w_f^{-1} = w_e w_f v' w_f$ (as Atkin–Lehner involutions commute—see end of §1) and a simple calculation shows that $w_f v' w_f \in B'(M)$. Thus the condition for $B'(M)$ to be a normal subgroup is just

$$\begin{bmatrix} 1 & 1/h(N) \\ 0 & 1 \end{bmatrix} \begin{bmatrix} ae & b/h(M) \\ cN/h(M) & de \end{bmatrix} \begin{bmatrix} 1 & -1/h(N) \\ 0 & 1 \end{bmatrix} \in B'(M).$$

The product of the matrices is

$$\begin{pmatrix} ae + cN/h(M)h(N) & * \\ cN/h(M) & -cN/h(M)h(N) + de \end{pmatrix}$$

https://doi.org/10.1017/S001708950000940X Published online by Cambridge University Press

where

$$* = \frac{b}{h(M)} + \frac{de}{h(N)} - \frac{ae}{h(N)} - \frac{cN}{h(M)(h(N))^2}.$$

Now $N/h(M)h(N) = KM/h(K)(h(M))^2$ is exactly divisible by e so that the condition for normality is that $* = u/h(M)$ where $u \in Z$. This reduces to $h(K) \mid e(d-a)$ and as $(h(K), e) = 1$ the condition for normality is just that $a \equiv d \bmod h(K)$.

As $h(K) \mid 24$ this is equivalent to the statement that $ad \equiv 1 \bmod h(K)$ (by the "curious" property of 24 cited at the beginning of Section 3 of [2], i.e. $h \mid 24$ implies that $ad \equiv 1 \bmod h$ if and only if $a \equiv d \bmod h$.) Now $ade - bcMK/e(h(M))^2 = 1$ so that $ade \equiv 1 \bmod h(K)$ is equivalent to the condition $e \equiv 1 \bmod h(K)$. We thus have

PROPOSITION 8. *If $N = MK$ where $(M, K) = 1$ then $B'(M) \lhd B(N)$ if and only if $e \equiv 1 \bmod h(K)$ for all exact divisors e of M.*

If $N = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ is the prime power decomposition of N and if $\Pi_i = N/p_i^{\alpha_i}$ then we have the following result.

COROLLARY. *$B(N) = \otimes B'(p_i^{\alpha_i})$ if and only if $p_i^{\alpha_i} \equiv 1 \bmod h(\Pi_i)$ for $i = 1, \ldots, r$.*

For example if $N = 2^\alpha 3^\beta$ where $\alpha \geq 3$ and $\beta \geq 1$ then $B(N) \cong B'(2^\alpha) \times B'(3^\beta)$ if and only if α and β are even. This is because $2^2 \equiv 1 \bmod 3$ and $3^2 \equiv 1 \bmod 8$. Also noting that $p^2 \equiv 1 \bmod 24$ for all primes $p \geq 5$ we see that $B(N) \cong \otimes B'(p_i^{\alpha_i})$ whenever N is a square.

4. The automorphism group of $X_0(N)$. We end with a few elementary remarks about the automorphism group of the associated Riemann surfaces. Let $Y_0(N)$ be the quotient of the upper half plane by $\Gamma_0(N)$ and let $X_0(N)$ be the compact Riemann surface obtained by filling in the punctures at the projections of the parabolic fixed points. By the formula for the number of classes of elliptic fixed points of $\Gamma_0(N)$ ([9]) we find that $\Gamma_0(2^\alpha 3^\beta)$ is torsion-free when $\alpha > 1$, $\beta > 1$. Hence in these cases every automorphism of $Y_0(N)$, and hence of $X_0(N)$, can be lifted to an element of $\Gamma_B(N)$ and so $\operatorname{Aut} X_0(N) \cong B(N)$, and can be calculated by the results of §2, 3. In general $\Gamma_0(N)$ will have elliptic fixed points and then it might happen that $\operatorname{Aut} X_0(N)$ properly contains $B(N)$. See [8].

There are some cases which are worth noting. If $N = 2^6$ then $|B(N)| = 96$ and the genus of $X_0(N)$ is 3 ([9]). Thus we obtain a Riemann surface of genus 3 with 96 automorphisms. This is the Riemann surface of genus 3 with the second largest automorphism group, (the largest being Klein's Riemann surface with 168 automorphisms). As described in [11 §8] there is a corresponding regular map which in this case is Dyck's map with 12 vertices, 32 faces and 48 edges ([10]). It could be built by choosing the 12 vertices to be the punctures of $Y_0(N)$. Similarly, if $N = 2^5$ we get one of the regular maps on the torus of type $\{4, 4\}$, and if $N = 2, 4, 8, 9, 16$ we get regular maps on the sphere, (platonic solids) which explains why in these cases $B(N)$ is a finite rotation group. If $N = 2^7$ we find that the genus of $X_0(N)$ is 9 and $|B(N)| = 128$. This gives an example of a Riemann surface of genus g admitting a nilpotent group of automorphisms of order $16(g-1)$, which by [12] is the largest possible order for a nilpotent group of automorphisms.

ACKNOWLEDGEMENT. We would like to thank Colin Maclachlan for pointing out an error in the first version of this paper.

REFERENCES

1. A. O. L. Atkin and J. Lehner, Hecke operators on $\Gamma_0(m)$. *Math. Ann.* **185** (1970) 134–160.

2. C. Conway and S. Norton, Monstrous moonshine. *Bull. London Math. Soc.* **11** (1979) 308–339.

3. H. M. S. Coxeter, The abstract group $G^{m,n,p}$. *Trans. Amer. Soc.* **45** (1939) 73–150.

4. D. L. Johnson, *Presentation of groups*. London Math. Soc. Lecture Notes No. 22, (Cambridge University Press, 1976).

5. J. Lehner and M. Newman, Weierstrass points on $\Gamma_0(N)$. *Ann. of Math.* **79** (1964) 360–368.

6. C. Maclachlan, Groups of units of zero ternary quadratic forms. *Proc. Roy. Soc. Edinburgh Sect. A,* **88** (1981) 141–157.

7. A. P. Ogg, Modular functions in Proceedings Santa Cruz Conference on Finite Groups, *Proc. Symp. Pure Math.* **37** (A.M.S. 1980).

8. A. P. Ogg, "Uber die Automorphismengruppe von $X_0(N)$". *Math. Ann.* **228** (1977) 279–292.

9. B. Schoeneberg, *Elliptic modular functions*. (Springer-Verlag, 1974).

10. F. A. Sherk, The regular maps on a surface of genus three. *Canad. J. Math.* **11** (1959), 452–480.

11. D. Singerman, Symmetries of Riemann surfaces with large automorphism group. *Math. Ann.* **210** (1974), 17–32.

12. R. Zomorrodian, Nilpotent automorphism groups of Riemann surfaces, *Trans. Amer. Math. Soc.* **288** (1985) 241–255.

FACULTY OF MATHEMATICAL STUDIES,
THE UNIVERSITY,
SOUTHAMPTON.