ON RIEMANN SURFACES WITH MAXIMAL AUTOMORPHISM GROUPS

by JOSEPH LEHNER AND MORRIS NEWMAN

(Received 2 August, 1966)

1. Introduction. Let S be a closed Riemann surface of genus

$$g > 1,$$

so that $\hat{S}$, the universal covering surface of S, is hyperbolic. We can then uniformize S by a discrete, nonabelian group Γ_1 of Möbius transformations of the upper half-plane $\mathscr{H}$. It follows that $N_1 = N_\Omega(\Gamma_1)$ is discrete; here N_1 is the normalizer of Γ_1 in Ω, the group of (conformal) automorphisms of $\mathscr{H}$. An automorphism of S can be lifted to a coset of N_1/Γ_1. Hence $C(S)$, the group of automorphisms of S, is isomorphic to N_1/Γ_1. The order of $C = C(S)$ equals the index of Γ_1 in N_1, which in turn equals $|\Gamma_1|/|N_1|$, where $|N_1|$ is the hyperbolic area of a fundamental region of N_1. Since Γ_1 uniformizes a surface, we have $|\Gamma_1| = 4\pi(g-1)$, while, by Siegel's results [7], $|N_1| \geqq \pi/21$ and N_1 can only be the triangle group (2, 3, 7). Hence in all cases the order of $C(S)$ is at most $84(g-1)$, an old result of Hurwitz [1]. The surfaces that permit a maximal automorphism group (= automorphism group of maximum order) can therefore be obtained by studying the finite factor groups of (2, 3, 7). Such a treatment, purely algebraic in nature, has been promised by Macbeath [5].

In this paper we use another device to gain information on the genera which permit an S for which $C(S)$ is maximal. Let us make a finite number of punctures in a surface S of genus $g > 1$; call the deleted surface $\dot{S}$ and its automorphism group $\dot{C} = C(\dot{S})$. The genus of $\dot{S}$ is still g. Any $\dot{\gamma} \in \dot{C}$ can be extended analytically to a $\gamma \in C$; consequently $\dot{C}$ is a subgroup of C. Hence *a punctured Riemann surface has at most* $84(g-1)$ *automorphisms.* Moreover if $\dot{C}$ is maximal, so is C.

The group Γ that uniformizes $\dot{S}$ will be a free group and its index in its normalizer $N = N_\Omega(\Gamma)$ will be $84(g-1)$ if $\dot{C}$ is maximal. In §3 we derive necessary and sufficient conditions on N and Γ in order that this be the case. We find that N is of genus 0 and the signature of N modulo Γ is (2, 3, 7). The latter means that three of the generators of N have exponents 2, 3, 7, respectively, modulo Γ, while the remaining generators are already in Γ. The parameters describing S may therefore be taken to be the following: the generators of N (either elliptic or parabolic) bearing the exponents 2, 3, 7, and the integer t, the number of parabolic classes in N. For our application we may just as well take $t = 1$. In §4 we exhibit three such groups, say N_2, N_3, N_7. For each N_i we find an infinite family of normal subgroups $\{\Gamma_{iq}, q = 1, 2, \ldots\}$ satisfying the above conditions on Γ. The corresponding surfaces $\Gamma_{iq}\backslash\mathscr{H}$, with the punctures filled in, all have maximal automorphism groups.

The surfaces determined by $\{\Gamma_{7q}\}$ are equivalent to those found by Macbeath in [5], and if we combine the results of [5] and [6] we find the surfaces determined by $\{\Gamma_{2q}\}$. On the other hand the groups $\{\Gamma_{3q}\}$ lead to new closed surfaces S_q with maximal automorphism

https://doi.org/10.1017/S001708950000015X Published online by Cambridge University Press

groups. The genus of S_q is $1+117q^{236}$ and S_q is uniformized by the group K^qK', where K is a Fuchsian group defined in §3.

Macbeath obtains his results by methods of surface topology, while our approach may be described as arithmetic; namely, we use explicit representations of these groups over certain algebraic number fields. Our methods can be applied directly to the triangle group (2, 3, 7), i.e., to *closed* surfaces, and will furnish infinitely many examples of genera for which there exists a surface with maximal automorphism groups. However we do not pursue this question here.

The method of this paper relates certain questions involving compact Fuchsian groups to similar questions involving non-compact groups. The non-compact groups are easier to study in some ways, since they are free products and their representations are found more easily (see [**4**]). Among these groups is of course the modular group. We remark that the open problem of determining all genera for which there exists a surface with maximal automorphism group can be stated in the terms of the normal subgroups of the modular group. If Γ denotes the modular group and Δ is the normal closure of $\begin{pmatrix} 1 & 7 \\ 0 & 1 \end{pmatrix}$ in Γ, then Γ/Δ is isomorphic to the (2, 3, 7) triangle group. Thus the normal subgroups of finite index in the (2, 3, 7) group correspond in a 1–1 manner to the normal subgroups of finite index in Γ that contain Δ, i.e., the normal subgroups of finite index in Γ of level 7.

2. Punctured surfaces with maximal automorphism group. Let $\dot{S}$ be a punctured Riemann surface of genus g with τ punctures, where we assume throughout the following that

$$g \geqq 2, \quad \tau \geqq 1. \tag{1}$$

The group Γ such that $\dot{S} = \Gamma\backslash\mathscr{H}$ then has the signature

$$\{g; - ; \tau\};$$

i.e., Γ is a discrete subgroup of Ω, its genus is g and it has τ classes of parabolic elements and no elliptic elements. A presentation of Γ is

$$\Gamma = \left\{P_1, \ldots, P_\tau, A_1, B_1, \ldots, A_g, B_g; \prod_{i=1}^{\tau} P_i \prod_{j=1}^{g} A_j B_j A_j^{-1} B_j^{-1} = 1\right\}.$$

Thus Γ is a free group of rank $\tau+2g-1$. We denote the hyperbolic area of a fundamental region of Γ by $|\Gamma|$; by the results of Siegel [**7**], this is independent of the particular fundamental region used. Moreover,

$$|\Gamma| = 4\pi(g-1+\tfrac{1}{2}\tau)$$

and so $|\Gamma|$ is finite.

Let N be the normalizer of Γ in Ω. Because of our assumption (1), Γ is non-abelian and so N is discrete and $|N| > 0$ [**3**, p. 403]. Since $|\Gamma| < \infty$ and the index $\mu = (N:\Gamma)$ satisfies

$$\mu = |\Gamma|/|N|,$$

https://doi.org/10.1017/S001708950000015X Published online by Cambridge University Press

we see that μ is finite. Suppose that N has signature

$$\{g_0;\, e_1, e_2, \ldots, e_s;\, t\}$$

and denote the parabolic generators of N by $Q_1, \ldots, Q_t$. Here $g_0 \geqq 0$, $s \geqq 0$. Since τ is positive, t must also be positive, and

$$|N| = 4\pi\left\{g_0 - 1 + \tfrac{1}{2}t + \tfrac{1}{2}\sum_{i=1}^{s}\left(1 - \frac{1}{e_i}\right)\right\}.$$

By comparing $|N|$ and $|\Gamma|$ we find that

$$g - 1 + \tfrac{1}{2}\tau = \mu\left\{g_0 - 1 + \tfrac{1}{2}t + \tfrac{1}{2}\sum_{i=1}^{s}\left(1 - \frac{1}{e_i}\right)\right\}. \tag{2}$$

However, Γ is normal in N and hence [**2**, p. 581]

$$\tau = \mu \sum_{i=1}^{t} \frac{1}{n_i},$$

where n_i is the exponent of Q_i modulo $\Gamma (1 \leqq i \leqq t)$.

Let us write

$$x_i = \begin{cases} e_i & \text{for} \quad i = 1, \ldots, s, \\ n_i & \text{for} \quad i = s+1, \ldots, r \qquad (n_i > 1), \\ n_i & \text{for} \quad i = r+1, \ldots, s+t \quad (n_i = 1). \end{cases} \tag{3}$$

Then (2) becomes

$$g - 1 = \mu\left\{g_0 - 1 + \tfrac{1}{2}\sum_{i=1}^{r}\left(1 - \frac{1}{x_i}\right)\right\}. \tag{4}$$

In (4) we set $\mu = k(g-1)$, so that $k > 0$. Then

$$\frac{2}{k} = 2g_0 - 2 + \sum_{i=1}^{r}\left(1 - \frac{1}{x_i}\right). \tag{5}$$

The automorphism group is maximal if and only if $k = 84$. Hence $r > 0$. If we assume $g_0 > 0$ we get $2/k \geqq r/2 \geqq 1/2$, or $k \leqq 4$. Hence $g_0 = 0$ and

$$\sum_{i=1}^{r}\left(1 - \frac{1}{x_i}\right) = 2 + \frac{1}{42}. \tag{6}$$

We require the well-known and easily proved

LEMMA 1. *Let $y_1, \ldots, y_n$ be integers such that $y_i \geqq 2$ $(1 \leqq i \leqq n)$ and*

$$\sum_{i=1}^{n}\left(1 - \frac{1}{y_i}\right) > 2.$$

Then

$$\sum_{i=1}^{n}\left(1-\frac{1}{y_i}\right) \geqq 2+\frac{1}{42},$$

with equality only for $n = 3$ *and* $(y_1, y_2, y_3) = (2, 3, 7)$.

The Lemma shows that $x_1 = 2$, $x_2 = 3$, $x_3 = 7$ and, from (3), $x_i = 1$ for $4 \leqq i \leqq s+t$.

Let us define the *signature* of N modulo Γ to be the unordered set $(x_1, \ldots, x_t)$. (Note that this is simply the set of exponents $x > 1$ of the generators of N modulo Γ.) Then a necessary condition that $\dot{S} = \Gamma\backslash\mathscr{H}$ have an automorphism group of maximal order is that $N = N_\Omega(\Gamma)$ be a non-compact group of genus 0 and that the signature of N modulo Γ be (2, 3, 7).

We must now show that the above condition is sufficient. That is, we wish to prove that, if N is a non-compact discrete subgroup of Ω of genus 0 and Γ is a free normal subgroup of N of finite index such that the signature of N modulo Γ is (2, 3, 7), then $\dot{S} = \Gamma\backslash\mathscr{H}$ is a punctured Riemann surface with maximal automorphism group. For this purpose it is sufficient to prove the following

LEMMA 2. *Under the above hypotheses there is no discrete normal overgroup* F *of* Γ *with* $\Omega \supset F \supset N$ *and* $1 < (F\colon N) < \infty$.

For then N is necessarily the normalizer of Γ in Ω and we can apply the previous results. From (4) we deduce that g, the genus of Γ, is greater than 1. From (5) we calculate that $k = 84$, and so $\dot{S}$ has a maximal automorphism group.

We go on to the proof of the Lemma. The signature of N is

$$\{0; e_1, \ldots, e_s; t\}, \quad \text{where} \quad t > 0.$$

Denote by $t_1 \leqq t$ the number of exponents n_i that are greater than 1. Thus $t - t_1$ is the number of parabolic generators Q_1 already in Γ. Assume the lemma false. Then there is an $F \supset N$ with signature

$$\{0; e_1, \ldots, e_s, e_1^*, \ldots, e_u^*; t^*\},$$

where $u \geqq 0$, $t^* > 0$. Let $(F\colon N) = \rho$. The parabolic generators of F may be taken from the parabolic generators Q_i of N; say $Q_1, \ldots, Q_{t^*}$. Let m_i be the exponent of Q_i modulo Γ $(1 \leqq i \leqq t^*)$, and define t_1^* to be the number of m_i that are greater than 1. Then $t_1 \geqq t_1^*$ and $m_i = n_i$ $(1 \leqq i \leqq t_1^*)$. Hence

$$\sum_{i=1}^{t_1^*}\frac{1}{m_1} \leqq \sum_{i=1}^{t_1}\frac{1}{n_i}. \tag{7}$$

Comparing the hyperbolic areas $|N|$ and $|F|$, we find that

$$t+E-2 = \rho(t^*+E^*+E-2) \geqq \rho(t^*+E-2), \tag{8}$$

where

$$E = \sum_{i=1}^{s}\left(1-\frac{1}{e_i}\right), \quad E^* = \sum_{i=1}^{u}\left(1-\frac{1}{e_i^*}\right).$$

https://doi.org/10.1017/S001708950000015X Published online by Cambridge University Press

Next compare $|\Gamma|$ and $|F|$. Recalling that Γ has τ parabolic classes and is normal in F of index $\rho\mu$, we have

$$\tau = \rho\mu\left(\sum_{i=1}^{t_1^*} \frac{1}{m_i} + t^* - t_1^*\right) \leqq \rho\mu\left(\sum_{i=1}^{t_1} \frac{1}{n_i} + t^* - t_1^*\right)$$

$$= \rho\mu(t^* - M),$$

where

$$M = \sum_{i=1}^{t_1}\left(1 - \frac{1}{n_i}\right).$$

Finally, comparing $|\Gamma|$ and $|N|$, we get

$$\tau = \mu\left(\sum_{i=1}^{t_1} \frac{1}{n_i} + t - t_1\right) = \mu(t - M).$$

These relations give

$$t \leqq M + \rho(t^* - M).$$

Combining this with (8), we obtain

$$(1-\rho)(M+E-2) \geqq 0.$$

Since (6) implies that $M+E-2 = 1/42$, it follows that $\rho \leqq 1$. Hence $\rho = 1$ and $F = N$. Therefore N is maximal and we have completed the proof of Lemma 2, and so of the following

THEOREM 1. *Every punctured Riemann surface of genus $g \geqq 2$ with maximal automorphism group can be written in the form $S = \Gamma\backslash\mathscr{H}$, where $\Gamma \subset \Omega$ is a free group and the signature of $N = N_\Omega(\Gamma)$ modulo Γ is* (2, 3, 7). *Conversely, if $N, \Gamma \subset \Omega$ are such that N is a non-compact F-group of genus* 0, *Γ is a free normal subgroup of N of finite index, and the signature of N modulo Γ is* (2, 3, 7), *then $S = \Gamma\backslash\mathscr{H}$ is a punctured Riemann surface with maximal automorphism group.*

3. Existence of surfaces of given type. So far we have not proved the existence of a single punctured Riemann surface with maximal automorphism group. The possible surfaces can be classified according to the signature of the normalizer N modulo Γ. Let N have s elliptic generators, where $0 \leqq s \leqq 3$; it must then have $3 - s = t_1$ parabolic generators with exponents $n_i > 1$. The remaining $t - t_1$ parabolic generators already lie in Γ. Suppose that $s < 3$; then $t_1 > 0$. Two groups N that differ only in the value of $t - t_1$ give rise to surfaces $\dot{S}$ that differ only in the punctures; when the punctures are filled in, the closed surfaces S will be the same. For our purpose, which is the construction of closed surfaces, we may assume that $t = t_1$. On the other hand, when $s = 3$, we have $t_1 = 0$ and then we must have $t > 0$ in order that N be compact; we may assume in this case that $t = 1$.

We treat the three cases for which

$$s = 2, \quad t = t_1 = 1.$$

Then (e_1, e_2, n_1) is a permutation of (2, 3, 7). The triple (e_1, e_2, n_1) will be called the signature of the Riemann surface.

In this section a theorem will be proved which shows the existence of infinitely many inequivalent surfaces of a given signature provided that one such surface exists (Theorem 2, below). In the following section we shall exhibit a surface of each of the three types under consideration.

THEOREM 2. *Suppose that N and F are F-groups such that F is a free normal subgroup of N of finite index, N is of genus 0 and has exactly one parabolic class, and the signature of N modulo F is (2, 3, 7). Let P be the generator of the parabolic class of N, and let Δ denote the normal closure of P^n in N, where n is the exponent of P modulo F. Define*

$$F_q = F^q F' \Delta \quad (q = 1, 2, \ldots).$$

Then each F_q is a free normal subgroup of N of finite index, the F_q are mutually distinct, and the signature of N modulo F_q is (2, 3, 7).

Proof. Let us first observe that F contains Δ as a normal subgroup. Since F is free and its parabolic classes consist of N-conjugates $P_2, P_3, \ldots, P_r$ of $P_1 = P^n$, its presentation is

$$F = \left\{ P_1, \ldots, P_r, A_1, B_1, \ldots, A_g, B_g; P_1 \ldots P_r \prod_{i=1}^{g} A_i B_i A_i^{-1} B_i^{-1} = 1 \right\},$$

where $g > 0$ is the genus of F [3, p. 235]. Now considering F as an abstract group, we obtain the presentation of F/Δ by setting $P_1 = P^n = 1$ in the above presentation, which involves setting all $P_i = 1$ $(i = 1, \ldots, r)$. Thus

$$K = F/\Delta = \left\{ A_1, \ldots, B_g; \prod_{i=1}^{g} A_i B_i A_i^{-1} B_i^{-1} = 1 \right\};$$

i.e., K is isomorphic to the fundamental group of a closed surface of genus g. The groups F and K have the same genus: dividing by Δ is equivalent to filling in the punctures in $K \backslash \mathscr{H}$.

Under the homomorphism $F \to K$, we have $F^m \to K^m$ and $F' \to K'$. Hence

$$F/F_q \cong K/K_q,$$

where we define

$$K_q = K^q K'.$$

But K/K_q is the product of $2g$ cyclic groups of order q and so

$$[K : K_q] = q^{2g} = [F : F_q].$$

Obviously the F_q are all distinct and each is of finite index in F, therefore in N. Since F_q is a characteristic subgroup of F and F is a normal subgroup of N, F_q is normal in N. As a subgroup of F, F_q is free. Finally, N has signature (2, 3, 7) modulo F_q, since $P^n \in F_q$. This completes the proof of Theorem 2.

Now suppose that N, F, and F_q are as in Theorem 2. Lemma 2 shows that $N = N_\Omega(F)$. Since the surface $F\backslash\mathscr{H}$ of genus g, say, has a maximal automorphism group, we have $[N:F] = 84(g-1)$. Let $N_1 = N/\Delta$; then from the presentation of N,

$$N = \{x, y, P \mid x^{e_1} = y^{e_2} = xyP = 1\},$$

we deduce that

$$N_1 = \{x, y \mid x^{e_1} = y^{e_2} = (xy)^{n_1} = 1\}.$$

That is, N_1 is the (2, 3, 7) group. Since $K = F/\Delta$ is normal in N_1, the surface $K\backslash\mathscr{H}$ is maximal and so $[N_1:K] = 84(g-1)$.

Next we have

$$[N_1 : K_q] = [N_1 : K][K : K_q] = 84(g-1)m^{2g}.$$

By applying the hyperbolic area formula to K and K_q we derive

$$g_q - 1 = m^{2g}(g-1), \tag{9}$$

where g_q = genus of K_q. Hence

$$[N_1 : K_q] = 84(g_q - 1),$$

so that $K_q\backslash\mathscr{H}$ is a closed surface with maximal automorphism group and genus given by (9). Thus we have proved

THEOREM 3. *If N, F, and F_q are as defined in Theorem 2, then there exist closed surfaces S_q with maximal automorphism group whose genus g_q is given by*

$$g_q = 1 + q^{2g}(g-1) \quad \textit{for} \quad q \geqq 1,$$

where g is the genus of F. The uniformizing group of S_q may be taken to be $K_q = K^q K'$, where $K = F/\Delta$.

4. Construction of the particular groups F. The final step is to exhibit a group F for each of the three cases $(e_1, e_2) = (2, 3), (2, 7), (3, 7)$, where e_1, e_2 are the orders of the elliptic generators of the overgroup N, and to calculate the genus of F. We can then apply Theorem 3.

The requirements on F are that it should be free, of finite index in N, and that the parabolic generator of N should have exponent n modulo F, where $\{e_1, e_2, n\} = \{2, 3, 7\}$.

For $(e_1, e_2, n) = (2, 3, 7)$, N is the modular group and we can take $F = \Gamma(7)$, the principal congruence subgroup of level 7. The genus of F is 3. Thus

$$g_q = 1 + 2q^6. \tag{10}$$

The corresponding surfaces are evidently the same as those obtained by Macbeath [5].

Suppose that $(e_1, e_2, n) = (2, 7, 3)$ or $(3, 7, 2)$. The group N is then isomorphic to the free product of two cyclic finite groups of orders e_1, e_2; representations of such groups have been discussed in [4].

Consider the case (2, 7, 3). Let E be the ring of integers in the field obtained by adjoining $\zeta = e^{\pi i/7}$ to the rationals. The representation of the F-group $N = \{0;\ 2, 7;\ 1\}$ given in [**4**] is over E. Define

$$N(3) = \{A \in N \mid A \equiv \pm I \,(\mathrm{mod}\,(3))\},$$

where (3) is the ideal generated by 3 in E. Clearly $N(3)$ is of finite index in N. If $N(3)$ contains an element B of finite order, then B is conjugate to a power of either E_2 or E_7, the elliptic generators of N. Suppose, for example, that $E_7^m \in N(3)$ $(0 < m < 7)$. Since $(m, 7) = 1$, it follows that $E_7 \in N(3)$, which is seen to be false from the representation

$$E_7 = \begin{pmatrix} 0 & -1 \\ 1 & 2\cos\frac{\pi}{7} \end{pmatrix}.$$

The remaining case is disposed of in the same way. But N is isomorphic to a free product; by Kurosch's Subgroup Theorem, any subgroup with no elements of finite order must be free. Thus $N(3)$ is free and we can take $F = N(3)$ in Theorem 3. The case (3, 7, 2) is handled similarly.

Let $M = N(3)$. Since the surface $M\backslash\mathscr{H}$ is maximal, $g_M - 1 = \mu/84$, $\mu = [N : M]$. In the next section the index is calculated as $\mu = 13 \,.\, 27 \,.\, 28$, so that

$$g_M = 118.$$

Writing $M_q = M^q M'$ and $g_q =$ genus of M_q, we get

$$g_q = 1 + 117q^{236} \quad (q = 1, 2, \ldots). \tag{11}$$

The corresponding surfaces cannot overlap with those in (10), since 6 does not divide 236.

A similar calculation for the case (3, 7, 2) yields $\mu = 504$, $g_M = 7$,

$$g_q = 1 + 6q^{14} \quad (q = 1, 2, \ldots). \tag{12}$$

For $q = 1$ this surface is found in Macbeath [**6**], and, if we make use of the methods of Macbeath [**5**], we obtain the surfaces for $q > 1$.

5. Calculation of a certain index. In this section we shall prove that the index $\mu = [N : M]$ is $13 \,.\, 27 \,.\, 28$, where N is the group $\{0;\ 2, 7;\ 1\}$ and $M = N(3)$. The remaining case, $N = \{0;\ 3, 7;\ 1\}$, $M = N(2)$, is handled in the same way but the details are far easier.

Let $\mathscr{Z}$ be the ring of integers of an algebraic number field. Let $\{\omega_i : i = 1, \ldots, n\}$ be an integral basis for $\mathscr{Z}$. We get

$$G = LF(2, \mathscr{Z}), K = \left\{ \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & \omega_i \\ 0 & 1 \end{pmatrix} \ (i = 1, \ldots, n) \right\},$$

$$G(\mathfrak{a}) = \{A \in G \mid A \equiv \pm I \,(\mathrm{mod}\,\mathfrak{a})\},$$

where $\mathfrak{a}$ is an ideal in $\mathscr{Z}$.

LEMMA 3. $KG(\mathfrak{a}) = G$.

Proof. $KG(\mathfrak{a})$ is defined, since $G(\mathfrak{a})$ is normal in G. Let

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in G.$$

Since α and γ are coprime in $\mathscr{Z}$, we can choose τ so that $\alpha\tau+\gamma$ is prime to $\mathfrak{a}$. Then

$$\begin{pmatrix} 1 & 0 \\ \tau & 1 \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma_1 & \delta_1 \end{pmatrix}$$

with γ_1 prime to $\mathfrak{a}$. Next solve the congruence $\alpha+\rho\gamma_1 \equiv 1 \pmod{\mathfrak{a}}$ for ρ and get

$$\begin{pmatrix} 1 & \rho \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ \gamma_1 & \delta_1 \end{pmatrix} \equiv \begin{pmatrix} 1 & \beta_2 \\ \gamma_1 & 1+\beta_2\gamma_1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \gamma_1 & 1 \end{pmatrix}\begin{pmatrix} 1 & \beta_2 \\ 0 & 1 \end{pmatrix} \pmod{\mathfrak{a}}.$$

Thus

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -\tau & 1 \end{pmatrix}\begin{pmatrix} 1 & -\rho \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ \gamma_1 & 1 \end{pmatrix}\begin{pmatrix} 1 & \beta_2 \\ 0 & 1 \end{pmatrix} P \tag{*}$$

with $P \in G(\mathfrak{a})$. Note that

$$\begin{pmatrix} 1 & 0 \\ -\tau & 1 \end{pmatrix} \in K$$

since

$$-\begin{pmatrix} 1 & 0 \\ -\tau & 1 \end{pmatrix} = T\begin{pmatrix} 1 & \tau \\ 0 & 1 \end{pmatrix}T, \quad T = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

and, similarly, the other matrices in the right member of (*) belong to K. Hence

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in KG(\mathfrak{a}),$$

as required.

Now let $\mathscr{Z}$ be the ring of integers in $Q(\zeta)$ with $\zeta^7 = -1$. Setting

$$\lambda = \zeta+\zeta^{-1} = 2\cos\tfrac{1}{7}\pi,$$

we find that the irreducible equation satisfied by λ over Q is

$$\lambda^3-\lambda^2-2\lambda+1 = 0. \tag{13}$$

Let

$$N = \left\{\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}\right\}.$$

Since $\{1, \lambda\}$ is not a basis for $\mathscr{Z}$, the group N does not satisfy the hypotheses for K, and Lemma 3 is not directly applicable.

We proceed as follows. Let $\mathfrak{a} = (3)$ and let $M = N(3)$, $\mu = [N:M]$. Since 3 is a prime in $\mathscr{Z}$ (because 3 is a primitive root of 7), we have

$$[G : G(3)] = \tfrac{1}{2}(N-1)N(N+1),$$

https://doi.org/10.1017/S001708950000015X Published online by Cambridge University Press

where N, the norm of 3 in $\mathscr{Z}$, equals 27, $G = LF(2, \mathscr{Z})$, and $G(3)$ is the principal congruence subgroup of G modulo (3). The idea will be to prove that

$$NG(3) = G. \tag{14}$$

Then, since $M = N \cap G(3)$, we shall have

$$G/G(3) \cong N/M$$

and so

$$\mu = [N : M] = [G : G(3)] = 13.27.28,$$

as asserted.

In any event $NG(3)$ is a subgroup of G and so the isomorphism shows that $\mu \mid 13 . 27 . 28$. We also know that $\mu = 84(g-1)$. Hence setting

$$\mu = 84\mu_1, \tag{15}$$

we have

$$\mu_1 \mid 9.13. \tag{16}$$

Let

$$R = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix} = \begin{pmatrix} 1+\lambda^2 & \lambda \\ \lambda & 1 \end{pmatrix} \in N.$$

Its trace $t = 2+\lambda^2$ satisfies the equation†

$$t^3 \equiv 2t^2+t-1 \pmod 3.$$

Using $R^2 = tR-I$, we calculate successive powers of R and find that

$$R^{13} \equiv I \pmod 3.$$

Thus $R^{13} \in M$ and hence $13 \mid \mu$; from (15) it follows that $13 \mid \mu_1$. Set

$$\mu_1 = 13\mu_2, \tag{17}$$

where $\mu_2 \mid 9$.

In order to prove $\mu_2 = 9$, we observe that

$$NG(3)/G(3) \cong N/M;$$

hence $[NG(3): G(3)] = \mu = 84 . 13 . \mu_2$. In the chain

$$G \supset NG(3) \supset G(3),$$

we have $[G: G(3)] = 13 . 27 . 28$; therefore $[G: NG(3)] = 9/\mu_2$.

Suppose that $S \in G$; then $S^k \in NG(3)$ for some k in $1 \leqq k \leqq 9/\mu_2$. Choose

$$S = \begin{pmatrix} \lambda & 0 \\ 0 & 1/\lambda \end{pmatrix}.$$

† For typographical convenience we write mod 3 instead of mod (3).

https://doi.org/10.1017/S001708950000015X Published online by Cambridge University Press

Because of $\lambda^{13} \equiv -1 \pmod 3$—as we calculate from (13)—it follows that $S^{13} \in NG(3)$. Hence $k \mid 13$, and $k < 13$ implies that $k = 1$, i.e., S is already in $NG(3)$.

Now $\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \in N$, and so, for each integer r,

$$S^r \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} S^{-r} = \begin{pmatrix} 1 & \lambda^{2r+1} \\ 0 & 1 \end{pmatrix} \in NG(3).$$

But the odd powers of λ form an integral basis for $\mathscr{Z}$, as we see from the equations

$$1 = \lambda^3 - 3\lambda + 1/\lambda, \quad \lambda^2 = 2 + \lambda - 1/\lambda.$$

Hence $NG(3)$ contains $\begin{pmatrix} 1 & \omega_i \\ 0 & 1 \end{pmatrix}$, where ω_i runs over a basis for $\mathscr{Z}$, and $NG(3)$ certainly contains $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, since N does. Let K be the subgroup of $NG(3)$ generated by

$$\left\{ \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & \omega_i \\ 0 & 1 \end{pmatrix} \right\}.$$

Applying Lemma 3 we see that $KG(3) = G$; hence $NG(3) = G$. This proves the correctness of (14) and completes the proof.

REFERENCES

1. A. Hurwitz, Über algebraische Gebilde mit eindeutigen Transformationen in sich, *Math. Ann.* **41** (1893), 403–442.

2. M. I. Knopp and M. Newman, Congruence subgroups of positive genus of the modular group, *Illinois J. Math.* **9** (1965), 577–583.

3. J. Lehner, *Discontinuous groups and automorphic functions*, American Math. Soc. (Providence, 1964).

4. J. Lehner and M. Newman, Real two-dimensional representations of the free product of two finite cyclic groups, *Proc. Cambridge Philos. Soc.* **62** (1966), 135–141.

5. A. M. Macbeath, On a theorem of Hurwitz, *Proc. Glasgow Math. Assoc.* **5** (1961), 90–96.

6. A. M. Macbeath, On a curve of genus 7, *Proc. London Math. Soc.* **15** (1965), 527–542.

7. C. L. Siegel, Some remarks on discontinuous groups, *Ann. of Math.* **46** (1945), 708–718.

University of Maryland
College Park
and
National Bureau of Standards
Washington, D.C.

National Bureau of Standards
Washington, D.C.