GROUPS RELATED TO COMPACT RIEMANN SURFACES

BY

CHIH-HAN SAH

University of Pennsylvania, Philadelphia, Penn., U.S.A.(1)

It has been known for a long time that the automorphism group of a compact Riemann surface of genus $g>1$ is a finite group. Indeed, Hurwitz gave the upper bound of $84(g-1)$ for the order. In [22, 23], Macbeath described a procedure to construct Riemann surfaces attaining this upper bound. He observed that these surfaces arise from normal subgroups of finite index in a particular abstract group. This abstract group is a discontinuous subgroup of conformal automorphisms of the upper half plane having the signature $\{2, 3, 7 \mid 0\}$. By considering homomorphisms of this abstract group G into a finite group PSL $(2, p^f)$ Macbeath found many normal subgroups of finite index in G. Later, Lehner and Newman [19] used another method to obtain several of the groups and surfaces discovered by Macbeath. The purpose of the present paper is to apply the available techniques and results of finite group theory to the study of the finite quotient groups of discontinuous groups connected with Riemann surfaces.

Section 1 deals with the two-dimensional projective representations of a triangular group in an algebraically closed field K. (The assumption that K be algebraically closed will be seen to be unnecessary.) Indeed, there are only a finite number of inequivalent representations. However, for higher dimensional representations, this is no longer the case (see Corollary of Proposition 2.7). Theorem 1.5 shows that all discontinuous groups acting on the upper half plane with fundamental domains having finite areas behave almost like free groups. In Theorem 1.6, under very mild restrictions on the signature, we give explicitly the number of distinct torsion-free normal subgroups of a triangular group with certain prescribed factor groups. After the completion of this paper, A. M. Macbeath kindly informed us that our section 1 overlaps results of his in a paper that will appear shortly.

Throughout section 2 we use freely some rather complicated results of finite group theory. We assume a familiarity with standard arguments involving Sylow's Theorem and

(1) This research was partially supported by a grant from the National Science Foundation.

transfer theory. The first half reviews some of the geometric interpretations of the results from section 1. The second half contains another procedure for finding finite quotient groups of our discontinuous groups. In particular, we show the existence of Riemann surfaces with maximal automorphism groups isomorphic to some of the recently discovered simple finite groups of Janko and Ree.

Throughout section 3 we use freely the identification of the homology groups of a compact Riemann surface (of positive genus) S and the homology groups of its fundamental group S, i.e., S is a $K(S, 1)$ Eilenberg–MacLane space. This section deals with the action of a finite group of automorphisms on the homology groups. Theorem 3.2 generalizes a result of Hurwitz to the effect that the automorphism group of a compact Riemann surface of genus greater than 1 acts faithfully on the space of holomorphic differentials. Results in this section can be combined with those in the preceding sections to determine the possible values of the genus (say below 100) for which there exists a Riemann surface with maximal automorphism group.

In a later publication, we hope to consider the possible generalizations to an abstract function field as well as the relation between the automorphism groups and the detailed analytic structures of the surfaces. For the convenience of the reader, we have included a rather lengthy appendix listing a number of more or less well-known results. The appendix also explains the notations to be used throughout this paper. The bibliography is by no means complete. We have included only those that are immediately relevant. After the completion of the manuscript several additional papers came to our attention by way of A. M. Macbeath. These are:

ACCOLA, R. D. M., On the number of automorphism of a closed Riemann surface. *Trans. Amer. Math. Soc.*, 131 (1968), 398–408.

HARVEY, W. J., Cyclic groups of automorphisms of a compact Riemann surface. *Quart. J. Math.*, 17 (1966), 86–97.

MACLACHLAN, C., Abelian groups of automorphisms of compact Riemann surfaces. *Proc. Lond. Math. Soc.*, 15 (1965), 699–712.

MACLACHLAN, C., A bound for the number of automorphisms of a compact Riemann surface. To appear.

1. Two dimensional projective representations

Throughout this section K will denote an algebraically closed field of characteristic p with prime field K_p. Let r, s and t be integers. Set

$$E(r, s, t) = \{(R, S, T) \mid R, S, T \in \mathrm{SL}(2, K),\ RS = T,\ \text{and}\ R, S, T \text{ have orders } r, s, t\}.$$

For any subfield M of K set $E(r, s, t)_M = \mathrm{SL}(2, M)^3 \cap E(r, s, t)$. $E(r, s, t)$ is a transformation space under conjugation by elements of SL $(2, K)$. It is clear that the traces (μ_r, μ_s, μ_t) depend only on the SL $(2, K)$ orbit of an element (R, S, T) in $E(r, s, t)$. We let $E(\mu_r, \mu_s, \mu_t)$ denote the subset of elements in $E(r, s, t)$ with trace signature (μ_r, μ_s, μ_t). A subfield M of K is called a splitting field for the orbit E if E_M is non-empty. For each (R, S, T) in $E(r, s, t)$, let Gp (R, S, T) be the subgroup of SL $(2, K)$ generated by R, S, T. Its image in PSL $(2, K)$ will be denoted by PGp (R, S, T). It is clear that the isomorphism classes of these groups depend only on the SL $(2, K)$ orbit of (R, S, T). We wish to determine the number of SL $(2, K)$ orbits in $E(r, s, t)$ as well as the minimal splitting field (if any) of each of the orbits. The problem has been analyzed by Macbeath [21; Theorem 44, p. 68]. His results did not take into consideration a number of degenerate cases; moreover, no general information was given concerning the minimal splitting field and the associated groups.

PROPOSITION 1.1. *Let K be an algebraically closed field of characteristic p. For each integer $i>0$ let i_0 be the largest divisor of i which is not divisible by p. Let $\mu_i = \zeta_i + \zeta_i^{-1}$, ζ_i a primitive i_0-th root of 1 in K. Let r, s and t be positive integers.*

(a) *$K_p(\mu_r, \mu_s, \mu_t)$ is a finite abelian extension field of K_p depending only on r, s and t. This field will be denoted by $K(r, s, t)$.*

(b) *If $E(r, s, t)_M$ is non-empty, then M contains $K(r, s, t)$.*

Proof. (a) $K_p(\zeta_r)$ is clearly a finite abelian extension field of K_p depending only on r. We must show that $K_p(\mu_r)$ is a uniquely determined subfield of $K_p(\zeta_r)$ depending only on r. Clearly we may assume that $p \nmid r$. When $p=0$ the Galois group of $Q(\zeta_r)$ over Q acts transitively on the primitive rth roots of 1. $Q(\mu_r)$ is then the unique totally real subfield of $Q(\zeta_r)$. When $p>0$ $K_p(\zeta_r)$ is a cyclic extension of degree f over K_p, where f is the order of p mod r_0. ζ_r satisfies the quadratic equation $X^2 - \mu_r X + 1 = 0$ over $K_p(\mu_r)$. It is easy to see that $K_p(\mu_r)$ is the unique subfield of degree f_r over K_p in $K_p(\zeta_r)$, where f_r is the least positive integer n such that r_0 divides one of p^n+1, p^n-1.

(b) follows easily from the fact that $K(r, s, t)$ is generated by the traces of (R, S, T) in $E(r, s, t)_M$, q.e.d.

PROPOSITION 1.2. *In the preceding notations,*

(a) The center of SL *$(2, K)$ consists of $\pm I$, I the identity. When $p \neq 2$, $-I$ is the unique element of order 2 in* SL *$(2, K)$.*

(b) *Let $p>0$. Every element of order divisible by p is conjugate to $P = \pm \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. The centralizer $C(P)$ of P in* SL *$(2, K)$ is $\{\pm \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \mid b \in K\}$.*

(c) Let $r>2$ and $p \nmid r$. Each element R of order r in SL *$(2, K)$ is conjugate to $\left(\begin{smallmatrix} 0 & -1 \\ 1 & \mu_r \end{smallmatrix}\right)$,*

μ_r = trace of R. The centralizer $C(R)$ of R in SL $(2, K)$ is $\{aI - bR \mid a, b \in K, a^2 - \mu_r ab + b^2 = 1\}$. *The number of such conjugate classes is $\varphi(r)/2$; φ denotes the Euler function.*

(*d*) *Let $p > 0$ and let $(R, S, T) \in E(r, s, t)$.*

(1) *$r, s, t \in \{p, 2p\}$.* PGp (R, S, T) *is either the direct product of at most two cyclic groups of order p or isomorphic to* PSL $(2, p)$.

(2) *$r, s \in \{p, 2p\}$ and $t \notin \{p, 2p\}$.* If $p = 2$, then PGp $(R, S, T) =$ Gp (R, S, T) *is the dihedral group of order $2t$, t odd. If $p > 2$, then* PGp (R, S, T) *is isomorphic to* PSL $(2, K_p(\mu_t))$ *except when $K_p(\mu_t)$ has 9 elements. In the exceptional case* PGp (R, S, T) *is isomorphic to the alternating group of degree* 5.

Proof. (a), (b) and (c) are straightforward.

(d) When $p = 2$, let $H = G$. When $p > 2$, let H be the subgroup of G generated by R^2 and S^2. In all cases, $G =$ Gp (R, S, T). Clearly $G \leqslant \{\pm H\}$ with equality holding when and only when $-I \in H$. Multiplying R and S by $\pm I$ allows us to assume that R and S have orders p and that one of T, $-T$ has order t. After a conjugation, we may take $R = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $S = \left(\begin{smallmatrix} a & b \\ c & 2-a \end{smallmatrix}\right)$, where $(a-1)^2 + bc = 0$, a, b and $c \in K$. The trace μ_t must then be one of $\pm(2 + c)$. According to assertion (b), we see that R and S commute if and only if $c = 0$; when this occurs, we have the first case of (1). Suppose that $c \neq 0$, we can then conjugate both R and S by $\left(\begin{smallmatrix} 1 & d \\ 0 & 1 \end{smallmatrix}\right)$ with $a + cd = 1$. A calculation shows that we may assume $a = 1$ and $b = 0$. When $p = 2$, (A7) of the appendix shows that we have a dihedral group. This is the first case of (2). When $p > 2$, $K_p(\mu_t) = K_p(c) = K(r, s, t)$. A theorem of Dickson [9; p. 44] shows that $-I \in H$ and that we have either the second case of (1) or the second case of (2), q.e.d.

COROLLARY. *Let $x, y \in$* PSL $(2, K)$, *K an algebraically closed field of characteristic $p > 0$. Suppose that x, y and xy have finite orders p, p, n respectively, $2/p + 1/n < 1$. The group G generated by x and y is one of the following types:*

(a) *$n = p$. G is either the direct product of at most two cyclic groups of order p or the simple group* PSL $(2, p)$, *$p > 3$.*

(b) *$p \nmid n$. G is either a simple group* PSL $(2, p^f)$ *or the alternating group of degree* 5.

Each of these types occurs. In particular, G is a group of positive curvature if and only if either G is cyclic of order p $(n = p)$ or $(p, p, n) = (3, 3, 5)$, $(5, 5, 2)$, $(5, 5, 3)$, $(5, 5, 5)$ and G is the alternating group of degree 5.

The corollary follows quickly from (A7) of the appendix together with the preceding proposition.

We now analyze the remaining case. Let $p \nmid r$ and $r > 2$. We wish to determine the num-

ber of SL $(2, K)$ orbits in $E(\mu_r, \mu_s, \mu_t)$ as well as the splitting field of each orbit. In such an orbit we select a representative (R, S, T) with $R=\left(\begin{smallmatrix}0 & -1\\ 1 & \mu_r\end{smallmatrix}\right)$. The calculations could be made simpler if R were taken in diagonal form. However, it would not be obvious what could serve as a minimal splitting field (if any). With this choice of R the triple (R, S, T) is unique up to conjugation by elements of $C(R)$. If we set $S=\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)$, then the condition that $(R, S, T)\in E(\mu_r, \mu_s, \mu_t\}$ becomes

$$\begin{cases} ad-bc=1 \\ a+d=\mu_s \\ b-c+\mu_r d=\mu_t \end{cases} \tag{1}$$

Eliminating c and d we see that S stands in bijective correspondence with its first row (a, b) which must satisfy

$$a^2-\mu_r ab+b^2-\mu_s a+(\mu_r\mu_s-\mu_t)b+1=0 \tag{2}$$

We must determine the action of $C(R)$ on the set of solutions of (2) through conjugation on S. Setting $x=a+a_0$ and $y=y+b_0$ so as to get rid of the terms of degree 1 in (2), after a calculation we obtain

$$x^2-\mu_r xy+y^2=-F(a_0, b_0), \tag{3}$$

$F(a, b)$ is the left side of (2), provided that a_0, b_0 satisfy

$$\begin{cases} -2a_0+\mu_r b_0=\mu_s \\ \mu_r a_0-2b_0=-(\mu_r\mu_s-\mu_t) \end{cases} \tag{4}$$

The hypotheses $p\nmid r$ and $r>2$ imply that $\mu_r^2\neq 4$. Thus equation (4) has a unique solution a_0, b_0 in $K(r, s, t)$ independent of the choice of SL $(2, K)$ orbit in $E(\mu_r, \mu_s, \mu_t)$. Using (1) and (4) we can transform (3) into

$$\begin{aligned} x^2-\mu_r xy+y^2=a_0^2-\mu_r a_0 b_0+b_0^2-1&=(4-\mu_r^2)^{-1}\{\mu_r^2+\mu_s^2+\mu_t^2-\mu_r\mu_s\mu_t-4\} \\ &=(4-\mu_r^2)^{-1}\{\mu_r-(\zeta_s\zeta_t+\zeta_s^{-1}\zeta_t)\}\{\mu_r-(\zeta_s\zeta_t^{-1}+\zeta_s^{-1}\zeta_t^{-1})\}. \end{aligned} \tag{5}$$

Set $S^{\#}=S+a_0 I-b_0 R$ so that $\sigma S^{\#}\sigma^{-1}=\sigma S\sigma^{-1}+a_0 I-b_0 R=(\sigma S\sigma^{-1})^{\#}$ for all σ in $C(R)$. Using (1) and (4) again we obtain $S^{\#}=(yI-xR)\left(\begin{smallmatrix}0 & 1\\ 1 & 0\end{smallmatrix}\right)$ so that

$$\sigma S^{\#}\sigma^{-1}=\sigma^2 S^{\#} \quad \text{for all } \sigma \text{ in } C(R). \tag{6}$$

The condition $4\neq\mu_r^2$ is equivalent with the non-degeneracy (or the non-defectivity when $p=2$) of the binary quadratic form $x^2-\mu_r xy+y^2$. $C(R)$ is then isomorphic to the multiplicative group of the algebraically closed field K. The solutions to (2) can be identified among the bijective correspondences: $S\leftrightarrow(a, b)\leftrightarrow(x, y)\leftrightarrow S^{\#}\leftrightarrow yI-xR$. (6) identifies the

action of σ in $C(R)$ as left multiplication by σ^2 on the set $\{yI-xR|x,\ y\in K \text{ satisfy } (5)\}$. We can conclude from the algebraic closure of K that σ^2 ranges over all of $C(R)$ as σ does. When the right side of (5) is not zero, $E(\mu_r, \mu_s, \mu_t)$ then gives a single SL $(2, K)$ orbit. The associated group PGp (R, S, T) is non-abelian. When the right side of (5) is zero, the solutions (x, y) form two distinct lines in a plane over K with intersection at the origin. It is clear that there are three SL $(2, K)$ orbits. The one corresponding to the origin is the only one leading to an abelian group PGp (R, S, T). Indeed, it is even cyclic.

PROPOSITION 1.3. *In the preceding notation, let* $r>2$ and $p\nmid r$.

(a) *The right side of equation* (5) *is zero if and only if* $\zeta_r\in\{\zeta_s\zeta_t, \zeta_s\zeta_t^{-1}, \zeta_s^{-1}\zeta_t, \zeta_s^{-1}\zeta_t^{-1}\}$.

(b) *If the right side of equation* (5) *is not zero, then* $E(\mu_r, \mu_s, \mu_t)$ *is a single* SL $(2, K)$ *orbit. The group* PGp (R, S, T) *is non-abelian.*

(c) *If the right side of equation* (5) *is zero, then* $E(\mu_r, \mu_s, \mu_t)$ *decomposes into three* SL $(2, K)$ *orbits. One of these has a cyclic associated group* PGp (R, S, T) *whose order is not divisible by* p. *The other two have solvable, non-abelian associated group* PGp (R, S, T) *which contains non-trivial unipotent elements. (If* $p>0$, *this means the order is divisible by* p.)

(d) *If* $p>0$, *then* $K(r, s, t)$ *is the minimal splitting field of each of the* SL $(2, K)$ *orbits in* $E(r, s, t)$.

(e) *If* $p=0$, *then* $Q(\zeta_r, \zeta_s, \zeta_t)$ *is a splitting field of each* SL $(2, K)$ *orbit in* $E(r, s, t)$.

Proof. (a) It is clear that the condition is sufficient. Conversely, by symmetry, we assume that $\mu_r=\zeta_s\zeta_t+\zeta_s^{-1}\zeta_t^{-1}$. Let the common value be B. It is clear that $X^2-BX+1=(X-\zeta_r)(X-\zeta_r^{-1})=(X-\zeta_s\zeta_t)(X-\zeta_s^{-1}\zeta_t^{-1})$ so that (a) holds.

(b) and the first part of (c) have been verified previously. For the remaining parts of (c) it is more convenient to use a different normal form for R. We take R to be in diagonal form. Thus let $R=\left(\begin{smallmatrix}e & 0\\ 0 & e^{-1}\end{smallmatrix}\right)$, $e=\zeta_r$ and let $S=\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)$. It is clear that a and d are uniquely determined by the conditions $a+d=\mu_s$, $\zeta_r a+\zeta_r^{-1}d=\mu_t$ and $ad-bc=1$. It is easy to see that the right side of (5) is zero if and only if $ad=1$. The three SL $(2, K)$ orbits mentioned in (c) correspond to: $b=0=c$; $b=0\neq c$; and $b\neq 0=c$. (c) now follows from inspection.

In order to verify (d) and (e) we refer back to the discussion preceding the proposition. All of our transformations are rational over the field $K(r, s, t)$. Equation (5) has all its coefficients in $K(r, s, t)$. When $p>0$, $K(r, s, t)$ is a finite field. It is well known that such an equation has non-trivial solutions in $K(r, s, t)$. When $p=0$, $\mu_r^2-4=(\zeta_r-\zeta_r^{-1})^2$ so equation (5) has non-trivial solutions in $Q(\zeta_r, \zeta_s, \zeta_t)$, q.e.d.

We now give an application of the preceding result. We refer the reader to the appendix for the notations. Let G be a group with finite signature $\{r, s, t|0\}$. A homomorphism σ from G into an arbitary group H is called non-degenerate if σ carries the generators of

order r, s and t onto elements of orders r, s and t in H respectively. When H is SL $(2, K)$, a non-degenerate homomorphism amounts to the selection of an element $(R, S, T) \in E(r, s, t)$, where R, S and T^{-1} are the respective images. If H is taken to be PSL $(2, K)$, then we have to adjust the integers r, s, t in order to describe the non-degenerate homomorphisms from G to H. In any event, two non-degenerate homomorphisms from G to H are called $(H-)$-equivalent if they differ by an inner automorphism of H. According to (A4) the kernel of a non-degenerate homomorphism is always a torsion-free normal subgroup.

We now consider the structure of the commutator quotient group of a group G with a finite signature $\{e(1), ..., e(m)|\gamma\}$. For each prime p the p-periods of G are defined to be $\{e_p(1), ..., e_p(m)\}$, where $e_p(i)$ is the highest power of p dividing $e(i)$. These numbers are the orders of the maximal cyclic p-subgroups of G. (We ignore the trivial periods.)

PROPOSITION 1.4. *Let G be a group with finite signature $\{e(1), ..., e(m)|\gamma\}$. Let G' be the commutator subgroup of G.*

(a) *Suppose that G has p-torsion. Then G' has p-torsion if and only if G has a unique maximal p-period.*

(b) *Suppose that G' is torsion-free. For each prime p let $d_p(1), ..., d_p(t_p)$ be the non-trivial p-periods of G listed in increasing order.*

(1) *G/G' is a direct product of cyclic groups of order $d_p(i)$, $1 \leqslant i \leqslant t_p - 1$, and a free abelian group of rank 2γ, where p ranges over all the prime divisors of the periods of G.*

(2) *Let e be the* l.c.m. *of all $e(i)$, equivalently, the product of all $d_p(t_p)$. G has a torsion-free normal subgroup S with G/S isomorphic to a cyclic group of order e if and only if the number of even periods is even, when the maximal 2-period is 2.*

The proof is an easy application of (A4) and elementary divisor theory. We will omit the details.

We now turn to the general situation where the group G has a signature which may be infinite.

THEOREM 1.5. *Let G be a group with signature $\{e(1), ..., e(m)|\gamma\}$.*

(a) *G is residually finite. (The intersection of the subgroups of finite index is* 1.)

(b) *G is perfect if and only if the following conditions hold:*

(1) $\gamma = 0$,

(2) *all $e(i)$ are finite, and*

(3) *$e(i)$'s are pairwise coprime.*

(c) *If G is not pefect, then G is residually finite and solvable. In fact, when G has negative curvature, there exists torsion-free normal subgroup S such that G/S is a finite solvable group with solvable length larger than any pre-assigned integer N.*

Proof. If the curvature of G is not negative, then all of our assertions can be obtained from (A7) and (A8) of the appendix by inspection. Thus we will assume that G has negative curvature.

Case 1. $e(i)=\infty$ for at least one i, say $e(m)$.

We can delete the parabolic generator x_m simultaneously with the two defining relations $x_m^\infty=1$, $x_1 \dots x_m[a_1, b_1] \dots [a_\gamma, b_\gamma]=1$. G is now clearly the free product of a free group of rank 2γ with $m-1$ cyclic groups of order $e(i)$, $1 \leqslant i \leqslant m-1$. The subgroup S of G generated by all commutators and all eth powers of elements of G is clearly a normal subgroup. When e is the l.c.m. of all the finite $e(i)$'s, it is clear that G/S is a finite abelian group and that S is torsion-free (see (A5)). Indeed, S is a free group of finite rank.

Case 2. $e(i)<\infty$ for all i, $\gamma>0$.

If $m=0$, then G is residually finite and solvable according to (A6). Let $m>0$ and let e be the l.c.m. of all the $e(i)$'s. Let H_1 be the direct product of cyclic groups of order $e(i)$, $1 \leqslant i \leqslant m$, with generators X_i of order $e(i)$. It is clear that $X=X_1 \dots X_m$ has order e in H_1. Let H_2 be the dihedral group $G\{2, 2, 2e\,|\,0\}$ of order $4e$ with generators A_1, B_1 and defining relations: $A_1^2=B_1^2=(A_1B_1)^{2e}=1$. A_1B_1 generates a cyclic normal subgroup of order $2e$ in H_2. It is clear that the element $XA_1B_1A_1B_1$ generates a normal subgroup of order e in the direct product of H_1 and H_2. Let H be the corresponding factor group of $H_1 \times H_2$. It is then clear that H is a finite solvable group. To x_i of G we assign the coset of X_i in H. To a_1, b_1 of G we assign the coset of A_1, B_1 in H respectively. To a_i, b_i of G, $i>1$, we assign the identity of H. It is clear that this can be extended uniquely to a surjective homomorphism from G to H. We may conclude from (A5) that the kernel S of this homomorphism is a torsion free surface subgroup with a finite solvable factor group G/S.

Case 3. $\gamma=0$, all $e(i)$'s are finite, and there exist a prime p and indices $j<k$ such that p divides both $e(j)$ and $e(k)$.

We first observe that the negativity of the curvature of G together with $\gamma=0$ force m to be at least 3. Moreover, the curvature of any subgroup of finite index in G is also negative (see (A_4)).

We may assume that $e(m-1)$ and $e(m)$ are divisible by p. Let H be a cyclic group of order p with generator h. We assign 1 of H to x_i, $i<m-1$. We assign h to x_{m-1} and h^{-1} to x_m. This assignment extends uniquely to a surjective homomorphism from G to H. According to (A4), the kernel G_1 of this homomorphism has periods $e(i)$, $1 \leqslant i \leqslant m-2$, each repeated p times, and $e(m-1)/p$, $e(m)/p$. The genus of G_1 is 0. Since $m>2$, we can find a prime q dividing $e(1)$. We repeat our argument with q in place of p and with the first two periods $e(1)$, $e(1)$ of G_1 in place of $e(m-1)$ and $e(m)$. We can therefore find a normal sub-

group G_2 of index q in G_1 such that G_2 has genus 0 and such that every period of G_2 appears with a multiplicity at least 2. According to Proposition 1.4, the commutator subgroup G_3 of G_2 is a torsion-free surface subgroup of finite index in G_2.

Case 4. $\gamma=0$, all $e(i)$'s are finite, and $e(i)$'s are pairwise coprime.

If we read the defining relations in the commutator quotient group of G, then we can conclude that each x_i must have order dividing $e(i)$ as well as the product of the remaining $e(j)$'s. It follows that G is perfect.

At this point, we have proved (*b*). We shall continue to show that, under Case 4, the group G nevertheless has a torsion-free normal subgroup of finite index. As we observed before, $m>2$.

Suppose that $m=3$. Let p be a prime greater than all $e(i)$. Let $(R, S, T)\in E(2e(1), 2e(2), 2e(3))_M$, $M=K(2e(1), 2e(2), 2e(3))$, according to Proposition 1.3. The cosets of R, S and T in PSL(2, M) have orders $e(1)$, $e(2)$ and $e(3)$ respectively. If we assign to x_1, x_2 and x_3 the cosets of R, S and T^{-1} in PSL(2, M), then we obtain a non-degenerate homomorphism from G to PSL (2, M). The kernel of this homomorphism is then a torsion-free normal subgroup of finite index in G.

Suppose that $m>3$. We proceed by induction on m. Let H be a group with signature $\{e(1), ..., e(m-1)|0\}$. By setting the last elliptic generator of G equal to 1 we see that H is a factor group of G. If H has a non-negative curvature, then the hypothesis that $e(i)$ are pairwise coprime together with (A7) and (A8) show that H is the icosahedral group. Thus $T=1$ is a torsion-free normal subgroup of finite index in H. If H has negative curvature, then the induction hypothesis produces a torsion-free normal subgroup T of finite index in H. Let S be the inverse image of T in G. It follows from (A4) that S has a finite signature with periods $e(m)$ repeated a finite number of times. Proposition 1.4 shows that the subgroup U of S generated by all the commutators and all the $e(m)$th powers of elements in S is a torsion-free normal subgroup of finite index in G.

We now make the observation that a subgroup of finite index in a group G always contains a normal subgroup of finite index in G. Thus the group G is residually finite if and only if it contains a residually finite subgroup of finite index. Assertion (a) now follows from the preceding analysis together with (A6).

(c) Assume now that G is not perfect. Cases 1 through 3 show that there is a sequence of subgroups $G=G_0\geqslant G_1\geqslant ...\geqslant G_n$ such that G_{i+1} is a normal subgroup in G_i with G_i/G_{i+1} a finite solvable group and such that G_n is either a free group, or a surface group.

We first assert that G_n contains a subgroup H_1 of finite index such that it is normal in G_{n-2} and such that G_{n-2}/H_1 is solvable. The verification follows from the observation that

G_{n-1} contains only a finite number of G_{n-2} conjugates of G_n; furthermore, each such conjugate is a normal subgroup in G_{n-1} with factor group isomorphic to the solvable group G_{n-1}/G_n. Let H_1 be the intersection of these finite number of G_{n-2} conjugates of G_n. H_1 is then a normal subgroup of finite index in G_{n-2}. The factor group G_{n-1}/H_1 is isomorphic to a subgroup of the direct product of $G_{n-1}/\sigma(G_n)$, where $\sigma(G_n)$ ranges over the finite number of G_{n-2} conjugates of G_n in G_{n-1}. It is now clear that G_{n-2}/H_1 is a finite solvable group. Repeating this argument a finite number of times we then obtain a torsion-free normal subgroup H of finite index in G with G/H a solvable group. H is either a free group or a surface group. The first assertion of (c) now follows from (A6) and the well-known fact that a free group is residually finite and solvable, see [20] and [24].

We next observe that the negativity of the curvature of G implies the negativity of the curvature of H. Consequently, H is either a surface group with genus $g>1$ or a free group of rank $g>1$. By setting the b_j's equal to 1 in a surface group of genus g we see that such a group has a free group of rank g as a factor group. It follows that the subgroup H always has a free factor group F of rank $g>1$. If we use (A4) and replace H by its subgroup generated by its commutators and nth powers with n large, then g can be made larger than any pre-assigned integer. Consequently, the free factor group F can be mapped surjectively onto a finite solvable group with a pre-assigned solvable length N. The procedure of the preceding paragraph can be repeated once more to produce a normal subgroup S contained in H so that G/S is a finite solvable group of solvable length at least N. This gives us the last assertion of (c), q.e.d.

Special cases of the preceding theorem had been known, see (A6), [24; pp. 414–419] and [18; p. 254].

We observe that the argument presented at the end of the proof in the preceding theorem shows that a group with signature has torsion-free normal subgroups of finite index whose factor group can be made to possess any pre-assigned finite simple group as a composition factor. The most one could expect is a classification of some of the maximal torsion-free normal subgroups of finite index. As an illustration, we will describe the possible homomorphic images of groups G with finite signature $\{l, m, n \mid 0\}$ and negative curvature in the group PSL $(2, K)$. We will estimate the number of distinct torsion-free normal subgroups of G with factor groups isomorphic to PSL $(2, M)$ or PGL $(2, M)$ for suitable finite fields M.

Let M be a finite field with p^f elements. The subgroups of PSL $(2, M)$ had been determined by Dickson [5; pp. 285–286]. They are of the following types: (A) groups with positive curvature; (B) subgroups of the upper triangular group; (C) PGL $(2, p^a)$, $2a \mid f$, $p>2$; and (D) PSL $(2, p^b)$, $b \mid f$.

Let σ be a non-degenerate homomorphism from $G=G\{l, m, n|0\}$ to PSL $(2, K)$, where G is assumed to have negative curvature and K is assumed to be algebraically closed and to have characteristic $p\geqslant 0$. It is clear that σ can be parametrized by an element (R, S, T) in $E(r, s, t)$ satisfying the following restrictions:

(1) $p=2$. $(r, s, t)=(l, m, n)$.

(2) $p\neq 2$, all l, m, n are odd. $(r, s, t)=(l, m, n)$ or $(2l, 2m, 2n)$.

(3) $p\neq 2$, not all l, m, n are odd. $(r, s, t)=(2l, 2m, 2n)$.

Proposition 1.2 shows that $E(r, s, t)$ in the above list is non-empty if and only if none of the periods l, m, n is a proper multiple of the characteristic p. It is clear that each SL $(2, K)$ orbit in $E(r, s, t)$ give rise to a single equivalence class of homomorphisms. Suppose that (R_i, S_i, T_i), $i=1, 2$, parametrize equivalent homomorphisms. Conjugating the triples by elements of SL $(2, K)$ allows us to assume that the triples differ by at most a factor of $\pm I$ in each of the three entries. It is clear that the factors are all equal to $+I$ when we are in cases (1) and (2). If we are in case (3), then there can be only an even number of factors $-I$'s entered in the entries corresponding to even periods of G. These alterations of signs must change the trace signature, because the curvature is negative. If $(l, m, n)=(p, p, p)$, p must be greater than 3. The corollary to Proposition 1.2 together with Proposition 1.4 imply that G has $p-2$, 1, 1 torsion-free normal subgroups with factor groups isomorphic to C_p, $C_p\times C_p$, PSL $(2, p)$ respectively, where C_p denotes a cyclic group of order p. If $(l, m, n)\neq(p, p, p)$, we may assume that $r>2$ and $p\nmid r$. With the exception of the singular cases described in Proposition 1.3, the discussion preceding Proposition 1.3 shows that each trace signature corresponds to a single SL $(2, K)$ orbit. We can deduce from the proof of Proposition 1.3 that the singular cases lead to homomorphisms of G into one of the two triangular subgroups of PSL $(2, K)$. If p does not divide any of the periods, then we can map G onto the diagonal subgroup via the triangular groups. This gives us a non-degenerate homomorphism from G onto a cyclic group. If p does divide some of the periods, then it divides exactly one such. The other two periods must then be equal. Now consider the non-singular cases. We can conclude from Proposition 1.3 and Dickson's classification that the image of G in PSL $(2, K)$, $p>0$, is either the alternating group of degree 5, or a group of type (C) or (D). Using the corollary and the proof of Proposition 1.2, it is easy to see that there is a unique torsion-free normal subgroup in G with factor group isomorphic to the alternating group when and only when the signature of G satisfies the restrictions of the corollary of Proposition 1.2. Suppose that the image of G is of type (C) or (D). We can then conclude from Proposition 1.3 that the image is either PSL $(2, M)$ or PGL $(2, L)$, where $M=K(r, s, t)$ and L is the unique subfield of M (when it exists) such that $[M:L]=2$. Thus the image must be PSL $(2, M)$ when M has odd degree f over K_p,

or when $p=2$. When $p>2$, PSL $(2, L)$ has index 2 in PGL $(2, L)$. Consequently, the image is again PSL $(2, M)$ when at least two of the periods of G are odd. We next observe that two homomorphisms with the same image and the same kernel must differ by an automorphism of the image. The automorphism groups of PSL $(2, M)$ and PGL $(2, L)$ are generated by conjugating with elements of PSL $(2, K)$ and by Galois automorphisms of M applied to the coefficients. Since the field $M=K(r, s, t)$ is generated by any of the trace signatures, the Galois group of M over K_p must act freely on the set of trace signatures. As a result, when f is odd, or when at least two of the periods of G are odd, or when $p=2$, the action of the Galois group and the action of changing signs must be independent on the trace signatures. Finally, suppose that these actions are not independent. The Galois group must have even order $f=2a$. The characteristic p must be odd. Let ϱ be the element of order 2 in the Galois group. We may assume: l, m are even and $\varrho(\mu_{2l}, \mu_{2m}, \mu_{2n})=(-\mu_{2l}, -\mu_{2m}, \mu_{2n})$. Modifying ϱ by a suitable inner automorphism we can then assume that ϱ carries the triple $(R, S, T)\in E(\mu_{2l}, \mu_{2m}, \mu_{2n})$ onto the triple $(-R, -S, T)\in E(-\mu_{2l}, -\mu_{2m}, \mu_{2n})$. It is now clear that PGp (R, S, T) is fixed by ϱ. It is easy to see that the fixed points of ϱ on PSL $(2, p^{2a})$ is conjugate to PGL $(2, p^a)$. We have assumed that the group PGp (R, S, T) is of type (C) or (D). It follows from Proposition 1.3 that PGp (R, S, T) must be isomorphic to PGL $(2, p^a)$. We observe that l, m even and p odd imply l and m are prime to p. $\varrho(\mu_{2l})=-\mu_{2l}$ if and only if $\varrho(\zeta_{2l})=-\zeta_{2l}$ or $-\zeta_{2l}^{-1}$. Since ϱ corresponds to raising to the p^ath power, and since ζ_{2l} is a primitive $2l$th root of 1, the equation is a congruence condition on $2l$. It is therefore clear that Galois action and the sign changing action are dependent if and only if (p, l, m, n) satisfy certain congruence conditions. The image is PSL$(2, p^f)$ if and only if the two actions are independent. Otherwise, the image is PGL $(2, p^{f/2})$. We now summarize our discussion into the following assertion:

THEOREM 1.6. *Let G be a group with finite signature $\{l, m, n|0\}$ and negative curvature. Let K be an algebraically closed field of characteristic $p>0$ so that none of the periods of G is a proper multiple of p. Let $M=K(2l, 2m, 2n)$ have degree f over K_p. Let u be the number of periods prime to p. Let v be the number of even periods. For each integer i let $\varphi_0(i)=\varphi(i_0)$, where φ is the Euler function, i_0 is the largest divisor of i which is not divisible by p. Let f_0 be equal to f unless $p>2$, f is even and $p^{f/2}$-power map alters the sign in precisely two of the three entries of $(\mu_{2l}, \mu_{2m}, \mu_{2n})$ (if one entry is zero, then the requirement is automatically satisfied); in the exceptional case let $f_0=f/2$.*

(a) *Every non-degenerate homomorphic image of G in* PSL $(2, K)$ *is a finite group.*

(b) *Except when $(p, l, m, n)=(3, 3, 3, 5)$, there exists at least* 1 *and at most $\varphi_0(2l)\varphi_0(2m)\varphi_0(2n)/2^{u+v-1}f_0$ distinct torsion-free normal subgroups S in G with G/S iso-*

morphic to PSL $(2, p^f)$ *when* $f=f_0$ *and to* PGL $(2, p^{f/2})$ *when* $f\neq f_0$. *In the exceptional case, the non-degenerate images of* G *in* PSL $(2, K)$ *are either solvable or isomorphic to* PSL $(2, 5)$.

(c) *Suppose* $(l, m, n)=(p, p, p)$ *and* C_p *is the cyclic group of order* p. G *has exactly* $p-2, 1, 1$ *torsion-free normal subgroups* S *with* G/S *isomorphic to* C_p, $C_p\times C_p$, PSL $(2, p)$ *respectively. These are the only types of non-degenerate images of* G *in* PSL $(2, K)$.

(d) *Suppose* $(p, l, m, n)\neq(3, 3, 3, 5)$ *or* (p, l, l, p) *or* (p, p, p, p). *The non-degenerate homomorphic images of* G *in* PSL $(2, K)$ *are of the following types:*

(1) *cyclic groups of order equal to the* l.c.m. *of the periods. These exist if and only if* G' *is torsion-free and not all periods are exactly divisible by* 2.

(2) PSL$(2, p^f)$. *These exist if and only if* $f=f_0$.

(3) PGL$(2, p^{f/2})$. *These exist if and only if* $f\neq f_0$.

The upper bound of (b) *is attained if and only if* (1) *does not occur.*

Proof. (a) follows from Propositions 1.2 and 1.3. We observe that the total number of trace signatures $(\mu_{2l}, \mu_{2m}, \mu_{2n})$ is given by $\varphi_0(2l)\varphi_0(2m)\varphi_0(2n)/2^u$. The remaining factors in (b) take into account of the sign-change action and the Galois action. We note also that the assumption of the negativity of the curvature of G forces two of the three entries of a trace signature to be non-zero and distinct from their negatives when $p>2$. The remaining assertions follow quickly from our discussion.

PROPOSITION 1.7. *Let* G *be a group with finite signature* $\{l, m, n\,|\,0\}$ *and negative curvature. Then,*

(a) G *is isomorphic to a unique (up to conjugates) discontinuous subgroup of* PSL $(2, \mathcal{R})$.

(b) *If the periods of* G *are pairwise coprime, then every non-degenerate homomorphism from* G *to* PSL $(2, \mathbb{C})$ *is injective.*

Proof. (a) follows easily from the fact that a fundamental domain of a triangular group $G\{l, m, n\,|\,0\}$ acting discontinuously on the upper half plane $\mathcal{H}$ is essentially uniquely determined. For a detailed discussion of fundamental domains in the general situation we refer to [16] and [17].

(b) follows easily from the observation that the Galois group of $\mathbb{Q}(\zeta_{2l}, \zeta_{2m}, \zeta_{2n})$ over $\mathbb{Q}$ acts transitively on the trace signatures $(\mu_{2l}, \mu_{2m}, \mu_{2n})$ so that we can adapt the discussion preceding Theorem 1.6, q.e.d.

PROPOSITION 1.8. *Let* G *be an abstract group. Let* G_i, $0\leqslant i\leqslant n$, *be distinct normal subgroups of finite index in* G *such that:*

(1) G/G_0 *is solvable,*

(2) G/G_i, $1 \leqslant i \leqslant n$, *is non-abelian and simple, then* $G/\bigcap G_i$ *is isomorphic to the direct product of* G/G_i, $0 \leqslant i \leqslant n$.

The proof follows easily from using induction and the theorem of Krull–Remak–Schmidt.

We can now couple Proposition 1.8 and Theorem 1.6 to produce a doubly infinite family of torsion-free normal subgroups of finite index in $G\{l, m, n|0\}$.

2. Applications to Riemann surfaces

We now describe the geometric interpretation of the results in the preceding section. Let S be a compact Riemann surface. We can view S as the quotient space $\pi_1(S)\backslash\mathcal{M}$, where the fundamental group $\pi_1(S)$ acts discontinuously and freely on the universal covering surface $\mathcal{M}$ of S. The isomorphism class of S stands in bijective correspondence with the conjugate class of $\pi_1(S)$ as embedded in $A_{co}(\mathcal{M})$, we refer to the notations of the appendix.

The procedure can be reversed and generalized. Let Γ be a discontinuous subgroup of $A_{is}(\mathcal{M})$ having a fundamental domain with finite invariant area. Then Γ is a group with signature. Let $\mathcal{F}(\Gamma)$ be the field of all functions meromorphic on $\mathcal{M}$ which are automorphic with respect to Γ, $\mathcal{F}(\Gamma)$ may then be viewed as the field of all meromorphic functions on the quotient space $\Gamma\backslash\mathcal{M}$. The assumption that there is a fundamental domain with finite area allows us to conclude that $\Gamma\backslash\mathcal{M}$ is a compact Riemann surface with a finite number of points removed, one for each parabolic generator of Γ. As a result, $\mathcal{F}(\Gamma)$ is an algebraic function field (of one variable) over the constant field of complex numbers $\mathbf{C}$. The associated Riemann surface is the compactification of $\Gamma\backslash\mathcal{M}$ in a natural way.

Let G be a fixed discontinuous subgroup of $A_{is}(\mathcal{M})$ having a finite signature $\{e(1), \ldots, e(m)|\gamma\}$ and compatible curvature. Let S be any torsion-free normal subgroup of finite index in G. $\mathcal{F}(S)$ is then a finite Galois extension field of $\mathcal{F}(G)$ with Galois group G/S. Assuming that we are in the non-trivial situation where $\mathcal{M}$ has non-positive curvature, each of the elliptic generators x_i of G then has a unique fixed point on $\mathcal{M}$. Let its projection on $G\backslash\mathcal{M}$ be denoted by $\mathfrak{p}_i$. The surface $S\backslash\mathcal{M}$ may then be viewed as a branched regular covering surface of $G\backslash\mathcal{M}$. The ramification occurs precisely over the m places $\mathfrak{p}_i$. We may select a place $\mathfrak{P}_i$ on $S\backslash\mathcal{M}$ lying above $\mathfrak{p}_i$ so that the decomposition group of $\mathfrak{P}_i$ in the Galois group G/S is the cyclic group of order $e(i)$ generated by x_iS. In the extension field $\mathcal{F}(S)$ the divisor $\mathfrak{p}_i$ decomposes into the divisor $\prod \sigma(\mathfrak{P}_i)^{e(i)}$, where σ ranges over a complete set of representatives of G/S with respect to the cyclic subgroup generated by x_iS. When G is torsion-free, we have an unramified regular covering surface. Conversely, when G is torsion-free, then

every regular unramified covering surface can be obtained in the manner described. In general, if we shrink S and pass to the limit, then we obtain an extension field of $\mathfrak{F}(G)$ which is Galois over $\mathfrak{F}(G)$ and which may be viewed as "maximal" with respect to the property of being ramified over $\mathfrak{p}_i$ with prescribed ramification indices $e(i)$, $1 \leqslant i \leqslant m$. In view of Theorem 1.5, the Galois group of this infinite extension field is in a natural way the pro-finite completion of G (completion with respect to the topology defined by all the subgroups of finite index).

Suppose we are given a compact Riemann surface $\mathcal{S}$ with genus $g > 1$. Its fundamental group can then be taken as a suitable discontinuous subgroup S of PSL(2, $\mathfrak{R}$) having signature $\{-|g\}$. The conformal automorphism group $A_{co}(\mathcal{S})$ of $\mathcal{S}$ is then isomorphic to G/S, where G is the normalizer $N(S)$ in PSL(2, $\mathfrak{R}$). The following result was obtained by H. A Schwarz:

PROPOSITION 2.1. *In the preceding notation, $A_{co}(\mathcal{S})$ is finite.*

The result was later generalized to algebraic function fields by H. L. Schmidt [29], Iwasawa–Tamagawa [12] and Rosenlicht [27]. In the classical situation Hurwitz strengthened Proposition 2.1. His analysis was based on the formula of (A4). It is easy to extract from his work [11; pp. 410–412] the following assertion:

PROPOSITION 2.2. *In the preceding notation, we have:*

(a) *$A_{co}(\mathcal{S}) = G/S$ is a finite group of order at most $84(g-1)$. The maximum is attained if and only if $G = N(S)$ has signature $\{2, 3, 7|0\}$.*

(b) *If $A_{co}(\mathcal{S})$ has order less than $84(g-1)$, then its order is at most $48(g-1)$. This second maximum is attained if and only if $G = N(S)$ has signature $\{2, 3, 8|0\}$.*

In general, if we specify the signature of G, then every torsion-free normal subgroup S of finite index will give rise to a Riemann surface $\mathcal{S}$ such that $A_{co}(\mathcal{S})$ has order at least equal to the order of G/S. When G has signature $\{2, 3, 7|0$ or $\{2, 3, 8|0\}$ we can deduce from Proposition 2.2 that $A_{co}(\mathcal{S})$ is equal to G/S. Proposition 2.2 shows that the problem of finding compact Riemann surfaces of genus $g > 1$ with conformal automorphism groups of order $84(g-1)$ and $48(g-1)$ is equivalent with the problem of finding torsion-free normal subgroups of finite index in $G\{2, 3, 7|0\}$ and $G\{2, 3, 8|0\}$ respectively. If S is such a subgroup, then every subgroup T of finite index in S and normal in G is again such a subgroup. $T\backslash\mathcal{H}$ is then a regular unramified covering surface of $\mathcal{S} = S\backslash\mathcal{H}$. The general algebraic problem breaks up naturally:

(A) Let G be a group with signature. What are the normal subgroups of finite index which are maximal with respect to the property of being torsion-free?

(B) Let S be a subgroup of type (A). What is the action of G on the normal subgroups

(of finite index) in S? Suppose that T is a normal subgroup of S normalized by G, what is the action of G on S/T?

Theorem 1.5 and its proof shows that we should not expect to find complete answers to either of the two algebraic problems. We will now describe another procedure that can be used in the study of problem (A).

Suppose the group G has the finite signature $\{l, m, n|0\}$. Suppose further that we are given the character table of the finite group H. Then there is a simple procedure to determine the existence of non-degenerate homomorphisms from G to H.

PROPOSITION 2.3. *Let x, y and z be random elements of the finite group H. Let $c(h)$ denote the order of the centralizer of the element h in H. Let $\lambda(x, y; z)$ be the number of solutions of the equation $uvz=1$, where u and v range over the conjugates of x and y in H respectively. Then:*

$$\lambda(x, y; z) = |H|c(x)^{-1}c(y)^{-1}\sum \chi(x)\chi(y)\chi(z)\chi(1)^{-1},$$

where χ ranges over the distinct irreducible complex characters of H.

We observe that $\lambda(1, z; z^{-1})=1$. This allows us to calculate $c(z)$. Consequently, the formula is completely determined by the character table of H. The verification of the formula is a simple application of the orthogonality relations among the characters, see [9, p. 128]. When x, y and z have orders l, m, n respectively, then $\lambda(x, y; z)\neq 0$ if and only if there exists a non-degenerate homomorphism from G to H sending x_1, x_2, x_3 onto u, v, z respectively. The kernel of this non-degenerate homomorphism is then a torsion-free normal subgroup of finite index; its factor group is isomorphic to the subgroup T of H generated by u, v, and z. The most difficult part of this procedure lies in the determination of T.

The character table of PSL(2, M), M a finite field, had been determined by Jordan [15]. An alternative approach to the results of section 1 could be based on the procedure just described. The main point of section 1 is that M can be prescribed in advance and that the image can be determined in most of the cases. Indeed, M is the field generated by the traces of the elliptic generators of G. This should be compared with the following assertion:

PROPOSITION 2.4. *Let σ: $\mathcal{G}\to$GL(d, K) be an irreducible representation of the finite group $\mathcal{G}$ in an algebraically closed field K of characteristic $p>0$. σ is then equivalent to a representation in* GL(d, M), *where M is the finite field generated by the traces of $\sigma(g)$, $g\in\mathcal{G}$,* [2; *p.* 101].

Suppose that $d>2$ and that we wish to determine the non-degenerate homomorphic images of $G\{l, m, n|0\}$ in GL(d, K) or one of its associated groups. The preceding result tells us that the finite images can be found in GL(d, M) for suitable finite fields M. In general, as we shall see, there is no bound on M.

The procedure following Proposition 2.3 can, in theory, be applied to groups with signature $\{e(1), ..., e(m)|0\}$, $m>3$. We simply introduce additional generators, y_3, ... and additional relations $x_1x_2=y_3$, $y_3x_3=y_4$, ..., $y_{m-1}x_{m-1}x_m=1$. y_3, ..., y_{m-1} can now be viewed as parameters. The formula of Proposition 2.4 can be expanded into a system parametrized by the orders of y_j.

Before we illustrate the procedure described following Proposition 2.3, we will show that the results of section 1 actually furnish complete answers to problem (A) in a number of cases.

PROPOSITION 2.5. *Let S be a compact Riemann surface with even genus $g>1$. Suppose that $A_{co}(S)$ has order $84(g-1)$ and that the fundamental group of S corresponds to the normal surface subgroup S of finite index in $G=G\{2, 3, 7|0\}$. Let G_0/S be the largest solvable normal subgroup of G/S.*

(a) *G_0/S must have odd order.*

(b) *G/G_0 is isomorphic to* PSL$(2, p^f)$ *for a uniquely determined prime $p\equiv\pm 3$* mod 8, *where $f=1$ or 3 according to p is or is not congruent to ± 1* mod 7.

(c) *The genus g of S must have the form $1+\{(2k+1)p^f(p^{2f}-1)/168\}$. In particular, $g\geqslant 14$ and equality is obtained for 3 non-isomorphic surfaces with automorphism group* PSL(2, 13). *When $g>14$, then it must be at least* 118. *This value is attained for a unique Riemann surface corresponding to the one found by Lehner–Newman* [19]; *its automorphism group is* PSL$(2, 3^3)$.

Proof. Let T/S be a maximal normal subgroup of G/S. The fact that the periods of G are distinct primes shows that T is a maximal normal subgroup of G and that T is torsion-free. Thus G/T is a non-abelian finite simple group. The theorem of Feit–Thompson and Burnside's transfer theorem in finite group theory imply that the 2-Sylow subgroup of G/T must be the direct product of two cyclic groups of order 2 and that T/S must be a solvable normal subgroup of odd order. It follows that $T=G_0$. (b) now follows from Theorem 1.6 together with Gorenstein–Walter's classification theorem of finite simple groups with dihedral 2-Sylow subgroups. The first two assertions of (c) follow quickly from (b). In order to show that the genus cannot fall between 14 and 118 we must show that when $p=13$ and $2k+1>1$, then $2k+1\geqslant 9$. If $1<2k+1<9$, then G/S must be a central extension of the cyclic group T/S of order 3, 5 or 7 by PSL(2, 13). The 2-dimensional cohomology groups of PSL$(2, q)$ with Q/Z coefficients has been calculated by I. Schur. Our extension must split so that G/S is not perfect. This is a contradiction, q.e.d.

The results of Feit–Thompson, Gorenstein–Walter are both very deep. For a sketch of these results as well as other results on finite groups we refer to [9].

The results of section 1 show that the genus of a Riemann surface S with maximal automorphism group can be congruent to 1 modulo an arbitrarily high power of 2. We will now illustrate the procedure following Proposition 2.3 by considering the case when the genus g is congruent to 3 mod 4.

PROPOSITION 2.6. *Let S be a normal subgroup of finite index in $G=G\{2, 3, 7|0\}$. Suppose that S is a surface group of genus g with $g\equiv 3 \bmod 4$. Let G_0/S be the largest solvable normal subgroup of G/S.*

(a) *G_0/S must have odd order.*

(b) *G/G_0 is a non-abelian simple group isomorphic to one of the following groups;*

(1) PSL(2, 8)

(2) PSL(2, p^f), $p\equiv 7$ *or* 9 mod 16 *and* $f=1$ *or* 3.

(3) *The Janko group J of order* $2^3\cdot 3\cdot 5\cdot 7\cdot 11\cdot 19=175\,560$.

(4) *A Ree group* $G_2^*(q)$, $q=3^{2n+1}$, $n>0$, *or a group of Ree type, of order* $q^3(q^3+1)(q-1)$.

Proof. We know that G/S is a perfect finite group whose order is divisible by 8 but not by 16. Let G_0/S be the largest normal subgroup of odd order in G/S. We need to verify (b). As before, we know that G_0 is a surface subgroup. We may therefore replace S by G_0 and and assume that G/S has no non-trivial normal subgroup of odd order. Using again Burnside's theorem and the fact that G/S is perfect, we can conclude that the 2-Sylow subgroup of G/S has to be either a dihedral group of order 8, a quaternion group of order 8, or a direct product of three cyclic groups of order two. In the first case, the classification theorem of Gorenstein–Walter [9; p. 462] shows that G/S must be a simple group of type described in (2), or be isomorphic to the alternating group of degree 7. It is easy to show that G cannot be mapped surjectively onto the alternating group of degree 7, see remark [21; p. 75]. In the second case, a theorem of Brauer–Suzuki [3; p. 1759] asserts that the center of G/S contains the only element of order 2. The images of the generators of order 3 and 7 must then commute with the image of the generator of order 2 in G/S. This forces G/S to be the trivial group, a contradiction.

Assume finally that G/S has a 2-Sylow subgroup which is the direct product of three cyclic groups of order 2. Burnside's transfer theorem together with the three hypotheses: G/S is perfect, G/S has no non-trivial normal subgroups of odd order, and G/S has an abelian 2-Sylow subgroup of order 8, imply quickly that G/S must be a non-abelian simple group; moreover, all elements of order 2 in G/S are conjugate. Let $C(\tau)$ denote the centralizer of an element of order 2 in G/S. If $C(\tau)$ is solvable, then a theorem of Gorenstein [9; p. 484] shows that G/S must be PSL(2, 8). If $C(\tau)$ is not solvable, then Walter (in results to be published) has shown that G/S must be of the type (3) or (4), q.e.d.

Results of section 1 show that groups of type (1) and (2) definitely can appear. Indeed, a Riemann surface discovered by Klein of genus 3 corresponds to the case $p=7$; its automorphism group is PSL(2, 7). Our result confirms its uniqueness. Similarly, the case $p=2$ leads to a unique normal subgroup with factor group PSL(2, 8). This corresponds to a unique Riemann surface of genus 7. It is the surface discovered by Macbeath [23].

The Janko group was described in detail in [13]. This fills a gap in [28], for details see [8]. Groups of Ree type were studied in detail by Janko–Thompson [14] and Ward [30]. In particular, with the exception of a few entries (of no importance for our purposes), Ward had determined the character tables of groups of Ree type. It is conjectured that the Ree groups $G_2^*(q)$, $q=3^{2n+1}$, $n>0$, [26], are the only groups of Ree type; a discussion of the works done in this direction can be found in [9; p. 480].

PROPOSITION 2.7. *Let G be a group with signature $\{2, 3, 7|0\}$.*

(a) *G has 7 distinct normal subgroups with factor group isomorphic to the Janko group.*

(b) *Let p be a prime greater than 3. Let $q=3^p$ and $m=3^{(p-1)/2}$. There are at least $(q-3m)/p$ distinct torsion-free normal subgroups of G with factor group isomorphic to the Ree group $G_2^*(q)$ of order $q^3(q^3+1)(q-1)$.*

Proof. (a) Janko's group has unique conjugate classes of elements of order 2, 3, 7. Its only perfect proper subgroups are isomorphic to PSL(2, 5) or PSL(2, 11). Janko's character table gives $\lambda(2, 3; 7)=49$, where we have replaced an element by its order. We obtain therefore 49 surjective homomorphisms from G to the Janko group. The image of the elliptic generator of order 7 is a fixed element z of order 7. It is known that $c(z)=7$ and that the Janko group has only inner automorphisms. As a result, the 49 surjective homomorphisms distribute themselves into 7 equivalence classes with respect to the centralizer of z. Assertion (a) now follows.

(b) Let $G(q)$ be the Ree group $G_2^*(q)$ of order $q^3(q^3+1)(q-1)$. It has only one conjugate class of elements of order 2. A representative is denoted by J in Ward's table [30; p. 88]. It is easy to see that 7 must divide one of the two coprime factors of $q^2-q+1=(q+3m+1)(q-3m+1)$. These elements are labelled as W and V respectively. $c(W)$ and $c(V)$ are respectively $q+3m+1$ and $q-3m+1$. There are 3 conjugate classes of elements of order 3. Their representatives are labelled T, T^{-1} and X. In particular, T and T^{-1} are not conjugate in $G(q)$. The automorphism group of $G(q)$ is generated by the inner automorphisms together with Galois automorphisms. Since the Galois group must have odd order, it is clear that T and T^{-1} are not conjugate with respect to the automorphism group of $G(q)$. Furthermore, $c(T)=2q^2$ and $c(J)=q(q^2-1)$; it is clear that 7 does not divide $q(q^2-1)$. It is now easy to

show that $\lambda(T, 7(\pm); J)=\lambda(T^{-1}, 7(\pm); J)=q(q^2-1)(q\mp 3m)/2$, where $7(\pm)$ denotes W or V, an element of order 7.

We must now determine the image of $G\{2, 3, 7\,|\,0\}$ corresponding to each of the homomorphisms. Let the image be denoted by H. H must be a perfect subgroup of $G(q)$. Let H_0 be the largest solvable normal subgroup of H. We know that the 2-Sylow subgroup of H must be of order 4 or 8. According to Propositions 2.5 and 2.6, H_0 must have odd order. According to a result of Janko–Thompson [14; Lemma 7.7] $H_0=1$. This shows that H is a simple group. By our choice H contains an element T of order 3 which is not conjugate to T^{-1} (even in $G(q)$). In the finite group PSL(2, M), M a finite field of characteristic not 3, an element of order 3 is always conjugate to its inverse. The same assertion goes for the Janko group. Thus H must either be of Ree type or be isomorphic to PSL(2, 3^u), u an odd integer greater than 1. Suppose that H is isomorphic to PSL(2, 3^u). In $G(q)$, distinct 3-Sylow subgroups have only the identity element in common. Moreover, the normalizer of a 3-Sylow subgroup has order $q^3(q-1)$. The normalizer of a 3-Sylow subgroup of H having order $3^u(3^u-1)/2$ must be contained in the normalizer of a 3-Sylow subgroup of $G(q)$. Thus $(3^u-1)\,|\,2(3^p-1)$. Since u is odd, 3^u-1 is not divisible by 4. Thus $(3^u-1)\,|\,(3^p-1)$ so that $\mathrm{GF}(3^u)\subset\mathrm{GF}(3^p)$ and $u\,|\,p$. Since p is a prime and $u>1$, we have $u=p$. Now, 7 must divide the order of H. This means $7\,|\,(q^2-1)$ or $7\,|\,(3^{2p}-1)$. We must then have $3\,|\,p$ or $3=p$. This contradicts the choice of p. Thus we can conclude that H must be a group of Ree type. This means that the centralizer in H of an element τ of order 2 must be the direct product of $\langle\tau\rangle$ with PSL(2, q'), a suitable simple subgroup of PSL(2, q). Since $q=3^p$, p an odd prime, Dickson's classification theorem shows that $q'=q$. Ward had shown that a group of Ree type must have order $q^3(q^3+1)(q-1)$, where q is the power of 3 determined by $c(\tau)=q(q^2-1)$. Thus H must be all of $G(q)$, and all of our homomorphisms are surjective.

The centralizer of J does not contain an element of order 7. The field automorphisms of $G(q)$ can be chosen to fix J; as before, they do not carry T onto T^{-1} so that the class of T and T^{-1} must be fixed by the field automorphisms. It is now clear that we must have at least $(q-3m)/p$ inequivalent (under the group of automorphisms of $G(q)$) surjective homomorphisms from $G\{2, 3, 7\,|\,0\}$ to $G(q)$. Consequently, these homomorphisms must have distinct kernels, q.e.d.

We observe that it is possible that additional surjective homomorphisms may exist by using the element X in place of T or T^{-1}. The problem of finding the image will be more tedious. In the present situation, we have exploited the fact that T and T^{-1} are not conjugate in $G(q)$. The Ree groups are isomorphic to groups of 7×7 matrices over an algebraically closed field K of characteristic 3. We have therefore proved the following assertion:

COROLLARY. *Let G be a group with signature $\{2, 3, 7|0\}$.*

(a) *There exist infinite number of inequivalent homomorphisms from G to* GL(7, K), *K an algebraically closed field of characteristic* 3.

(b) *The number $f(G, H)$ of distinct normal subgroups of G with factor group isomorphic to the simple finite group H is unbounded as a function of H.*

It is well known a group with signature $\{2, 3, \infty|0\}$ is isomorphic to the modular group PSL(2, $\mathfrak{Z}$). $G\{2, 3, 7|0\}$ is a homomorphic image of PSL(2, $\mathfrak{Z}$) so that any subgroup of finite index of $G\{2, 3, 7|0\}$ is the image of a subgroup of finite index in PSL(2, $\mathfrak{Z}$). One could raise the question "Is it true that all subgroups of finite index in $G\{2, 3, 7|0\}$ are images of the congruence subgroups of PSL(2, $\mathfrak{Z}$)?" The answer to such a question is in the negative. Indeed, factor groups of the congruence subgroups of PSL(2, $\mathfrak{Z}$) must be the extension of a solvable finite group by the direct product of PSL(2, p) with p ranging over a finite set of primes. It is immediate that the normal subgroups of the type described in Proposition 2.8 could not be the image of a congruence subgroup. Our remark is quite general. In fact, let V be a normal subgroup of the subgroup U in GL(d, D), where D is the ring of integers of an algebraic number field. A subgroup T between U and V is called a congruence subgroup if it contains the intersection of U with the kernel of the reduction homomorphism from GL(d, D) to GL(d, D/I), where I is a suitable non-zero ideal of D. If U/V is a group with signature having negative curvature, then U has subgroups T of finite index in U and T/V torsion-free such that T is not a congruence subgroup. This can be seen most easily from the proof of Theorem 1.5. Any group G with signature having negative curvature contains normal subgroups S such that G/S is a finite group which involves a symmetric group of arbitrarily pre-assigned degree. S can be taken to be torsion-free. On the other hand, GL(d, D/I) is the extension of a solvable finite group by the direct product of a finite number of GL(n, p^t), where t is bounded by a constant C depending only on D. It is then easy to see that the symmetric group of degree 2^N, $N > Cd(d+1)$, is not isomorphic to any subgroup of GL(d, p^t) for any prime p. Consequently, a composition factor of G/S cannot occur as a composition factor associated to a congruence subgroup. Our observation apparently had already been noted by Shafarevitch during the Moscow congress.

3. Action of $A_{\infty}(S)$ on the homology groups of S

We now turn our attention to the problem (B) described at the beginning of the preceding section. Again, Theorem 1.5 shows that we should restrict to situations which arise naturally from the geometric context.

3 – 692907 *Acta mathematica*. 123. Imprimé le 10 Septembre 1969.

Let S be a compact Riemann surface of genus $g>0$. Let $\mathcal{G}$ be a finite subgroup of $A_{co}(S)$. $\mathcal{G}$ then induces a group of ring automorphisms on the chohomology ring $H^*(S)$, where, unless specified otherwise, the coefficient is taken to be $\mathbb{Z}$. Duality theory allows us to identify $H^*(S)$ with the homology ring $H_*(S)$, where cup-product corresponds to the intersection-product. We know that $H^i(S)$ is a free abelian group of non-zero rank 1, $2g$, 1 only when $i=0$, 1, 2. Moreover, $H^1(S)\cong H_1(S)$ are isomorphic to the commutator quotient group S/S' of the fundamental group S of S. The cup-product provides us with a symplectic form with determinant 1 on $H^1(S)$. The universal coefficient theorem allows us to identify $H^*(S, C)$ with $C\otimes H^*(S)$. $H^i(S, C)$ then provides a complex representation of $\mathcal{G}$ with associated character denoted by ϱ_i. Of course, ϱ_i is also the trace function defined on $\mathcal{G}$ by $H^i(S)$ so that ϱ_i is an integer-valued function on $\mathcal{G}$. It is clear that $\varrho_0=\varrho_2=1$, the trivial character on $\mathcal{G}$ (recall that $\mathcal{G}$ preserves orientation). De Rham's theorem allows us to decompose $H^1(S, C)$ into the direct sum of subspaces $H^{1,0}$ and $H^{0,1}$ corresponding to the spaces of holomorphic and anti-holomorphic differentials on S. It is clear that these two subspaces are stable under $\mathcal{G}$. Let the corresponding characters on $\mathcal{G}$ be denoted by $\varrho_{1,0}$ and $\varrho_{0,1}$; thus, we have $\varrho_1=\varrho_{1,0}+\varrho_{0,1}$. With respect to the cup-product $H^{1,0}$ and $H^{0,1}$ are both totally degenerate subspaces, see [10; § 5]. It is now immediate that the representation associated to $\varrho_{1,0}$ is the transpose-inverse of the representation associated to $\varrho_{0,1}$. Since $\mathcal{G}$ is a finite group, we know that $\varrho_{1,0}=\overline{\varrho_{0,1}}$ as complex-valued functions on $\mathcal{G}$. The Lefschetz fixed point theorem translates into the following assertion:

PROPOSITION 3.1. *The function $2-\varrho_1$ on $\mathcal{G}$ is such that:*

(a) $2-\varrho_1(1)=2-2g$.

(b) $2-\varrho_1(\sigma)$ *is the (algebraic) number of fixed points of $\sigma\neq 1$ acting on the compact Riemann surface S of genus g.*

Hurwitz [11; p. 416] proved that $A_{co}(S)$ acts faithfully on $H^{1,0}$ when $g>1$. We will use Proposition 3.1 to generalize this assertion. For this purpose, we represent S as $S\backslash\mathcal{M}$, where S is the fundamental group of S, and $\mathcal{M}$ is the universal covering surface of S. $\mathcal{G}$ can now be realized as G/S, where G is a suitable discontinuous subgroup of $A_{is}(\mathcal{M})$ having a finite signature $\{e(1), \ldots, e(m)\,|\,\gamma\}$. $\mathcal{G}=G/S$ is then the group of cover transformations associated to the regular, branched, covering surface S of $G\backslash\mathcal{M}$. The permutation action of $\mathcal{G}$ on points $\mathfrak{P}$ lying over $\mathfrak{p}$ is the permutation representation induced by the trivial representation of the decomposition group of $\mathfrak{P}$ in G/S. If we triangulate $G\backslash\mathcal{M}$ in such a way that all m ramified points $\mathfrak{p}_i$ are included among the vertices, then we can lift the triangulation into a triangulation of S. Relative to this triangulation, the action of $\mathcal{G}$ on S is simplicial. Consequently, the algebraic number of fixed points of $\sigma\neq 1$ in $\mathcal{G}$ on S is

equal to the actual number of fixed points. We now have the following generalization of the assertion of Hurwitz:

THEOREM 3.2. *In the preceding notation, assume* $g>0$.

(a) *The trivial representation of* $\mathcal{G}$ *occurs as a component of* $\varrho_{1,0}$ *exactly* γ *times.*

(b) $\gamma \leqslant g$ *and equality holds if and only if either* $\mathcal{G}=1$, *or* $g=1$ *and* $m=0$ (*no ramification*). *In particular, when* $g>1$, $\mathcal{G}$ *is faithful on* $H^{1,0}(S, C)$ *and on* $H^1(S)$.

Proof. As usual, we define the inner product between two complex-valued class functions χ and ψ on the finite group $\mathcal{G}$ by:

$$\langle \chi, \psi \rangle = |\mathcal{G}|^{-1} \sum \chi(\sigma) \overline{\psi(\sigma)},$$

where σ ranges over the elements of $\mathcal{G}$. If χ belongs to the character ring (consisting of all integral combinations of irreducible complex characters) of $\mathcal{G}$ and if χ is an irreducible character of $\mathcal{G}$, then the preceding product provides the multiplicity (or the Fourier coefficient) of ψ in the expansion of χ.

Let $\mathfrak{p}_i$, $1 \leqslant i \leqslant m$, be the points of $G\backslash\mathcal{M}$ ramified in S. The decomposition group (isotropy group) of $\mathfrak{P}_i$ over $\mathfrak{p}_i$ is the cyclic group of order $e(i)$ generated by $x_i S$ of G/S. The number of points lying over $\mathfrak{p}_i$ is $|\mathcal{G}|/e(i)$. It is clear that $|\mathcal{G}|\langle 2-\varrho_1, 1\rangle - (2-2g)$ is the total number of fixed points of the non-identity elements of $\mathcal{G}$. This is also equal to the total number of non-identity elements in the isotropy groups summed over all the points of S. This latter summation can be restricted to the branched points. We therefore have:

$$\langle 2-\varrho_1, 1\rangle = |\mathcal{G}|^{-1}\{2-2g+|\mathcal{G}| \sum (1-e(i)^{-1})\}.$$

The genus formula of (A5) in the appendix shows that the right side of the equation is $2-2\gamma$ so that $\langle \varrho_1, 1\rangle = 2\gamma$. (a) now follows from $\varrho_1 = \varrho_{1,0} + \overline{\varrho_{1,0}}$.

$\varrho_{1,0}$ is the character of a g-dimensional representation of $\mathcal{G}$. We can deduce from (a) that $\gamma \leqslant g$ and that equality holds if and only if $\varrho_{1,0}$ is the trivial representation repeated g times. Putting $g=\gamma$ in the genus formula of (A5), we have:

$$0 \geqslant (|\mathcal{G}|-1)(2-2g) = |\mathcal{G}| \sum (1-e(i)^{-1}) \geqslant 0.$$

First part of (b) now follows. The second part of (b) follows by considering the kernel of the representation $\varrho_{1,0}$ of Aut (S), q.e.d.

The Lefschetz fixed point formula provides us with the values of the character ϱ_1 on $\mathcal{G}$. If $\varrho_{1,0}$ were known to be real-valued, then we can extract the values of $\varrho_{1,0}$ from the values of ϱ_1 through division by 2. However, in general, $\varrho_{1,0}$ does not have to be real-valued. We can invoke the following consequence of the Atiyah–Bott fixed point formula [1; p. 12, Example 1].

PROPOSITION 3.3. *In the preceding notation, we have:*

(a) $1-\varrho_{1,0}(1)=1-g$,

(b) $1-\varrho_{1,0}(\sigma)=\sum(1-\sigma'(z))^{-1}$, *where* z *ranges over the set of fixed points of* σ *on* S *and* σ' *is the derivative of the holomorphic automorphism* $\sigma \neq 1$.

It is clear that the value $1-\varrho_{1,0}(\sigma)$ can be calculated in any particular case. For example, at the point $\mathfrak{P}_j$, $\sigma=x_jS$ corresponds to a rotation through an angle of $2\pi/e(j)$ so that $\sigma'(\mathfrak{P}_j)=\exp(2\pi i/e(j))$. We can deduce immediately the following assertion:

PROPOSITION 3.4. *In the preceding notation, we have:*

(a) $\varrho_{1,0}(xS)=1$ *when* xS *is not conjugate to any element of the form* $x_i^tS, 1\leqslant i\leqslant m, 1\leqslant t\leqslant e(i)$.

(b) $\varrho_{1,0}$ *is an integral-valued function on* $\mathcal{G}$ *if and only if* $\varrho_{1,0}(xS)$ *is real for all elliptic elements* x *in* G.

(c) *If* x_iS *and* $x_i^{-1}S$ *are conjugate in* G/S *for all* i, *then* $\varrho_{1,0}$ *is an integral-valued function on* $\mathcal{G}=G/S$.

We note further that the calculation of the values of ϱ_1 is especially simple when the periods of G are pairwise coprime. For each divisor $d(i)>1$ of $e(i)$, let $n(d(i))$ be the order of the normalizer in G/S of the cyclic subgroup generated by $x^{e(i)/d(i)}S$. We assert that the number of points on S fixed by any generator of the cyclic group $\langle x^{e(i)/d(i)}S\rangle$ is $n(d(i))/e(i)$. To prove this we observe that a consequence of the coprime hypothesis is that the only points on S fixed by the element in question must lie over $\mathfrak{p}_i$. We know that the isotropy group of $\mathfrak{P}_i$ is the cyclic group $\langle x_iS\rangle$. Thus $\sigma(\mathfrak{P}_i)$ is fixed by $\langle x_i^{e(i)/d(i)}S\rangle$ if and only if σ normalizes $\langle x_i^{e(i)/d(i)}S\rangle$. The number of fixed points is therefore equal to $n(d(i))/e(i)$. In such a situation, we can calculate $\langle\varrho_1,\varrho_1\rangle=\sum a_j^2$, where $\varrho_1=\sum a_j\chi_j$ is the expansion of ϱ_1 in terms of its components. If the genus g is small, this calculation together with the character table of G/S can give enough information to allow us to find the complete decomposition of ϱ_1.

The decomposition of ϱ_1 into its irreducible components furnishes us some information concerning the action of G/S on $S/S'S^p$, where $S'S^p$ is the subgroup of S generated by all the commutators and all the pth powers of elements of S. If p is a prime, then the universal coefficient theorem allows us to identify $S/S'S^p$ with $H_1(S, \mathrm{GF}(p))$ or with $H^1(S, \mathrm{GF}(p))$. The action of G/S on $S/S'S^p$ is a modular representation of G/S; it may be viewed as the reduction mod p of ϱ_1. If p does not divide the order of G/S, then the reduction is non-degenerate. We can deduce the following assertion from Theorem 3.2.

PROPOSITION 3.5. *In the preceding notation, we have:*

(a) *for a prime* p *not dividing* $|G/S|$, *the fixed point set of* G/S *on* $S/S'S^p$ *has dimension* 2γ *over* $\mathrm{GF}(p)$.

(b) *for a prime p dividing $|G/S|$, the fixed point set of G/S on $S/S'S^p$ has dimension at least 2γ over* GF(p).

Proof. The condition that an element of $H^1(\mathcal{S}, Q)$ be fixed under G/S involves a system of linear equations. The independence of a set of such elements also involves a system of linear equations. All the equations in question have coefficients in Q. Theorem 3.2 implies that the given system of equations have 2γ linearly independent solutions in C. Hence, the same holds over Q. We may select representatives in $\mathfrak{Z}$ which remain independent mod p. Consequently, 2γ is a lower bound of the dimension in all cases. When p does not divide the order of $|G/S|$, every irreducible representation of G/S in the algebraic closure of GF(p) can be lifted to one in C. Consequently, we must have equality, q.e.d.

When p does divide the order of G/S, the precise action of G/S on $S/S'S^p$ requires a more detailed analysis of the decomposition numbers of the characters of G/S in the sense of modular representation theory. When the genus g of $\mathcal{S}$ is small, the analysis is fairly simple. Indeed, Brauer's block theory can often be used to obtain very precise information. In the few cases considered by us, the quantity 2γ appears to be the dimension of the largest factor space of $S/S'S^p$ which is trivial under the action of G/S. We conclude by giving (without details) some examples illustrating the preceding discussion.

Let $G=G\{2, 3, 7|0\}$. Let p be a prime and let S be one of the normal subgroups of G such that G/S is isomorphic to PSL $(2, p^f)$, f is the least exponent of p such that 7 divides $p^f(p^{2f}-1)$.

(a) $\varrho_{1,0}$ is real if and only if $p \neq 3, 7$. $\varrho_{1,0}$ is irreducible if and only if $p=7$, 2 and 13 corresponding to $g=3$, 7 and 14 respectively.

(b) Let $p=7$. For each prime $q \neq 7$, $S/S'S^q$ is the direct sum of 2 non-isomorphic absolutely irreducible G/S-modules of dimension 3 each. $S/S'S^7$ has two isomorphic absolutely irreducible composition factors. When $q=2$ or 3, we obtain surfaces of genera 17 and 55; each of these is an unramified covering surface of the Klein surface and each has a maximal automorphism group. These are the only such surfaces with genus at most 100.

(c) Let $p=2$. ϱ_1 decomposes into $\varrho_{1,0}+\varrho_{1,0}$ over Q. For each prime $q \neq 2$, $S/S'S^q$ is the direct sum of two isomorphic absolutely irreducible G/S-modules of dimension 7. The G/S composition factors of $S/S'S^2$ have dimension 6, 6, 1 and 1. The corresponding modules of dimension 6 are reducible over the algebraic closure (indeed, over GF(8)). $S/S'S^2$ does not have a G/S-factor module of dimension 1.

(d) Let $p=13$. ϱ_1 decomposes into $\varrho_{1,0}+\varrho_{1,0}$ over Q. For each prime $q \neq 13$, $S/S'S^q$ is the direct sum of two isomorphic absolutely irreducible G/S-modules of dimension 14. $S/S'S^{13}$ does not have a G/S-factor module of dimension $\leqslant 2$.

(e) Let S be a compact Riemann surface of genus g with $1<g\leqslant 100$ such that $A_{co}(S)$ has maximal order $84(g-1)$. If g is not congruent to 1 mod 4, then $g=3$, 7, 14 or 55. If g is congruent to 1 mod 4, then it appears that the only likely value for g other than 17 is 73 corresponding to PSU $(3, 3)\cong G_2(2)'$.

We observe that a corollary of (d) is the confirmation of a conjecture of Macbeath [4; footnote, p. 97] to the effect that the group $G\{2, 3, 7\,|\,0\}$ does not have a factor group of order 2184. This is twice the order of PSL (2, 13). The point is that such a factor group must, according to our results, be a central extension of a cyclic group of order 2 by PSL (2, 13). (d) tells us that this is not possible.

4. Appendix

Let $\mathcal{M}$ be a simply connected, complete Riemannian 2-manifold with constant curvature $\varkappa(\mathcal{M})$. According to $\varkappa(\mathcal{M})$ is positive, zero, or negative, we can take as a model for $\mathcal{M}$ the 2-sphere (viewed as the projective line $\mathcal{P}$ over the complex numbers), the Euclidean plane (viewed as the affine line C over the complex numbers), or the upper half plane $\mathcal{H}$ (equivalently, the unit disk, each with the appropriate hyperbolic metric). Each of these models is endowed with a natural complex structure. The conformal automorphism group $A_{co}(\mathcal{M})$ is respectively: PSL (2, C), Aff (1, C), PSL (2, R), where Aff (1, C) is the split extension of the additive group of C by the multiplicative group of C. The subgroup preserving the orientation and the respective metric $A_{is}(\mathcal{M})$ is respectively: PSU (2, C) (isomorphic to SO(3, R)), $E^+(2, R)$ (the group of proper Euclidean motions, it is the split extension of the group of translations by the group of rotations), PSL (2, R) (i.e., a conformal automorphism of the upper half plane automatically preserves the orientation and the hyperbolic metric). Any discontinuous subgroup Γ of $A_{co}(\mathcal{M})$ is conjugate to a subgroup of $A_{is}(\mathcal{M})$. This assertion is automatic when $\mathcal{M}=\mathcal{H}$. When $\mathcal{M}=\mathcal{P}$, the compactness of $\mathcal{M}$ forces Γ to be a finite group; the assertion follows from the fact that every complex representation of a finite group is equivalent to a unitary representation. When $\mathcal{M}=C$, we can use the explicit structure of Aff (1, C) together with discontinuity to obtain the desired conclusion. From now on we will consider only discontinuous subgroups of $A_{is}(\mathcal{M})$.

Let G be an abstract group with generators:

(1) x_i, $0\leqslant i\leqslant m<\infty$; a_j, b_j, $0\leqslant j\leqslant\gamma<\infty$, and defining relations:

(2) $x_i^{e(i)}=1$, $2\leqslant e(i)\leqslant\infty$; $x_1 \dots x_m[a_1, b_1] \dots [a_\gamma, b_\gamma]=1$,

where $[x, y]=xyx^{-1}y^{-1}$ and $x^\infty=1$ is vacuous. G is called a group with signature $\{e(1), \dots, e(m)\,|\,\gamma\}$. γ is called the genus of G and $e(i)$'s are called the periods (after a trivial normalization given below). x_i is called an elliptic (respectively parabolic) generator of G if $e(i)$ is

finite (respectively infinite). If we replace the generator x_i and x_{i+1} by $x_i x_{i+1} x_i^{-1}$ and x_i, then it becomes clear that the isomorphism class of G depends only on the unordered m-tuple of periods and on the genus. The quantity:

(3) $\varkappa = 2 - 2\gamma - \sum(1 - e(i)^{-1})$

will be called the curvature of G. We normalize the signature as follows:

(A1) $G\{-|0\}$ and $G\{t|0\}$ are both the trivial group. $G\{s, t|0\}$ is a cyclic group of order equal to the g.c.d. of s and t. We will admit only $G\{-|0\}$ and $G\{d, d|0\}$, $2 \leqslant d \leqslant \infty$.

(A2) Every group G with signature is isomorphic to a suitable discontinuous subgroup of $A_{is}(\mathcal{M})$. The isomorphism can be selected so that $\varkappa(\mathcal{M})$ is a positive multiple of the curvature of G and so that when $\mathcal{M} = \mathcal{H}$ a fundamental domain for G has a finite (invariant) area. Conversely, every discontinuous subgroup G of $A_{is}(\mathcal{M})$ having a fundamental domain Δ such that Δ has finite area when $\mathcal{M} = \mathcal{H}$ is a group with signature. Moreover, Δ is relatively compact in $\mathcal{M}$ (equivalently, $G\backslash\mathcal{M}$ is compact) if and only if the signature is finite.

The first assertion was proved by Poincaré. The second assertion was completely proved by Siegel. They considered the hard case of negative curvature. There is no difficulty in generalizing the assertions to the other cases. An account of the existence of a canonical fundamental domain can be found in [16] and [17].

(A3) Let G be a group with signature $\{e(1), \ldots, e(m)|\gamma\}$.

(a) x_i has order $e(i)$, $1 \leqslant i \leqslant m$.

(b) An element $g \neq 1$ has finite order in G if and only if g is conjugate to x_i^t for a uniquely determined index i and a uniquely determined exponent t with $1 \leqslant t < e(i) < \infty$. Each cyclic subgroup $\langle x_i \rangle$ (including those for which $e(i) = \infty$) is a maximal cyclic subgroup of G; each is the normalizer in G of any of its non-identity subgroups.

(c) If all $e(i)$ are finite, then G/TG' is a free abelian group of rank 2γ, where T is the normal subgroup of G generated by all elements of finite order and G' is the commutator subgroup of G.

The verification of (a) and (b) is best carried out geometrically. We consider G as a discontinuous subgroup of $A_{is}(\mathcal{M})$. The results follow from an analysis of fixed points. (c) follows easily from (a) and (b). It is now clear that for groups with finite signatures, the isomorphism class of the group stands in bijective correspondence with the signature.

(A4) Let $S \leqslant G$ be discontinuous subgroups of PSL $(2, \mathcal{R})$ so that S has finite index d in G. G is a group with signature if and only if S is a group with signature. When this is so, the signature of G is finite if and only if the signature of S is finite. Moreover,

(a) The invariant area of a fundamental domain $\Delta(G)$ for G is $-2\pi\varkappa(G)$. Consequently, $d\varkappa(G) = \varkappa(S)$.

(b) Assume that G has finite signature $\{e(1), \ldots, e(m)|\gamma\}$. Assume further that S is a normal subgroup in G so that x_iS has order $t(i)$. Set $f(i,j)=e(i)/t(i)$, $1\leqslant j\leqslant d/t(i)$. Then

(1) S has periods $f(i,j)$, $1\leqslant j\leqslant d/t(i)$, $1\leqslant i\leqslant m$, where $f(i,j)=1$ are deleted.

(2) S has genus δ with $2-2\delta=d\{2-2\gamma-\sum(1-t(i)^{-1})\}$.

The first two assertions follow from the observation that a fundamental domain for G can be formed by the union of d copies of the fundamental domain for S. (a) is a consequence of the Gauss–Bonnet formula. In order to prove (b) we first observe that S has finite signature. Let y be an elliptic generator of S. y must be conjugate in G to x_i^j for a unique index i. Since S is normal in G and x_iS has order $t(i)$, we can conclude that $\langle x_i^j\rangle$ and $\langle x_i^{t(i)}\rangle$ coincide so that y must have order $e(i)/t(i)$. We must show that the G-conjugates of $\langle x_i^{t(i)}\rangle$ fall into $d/t(i)$ S-conjugate classes in S. This follows easily from (b) of (A3). We can now conclude that (1) must hold. (2) is an easy consequence of (1) together with (a).

A group G with signature $\{-|g\}$ is called a surface group. It is the fundamental group of a compact surface of genus g. Such a group is torsion-free. (A4) specializes to

(A5) Let S be a normal subgroup of finite index d in a discontinuous subgroup G of PSL $(2, \mathfrak{R})$. Assume that G has finite signature $\{e(1), \ldots, e(m)|\gamma\}$ and negative curvature $\varkappa$.

(a) Equivalent statements are:

(1) S is torsion-free.

(2) S is a surface group

(3) Each x_iS has order $e(i)$ in G/S, where x_i, $1\leqslant i\leqslant m$, are the elliptic generators of G.

(b) When S is a surface subgroup, its genus g is given by

$$2-2g=d\varkappa=d\{2-2\gamma-\sum(1-e(i)^{-1})\}.$$

An abstract group G is said to be residually finite (and/or solvable, etc.) if the intersection of the normal subgroups with finite (and/or solvable, etc.) factor groups is 1.

(A6) $G\{-|g\}$ is residually finite (even residually a finite 2-group).

This was proved by Frederick [7]. It is in fact valid for all groups with signature. (See Theorem 1.5.)

As a matter of convenience, we will now list all the groups with non-negative curvatures (normalized according to (A1)). It is clear from inspection that they are residually finite (and even solvable except for the icosahedral group which is the unique simple non-abelian group of least order 60).

(A7) Groups with positive curvatures are finite. They are:

(a) Trivial group $G\{-|0\}$

(b) Cyclic group $G\{d, d|0\}$ of order d.

(c) Dihedral group $G\{2, 2, t|0\}$ of finite order $2t$.

(d) Tetrahedral group $G\{2, 3, 3|0\}$ of order 12 isomorphic to the alternating group of degree 4.

(e) Octahedral group $G\{2, 3, 4|0\}$ of order 24 isomorphic to the symmetric group of degree 4.

(f) Icosahedral group $G\{2, 3, 5|0\}$ of order 60 isomorphic to the alternating group of degree 5.

(A8) Groups with zero curvature are split extensions of a free abelian group T_i of rank $i=1$ or 2 by a cyclic group C_j of order j dividing 4 or 6 such that C_j acts freely on T_i. They are

(a) Free abelian groups $T_1=G\{\infty, \infty|0\}$ and $T_2=G\{-|0\}$.

(b) Infinite dihedral group $T_1C_2=G\{2, 2, \infty|0\}$ where C_2 acts according to the matrix (-1).

(c) $G\{2, 3, 6|0\}=T_2C_6$ where C_6 acts according to $\left(\begin{smallmatrix}0 & -1\\ 1 & 1\end{smallmatrix}\right)$. This was studied by G. A. Miller [25] using generators and relations.

(d) $G\{2, 4, 4|0\}=T_2C_4$ where C_4 acts according to $\left(\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right)$

(e) $G\{3, 3, 3|0\}=T_2C_3$ where C_3 acts according to $\left(\begin{smallmatrix}0 & -1\\ 1 & -1\end{smallmatrix}\right)$. This was considered by Feit–Thompson [6] in the study of a special class of finite groups.

f) $G\{2, 2, 2, 2|0\}=T_2C_2$ where C_2 acts according to $\left(\begin{smallmatrix}-1 & 0\\ 0 & -1\end{smallmatrix}\right)$.

References

[1]. Atiyah, M. & Bott, R., *Notes on the Lefshetz fixed point theorem for elliptic complexes.* Harvard University Seminar notes, Cambridge, 1964.

[2]. Brauer, R., Über Systeme hypercomplexer Zahlen. *Math. Z.*, 30 (1929), 79–107.

[3]. Brauer, R. & Suzuki, M., On finite groups of even order whose 2-Sylow group is a quaternion group. *Proc. Nat. Acad. Sci.*, 45 (1959), 1757–1759.

[4]. Coxeter, H. S. M. & Moser, W. O., *Generators and relations for discrete groups.* Ergebnisse der Math., 14 (1965), Springer-Verlag, New York.

[5]. Dickson, L. E., *Linear groups.* Dover, New York, 1958.

[6]. Feit, W. & Thompson, J., Finite groups which contain a self-centralizing subgroup of order 3. *Nagoya Math. J.*, 21 (1962), 185–197.

[7]. Frederick, K., The Hopfian property for a class of fundamental groups. *Comm. Pure Appl. Math.*, 16 (1962), 1–8.

[8]. Gagen, T. M., On groups with abelian Sylow 2-groups. *Math. Z.*, 90 (1965), 268–272.

[9]. Gorenstein, D., *Finite groups.* Harper and Row, New York, 1968.

[10]. Gunning, R. C., *Lectures on Riemann surfaces.* Princeton University Lecture Notes, Princeton, 1966.

[11]. Hurwitz, A., *Mathematische Werke.*, 1 (1932), Basel.

[12]. Iwasawa, K. & Tamagawa, T., On the group of automorphisms of a function field, *J. Math. Soc. Japan*, 3 (1951), 137–147; 4 (1952), 100–101 and 203–204.

[13]. Janko, Z., A new finite simple group with abelian Sylow 2-subgroups and its characterization. *J. of Algebra*, 4 (1966), 147–186.

[14]. JANKO, Z. & THOMPSON, J., On a class of finite simple groups of Ree. *J. of Algebra*, 4 (1966), 274–292.

[15]. JORDAN, H. E., Group characters of various types of linear groups. *Amer. J. Math.*, 29 (1907), 387–485.

[16]. KEEN, L., Canonical polygons for finitely generated Fuchsian groups. *Acta Math.*, 115 (1966), 1–16.

[17]. —— Intrinsic moduli on Riemann surfaces. *Ann. of Math.*, 84 (1966), 404–420.

[18]. LEHNER, J., *Discontinuous groups and automorphic functions*. Amer. Math. Soc. Surveys, 8 (1964), New York.

[19]. LEHNER, J. & NEWMAN, M., On Riemann surfaces with maximal automorphism groups. *Glasgow Math. J.*, 8 (1967), 102–112.

[20]. LEVI, F., Über die Untergruppen der freien Gruppen, II. *Math. Z.*, 37 (1933), 90–97.

[21]. MACBEATH, A. M., *Fuchsian groups*. Dundee Summer School Proc. 1962.

[22]. —— On a theorem of Hurwitz. *Glasgow Math. J.*, 5 (1961), 90–96.

[23]. —— On a curve of genus 7. *Proc. Lond. Math. Soc.*, 15 (1965), 527–542.

[24]. MAGNUS, W., KARRASS, A. & SOLITAR, D., *Combinatorial group theory*. Interscience, New York, 1966.

[25]. MILLER, G. A., On the groups generated by two operators of orders two and three respectively whose product is of order six. *Quarterly J. Math.*, 33 (1901), 76–79.

[26]. REE, R., A family of simple groups associated with the simple Lie algebra of type (G_2). *Amer. J. Math.* 83 (1961), 432–462.

[27]. ROSENLICHT, M., Automorphisms of function fields. *Trans. Amer. Math. Soc.*, 79 (1955), 1–11.

[28]. SAH, C. H., A class of finite groups with abelian 2-Sylow subgroups. *Math. Z.*, 82 (1963), 335–346.

[29]. SCHMIDT, H. L., Über die Automorphismen eines algebraischen Funktionenkörpers von Primzahlcharakteristik. *J. Reine Angew. Math.*, 179 (1938), 5–15.

[30]. WARD, H. N., On Ree's series of simple groups. *Trans. Amer. Math. Soc.*, 121 (1966), 62–89

Received June 8, 1968, in revised form March 9, 1969