PACIFIC JOURNAL OF MATHEMATICS
Vol. 78, No. 2, 1978

REMARKS ON A THEOREM OF L. GREENBERG ON THE MODULAR GROUP

A. W. MASON AND W. W. STOTHERS

Introduction. For integers a and b, each greater than 1, let $T(a, b)$ be the free product of cyclic groups of orders a and b. Then $T(a, b)$ has presentation

$$\langle X, Y: X^a = Y^b = 1\rangle .$$

Suppose that $G \lhd T(a, b)$. If XYG has finite order in $T(a, b)/G$, then the order is the *level* of G, denoted by $n(G)$. We put $U = XY$. When G has finite index $\mu(G)$, then $n(G)$ is defined, and divides $\mu(G)$. In such a case, $t(G) = \mu(G)/n(G)$ is the *parabolic class number* of G. These definitions agree with the usual ones for $T(2, 3)$, the classical modular group.

For $T(2, 3)$, Newman [7] raised the question of whether there were infinitely many normal subgroups with a given parabolic class number. In [3], L. Greenberg showed that this was not possible by proving that, for $t > 1$,

$$\mu \leqq t^4 .$$

Here, as later, we write μ, t for $\mu(G)$, $t(G)$ when the group is clear from the context.

Mason [5] improved this to

$$(1) \qquad \mu \leqq t^3 .$$

This was also proved by Accola [1]. Implicit in his proof is a proof that (1) holds when a and b are distinct primes.

Here, we show that, when a and b are coprime, there is a constant $c(a, b)$ such that, for $t > 1$,

$$(2) \qquad \mu \leqq c(a, b)t^2(t-1) .$$

The constant is 1 when a and b are distinct primes, e.g., for the modular group. There is no corresponding result when a and b are not coprime.

We give examples to show that we can have equality in (2), but only a finite number of times for given a and b. Finally, we obtain a better result for large t.

The referee has drawn our attention to a paper of Morris Newman, '2-generator groups and parabolic class numbers', Proc. Amer. Math. Soc., 31 (1972), 51–53, which contains the weaker result

$$\mu \leqq ab\, t^{a+1} .$$

1. Preliminary results.

PROPOSITION 1.1. *Suppose that* K *is a finite group, and that* $H = \langle U \rangle$ *is a cyclic subgroup with order* $k < |K|$, *and with* $\bigcap_{V \in K} VHV^{-1} = \{1\}$. *If* $K = \langle X, U \rangle$, *then* $H \cap XHX^{-1} = \{1\}$, *and the cosets* $H, XH, UXH, \cdots, U^{k-1}XH$ *are distinct.*

Proof. Let $E = H \cap XHX^{-1}$. As H is cyclic, so is E, and hence $E \triangleleft K$. Thus, $E = \{1\}$. The last clause follows at once.

We observe that, in the situation described in 1.1, K acts as a transitive permutation group on the cosets on H.

PROPOSITION 1.2. *Suppose that* a *and* b *are coprime, and that* $G \triangleleft T(a, b)$ *with index* $\mu(G)$. *Then there is a normal subgroup* G^* *of* $T(a, b)$ *with* $G \leqq G^*$ *and such that*

(i) $t(G^*) = t(G)$, $=t$ *say,*

(ii) *if* $t > 1$, *then* $\mu(G^*) \leqq t(t-1)$,

(iii) G^*/G *is central in* $T(a, b)/G$.

Proof. Let $D = \langle U, G \rangle$, then $|T(a, b): D| = t(G)$.

Let $G^* = \bigcap_{V \in T(a,b)} VDV^{-1}$, so that $G \leqq G^* \triangleleft T(a, b)$. As D/G is cyclic, $G^* = \langle U^k, G \rangle$, for a least positive integer k. As $D = \langle U, G^* \rangle$, $n(G^*) = k$, so (i) holds.

If $t > 1$, then D is proper. From 1.1 applied to $K = T(a, b)/G^*$ and $H = D/G^*$, it follows that $t \geqq k + 1$, so (ii) holds.

For $V \in T(a, b)$, let $[V]$ denote the corresponding element of $\mathrm{Aut}(G^*/G)$. Then $[X]^a = [Y]^b = 1$, and $[X][Y] = [U] = 1$, so (iii) holds. (Cf. Lemma 3 of [3].)

COROLLARY 1.3. *With the notation of* 1.2,

(i) *if* X *or* $Y \in G$, *then* $t(G) = 1$,

(ii) *if* $t(G) = 1$, *then* $\mu(G) | ab$.

Proof. We observe that $t(G) = 1$ if and only if $D = T(a, b)$.

If X or $Y \in G$, then $D = T(a, b)$, and (i) holds.

If $t(G) = 1$, then $G^* = T(a, b)$. By 1.2 (iii), $T(a, b)/G$ is abelian, so that (ii) holds.

For integers a and b with $1/a + 1/b < 1$, there is a Fuchsian group of the first kind isomorphic to $T(a, b)$. The details can be found in [4]. We write $T(a, b)$ for the Fuchsian group as well as for its abstract counterpart, taking the isomorphism so that U corresponds to a mapping $\omega \mapsto \omega + \alpha$, with $\alpha > 0$.

Also from [4], a subgroup of finite index in $T(a, b)$ has a presentation

$$\left\langle E_1, \cdots, E_r, P_1, \cdots, P_t, A_1, B_1, \cdots, A_g, B_g \colon E_i \text{ elliptic}, \prod_{i=1}^{r} E_i \prod_{j=1}^{t} P_j \prod_{s=1}^{g} [A_s, B_s] = 1 \right\rangle . \tag{3}$$

In this presentation, $P_1, \cdots, P_t$ are parabolic, i.e., each is $T(a, b)$-conjugate to a power of U. The *amplitude* of a parabolic element is the exponent of U. We can choose the presentation with each P_i operating anti-clockwise. This will be described as the standard presentation.

PROPOSITION 1.4. *In the standard presentation for a subgroup of $T(a, b)$, each parabolic generator has negative amplitude.*

The proof is exactly that given for Theorem 1 in [5].

2. **The inequality (2).** We write n' for the largest proper divisor of a positive integer n.

THEOREM 2.1. *Suppose that a and b are coprime, and that $G \lhd T(a, b)$ with index μ. If $t > 1$, then*

$$\mu \leqq a'b't^2(t - 1) .$$

Proof. By 1.2, there is a subgroup G^* of index kt, with $k \leqq t - 1$, and with properties (i), (ii), and (iii).

By a standard argument on Fuchsian groups, a finite subgroup of G^* is $T(a, b)$-conjugate to a subgroup of $\langle X \rangle$ or of $\langle Y \rangle$. As G^* is normal, we can divide such subgroups into those of order e, with $e|a$, and those of order f, with $f|b$. As $t > 1$, 1.3 applies, so $e \leqq a'$ and $f \leqq b'$.

In the standard presentation of G^*, each elliptic generator has order e or f. Using 1.4 and the normality of G^*, each parabolic generator has amplitude $-k$. As G^*/G is central, the efth power of the relation in (3) yields

$$U^{-efkt} \equiv 1 \quad (\text{mod. } G) .$$

Thus, $n(G)|efkt$. The result follows.

COROLLARY 2.2. *If a and b are distinct primes, and G is as in the theorem, then $\mu \leqq t^2(t - 1)$.*

The inequality (2) is best possible, as the following examples show:

(a) in the notation of [7], $(\Gamma^2)'$ and $G_{3,4}$ are normal subgroups of $\boldsymbol{T}(2, 3)$ and have, respectively, $\mu = 18, t = 3$ and $\mu = 48, t = 4$,

(b) in $\boldsymbol{T}(3, 4)$, $\boldsymbol{G} = \langle X, YXY^3, Y^2\rangle$ has index 2 and is isomorphic to the free product $\boldsymbol{C}_2^* \boldsymbol{C}_3^* \boldsymbol{C}_3$. The product of the generators is $(XY)^2$, so $n(\boldsymbol{G}) = 2$ and $t(\boldsymbol{G}) = 1$. Thus, $\boldsymbol{G}' \lhd \boldsymbol{T}(3, 4)$ and has $\mu = 36, t = 3$. Example (b) is analogous to the first example in (a). As we shall see in § 4, there are no further examples for $\boldsymbol{T}(2, 3)$.

3. **Non-coprime cases.** In this section, we suppose that a and b have g.c.d. $(a, b) = d$, with $d > 1$. We produce an infinite collection of subgroups of $\boldsymbol{T}(a, b)$, each with parabolic class number d. Intersecting these with other normal subgroups, we see that there can be no inequality of the form $\mu \leqq f(t)$.

We begin by considering $\boldsymbol{T}(d, d)$. Let $\boldsymbol{H} = \langle XY, \boldsymbol{T}(d, d)'\rangle$. Then the Reidemeister-Schreier method shows that H, which is normal in $\boldsymbol{T}(d, d)$, has presentation

$$\left\langle A_r = Y^r X Y^{1-r},\ r = 0, 1, \cdots, d-1 \colon \prod_{r=0}^{d-1} A_r = 1 \right\rangle .$$

Then $\boldsymbol{H}$ is free on the first $d - 1$ of these generators. Further, $\boldsymbol{T}(d, d) = \langle Y, \boldsymbol{H}\rangle$, so that $|\boldsymbol{T}(d, d) \colon \boldsymbol{H}| = d$. Finally, $A_0 = XY$, so that $n(\boldsymbol{H}) = 1$ and $t(\boldsymbol{H}) = d$.

As $d > 1$, Dirichlet's theorem states that there are an infinite number of primes congruent to 1 modulo d. For any such prime, there is an integer e with $\mathrm{ord}_p(e) = d$. We define $\boldsymbol{H}(p, e)$ by

$$\boldsymbol{H}(p, e) = \boldsymbol{H}' \cdot \langle (A_0)^p,\ B_r = (A_{r-1})^{-e} A_r,\ r = 1, \cdots, d-2\rangle .$$

This is invariant under XY. Also, for $r = 0, \cdots, d-2$, $YA_rY^{-1} = A_{r+1}$, so that, for $r = 1, \cdots, d-3$, $YB_rY^{-1} = B_{r+1}$. Finally, $YB_{d-2}Y^{-1}$ can be expressed, modulo $\boldsymbol{H}'$, in terms of the B_r and $(A_0)^p$. Thus, $\boldsymbol{H}(p, e)$ is normal. (The proof for $d = 2$ is simpler.)

Since $A_0 = XY$, $\boldsymbol{H}(p, e)$ has level p. Also, $|\boldsymbol{H} \colon \boldsymbol{H}(p, e)| = p$ and $|\boldsymbol{T}(d, d) \colon \boldsymbol{H}| = d$, so that $t(\boldsymbol{H}(p, e)) = d$.

To obtain subgroups of $\boldsymbol{T}(a, b)$, we observe that, if $\boldsymbol{N}$ is the normal closure of $\langle X^d, Y^d\rangle$ in $\boldsymbol{T}(a, b)$, then $\boldsymbol{T}(d, d) \cong \boldsymbol{T}(a, b)/\boldsymbol{N}$. Then $\boldsymbol{T}(a, b)$ has subgroups with level p and parabolic class number d for an infinite set of p.

4. **Frobenius factor groups.** Throughout this section, we shall assume that a and b are coprime, and that $t > 1$. We adopt the notation of 1.2, and of 1.1 with $\boldsymbol{K} = \boldsymbol{T}(a, b)/\boldsymbol{G}$ and $\boldsymbol{H} = \boldsymbol{D}/\boldsymbol{G}$, and write $\boldsymbol{K}^*$ and $\boldsymbol{H}^*$ for the corresponding groups with $\boldsymbol{G}$ replaced by $\boldsymbol{G}^*$. We regard $\boldsymbol{K}$ (resp. $\boldsymbol{K}^*$) as a transitive group on the cosets of $\boldsymbol{H}$ (resp. $\boldsymbol{H}^*$). Our results describe the situation where there is equality in 1.2 (ii).

THEOREM 4.1. *If $k = t - 1$, then K^* is primitive.*

Proof. In this case, 1.1 shows that K^* is doubly transitive.

THEOREM 4.2. *Suppose that K^* is primitive. Then K^* is a Frobenius group with kernel $(K^*)'$, which is elementary abelian. Further, there is a prime p with $t = p^n \equiv 1 \pmod k$, and $n = \mathrm{ord}_k(p)$. Finally, $k \mid ab$.*

Proof. Note that $H^* \neq K^*$, since $t > 1$. Suppose that $V \in K^* - H^*$. As K^* is primitive, H^* is maximal, so that $K^* = \langle V, UG^* \rangle$. By 1.1, if $VH^* \neq WH^*$, then $VH^*V^{-1} \cap WH^*W^{-1} = \{1\}$. Thus, K^* is Frobenius with kernel N where $|N| = t$. By [10, p. 30], N is elementary abelian, so that $t = p^n$.

Let $M \lhd K^*$ with $M \leqq N$. If $1 < M < N$, then $H^* < H^* \cdot M < K^*$ which contradicts the maximality of H^*. Thus $M = \{1\}$ or N. As $K^*/N \cong H^*$, $(K^*)' \leqq N$, so that $(K^*)' = N$.

By the general theory of Frobenius groups, $k = |H^*|$ divides $p^n - 1 = |N| - 1$. As U acts irreducibly on N, [2, p. 212] shows that, if ω is a primitive k-th root of unity over $GF(p)$, then ω^{p^i}, $i = 1, \cdots n - 1$, are distinct. Hence $n = \mathrm{ord}_k(p)$.

For the last part, we observe that $k = |T(a, b) : (T(a, b))' \cdot G^*|$ which divides $|T(a, b) : (T(a, b))'| = ab$.

Combining 4.1 and 4.2, we obtain

COROLLARY 4.3. *If $k = t - 1$, then $(t - 1) | ab$. For fixed a and b, there are finitely many normal subgroups with equality in* (2).

COROLLARY 4.4. *If $1/2t \leqq k < t - 1$, K^* is imprimitive.*

Proof. This follows at once, since we cannot have $t \equiv 1 \pmod k$.

We note that, if $G \lhd T(2, 3)$ has genus 1 and $t > 4$, then $G^* = G$ and $k = 6$, see [7]. By [9, p. 181], if $6 | t - 1$, then K^* is Frobenius, so that K^* Frobenius does not imply K^* primitive. Further, for a prime $p > 3$, there is a primitive K^* with $k = 6$, $t = p^n$, where $n = \mathrm{ord}_3(p)$. These subgroups have $k < t/2$ in general.

Theorem 4.2 has a converse, as we shall now show. Let p be a prime and k an integer prime to p. Let $n = \mathrm{ord}_k(p)$, and write S for the cyclic subgroup of order k in $GF(p^n)^*$. Let $F = \{(x, y) : x \in S, y \in GF(p^n)\}$, and define multiplication on F by

$$(x, y) \cdot (u, v) = (xu, yu + v) .$$

PROPOSITION 4.5. *F is a primitive Frobenius group on p^n symbols. The kernel is F', which is elementary abelian, and the complement C is cyclic of order k.*

Proof. It is clear that F is Frobenius with kernel $N = \{(1, y): y \in GF(p^n)\}$ and complement $C = \{(x, 0): x \in S\}$.

If $1 < M < N$ with $M \lhd F$, then, by [9, p. 183], F/M is Frobenius with kernel N/M. Then $k = |C|$ divides $|N: M| - 1 = p^m - 1$, where $1 \leqq m < n$. This contradicts the definition of n. Hence, $N = F'$.

If $C < M < F$, then $|M| = p^r k$, where $1 \leqq r < n$. Then $|M \cap N| = p^r$ and, by [9, p. 183], M is Frobenius with kernel $M \cap N$. Hence, $k | (p^r - 1)$, again a contradiction. Thus, C is maximal and F is primitive on the cosets of C.

PROPOSITION 4.6. *With the above notation, suppose that $k = ef$, with $(e, f) = 1$. Then we have,*

(i) *if $e, f > 1$, then $F = \langle x, y \rangle$, with x of order e, y of order f.*

(ii) *if $e = 1$, then $F = \langle x, y \rangle$, with x of order p, y of order k.*

Proof. (i) As $e, f | k$, we can take $x \in C$, $y \in C^z$, with $z \in F - C$, with x of order e and y of order f. Let $M = \langle x, y \rangle$. As $[x, y] \in N - \{1\}$, then $|M| = p^r k$, where $1 \leqq r \leqq n$. By [9, p. 183], $k | (p^r - 1)$, so that $r = n$ and $M = F$.

(ii) We take $x \in N$, of order p and y a generator of C. The result follows as in (i).

Since the center of a Frobenius group is trivial,

LEMMA 4.7. *If $G \lhd T(a, b)$ with K Frobenius, then $G = G^*$.*

LEMMA 4.8. *Let $G \lhd T(a, b)$ with K a primitive Frobenius group with elementary p-abelian kernel and complement C cyclic of order k. Then,* (i) *C is conjugate to H, and*

(ii) *if $n(G)$ is prime to a, then $p|a$.*

Proof. By 4.7, $G = G^*$, so that $H = H^*$ and $K = K^*$. Let $M/G = N$ be the kernel of K, and let $|K| = p^n k$, so $(p, k) = 1$.

(i) Since $T(a, b)/M = C$, $n(M) = k$. Hence $(UG)^{kp} = 1$ in K. By [9, p. 182], either $(UG)^k = 1$ or $(UG)^p = 1$. It follows that $(UG)^k = 1$ and so $N \cap H = \{1\}$. Thus, H is a complement of N in K. By [9, p. 186], H is a conjugate of C.

(ii) Since $M \lhd T(a, b)$ and $|T(a, b): M| = k$, $X \in M$. Thus, $X^p \in G$ and, if $(a, p) = 1$, then $X \in G$ which would imply that K is abelian. Thus, $p|a$.

THEOREM 4.9. *Given $k > 1$, a divisor of ab, and p prime to k (with $p|a$ if $(k, a) = 1$, $p|b$ if $(k, b) = 1$), there is a subgroup $G \lhd T(a, b)$ with K^* primitive Frobenius of order $p^n k$, where* $n = \mathrm{ord}_k(p)$.

Proof. Let $k = ef$, where $e|a$ and $f|b$, so that $(e, f) = 1$. The result follows from 4.5, 4.6, 4.7, and 4.8.

Thus, when $ab + 1$ is p^n with p prime, there is a subgroup of maximal index with equality in 1.2 (ii). However, there is no corresponding subgroup with equality in (2), as we now show.

THEOREM 4.10. $(\boldsymbol{T}(a, b))''$ *has level ab.*

Proof. It is clear that $(\boldsymbol{T}(a, b))'$ is free, has level ab and parabolic class number 1. The standard presentation shows that $U^{ab} \in (\boldsymbol{T}(a, b))''$. Since the level is a multiple of ab, the result follows.

This is proved for $a = 2$ and $b = 3$ in [8].

THEOREM 4.11. *If $k = t - 1 = ab$, then $\boldsymbol{G} = \boldsymbol{G}^*$.*

Proof. Assume that $k = t - 1 = ab$, but that $\boldsymbol{G} \neq \boldsymbol{G}^*$. By 4.1 and 4.2, $\boldsymbol{K}^*$ is Frobenius with kernel of index $k = ab$. Also, $t = p^n$, p prime. Let $\boldsymbol{M}/\boldsymbol{G}^*$ be the kernel. Then $|\boldsymbol{T}(a, b): \boldsymbol{M}| = ab$. As $\boldsymbol{T}(a, b)/\boldsymbol{M}$ is cyclic, $\boldsymbol{M} = \boldsymbol{T}(a, b)'$. Thus, $\boldsymbol{G}^*$ is free, so that the proof of 2.1 shows that $|\boldsymbol{G}^*: \boldsymbol{G}| = p^s$, with $s \geqq 1$. By 1.2 (iii), there is a subgroup $\boldsymbol{L} \lhd \boldsymbol{T}(a, b)$ with $\boldsymbol{G} \leqq \boldsymbol{L} \leqq \boldsymbol{G}^*$ and $|\boldsymbol{G}^*: \boldsymbol{L}| = p$.

Let $\boldsymbol{A} = \boldsymbol{T}(a, b)/\boldsymbol{M}$ and $\boldsymbol{P} = \boldsymbol{M}/\boldsymbol{L}$. By 4.10, $\boldsymbol{M}' \cdot \boldsymbol{L} = \boldsymbol{G}^*$, so $\boldsymbol{P}' = \boldsymbol{G}^*/\boldsymbol{L}$. Now, $\boldsymbol{P}' \leqq \boldsymbol{Z}(\boldsymbol{P})$, and, since $\boldsymbol{T}(a, b)/\boldsymbol{M}$ acts irreducibly on $\boldsymbol{M}/\boldsymbol{G}^*$, $\boldsymbol{P}' = \boldsymbol{Z}(\boldsymbol{P})$. The Frattini subgroup $\Phi(\boldsymbol{P})$ of $\boldsymbol{P}$ is the smallest normal subgroup with elementary abelian factor, [2, p. 174]. Thus, $\boldsymbol{P}' = \boldsymbol{Z}(\boldsymbol{P}) = \Phi(\boldsymbol{P})$, so that $\boldsymbol{P}$ is an extra-special p-group, [2, p. 183].

Let $\boldsymbol{A} = \langle \alpha \rangle$, with α regarded as an element of order d of $\mathrm{Aut}(\boldsymbol{P})$. Then, in $\mathrm{Aut}(\boldsymbol{P}/\boldsymbol{P}')$, $\alpha^d = 1$. Considering the action of $\boldsymbol{A}$ on $\boldsymbol{M}/\boldsymbol{G}^*$, α has order $p^n - 1$ as an element of $\mathrm{Aut}(\boldsymbol{P}/\boldsymbol{P}')$. Thus, $d = p^n - 1$.

By [2, p. 213], $p^n - 1 | p^r + 1$, with $r \leqq n/2$. Thus, $p^n = 4$, so that $ab = 3$. As $(a, b) = 1$, this is impossible. Hence $\boldsymbol{G} = \boldsymbol{G}^*$.

COROLLARY 4.12. *If $\boldsymbol{G} \lhd \boldsymbol{T}(2, 3)$ gives equality in (2), then $t = 3$ or 4.*

Proof. By 4.3, 4.1 and, 4.2, $t=3$, 4 or 7. By 4.11, $t=7$ implies $\boldsymbol{G} = \boldsymbol{G}^*$ and so gives strict inequality. For $t = 3, 4$, see end of § 2.

5. Imprimitive factor groups. By 4.4, $\boldsymbol{K}^*$ will be imprimitive when $1/2t \leqq k < t - 1$. For this range, we have one general result.

THEOREM 5.1. *If* $k \geqq t/2$, *then* $\boldsymbol{K}^* = \langle V, U\boldsymbol{G}^*\rangle$, *with* $V^2 = 1$.

PROOF. By 1.1, the stabilizer of $\boldsymbol{H}^*$ has an orbit $\boldsymbol{T} = \{X\boldsymbol{H}^*, \cdots, U^{k-1}X\boldsymbol{H}^*\}$ of length k. By [10, p. 44], there is a paired orbit T' of the same length k. As $k \geqq t/2$, $\boldsymbol{T} = \boldsymbol{T}'$.

By [10, p. 45], there is an element $V \in \boldsymbol{K}^*$ with $VX\boldsymbol{H}^* = \boldsymbol{H}^*$ and $V\boldsymbol{H}^* = X\boldsymbol{H}^*$. Then $VX = U^r$ and $X^{-1}V = U^s$, for some r, s. Thus, $\boldsymbol{K}^* = \langle V, \boldsymbol{H}^*\rangle$, and $V^2 = X^{-1}V^2X = U^{r+s}$. As $\boldsymbol{H}^* \cap X\boldsymbol{H}^*X^{-1} = \{1\}$, $V^2 = 1$.

COROLLARY 5.2. *If* kt *is odd, then* $k < t/2$.

For $\boldsymbol{T}(2, 3)$, there are subgroups with $k > t/2$. For example, the subgroups $\Omega(2, m)$, defined in [6], have $\Omega(2, m)^* = \Omega(2, m)$, so that $t(\Omega(2, m)) = 3m$, $k(\Omega(2, m)) = 2m$.

If we restrict k further, the imprimitivity can be described more precisely. For convenience, we put $h = t - k$.

THEOREM 5.3. *If* $k \neq t - 1$, *then* $k \leqq h^2$.

Proof. If $k \neq t - 1$, then $h > 1$, and we may suppose that we have $k > \max\{h, (h-1)^2\}$.

Consider the action of U on the cosets of $\boldsymbol{H}^*$. It fixes $\boldsymbol{H}^*$, and permutes the $U^iX\boldsymbol{H}^*$ cyclically. We choose $V_1, \cdots, V_h$ so that

$$\boldsymbol{K}^* = V_1\boldsymbol{H}^* \cup V_2\boldsymbol{H}^* \cup \cdots \cup V_h\boldsymbol{H}^* \cup X\boldsymbol{H}^* \cup UX\boldsymbol{H}^* \cup \cdots \cup U^{k-1}X\boldsymbol{H}^* ,$$

where we may assume that $V_1 = 1$.

Clearly, $V_2\boldsymbol{H}^*, \cdots, V_h\boldsymbol{H}^*$ belong to cycles of length at most $h - 1$. Thus, for $i = 2, \cdots, h$,

$$\boldsymbol{H}^* \cap V_i\boldsymbol{H}^*(V_i)^{-1} = \langle U^{s(i)}\boldsymbol{G}^*\rangle ,$$

with $0 < s(i) \leqq h - 1$. If $2 \leqq i, j \leqq h$, then

$$U^{s(i)}U^{s(j)}\boldsymbol{G}^* \in V_i\boldsymbol{H}^*V_i^{-1} \cap V_j\boldsymbol{H}^*V_j^{-1} .$$

Since $s(i)s(j) \leqq (h-1)^2 < k$, the intersection is nontrivial. It can be shown similarly that, for $1 \leqq i \leqq h$ and $0 \leqq j \leqq k - 1$,

$$V_i\boldsymbol{H}^*V_i^{-1} \cap (U^jX)\boldsymbol{H}^*(U^jX)^{-1} = \{1\} .$$

Let $[\boldsymbol{H}^*] = \{V_i\boldsymbol{H}^* : i = 1, \cdots, h\}$ and let $W \in \boldsymbol{K}^*$. Suppose that, for some i and j, $V_i\boldsymbol{H}^* = WV_j\boldsymbol{H}^*$. Then, for any r, $V_i\boldsymbol{H}^*V_i^{-1}$ and

$WV_r\boldsymbol{H}^*(WV_r)^{-1}$ have nontrivial intersection. Hence $[\boldsymbol{H}^*]$ is a block and so $h|k$. We put $m = k/h$.

Let $\boldsymbol{K}_0$ be the subgroup which fixes blocks setwise. If $V \in \boldsymbol{K}_0$ fixes two cosets belonging to different blocks, we may suppose that $V\boldsymbol{H}^* = \boldsymbol{H}^*$, so $V = U^q\boldsymbol{G}^*$ for some q. Since V also fixes a coset of the form $U^rX\boldsymbol{H}^*$, 1.1 shows that $V = 1$. Thus, no two elements of $\boldsymbol{K}_0$ have the same effect on $\boldsymbol{H}^*$ and on $X\boldsymbol{H}^*$, so that

$$|\boldsymbol{K}_0| \leqq h^2 . \tag{4}$$

The blocks are $[\boldsymbol{H}^*]$ and $\{U^{i+jm}X\boldsymbol{H}^*: j = 0, \cdots, h-1\}$ for $i = 0, \cdots, m-1$. Thus, $U^m\boldsymbol{H}^*, \cdots, U^{m(h-1)}\boldsymbol{H}^*$ fix the blocks. None of these fixes a coset $U^rX\boldsymbol{H}^*$. Taking conjugates, we obtain a similar set for each block, i.e., fixing one element of the block, but none in any other block. All of these are distinct and nontrivial, so

$$|\boldsymbol{K}_0| \geqq 1 + (h-1)t/h . \tag{5}$$

Combining (4) and (5), we get the result.

From 5.3 and 4.3, we obtain

COROLLARY 5.4. *If $t > ab + 1$, then $\mu \leqq a'b't^2(t - t^{1/2})$.*

LEMMA 5.5. *In the notation of 5.3, if $k > \max(h, (h-1)^2)$, then $|\boldsymbol{K}_0| = h^2$.*

Proof. With $m = k/h$ as in 5.3, $A = U^m\boldsymbol{G}^*$, $B = XU^mX^{-1}\boldsymbol{G}^*$ fix $[\boldsymbol{H}^*]$, $[X\boldsymbol{H}^*]$ respectively, and each has order h. Suppose that we have $A^rB^s = A^iB^j$, with $0 \leqq r, s, i, j < h$, then $A^{i-r} = B^{s-j}$. Then, since A fixes $\boldsymbol{H}^*$ and B fixes $X\boldsymbol{H}^*$ and only the identity fixes both, we must have $r = i$ and $j = s$. Hence, $\boldsymbol{K}_0 = \{A^rB^s: 0 \leqq r, s < h\}$.

LEMMA 5.6. *If $k = h^2 > 1$, then h is prime.*

Proof. If A, as in 5.5, does not fix $[\boldsymbol{H}^*]$ elementwise, then it has a conjugate distinct from A which fixes some $V_i\boldsymbol{H}^*$ not fixed by A. From the description of $\boldsymbol{K}_0$ in 5.5, this conjugate is a power of A. Considering the effect on $[\boldsymbol{H}^*]$, this must be A^e, with $(e, h) > 1$. As $(e, h) > 1$, A^e does not act as a cycle on $[X\boldsymbol{H}^*]$. This is a contradiction since a conjugate of A would have this effect.

Thus, A fixes $[\boldsymbol{H}^*]$ elementwise and has the effect of an h-cycle on the other blocks. As $k = h^2$, there are $h + 1(>2)$ blocks. We label the blocks so that $[\boldsymbol{H}^*]$ is block zero, $[X\boldsymbol{H}^*]$ block one, and so on. Then we have

$$A = c_0c_1 \cdots c_h ,$$

where c_0 is 1 and c_i an h-cycle on block i, $i = 1, \cdots, h$. Similarly,

$$B = d_0 d_1 \cdots d_h ,$$

where d_1 is 1 and d_j an h-cycle on block j, $j = 0$ and $j = 2, \cdots, h$.

Suppose that C is a conjugate of A fixing cosets in block two. Then, for some r, s, $C = A^r B^s$. As C acts as an h-cycle on block zero, $(d_0)^s$ is an h-cycle, so that $(s, h) = 1$. Similarly, $(r, h) = 1$. Considering the effect on block two, we must have $(c_2)^r(d_2)^s = 1$, so that $d_2 = (c_2)^{w(2)}$, with $(w(2), h) = 1$. For the other blocks, we have corresponding integers $w(3), \cdots, w(h)$. Since no element fixes cosets in two blocks, the $w(i)$ are distinct modulo h. As there are $h - 1$ of them, h is prime.

LEMMA 5.7. *With the notation of* 5.5, *if* $\boldsymbol{G}_0$ *is the subgroup of* $\boldsymbol{T}(a, b)$ *corresponding to* $\boldsymbol{K}_0$, *then* $(\boldsymbol{G}_0)^* = \boldsymbol{G}_0$ *and* $k(\boldsymbol{G}_0) = k/h$.

Proof. By definition, $(\boldsymbol{G}_0)^*$ is generated over $\boldsymbol{G}_0$ by U^s, where s is the least positive integer with $X^{-1}U^sXU^{-s} \in \boldsymbol{G}_0$. The corresponding element of $\boldsymbol{K}_0$ sends $\boldsymbol{H}^*$ to $V_i\boldsymbol{H}^*$ for some i. Thus, $U^sX\boldsymbol{H}^* = XV_i\boldsymbol{H}^*$. As $XV_i\boldsymbol{H}^* \in [X\boldsymbol{H}^*]$, $U^s\boldsymbol{G}^*$ fixes $[X\boldsymbol{H}^*]$ and $[\boldsymbol{H}^*]$. Thus, $U^s \in \boldsymbol{G}_0$, so that $(\boldsymbol{G}_0)^* = \boldsymbol{G}_0$. From the proof of 5.5, $k(\boldsymbol{G}_0) = n(\boldsymbol{G}_0) = k/h$.

LEMMA 5.8. *If* $k = h^2$, *then* $h|ab$ *and* $h + 1$ *is a prime power.*

Proof. With $\boldsymbol{G}_0$ as in 5.7, $|\boldsymbol{T}(a, b): \boldsymbol{G}_0| = kt/h^2$, and $k(\boldsymbol{G}_0) = k/h$, so $t(\boldsymbol{G}_0) = h + 1 (= 1 + k(\boldsymbol{G}_0))$. As in § 4, $\boldsymbol{T}(a, b)/\boldsymbol{G}_0$ is Frobenius and $(k/h)|ab$, and $h + 1$ is a prime power.

THEOREM 5.9. *If* $k = h^2 > 1$, *then* $h = 2$ (*with* $\boldsymbol{K}^* \cong \boldsymbol{S}_4$).

Proof. From the previous results, $\boldsymbol{K}^*/\boldsymbol{K}_0$ is Frobenius of order $h(h + 1)$, $\boldsymbol{K}_0 \cong \boldsymbol{C}_h \times \boldsymbol{C}_h$, h is prime and $h + 1$ a prime power.

If $V \in \boldsymbol{K}^*$ centralizes $\boldsymbol{K}_0$, then $AV\boldsymbol{H}^* = VA\boldsymbol{H}^* = V\boldsymbol{H}^*$, where A is as in 5.5. Since A fixes cosets in $[\boldsymbol{H}^*]$ only, V fixes $[\boldsymbol{H}^*]$. On considering conjugates of A, V fixes each block setwise, and so belongs to $\boldsymbol{K}_0$. Hence, there is a monomorphism $\boldsymbol{K}^*/\boldsymbol{K}_0 \to \mathrm{Aut}(\boldsymbol{K}_0) \cong \mathrm{GL}(2, h)$. Thus, $\mathrm{GL}(2, h)$ has a subgroup which is Frobenius of order $h(h + 1)$. Its kernel $\boldsymbol{N}$ is elementary abelian of order $h + 1$.

If $h > 2$, then $h + 1 = 2^s$, and $\boldsymbol{N} \cap \mathrm{SL}(2, h)$ is elementary-abelian of order at least 2^{s-1}. The only element of order 2 in $\mathrm{SL}(2, h)$ is $-\boldsymbol{I}$, but this is central in $\mathrm{GL}(2, h)$. Hence, $s = 1$, which is impossible.

Thus, $h = 2$, and $\boldsymbol{K}^*$ the semidirect product of $\boldsymbol{C}_2 \times \boldsymbol{C}_2$ by $\mathrm{GL}(2, 2)$, i.e., $\boldsymbol{K}^* \cong \boldsymbol{S}_4$. It is clear that this will occur if and only if one of a and b is even and the other divisible by 3, see 4.8 and

4.9. For the modular group, $\Gamma/\Gamma(4) \cong \boldsymbol{S}_4$.

It follows that we must have strict inequality in 5.3, at least when $t > 6$.

6. A final remark. Our results can be restated as results on finite groups, e.g.,

THEOREM 6.1. *If* $\boldsymbol{K}$ *is a noncyclic* (a, b, k)*-group, with* $(a, b) = 1$, *then*,

$$|\boldsymbol{K}| \geqq \frac{1}{2}k + k^{3/2}/(a'b')^{1/2} .$$

If, in addition, $\boldsymbol{K}$ *is simple, then*

$$|\boldsymbol{K}| \geqq k^2 + k .$$

The second part is trivial when we observe that, in an obvious notation, $\boldsymbol{K} = \boldsymbol{K}^*$ whenever the former is simple.

We should like to express our gratitude to Dr. N. K. Dickson (University of Glasgow) for his assistance with various aspects of this paper, particularly with the group theory in § 4.

REFERENCES

1. R. W. D. Accola, *On the number of automorphisms of a closed Riemann surface*, Trans. Amer. Math. Soc., **131** (1968), 398–408.
2. D. Gorenstein, *Finite Groups*, Harper & Row, New York, (1968).
3. L. Greenberg, *Note on normal subgroups of the modular group*, Proc. Amer. Math. Soc., **17** (1966), 1195–1198.
4. A. M. Macbeath, *Fuchsian Groups*, Queen's College, Dundee, (1961).
5. A. W. Mason, *On a theorem by Leon Greenberg*, Proc. Amer. Math. Soc., **23** (1969), 18–23.
6. ———, *Lattice subgroups of free congruence groups*, Glasgow Math. J., **10** (1969), 106–115.
7. M. Newman, *Classification of normal subgroups of the modular group*, Trans. Amer. Math. Soc., **126** (1967), 267–277.
8. ———, *A note on modular groups*, Proc. Amer. Math. Soc., **14** (1963), 124–125.
9. D. S. Passman, *Permutation Groups*, Benjamin, New York, (1968).
10. H. Wielandt, *Finite Permutation Groups*, Academic Press, New York, (1964).

Received April 25, 1977.

UNIVERSITY OF GLASGOW
GLASGOW G12 8QW, SCOTLAND