Proceedings of the Edinburgh Mathematical Society (1987) **30**, 97–101

SOME MAXIMAL NORMAL SUBGROUPS OF THE MODULAR GROUP

by GARETH A. JONES*

(Received 10th August 1985)

1. Introduction

For each finite group G, let $\mathcal{N}_G$ denote the set of all normal subgroups of the modular group $\Gamma = PSL_2(\mathbb{Z})$ with quotient group isomorphic to G; since Γ is finitely generated, the number $N_G = |\mathcal{N}_G|$ of such subgroups is finite. We shall be mainly concerned with the case where G is the linear fractional group $PSL_2(q)$ over the Galois field $GF(q)$, in which case we shall write $\mathcal{N}(q)$ and $N(q)$ for $\mathcal{N}_G$ and N_G; for $q > 3$, $PSL_2(q)$ is simple, so the elements of $\mathcal{N}(q)$ will be maximal normal subgroups of Γ.

When q is a prime p, there is one obvious element of $\mathcal{N}(p)$: for each $n \in \mathbb{N}$, the principal congruence subgroup

$$\Gamma(n) = \{\pm A \in \Gamma \mid A \equiv \pm I \bmod n\},$$

of level n, is the kernel of the reduction $\bmod n$ from Γ to $PSL_2(\mathbb{Z}_n)$; this is an epimorphism, so if we take n to be a prime p we find that $\Gamma(p) \in \mathcal{N}(p)$. A natural question is whether there are any other elements of $\mathcal{N}(q)$ for any q; it follows from the normal subgroup structure of $PSL_2(\mathbb{Z}_n)$ (see [6] for instance) that apart from the single exception $\Gamma(5) \in \mathcal{N}(4)$, arising from the isomorphism $PSL_2(5) \cong PSL_2(4)$, any such element would be a non-congruence subgroup of Γ, that is, would contain no $\Gamma(n)$.

In 1936, Philip Hall [2] published an extension of the Möbius inversion formula which allows one to calculate N_G provided one knows the subgroup structure and the number of automorphisms of G (indeed, his method also applies to other finitely generated groups besides Γ). Hall concentrated mainly on the groups $G = PSL_2(p)$, where p is prime, and showed that $N(p) = \frac{1}{2}(p - c)$ where c is a constant (which he computed) depending on the congruence class of $p \bmod 120$; this result was rediscovered by Sinkov [9], using a different method, in 1969. In particular, for each prime $p \geqq 13$ we have $N(p) \geqq 2$, so that $\mathcal{N}(p)$ contains a non-congruence subgroup (Newman [7] also demonstrated the existence of such subgroups in $\mathcal{N}(p)$ for primes $p \geqq 37$ in 1968).

The techniques used by Newman and Sinkov are specific to quotient groups of type PSL_2, as are those of Macbeath [5] who proved in 1967 that $\mathcal{N}(q)$ is non-empty for

*This paper forms part of the Proceedings of the conference Groups–St Andrews 1985.

E

each prime-power $q \neq 9$, thus giving further examples of maximal normal subgroups of Γ which are non-congruence subgroups. The aim of this note is to show how one can use Hall's method to strengthen Macbeath's result by explicitly calculating $N(q)$. For simplicity, we will restrict our attention to the case where $q=2^e$; however, the method is quite general, and indeed Martin Downs (private communication) has calculated $N(q)$ for odd q.

Theorem. *The number $N(2^e)$ of normal subgroups of the modular group with quotient group isomorphic to $PSL_2(2^e)$ is*

$$\frac{1}{e}\sum_f \mu\left(\frac{e}{f}\right)(2^f - 1);$$

thus $N(2)=1$, and $N(2^e)=(1/e)\sum_f \mu(e/f)2^f$ for all $e>1$.

(Here μ is the Möbius function, and $\sum_f$ denotes summation over all positive divisors f of e.)

For small e we have the following values:

e	1	2	3	4	5	6	7	8	9	10	11	12	...
$N(2^e)$	1	1	2	3	6	9	18	30	56	99	186	335	...

The theorem implies that $N(2^e) \geqq 1$ for all e, so we have:

Corollary. *If $e \geqq 1$ there is a normal subgroup $N \trianglelefteq \Gamma$ with $\Gamma/N \cong PSL_2(2^e)$; if $e=1$ or $e=2$ then $N=\Gamma(2)$ or $N=\Gamma(5)$, but if $e \geqq 3$ each such N is a non-congruence subgroup of Γ.*

2. Hall's method

We will briefly outline Hall's method [2], restricting attention to the case of quotients of Γ; the extension to other finitely generated groups is obvious.

Let G be any finite group; then each epimorphism $\phi:\Gamma \to G$ determines an element $N = \ker \phi \in \mathcal{N}_G$, and every element of $\mathcal{N}_G$ arises in this way. Two epimorphisms ϕ, $\psi:\Gamma \to G$ have the same kernel if and only if $\psi = \phi \circ \alpha$ for some $\alpha \in \operatorname{Aut} G$, so N_G is the number of orbits in this action of $\operatorname{Aut} G$ on the set of epimorphisms $\phi:\Gamma \to G$.

Now Γ has a presentation

$$\Gamma = \langle X, Y \mid X^2 = Y^3 = 1 \rangle$$

(see [8]), so if $|G| > 3$ then epimorphisms $\phi:\Gamma \to G$ are in one-to-one correspondence with pairs of elements $x = X\phi$ and $y = Y\phi$ of G such that

(i) x and y have orders 2 and 3 respectively,

(ii) x and y generate G.

Let us call $(x, y) \in G \times G$ a *modular pair* if it satisfies (i), and a *modular generating pair* (for G) if it satisfies (i) and (ii). Then N_G is the number of orbits of Aut G in its natural action on the set $\mathcal{G}_G$ of all modular generating pairs for G. Only the identity automorphism can fix such a pair, so Aut G acts semi-regularly on $\mathcal{G}_G$; hence

$$N_G = \frac{n_G}{|\mathrm{Aut}\, G|}, \tag{2.1}$$

where $n_G = |\mathcal{G}_G|$ is the number of modular generating pairs for G.

3. Proof of the theorem

We now take G to be the group $G_e = PSL_2(q)$, where $q = 2^e$. We write N_e for $N(q) = N_{G_e}$ etc. Now Aut $G_e = P\Gamma L_2(q)$ has order $e\omega_e$ where $\omega_e = q(q^2 - 1)$ is the order of G_e.

To calculate $n_e = |\mathcal{G}_e|$, let m_e be the number of modular pairs in G_e; clearly $m_e = \tau_e \theta_e$, where τ_e and θ_e are the numbers of elements of orders 2 and 3 in G_e. Suppose first that e is *odd*. Then $\tau_e = q^2 - 1$ and $\theta_e = q^2 - q$, so

$$\begin{aligned} m_e &= (q^2 - 1)(q^2 - q) \\ &= (q - 1)\omega_e. \end{aligned} \tag{3.1}$$

Each modular pair generates a unique subgroup H of G, and each subgroup H is generated by n_H such pairs, so

$$m_e = \sum_{H \leqq G} n_H. \tag{3.2}$$

Dickson ([**1**], Chapter XII) lists the subgroups H of G_e, and by inspection the only ones which can be generated by a modular pair are the subgroups $H \cong G_f = PSL_2(2^f)$, where f divides e. There are $|G_e : G_f| = \omega_e / \omega_f$ such subgroups for each f, and each of them is generated by $n_f = n_{G_f}$ modular pairs, so (3.2) becomes

$$m_e = \sum_f \frac{\omega_e}{\omega_f} \cdot n_f. \tag{3.3}$$

Combining (3.1) and (3.3), and cancelling ω_e, we get

$$\sum_f \frac{n_f}{\omega_f} = 2^e - 1. \tag{3.4}$$

Applying the Möbius inversion formula to this, we deduce that

$$\frac{n_e}{\omega_e} = \sum_f \mu\left(\frac{e}{f}\right)(2^f - 1). \tag{3.5}$$

In (2.1), we now put $n_G = n_e$ and $|\text{Aut}\, G| = e\omega_e$, so that (3.5) gives

$$N_G = N_e = \frac{n_e}{e\omega_e} = \frac{1}{e}\sum_f \mu\left(\frac{e}{f}\right)(2^f - 1).$$

If $e > 1$ then $\sum_f \mu(e/f) = 0$, so

$$N_G = \frac{1}{e}\sum_f \mu\left(\frac{e}{f}\right)2^f.$$

When e is *even*, the only changes are that θ_e is now $q^2 + q$, and that G_e has $\omega_e/12$ subgroups $H \cong A_4$, each of which can be generated by 24 modular pairs. Thus we must add $2\omega_e$ to the right-hand sides of (3.1) and (3.3). However, these extra terms cancel in (3.4), so the final result is the same as for odd e.

4. Proof of the corollary

If $\sum_f \mu(e/f)2^f = 0$ then by taking the negative terms across to the right-hand side we obtain two different binary representations of the same integer, which is absurd. Thus $N(2^e) \neq 0$ so there exists $N \in \mathcal{N}(2^e)$. If $e = 1$ or $e = 2$ then by inspection $N = \Gamma(2)$ or $N = \Gamma(5)$, so let $e \geqq 3$. If $N \geqq \Gamma(n)$ for some n, then $PSL_2(2^e)$ is a homomorphic image of $PSL_2(\mathbb{Z}_n)$; however, the only non-abelian composition factors of $PSL_2(\mathbb{Z}_n)$ are the groups $PSL_2(p)$ for primes $p \geqq 5$ dividing n (see [**6**], [**8**]), and $PSL_2(2^e)$ is not isomorphic to one of these, as can be seen by comparing orders. Thus N is a non-congruence subgroup.

5. Remarks

1. Hall's method can be applied to quotient groups G of Γ for which the subgroup structure is more complicated than that of $PSL_2(2^e)$. Let $\mathcal{S}$ be the set of subgroups $H \leqq G$ which have modular generating pairs (that is, $n_H > 0$). One defines $\mu_{\mathcal{S}}(H)$, for each $H \in \mathcal{S}$, by

$$\mu_{\mathcal{S}}(G) = 1, \qquad \sum_{K \geqq H} \mu_{\mathcal{S}}(K) = 0 \quad \text{if} \quad H < G \tag{5.1}$$

(the summation being over all $K \in \mathcal{S}$ containing H). If m_H and n_H are the numbers of modular pairs and of modular generating pairs in H, then the analogues of (3.2) and (3.5) are

$$m_G = \sum_{H \leqq G} n_H \tag{5.2}$$

and

$$n_G = \sum_{H \leqq G} \mu_{\mathcal{S}}(H) m_H \tag{5.3}$$

https://doi.org/10.1017/S0013091500018010 Published online by Cambridge University Press

(again, both summations are restricted to $H \in \mathscr{S}$); this last equation can be verified by applying (5.1) and (5.2) to the right-hand side. Knowing the subgroup structure of G, one can calculate $\mu_{\mathscr{S}}(H)$ and m_H for each $H \in \mathscr{S}$, and hence determine n_G from (5.3); then (2.1) gives N_G. For the general form of Hall's theory, the reader is strongly urged to read [**2**].

2. The formula for $N(2^e)$ in the theorem also gives the number of irreducible polynomials of degree e over $GF(2)$, or equivalently the number of orbits of length e in the action of the cyclic group C_e on its power-set. It would be interesting to find a natural parametrization of the elements of $\mathscr{N}(2^e)$ using these polynomials or orbits.

3. As shown in [**3, 4**], there is a bijection between triangular maps $\mathscr{M}$ on orientable surfaces and conjugacy classes of subgroups $M \leqq \Gamma$; the map $\mathscr{M}$ is regular if and only if M is normal, in which case the orientation-preserving automorphism group $\mathrm{Aut}^+ \mathscr{M}$ is isomorphic to Γ/M. Thus for any finite group G, N_G is the number of regular orientable triangular maps $\mathscr{M}$ with $\mathrm{Aut}^+ \mathscr{M} \cong G$. For instance, the fact that $N(4)=1$ shows that there is just one such map with $\mathrm{Aut}^+ \mathscr{M} \cong PSL_2(4)$; it is, of course, the icosahedron.

Acknowledgement. The author is grateful to the referee for some very helpful comments.

REFERENCES

1. L. E. Dickson, *Linear groups* (Teubner, Leipzig, 1901; reprinted Dover, New York, 1958).

2. P. Hall, The Eulerian functions of a group, *Quarterly J. Math. Oxford* **7** (1936), 134–151.

3. G. A. Jones, Triangular maps and non-congruence subgroups of the modular group, *Bull. London Math. Soc.* **11** (1979), 117–123.

4. G. A. Jones and D. Singerman, Theory of maps on orientable surfaces, *Proc. London Math. Soc.* (3) **37** (1978), 273–307.

5. A. M. Macbeath, Generators of the linear fractional groups, *Proc. Sympos. Pure Math.* vol. **12** (Amer. Math. Soc., Providence, R.I., 1967), 14–32.

6. D. L. McQuillan, Classification of normal congruence subgroups of the modular group, *Amer. J. Math.* **87** (1965), 285–296.

7. M. Newman, Maximal normal subgroups of the modular group, *Proc. Amer. Math. Soc.* **19** (1968), 1138–1144.

8. M. Newman, *Integral matrices* (Academic Press, New York, 1972).

9. A. Sinkov, The number of abstract definitions of $LF(2,p)$ as a quotient group of $(2,3,n)$, *J. Algebra* **12** (1969), 525–532.

Department of Mathematics
University of Southampton
Southampton SO9 5NH