SYMMETRIES OF SURFACES: AN EXTENSION OF KULKARNI'S THEOREM

by GARETH A. JONES

(Received 6 October, 1992)

1. Introduction. In [6], Kulkarni considered the set of values of g for which a given finite group G acts faithfully as a group of orientation-preserving self-homeomorphisms of a compact, connected, orientable surface Σ_g of genus g. Let us denote this set by $\mathcal{S}(G)$. Then Kulkarni showed that there exists a positive integer K, depending only on the order $d = |G|$ of G, the exponent $e = \exp G$ of G, and the structure of a Sylow 2-subgroup G_2 of G, satisfying:

THEOREM 1. (Kulkarni [6]) *$\mathcal{S}(G)$ consists of all but finitely many non-negative integers $g \equiv 1 \bmod K$.*

REMARKS 1. The precise determination of $\mathcal{S}(G)$ is, in general, a very difficult task (see [7] for cyclic groups of prime-power order).

2. Kulkarni restricted attention to genera $g \geq 2$, but in fact there is no need to exclude the values $g = 0$ and 1.

My aim here is to consider the sets

$$\mathcal{S}_h(G) = \{g \mid G \text{ acts on } \Sigma_g \text{ with quotient-surface } \Sigma_h\}$$

for each $h \in \mathbb{N}$. I shall show that there exists an integer J, again depending only on d, e and G_2, which satisfies:

THEOREM 2. *$\mathcal{S}_h(G)$ consists of all but finitely many non-negative integers $g \equiv d(h-1)+1 \bmod J$.*

Since $\mathcal{S}(G) = \bigcup_{h \geq 0} \mathcal{S}_h(G)$, Theorem 1 can be deduced from Theorem 2 (see Section 6).

For the definitions of J and K, see Section 2. Although J and K depend only on d, e and G_2, the sets $\mathcal{S}(G)$ and $\mathcal{S}_h(G)$ themselves may depend on additional properties of G. For example, although the cyclic and dihedral groups $G = C_{2p}$ and D_p (for primes $p > 2$) both have $d = e = 2p$ and $G_2 \cong C_2$, we will see in Section 8 that the sets $\mathcal{S}(G)$ and $\mathcal{S}_h(G)$ are generally different for these two groups.

One motive for considering $\mathcal{S}_h(G)$ is the desire to describe, for each h and G, the branched coverings of Σ_h with monodromy group G (see [3, 5, 8] for the case $h = 0$, which is relevant to the Inverse Galois Problem [10], namely Hilbert's conjecture that every finite group is a Galois group over $\mathbb{Q}$). Any such covering-surface is a quotient, by some subgroup of G, of a regular (or Galois) covering $\Sigma_g \to \Sigma_h$ with monodromy group G, or equivalently of a covering $\Sigma_g \to \Sigma_g/G \approx \Sigma_h$ induced by a faithful action of G on Σ_g for some $g \in \mathcal{S}_h(G)$, so it is useful to determine $\mathcal{S}_h(G)$.

It is also of interest to consider the set $\mathcal{F}(G)$ of g such that G acts freely on Σ_g, that is, for which the covering $\Sigma_g \to \Sigma_g/G$ is unbranched. It is easy to prove (and probably widely-known) that for each G there exists some $g_0 \equiv 1 \bmod d$ satisfying:

THEOREM 3. *$\mathcal{F}(G) = g_0 + d\mathbb{N}$. (Thus $\mathcal{F}(G)$ consists of all but finitely many $g \equiv 1 \bmod d$.)*

After giving some preliminary definitions and notation in Section 2, proving an

elementary but useful number-theoretic lemma in Section 3, and stating some important background theorems in Section 4, I shall prove Theorem 2 in Section 5 and deduce Kulkarni's Theorem 1 in Section 6. Theorem 3 is proved in Section 7, and in Section 8 I shall illustrate these results by determining the sets $\mathscr{S}(G)$, $\mathscr{S}_h(G)$ and $\mathscr{F}(G)$ in a few fairly straightforward cases. Relations between different sets $\mathscr{S}_h(G)$ are investigated in Section 9.

I am grateful to Grzegorz Gromadzki and David Singerman for some very helpful and stimulating conversations on this topic.

2. Definitions. Throughout this paper, G will be a finite group of order $d = |G| = \prod_p p^{n_p}$ and exponent $e = \exp G = \prod_p p^{e_p}$ (p prime); thus a Sylow p-subgroup G_p of G has order p^{n_p} and exponent p^{e_p}. An *action* of G on a compact, connected, orientable surface Σ_g of genus $g \geq 0$ is a faithful (i.e. effective) representation of G as a group of orientation-preserving self-homeomorphisms $\Sigma_g \to \Sigma_g$. We let

$$\mathscr{S}(G) = \{g \in \mathbb{N} \mid G \text{ acts on } \Sigma_g\}.$$

If G acts on Σ_g then $\Sigma_g/G \approx \Sigma_h$ for some $h \in \mathbb{N}$, so $\mathscr{S}(G) = \bigcup_{h \in \mathbb{N}} \mathscr{S}_h(G)$ where

$$\mathscr{S}_h(G) = \{g \in \mathbb{N} \mid G \text{ acts on } \Sigma_g \text{ with } \Sigma_g/G \approx \Sigma_h\}.$$

Define

$$n' := \frac{d}{n} \text{ for each } n \text{ dividing } d,$$

$$\Gamma := \{n > 1 \mid G \text{ has an element of order } n\},$$

$$\Delta := \{n \in \Gamma \mid n \text{ is a prime-power}\},$$

$$M_1 := \gcd\{(n-1)n' \mid n \in \Gamma\},$$

$$M_2 := \gcd\{(n-1)n' \mid n \in \Delta\},$$

$$\Pi := \{p \mid p \text{ is a prime dividing } d\},$$

$$\Pi - 1 := \{p - 1 \mid p \in \Pi\},$$

$$M := \frac{d}{e} \cdot \gcd(\Pi - 1).$$

(Note that d/e is an integer coprime to $\gcd(\Pi - 1)$.) In Section 3 we will see that $M_1 = M_2 = M$.

If T is a finite 2-group, let us define $g \in T$ to be *long* if g has order $o(g) = \exp T$, and *short* if $o(g) < \exp T$. Let us denote by T^σ the set of short elements of T, and call T *balanced* if T^σ is a subgroup of index 2 in T.

LEMMA 2.1. *A non-trivial 2-group T is balanced if and only if every relation of the form*

$$\prod_{k=1}^{m} g_k = 1 \quad (g_k \in T) \tag{2.1}$$

involves an even number of long elements g_k.

Proof. To see that the condition is necessary, apply the epimorphism $T \to T/T^o \cong \mathbb{Z}_2$ to (2.1). For the converse, define $\phi: T \to \mathbb{Z}_2$ by $\phi(g) = 0$ or 1 as g is short or long, and check that ϕ is an epimorphism with $\ker \phi = T^o$. □

REMARK. It is possible for T^o to *generate* a subgroup of index 2 without *forming* one: consider $T = C_4 \times D_4$, of order 32 and exponent 4, for example, where T^o generates $C_2 \times D_4$, which contains long elements.

Among finite 2-groups, non-trivial cyclic groups are balanced, but dihedral groups and elementary abelian groups of rank >1 are not. There exist non-cyclic balanced 2-groups: for instance, if T_1 and T_2 are 2-groups, with T_1 balanced and $\exp T_1 > \exp T_2$, then $T_1 \times T_2$ is balanced. Kulkarni's "type I" [**6**, Section 2.2] is equivalent to "unbalanced or cyclic", and "type II" to "balanced and non-cyclic". Let us define a finite group G to be *balanced* if its Sylow 2-subgroups G_2 are balanced. Then we define

$$J = J(G) := \begin{cases} M & \text{if } G \text{ is balanced,} \\ \frac{1}{2}M & \text{otherwise,} \end{cases}$$

and

$$K = K(G) := \begin{cases} \dfrac{d}{e} & \text{if } G_2 \text{ is balanced or trivial,} \\ \dfrac{d}{2e} & \text{otherwise.} \end{cases}$$

REMARKS 1. This definition of the modulus K in Theorem 1 is superficially different from but logically equivalent to that given by Kulkarni [**6**, §2], who denotes it by N or $2N$ depending on the structure of G_2.

2. M is odd if and only if G_2 is non-trivial and cyclic, in which case G is balanced; thus J is always an integer, and likewise so is K.

Finally, some notation: I shall write $m \mid n$ to denote that m divides n, and $p^f \parallel n$ to denote that p^f is the highest power of p dividing n (where p is prime). If A and B are sets, let $A \subseteq B$ mean that A is a cofinite subset of B, that is, $A \subseteq B$ with finite complement $B - A$. The cyclic and dihedral groups of order n and $2n$ are denoted by C_n and D_n, while $[a, b]$ denotes the commutator $a^{-1}b^{-1}ab$. The natural numbers are $\mathbb{N} = \{0, 1, \ldots\}$. I have followed Kulkarni's notation in [**6**] are much as possible, but internal consistency has required a few changes.

3. An elementary lemma.

LEMMA 3.1. $M_1 = M_2 = M$.

Proof. It is sufficient to show that M_1, M_2 and M are all divisible by the same powers p^f of each prime p.

(i) Let $p \in \Pi$. If we take any $n \in \Gamma$, then $n \mid e$ and $p^{n_p} \mid d$, so $p^{n_p - e_p} \mid d/n = n'$ and hence $p^{n_p - e_p} \mid n'(n-1)$; if we take $n = p^{e_p} (\in \Gamma)$, then $p^{n_p - e_p} \parallel n'(n-1)$; thus $p^{n_p - e_p} \parallel M_1$. A similar argument gives $p^{n_p - e_p} \parallel M_2$. Since $p \in \Pi$, p is coprime to $\gcd(\Pi - 1)$, so $p^{n_p - e_p} \parallel M$.

(ii) Let $p \notin \Pi$. Then d, e and n' $(n \in \Gamma)$ are all coprime to p, so we have

$$p^f \mid M_1 \Leftrightarrow p^f \mid \gcd(\Gamma - 1),$$
$$p^f \mid M_2 \Leftrightarrow p^f \mid \gcd(\Delta - 1),$$
$$p^f \mid M \Leftrightarrow p^f \mid \gcd(\Pi - 1).$$

https://doi.org/10.1017/S0017089500030718 Published online by Cambridge University Press

The elements of Δ are just powers $q, q^2, \ldots, q^{e_q}$ of primes $q \in \Pi$, and $\gcd\{q-1, q^2-1, \ldots\} = q-1$, so $\gcd(\Delta - 1) = \gcd(\Pi - 1)$. Now Γ contains Δ, and every element of Γ is a product of elements of Δ, so each $n \in \Gamma$ is $\equiv 1 \bmod p^f$ if and only if each $n \in \Delta$ is $\equiv 1 \bmod p^f$. Thus the same powers p^f of p divide the greatest common divisors of $\Gamma - 1$, $\Delta - 1$ and $\Pi - 1$. □

4. Some background theorems. In [4], Hurwitz proved that a finite group G acts on Σ_g, with $\Sigma_g/G \approx \Sigma_h$, if and only if G has generators

$$a_1, b_1, \ldots, a_h, b_h, c_1, \ldots, c_k$$

such that

$$\prod_{i=1}^{h} [a_i, b_i] \cdot \prod_{i=1}^{k} c_i = 1 \tag{4.1}$$

and

$$2 - 2g = d\left(2 - 2h - \sum_{i=1}^{k} \left(1 - \frac{1}{n_i}\right)\right), \tag{4.2}$$

where $d = |G|$ and $n_i = o(c_i)$. Here $c_1, \ldots, c_k$ generate stabilisers of points in the k distinct non-regular orbits of G on Σ_g; by choosing these points appropriately (i.e. replacing generators with suitable conjugates) we can arrange the factors c_i in (4.1) in any required order. If x_n denotes the number of generators c_i of order n, then by using the notation introduced in Sections 1–2 we can restate Hurwitz's Theorem as follows: $g \in \mathcal{S}_h(G)$ if and only if G has elements a_i, b_i $(1 \le i \le h)$ and $c_{i,n}$ $(1 \le i \le x_n,\ n \in \Gamma)$ satisfying

(i) the elements a_i, b_i and $c_{i,n}$ generate G,

(ii) $\prod_{i=1}^{h} [a_i, b_i] \cdot \prod_{i,n} c_{i,n} = 1$ for some ordering of the elements $c_{i,n}$,

(iii) each $c_{i,n}$ has order n $(1 \le i \le x_n)$,

(iv) $2(g-1) - 2d(h-1) = \sum_{n \in \Gamma} (n-1) n' x_n$.

Let us call such a set of elements a *Hurwitz set* for G of *signature* $(h; x)$, where x is the function $n \mapsto x_n$.

Equation (4.2), or equivalently (iv), is the *Riemann–Hurwitz formula*; as in [6], in order to study its solutions we will need to consider additive subsemigroups of $\mathbb{N}$ of the form

$$\mathbb{N}\Phi = \left\{ \sum_{m \in \Phi} x_m m \mid x_m \in \mathbb{N} \right\},$$

where Φ is a finite set of positive integers. It is well-known (and easily proved) that

$$\mathbb{N}\Phi \subseteq \mathbb{N} \cdot \gcd(\Phi). \tag{4.3}$$

(This is sometimes called the *Post Office Theorem*: if stamps are available, in unlimited supply, in denominations $m \in \Phi$ then the attainable postal rates form the set $\mathbb{N}\Phi$.) A simple extension of (4.3) asserts that if $k_m \in \mathbb{N}$ for each $m \in \Phi$ then

$$\left\{ \sum_{m \in \Phi} x_m m \mid x_m \in \mathbb{N}, x_m \ge k_m \right\} \subseteq \mathbb{N} \cdot \gcd(\Phi). \tag{4.4}$$

https://doi.org/10.1017/S0017089500030718 Published online by Cambridge University Press

5. Proof of Theorem 2. If we define

$$\mathcal{T}_h(G) = \mathbb{N}J + d(h-1) + 1,$$

then it is sufficient to prove the following slightly stronger result:

THEOREM 2'. $\mathcal{S}_h(G) \subseteq \mathcal{T}_h(G)$.

Proof. (1) First we show that $\mathcal{S}_h(G) \subseteq \mathcal{T}_h(G)$.

If $g \in \mathcal{S}_h(G)$ then G has a Hurwitz set satisfying the Riemann–Hurwitz formula

$$2(g-1) - 2d(h-1) = \sum_{n \in \Gamma} (n-1)n'x_n, \tag{5.1}$$

where $x_n (\in \mathbb{N})$ is the number of orbits of G with stabilisers of order n. By Lemma 3.1 the coefficients $(n-1)n'$ $(n \in \Gamma)$ in (5.1) have greatest common divisor M, so $\Sigma(n-1)n'x_n \in \mathbb{N}M$, say

$$\sum_{n \in \Gamma} (n-1)n'x_n = tM \quad (t \in \mathbb{N}). \tag{5.2}$$

If G is not balanced then $M = 2J$, so (5.1) and (5.2) give $g \in \mathcal{T}_h(G)$ as required. Hence assume that G is balanced, so that $J = M$. Now the Riemann–Hurwitz formula for the action of a Sylow 2-subgroup G_2 of G on Σ_g is

$$2(g-1) - 2^{\nu+1}(\gamma - 1) = \sum_{i=1}^{\varepsilon} (2^i - 1)2^{\nu-i}z_i, \tag{5.3}$$

where for notational convenience $\nu = n_2$ and $\varepsilon = e_2$ (so $|G_2| = 2^\nu$ and $\exp G_2 = 2^\varepsilon$), while γ is the genus of Σ_g/G_2, and z_i is the number of G_2-orbits with stabilisers of order 2^i $(1 \le i \le \varepsilon)$. Since G_2 is balanced, by applying Lemma 2.1 to the relation (4.1) for G_2 we see that z_ε must be even, so (5.3) implies that $g \equiv 1 \bmod 2^{\nu-\varepsilon}$. Clearly $d \equiv 0 \bmod 2^{\nu-\varepsilon}$, so by (5.1) we have $2^{\nu-\varepsilon+1} \mid \Sigma(n-1)n'x_n = tM$. Since G is balanced, d is even and so $\gcd(\Pi - 1) = 1$. Thus $2^{\nu-\varepsilon} \parallel M$, by definition of M, so t is even and therefore (5.1) gives $g - 1 - d(h-1) = \frac{1}{2}tM \in \mathbb{N}M = \mathbb{N}J$, as required.

(2) We now show that each sufficiently large integer $g \in \mathcal{T}_h(G)$ is in $\mathcal{S}_h(G)$ by showing that G has a Hurwitz set, satisfying conditions (i) to (iv) of Section 4. In fact it is sufficient (and simpler) to show that these conditions can be satisfied with the additional restriction that each of the generators $c_{i,n}$ has prime-power order, that is, $n \in \Delta$, so that (iv) is replaced with

(iv)' $2(g-1) - 2d(h-1) = \sum_{n \in \Delta} (n-1)n'x_n$.

(Of course, those g satisfying (i), (ii), (iii) and (iv)' may form a proper subset of $\mathcal{S}_h(G)$.)

First define $a_i = b_i = 1$ for $i = 1, \ldots, h$. We must now find elements $c_{i,n} \in G$ $(1 \le i \le x_n,\ n \in \Delta)$ satisfying (iii), (iv)' and

(i)' the elements $c_{i,n}$ generate G,

(ii)' $\prod_{i,n} c_{i,n} = 1$ for some ordering of the generators $c_{i,n}$.

By (4.4) and Lemma 3.1, given any constants $k_n \in \mathbb{N}$ $(n \in \Delta)$, each sufficiently large multiple of M has the form $\sum_{n \in \Delta} (n-1)n'x_n$ with integers $x_n \ge k_n$, so each sufficiently large $g \in \mathcal{T}_h(G) = \mathbb{N} + d(h-1) + 1 \subseteq \mathbb{N} \cdot \frac{1}{2}M + d(h-1) + 1$ satisfies (iv)' with $x_n \ge k_n$. Now G has a generating set whose elements have prime-power orders $n \in \Delta$, so by choosing each k_n sufficiently large we can include among the elements $c_{i,n}$ all these generators (so that

https://doi.org/10.1017/S0017089500030718 Published online by Cambridge University Press

(i)′ holds) together with their inverses, arranged in adjacent pairs which cancel in the product in (ii)′.

Depending on the value of x_n in (iv)′, we may need to define further elements $c_{i,n}$ of order n. *First suppose that n is odd*, and let u be any element of order n in G. If an even number of elements $c_{i,n}$ are required, we can use consecutive pairs u and u^{-1}, cancelling in (ii)′; for an odd number (which we may assume is at least 3 by taking k_n sufficiently large) we can use $u, u^{-1}, u, \ldots, u^{-1}, u, u, u^{-2}$ (of order n since n is odd), again cancelling in (ii)′.

Now consider powers of 2 in Δ. Define $r = 2^{\nu} = 2^{n_2}$ and $s = 2^{\varepsilon} = 2^{e_2}$, the order and exponent of G_2. *First suppose that G is balanced*, so $J = M$. Since $g \in \mathcal{T}_h(G) = \mathbb{N}M + d(h-1)+1$, with r/s dividing M, we see that $2r/s$ divides the left-hand side of (iv)′. Each coefficient $(n-1)n'$ $(n \in \Delta, n \neq s)$ on the right-hand side of (iv)′ is divisible by $2r/s$, with the single exception of the coefficient corresponding to $n = s$, for which $r/s = 2^{\nu-\varepsilon} \,||\, (s-1)s'$. It follows that, in our chosen solution of (iv)′, x_s must be even.

For each $n = 2^j < s$ in Δ, choose an element $u \in G_2$ of order n. If x_n is even then we can, as before, define the remaining elements $c_{i,n}$ (of which we require an even number) to be $u, u^{-1}, \ldots, u, u^{-1}$. If x_n is odd then since G_2 is balanced and u is short, we can write $u = vw$ for long elements $v, w \in G_2$; we define the remaining elements $c_{i,n}$ to be $u, u^{-1}, \ldots, u^{-1}, u$, and define two of the elements $c_{i,s}$ of order s to be w^{-1} and v^{-1}, with the factors in (ii)′ arranged so that $u \,.\, u^{-1} \,.\, \ldots \,.\, u^{-1} \,.\, u = u$ cancels with $w^{-1} \,.\, v^{-1} = u^{-1}$. By choosing k_s large enough we can find such a pair $c_{i,s} = w^{-1}, v^{-1}$ for each $n = 2^j < s$ with x_n odd. Since x_s is even, and since we have so far chosen elements $c_{i,s}$ of order s in pairs, there remain an even number to be defined, and as before we can take these to be mutually inverse pairs, all cancelling in (ii)′. Thus (ii)′ is satisfied.

Now suppose that G is not balanced. If x_s is even then we can proceed as in the balanced case, choosing the required elements u, v, w from a fixed cyclic (and hence balanced) subgroup of order s. Hence suppose that x_s is odd. Since G_2 is not balanced, Lemma 2.1 implies that there is a relation

$$\prod_{k=1}^{m} u_k = 1 \quad (u_k \in G_2) \tag{5.4}$$

involving an odd number of long terms u_k. By taking the constants k_n $(n = 2^j \leq s)$ sufficiently large we can include $u_1, \ldots, u_m$ among the elements $c_{i,n}$, cancelling in (ii)′ by (5.4). This leaves us with an even number of terms $c_{i,s}$ to define, so we can proceed as in the case where x_s is even. □

REMARK. At the point in the original proof of Theorem 1 corresponding to this last case [**6**, §2.10, Case (3)], the possibility that the short elements may generate a subgroup P of index 2 in G_2 is overlooked. This situation can arise (see the remark following Lemma 2.1), but the proof is easily remedied, as above. Note also that in Cases (2) and (3) of §2.10, r should be replaced with s.

6. Proof of Theorem 1. From the definitions of J and d, we see that

$$\gcd(J, d) = \begin{cases} \dfrac{d}{e} & \text{if } G_2 \text{ is balanced or trivial,} \\ \dfrac{d}{2e} & \text{otherwise} \end{cases}$$

$$= K. \tag{6.1}$$

https://doi.org/10.1017/S0017089500030718 Published online by Cambridge University Press

If we define $H = J/K$ then $\mathcal{T}_{H+h}(G) \subseteq \mathcal{T}_h(G)$ for all $h \geq 0$, so $\bigcup_{h\geq 0} \mathcal{T}_h(G)$ is the union of just *finitely* many sets $\mathcal{T}_h(G)$. Since $\mathcal{S}(G) = \bigcup_{h\geq 0} \mathcal{S}_h(G)$, with $\mathcal{S}_h(G) \subseteq \mathcal{T}_h(G)$ for all h by Theorem 2', it follows that

$$\begin{aligned}\mathcal{S}(G) &\subseteq \bigcup_{h\geq 0} \mathcal{T}_h(G) \\ &= \bigcup_{h\geq 0} (\mathbb{N}J + d(h-1) + 1) \\ &= \mathbb{N}J + \mathbb{N}d - d + 1 \\ &\subseteq \mathbb{N}K - d + 1\end{aligned}$$

(this last step requiring (4.3) and (6.1)). Since $K \mid d$, this proves Theorem 1.

7. Proof of Theorem 3. It is interesting (and considerably simpler) to consider the set $\mathcal{F}(G) \subseteq \mathcal{S}(G)$ of $g \in \mathbb{N}$ for which G acts freely (i.e. without fixed-points) on Σ_g, or equivalently, for which the regular covering $\Sigma_g \to \Sigma_h$ induced by G is unbranched. This corresponds to the case where $x_n = 0$ for all $n \in \Gamma$ in (5.1), so that g and h are directly related by

$$g = d(h-1) + 1; \tag{7.1}$$

thus it is sufficient to determine the set $\mathcal{H}(G)$ of values of h corresponding to genera $g \in \mathcal{F}(G)$. By Hurwitz's Theorem (Section 4), $h \in \mathcal{H}(G)$ if and only if G has generators $a_1, b_1, \ldots, a_h, b_h$ satisfying

$$\prod_{i=1}^{h} [a_i, b_i] = 1. \tag{7.2}$$

Now G certainly has such a generating set for some h: we can take $a_1, b_1, \ldots, a_r, b_r$ to be any set of $2r$ generators, define $a_{r+1} = b_{r+1-i}$ and $b_{r+1} = a_{r+1-i}$ for $i = 1, \ldots, r$, and put $h = 2r$, so that each commutator

$$[a_{r+i}, b_{r+i}] = [b_{r+1-i}, a_{r+1-i}] = [a_{r+1-i}, b_{r+1-i}]^{-1}$$

cancels with $[a_{r+1-i}, b_{r+1-i}]$ in (7.2). Thus $\mathcal{H}(G)$ is non-empty, and moreover if $h \in \mathcal{H}(G)$ then $h+1 \in \mathcal{H}(G)$, since we can simply add a commuting pair $a_{h+1}, b_{h+1} \in G$ to a generating set satisfying (7.2). This proves that $\mathcal{H}(G) = h_0 + \mathbb{N}$ for some minimum $h_0 \in \mathcal{H}(G)$ (with $h_0 \leq 2\lceil \frac{1}{2} \operatorname{rank} G \rceil$), and so

$$\begin{aligned}\mathcal{F}(G) &= d(\mathcal{H}(G) - 1) + 1 \\ &= d(h_0 + \mathbb{N} - 1) + 1 \\ &= g_0 + d\mathbb{N},\end{aligned}$$

where

$$g_0 = d(h_0 - 1) + 1 \equiv 1 \bmod d. \quad \square$$

REMARKS 1. The above argument shows that every 2-generator finite group G is the monodromy group of an unbranched regular covering $\Sigma_g \to \Sigma_h$ for each $h \geq 2$ (since $h_0 \leq 2$). In particular, this applies to every finite simple group, since Miller [**9**], Steinberg [**11**], and Aschbacher and Guralnick [**1**] have respectively shown that the alternating,

https://doi.org/10.1017/S0017089500030718 Published online by Cambridge University Press

Lie-type and sporadic simple groups all have two generators (see [2] for a good survey on generators for finite simple groups).

2. If $h \geq h_0$ then $h \in \mathcal{H}(G)$, and by (4.2) the corresponding genus $g = d(h-1)+1$ must be the least element of $\mathcal{S}_h(G)$. If $h < h_0$, however, the least element g of $\mathcal{S}_h(G)$ cannot correspond to a free action of G on Σ_g: see Section 8 for examples.

8. Examples. This section illustrates the preceding results by giving the sets $\mathcal{S}(G)$, $\mathcal{S}_h(G)$ and $\mathcal{F}(G)$ in a few simple cases. The method is to determine the values of h and x_n ($n \in \Gamma$) such that G has a Hurwitz set a_i, b_i ($1 \leq i \leq h$) and $c_{i,n}$ ($1 \leq i \leq x_n$), satisfying $o(c_{i,n}) = n$ and

$$\prod_i [a_i, b_i] \cdot \prod_{i,n} c_{i,n} = 1. \tag{8.1}$$

The values of g are then given by the Riemann–Hurwitz formula in the form

$$g = \frac{1}{2} \sum_{n \in \Gamma} (n-1) n' x_n + d(h-1) + 1, \tag{8.2}$$

with those $g \in \mathcal{F}(G)$ corresponding to the cases $x_n = 0$ for all $n \in \Gamma$.

For each G, a diagram shows the pairs $(g, h) \in \mathbb{N}^2$ such that $g \in \mathcal{S}_h(G)$, with white dots representing unbranched coverings $\Sigma_g \to \Sigma_h$ (that is, $g \in \mathcal{F}(G)$). Thus $\mathcal{S}(G)$ and $\mathcal{F}(G)$ can be seen by projecting all the dots or the white dots onto the g-axis.

a) $G = C_2$. This group is balanced, with $d = e = 2$, so $J = K = 1$. Thus Theorem 1 asserts that $\mathcal{S}(C_2) \subseteq \mathbb{N}$, and Theorem 2′ that $\mathcal{S}_h(C_2) \subseteq \mathbb{N} + 2(h-1) + 1 = \mathbb{N} + 2h - 1$.

Since $\Gamma = \{2\}$ in this case, (8.2) becomes

$$g = \tfrac{1}{2} x_2 + 2h - 1. \tag{8.3}$$

Now one can choose generators a_i, b_i ($1 \leq i \leq h$) and $c_{i,2}$ ($1 \leq i \leq x_2$) satisfying $o(c_{i,2}) = 2$ and (8.1) if and only if x_2 is even, with $x_2 \geq 2$ if $h = 0$. Applying this to (8.3), we see that $\mathcal{S}_0(C_2) = \mathbb{N}$ and $\mathcal{S}_h(C_2) = \mathbb{N} + 2h - 1$ for all $h \geq 1$, so $\mathcal{S}(C_2) = \cup_h \mathcal{S}_h(C_2) = \mathbb{N}$. Putting $x_2 = 0$ in (8.3), so that $h \geq 1$, we also see that $\mathcal{F}(C_2) = 2\mathbb{N} + 1$, that is, $g_0 = 1$ in Theorem 3. These results are illustrated in Fig. 1.

b) $G = C_p$ (prime $p > 2$). This group is unbalanced, with $d = e = p$, so $J = \frac{1}{2}(p-1)$ and $K = 1$. Thus Theorems 1 and 2′ assert that $\mathcal{S}(C_p) \subseteq \mathbb{N}$ and $\mathcal{S}_h(C_p) \subseteq \frac{1}{2}(p-1)\mathbb{N} + p(h-1) + 1$.

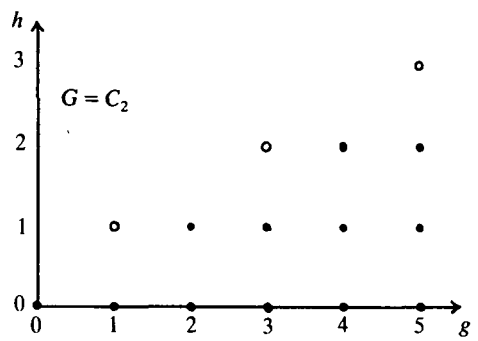

Figure 1.

https://doi.org/10.1017/S0017089500030718 Published online by Cambridge University Press

Since $\Gamma = \{p\}$, (8.2) becomes

$$\begin{aligned} g &= \tfrac{1}{2}(p-1)x_p + p(h-1) + 1 \\ &= \tfrac{1}{2}(p-1)(x_p - 2) + ph. \end{aligned} \tag{8.4}$$

If $h = 0$ we can take any $x_p \geq 2$, so $\mathscr{S}_0(C_p) = \frac{1}{2}(p-1)\mathbb{N}$. If $h \geq 1$ we can take any $x_p \neq 1$, so

$$\mathscr{S}_h(C_p) = \{ph - p + 1\} \cup (\tfrac{1}{2}(p-1)\mathbb{N} + ph).$$

Hence

$$\mathscr{S}(C_p) = \left\{0, 1, \frac{p-1}{2}, p-1, p, p+1, \frac{3p-3}{2}, \frac{3p-1}{2}, 2p-2, 2p-1, 2p, 2p+1, \frac{5p-5}{2}, \ldots\right\},$$

containing all but $\frac{1}{4}(p-3)^2$ elements of $\mathbb{N}$ (see Figure 2). Putting $x_p = 0$ (so that $h \geq 1$) in (8.4), we that $\mathscr{F}(C_p) = p\mathbb{N} + 1$, so $g_0 = 1$.

c) $G = D_p$ (prime $p > 2$). This group is balanced, with $d = e = 2p$, so $J = K = 1$ and Theorems 1 and 2′ give $\mathscr{S}(D_p) \subsetneq \mathbb{N}$ and $\mathscr{S}_h(D_p) \subsetneq \mathbb{N} + 2p(h-1) + 1$.

We have $\Gamma = \{2, p\}$, so (8.2) becomes

$$g = \tfrac{1}{2}px_2 + (p-1)x_p + 2p(h-1) + 1. \tag{8.5}$$

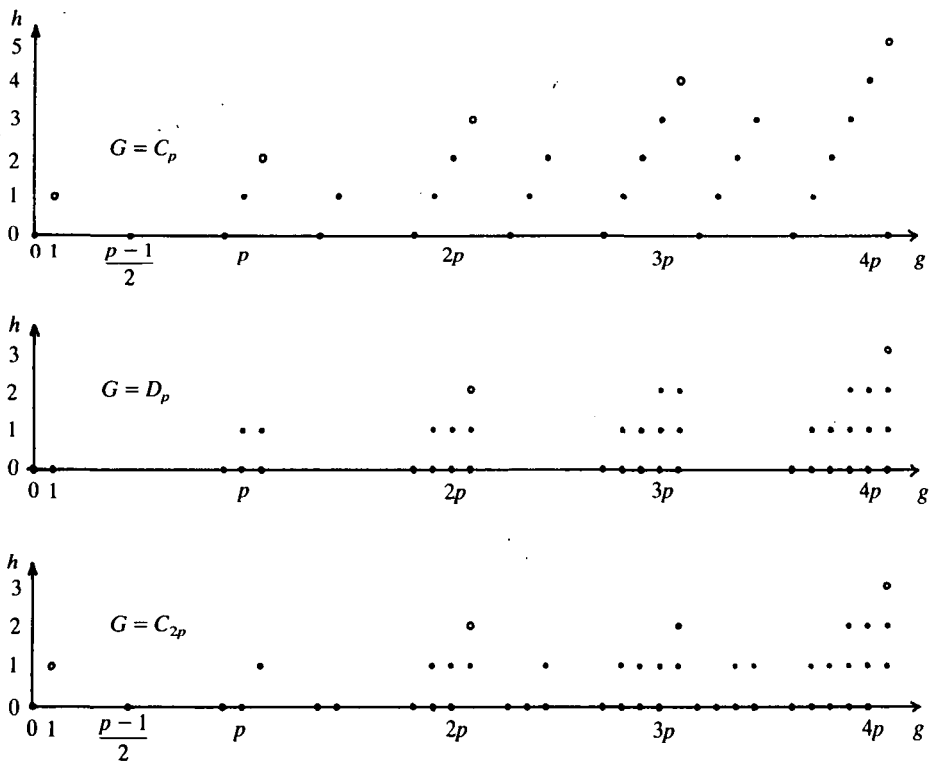

Figure 2.

https://doi.org/10.1017/S0017089500030718 Published online by Cambridge University Press

To satisfy (8.1), x_2 must be even. If $h=0$, then to generate G we need $x_2 \geq 2$, and if $x_2 = 2$ then (8.1) requires $x_p \geq 1$; these conditions are also sufficient, so

$$\mathcal{S}_0(D_p) = \{0, 1, p-1, p, p+1, 2p-2, 2p-1, 2p, 2p+1, 3p-3, \ldots\}.$$

If $h = 1$ the corresponding conditions are $x_2 \geq 0$, with $x_p \geq 1$ if $x_2 = 0$, so

$$\mathcal{S}_1(D_p) = \mathcal{S}_0(D_p) + p.$$

If $h > 1$ we can take any x_2, $x_p \geq 0$, so

$$\mathcal{S}_h(D_p) = (\mathcal{S}_1(D_p) \cup \{1\}) + 2p(h-1).$$

Since $\mathcal{S}_0(D_p) \supseteq \mathcal{S}_1(D_p) \supseteq \mathcal{S}_2(D_p) \supseteq \ldots$, we have $\mathcal{S}(D_p) = \mathcal{S}_0(D_p)$, containing all but $\frac{1}{2}(p-3)(p-2)$ elements of $\mathbb{N}$. If $x_2 = x_p = 0$ then $h \geq 2$, so

$$\mathcal{F}(D_p) = 2p\mathbb{N} + 2p + 1,$$

giving $g_0 = 2p+1$.

Notice that since C_2, $C_p \leq D_p$ we have $\mathcal{S}(D_p) \subseteq \mathcal{S}(C_2) \cap \mathcal{S}(C_p)$ and $\mathcal{F}(D_p) \subseteq \mathcal{F}(C_2) \cap \mathcal{F}(C_p)$.

d) $G = C_{2p}$ (prime $p > 2$). This group is balanced, with $d = e = 2p$, so $J = K = 1$ and Theorems 1 and 2′ give $\mathcal{S}(C_{2p}) \subseteq \mathbb{N}$ and $\mathcal{S}_h(C_{2p}) \subseteq \mathbb{N} + 2p(h-1) + 1$, as in (c).

In this case, however, $\Gamma = \{2, p, 2p\}$, so (8.2) becomes

$$g = \tfrac{1}{2}px_2 + (p-1)x_p + (p-\tfrac{1}{2})x_{2p} + 2p(h-1) + 1, \tag{8.6}$$

and with three variables x_n, the determination of $\mathcal{S}_h(C_{2p})$ is significantly more tedious than in the previous examples. If $h = 0$, one can choose elements $c_{i,n}$ to generate C_{2p} if and only if $x_{2p} \geq 1$ or both x_2, $x_p \geq 1$, and to satisfy the relation (8.1) if and only if $x_2 + x_{2p}$ is even and $x_p + x_{2p} \neq 1$; by considering the cases $x_{2p} = 0, 1, 2, \ldots$ in turn one eventually finds that

$$\mathcal{S}_0(C_{2p}) = \left\{0, \frac{p-1}{2}, p-1, p, \frac{3p-3}{2}, \frac{3p-1}{2}, 2p-2, 2p-1, 2p, \frac{5p-5}{2}, \ldots\right\}.$$

If $h = 1$, one can generate C_{2p} with any x_2, x_p, $x_{2p} \geq 0$, and satisfy (8.1) if and only if $x_2 + x_{2p}$ is even and $x_p + x_{2p} \neq 1$; this leads to

$$\mathcal{S}_1(C_{2p}) = \left\{1, p+1, 2p-1, 2p, 2p+1, \frac{5p-1}{2}, 3p-2, 3p-1, 3p, 3p+1, \frac{7p-3}{2}, \frac{7p-1}{2}, 4p-3, \ldots\right\}.$$

If $h > 1$ the same conditions on x_2, x_p and x_{2p} apply (see Lemma 9.1 for a generalisation of this), so $\mathcal{S}_h(C_{2p}) = \mathcal{S}_1(C_{2p}) + 2p(h-1) \subseteq \mathcal{S}_1(C_{2p})$ and hence

$$\mathcal{S}(C_{2p}) = \mathcal{S}_0(C_{2p}) \cup \mathcal{S}_1(C_{2p}) = \left\{0, 1, \frac{p-1}{2}, p-1, p, p+1, \frac{3p-3}{2}, \frac{3p-1}{2}, 2p-2, 2p-1, 2p, 2p+1, \frac{5p-5}{2}, \ldots\right\}.$$

https://doi.org/10.1017/S0017089500030718 Published online by Cambridge University Press

If we put $x_2 = x_p = x_{2p} = 0$ we can take any $h \geq 1$, so

$$\mathcal{F}(C_{2p}) = 2p\mathbb{N} + 1,$$

giving $g_0 = 1$.

Notice that although D_p and C_{2p} have the same order, exponent and Sylow 2-subgroups, so that $K(D_p) = K(C_{2p})$ and $J(D_p) = J(C_{2p})$, nevertheless $\mathcal{S}(D_p) \neq \mathcal{S}(C_{2p})$ (unless $p = 3$) and $\mathcal{S}_h(D_p) \neq \mathcal{S}_h(C_{2p})$ for all $h \geq 0$: the elements of order $2p$ in C_{2p} permit patterns of branching over Σ_h not available for D_p.

Since $C_p \leq C_{2p}$, $\mathcal{S}(C_{2p})$ is contained in $\mathcal{S}(C_p)$; in fact, the calculations in (b) and (d) show that these two sets are equal. This is a little surprising, since the inclusion $C_p \leq D_p$ does not lead to a similar equality. (See Fig. 2 to compare $\mathcal{S}(C_p)$, $\mathcal{S}(D_p)$ and $\mathcal{S}(C_{2p})$.)

9. Relations between sets. Theorem 2 shows that each set $\mathcal{S}_h(G)$, like $\mathcal{S}(G)$ and $\mathcal{F}(G)$, is eventually periodic. The sets $\mathcal{S}_h(G)$, for a given group G, also display a weak form of periodicity with respect to the parameter h.

LEMMA 9.1. *For all sufficiently large h,*

$$\mathcal{S}_{h+1}(G) = \mathcal{S}_h(G) + d.$$

Proof. There exists $h_1 \in \mathbb{N}$ such that if $h \geq h_1$ then every element c of the derived group G' has the form $c = \prod_{i=1}^{h} [a_i, b_i]$ where $a_1, b_1, \ldots, a_h, b_h$ generate G. For instance, we can take $h_1 = k + l$, where $k = \lceil \frac{1}{2} \operatorname{rank} G \rceil$ (so $a_1, b_1, \ldots, a_k, b_k$ can be chosen to generate G) and l is sufficiently large that every element of G' is a product of l commutators (so $a_{k+1}, b_{k+1}, \ldots, a_h, b_h$ can be chosen to satisfy $c = \prod [a_i, b_i]$).

It follows that if $h \geq h_1$, then G has a Hurwitz set with signature $(h; x)$ if and only if it has one with signature $(h + 1; x)$: for we can increase the genus simply by defining $a_{h+1} = b_{h+1} = 1$, and decrease it by rewriting $\prod_{i=1}^{h+1} [a_i, b_i]$ as a product of h commutators (of generators of G, if necessary). Since x remains unchanged, these transformations increase or decrease the genus g in (4.2) by d, so the result follows from Hurwitz's Theorem. □

REMARK. The "increasing" part of this argument in fact shows that $\mathcal{S}_h(G) + d \subseteq \mathcal{S}_{h+1}(G)$ for *all* $h \in \mathbb{N}$.

LEMMA 9.2. If $n \in \Gamma$ *then*

$$\mathcal{S}_h(G) + (n-1)n' \subseteq \mathcal{S}_h(G).$$

Proof. By adjoining an extra pair c, c^{-1} of elements $c_{i,n}$ of order n to a Hurwitz set for G, we obtain another Hurwitz set with h unchanged and g increased by $(n-1)n'$, so Hurwitz's Theorem gives the result. □

COROLLARY 9.3. *If $n \in \Gamma$ then*

$$\mathcal{S}_{h+n-1}(G) \subseteq \mathcal{S}_h(G)$$

for all sufficiently large h.

Proof. If Lemmas 9.1 and 9.2 are iterated $n-1$ and n times respectively, we obtain $\mathcal{S}_{h+n-1}(G) = \mathcal{S}_h(G) + (n-1)d \subseteq \mathcal{S}_h(G)$. □

https://doi.org/10.1017/S0017089500030718 Published online by Cambridge University Press

COROLLARY 9.4. *If G has even order then*

$$\mathcal{S}_{h+1}(G) \subseteq \mathcal{S}_h(G)$$

for all sufficiently large h. □

REMARKS 1. Theorem 2 implies that the symbol $\subsetneq$ can replace $\subseteq$ in the various inclusions proved above.

2. The examples in Section 8 illustrate these results. For instance, C_2, C_p and C_{2p} satisfy Lemma 9.1 for all $h \geq 1$ (but not $h = 0$), while D_p satisfies it for all $h \geq 2$ (but not $h \leq 1$). Similarly C_2 and D_p satisfy Corollary 9.4 for all $h \geq 0$, while C_{2p} satisfies it for all $h \geq 1$ (but not $h = 0$).

REFERENCES

1. M. Aschbacher and R. Guralnick, Some applications of the first cohomology group, *J. Algebra*, **90** (1984), 446–460.

2. L. Di Martino and M. C. Tamburini, 2-generation of finite simple groups and some related topics, in *Generators and Relations in Groups and Geometries* (ed. A. Barlotti *et al.*), (Kluwer, 1991).

3. R. M. Guralnick and J. G. Thompson, Finite groups of genus zero, *J. Algebra*, **131** (1990), 303–341.

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

5. K. Kuiken, On the monodromy groups of Riemann surfaces of genus zero, *J. Algebra*, **59** (1979), 481–489.

6. R. S. Kulkarni, Symmetries of surfaces, *Topology*, **26** (1987), 195–203.

7. R. S. Kulkarni and C. Maclachlan, Cyclic p-groups of symmetries of surfaces, *Glasgow Math. J.*, **33** (1991), 213–221.

8. M. Liebeck and J. Saxl, Minimal degrees of primitive permutation groups, with an application to monodromy groups of covers of Riemann surfaces, *Proc. London Math. Soc.*, (3) **63** (1991), 266–315.

9. G. A. Miller, On the groups generated by two operators, *Bull. Amer. Math. Soc.*, **7** (1901), 424–426.

10. J-P. Serre, Groupes de Galois sur $\mathbb{Q}$, *Astérisque*, **161–162** (1988), 73–85.

11. R. Steinberg, Generators for simple groups, *Canad. J. Math.*, **14** (1962), 277–283.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF SOUTHAMPTON
SOUTHAMPTON SO9 5NH
ENGLAND