

# AN EXTENSION OF A THEOREM OF KUROSH AND APPLICATIONS TO FUCHSIAN GROUPS

Ravi S. Kulkarni

**1. Introduction.** A well known theorem of Kurosh (cf. [10, §34], [13, ch. 7], or [12] and the references there) elucidates the structure of a subgroup of a free product as a free product of factors of certain specified types. If the Euler characteristics (cf. [3], [4]) of the groups in question can be defined, then the generalized Riemann–Hurwitz formula imposes a further limitation for subgroups of finite index on the frequency of occurrence of factors of these various types. In the special case of noncompact Fuchsian groups there is a further limitation coming from the consideration of “genus and cusps”. However, these obvious necessary conditions do *not* ensure the existence of a subgroup of a specified type. From the covering space interpretation of Kurosh’s theorem we derive a further necessary Diophantine condition and show that this condition, in conjunction with the previously noted conditions, is necessary and sufficient for the existence of a subgroup of a given type.

Throughout the paper  $F_r$  denotes a free group of rank  $r$  and  $\prod^*$  denotes a free product of groups.

The extension of Kurosh’s theorem referred to in the title is the following.

**THEOREM 1.** *Let  $\Gamma_i$  be groups and  $\Phi_{ij}$  be subgroups of  $\Gamma_i$  of indices  $d_{ij}$  where  $1 \leq i \leq n$ ,  $1 \leq j \leq r_i$ . Let  $\Gamma = \prod_i^* \Gamma_i$  and  $\Phi = F_r * \prod_{i,j}^* \Phi_{ij}$ . Then  $\Phi$  occurs as a subgroup of finite index  $d$  if and only if*

- (1) *(the degree condition),  $d = \sum_{j=1}^{r_i} d_{ij}$ ,  $i=1, 2, \dots, n$ , and*
- (2) *(the connectedness condition),  $d(n-1) - \sum_{i=1}^n r_i + 1 = r$ .*

The implication for Fuchsian groups is the following.

**THEOREM 2.** *Let  $\Gamma = F_t * \prod_i^* \mathbf{Z}_{n_i}$ ,  $1 \leq i \leq k$  and  $\Phi = F_s * \prod_u^* \mathbf{Z}_{m_u}$ ,  $1 \leq u \leq L$ . Assume that  $m_1, \dots, m_l$  is a maximal set of distinct  $m_u$ ’s and each  $m_q$  occurs  $b_q$  times,  $1 \leq q \leq l$ . Let  $d$  be a positive integer. Then  $\Phi$  can be embedded in  $\Gamma$  as a subgroup of index  $d$  if and only if*

- ( $\alpha$ ) *(the torsion condition), each  $m_q$  divides some  $n_i$ ,*
- ( $\beta$ ) *(the R.H. condition),*

$$\sum_u \frac{1}{m_u} - L - s + 1 = d \left\{ \sum_i \frac{1}{n_i} - k - t + 1 \right\},$$

- ( $\gamma$ ) *(the end condition),  $t \leq s$ , and*
- ( $\delta$ ) *(the Diophantine condition), let  $m_0 = 1$  and set*

---

Received March 9, 1982. Revision received March 21, 1983.

The author was partially supported by an NSF grant and a Guggenheim fellowship. Michigan Math. J. 30 (1983).

$$\epsilon_{iq} = \begin{cases} 0 & \text{if } m_q \nmid n_i \\ 1 & \text{if } m_q \mid n_i \end{cases}, \quad \delta_{iq} = \frac{n_i}{m_q} \epsilon_{iq};$$

then the system

$$(i) \sum_i \epsilon_{iq} x_{iq} = b_q, \quad 1 \leq i \leq k, \quad 1 \leq q \leq l,$$

$$(ii) \sum_q \delta_{iq} x_{iq} = d, \quad 1 \leq i \leq k, \quad 0 \leq q \leq l.$$

has a solution for  $x_{iq}$ 's in nonnegative integers.

The R.H. condition can be stated more succinctly as  $\chi(\Phi) = d\chi(\Gamma)$ , where  $\chi$  denotes the Euler characteristic of a group (cf. [3], [4] and the references there). Note also that if  $t=0$  the end condition is vacuous. The use of the Diophantine condition is illustrated in §5 where I have classified subgroups of finite index in  $\mathbf{Z} * \mathbf{Z}_n$  or  $\mathbf{Z}_p * \mathbf{Z}_q$  where  $p, q$  are primes. In particular, for the modular group ( $p=2, q=3$ ) the result is that every finite free product of a free group,  $\mathbf{Z}_2$ 's and  $\mathbf{Z}_3$ 's different from  $\mathbf{Z}$ ,  $\mathbf{Z}_2$ ,  $\mathbf{Z}_3$  or  $\mathbf{Z}_2 * \mathbf{Z}_2$  occurs as a subgroup of finite index. This follows from [16] but, curiously, to the best of my knowledge this result does not appear in the classical treatises of this vast subject. More general results of this type will appear in [8].

The Diophantine condition is really a formalization of the *diagrams* introduced in §4. These diagrams provide an alternative to the use of fundamental domains (cf. [11], [14]) or the permutation method (cf. [15], [16], [18], [19]) or the coset graphs (cf. [2, p. 15] or [21]). In Appendix 1, I bring the diagrams closer to their 2-dimensional aspects and discuss congruence subgroups and Petersson's cycloidal groups in terms of the "thickened" diagrams.

In general it is difficult to describe the precise set of solutions of the Diophantine system ( $\delta$ ). In Appendix 2 I have given a generating function and a systematic method of obtaining solutions in nonnegative integers of a linear Diophantine system with nonnegative coefficients. The generating function turns out to be a *rational* function. It may be remarked that certain types of generating functions available in the literature are readily deduced from the general algorithm of Appendix 2.

A final remark: Theorem 2 completely leaves aside the question of recognizing a *normal* subgroup of finite index. This problem has an additional arithmetic aspect which goes considerably deeper. Secondly, the analogue of Theorem 2 for cocompact Fuchsian groups is false. It is valid for *torsion-free* subgroups (cf. [6], [7]). In these papers (and in [8], [9]), further algebraic and geometric methods are developed to deal with not necessarily torsion-free subgroups and normal subgroups of finite index in cocompact Fuchsian groups.

ACKNOWLEDGMENT. I am grateful to R. Lyndon for guiding me to the existing literature, for detailed comments on the first draft of this paper and for simplifying some proofs.

**2. Proof of Theorem 1.** Let  $X_i$  be a connected CW-complex with  $\prod_1 (X_i, x_i) \approx \Gamma_i$ . Let  $e_i$ ,  $1 \leq i \leq n$ , be  $n$  copies of the unit interval  $[0, 1]$ . Construct a complex  $A$  from  $\bigcup_i e_i$  by identifying the initial endpoints to a single point called 0, and

construct  $X$  from  $A \cup X_1 \cup \cdots \cup X_n$  by identifying the final endpoint of  $e_i$  with the basepoint  $x_i$  of  $X_i$ . Clearly  $\Pi_1(X, 0) \approx \Pi^* \Gamma_i$ . We are going to show the existence of a subgroup  $\approx \Phi$  by constructing an appropriate connected covering  $\tilde{X}$  of  $X$ . Let  $p_{ij}: \tilde{X}_{ij} \rightarrow X_i$  be the covering corresponding to the subgroup  $\Phi_{ij}$  of  $\Gamma_i$ . Then  $p_{ij}^{-1}(x_i)$  consists of  $d_{ij}$  points  $\{\tilde{x}_{ij}\}$ . Let  $B_0$  be the union of  $d$  disjoint copies  $A_1, A_2, \dots, A_d$  of  $A$ . So  $B_0$  has  $d$  components and  $d$  edges with index  $i$ ,  $1 \leq i \leq n$ . Out of the  $d$  edges with index 1 choose any subset of  $d_{1j}$  edges and attach their final endpoints to  $\tilde{X}_{1j}$ , at  $\tilde{x}_{1j}$ ,  $j=1, 2, \dots, r_1$ . The resulting complex  $B_1$  now has  $d - \sum_j (d_{1j} - 1)$  components. Now attach  $d_{2j}$  edges indexed 2 to  $\tilde{X}_{2j}$  at  $\tilde{x}_{2j}$  choosing the edges from *different* components of  $B_1$  as far as possible. The resulting complex  $B_2$  has

$$(2.1) \quad \max \left( 1, d - \sum_{j=1}^{r_1} (d_{1j} - 1) - \sum_{j=1}^{r_2} (d_{2j} - 1) \right)$$

components. Continuing this way we obtain a complex  $B_n = \tilde{X}$  with

$$(2.2) \quad \max \left( 1, d - \sum_{i,j} (d_{ij} - 1) \right)$$

components. The second term in the above bracket is  $-d(n-1) + \sum_{i=1}^n r_i$  since by assumption  $\sum_j d_{ij} = d$  for  $i=1, 2, \dots, n$ . Now condition (2) in the theorem ensures that  $-d(n-1) + \sum_{i=1}^n r_i \leq 1$ . So  $\tilde{X}$  is connected.

Now there is an obvious  $d$ -fold covering map  $p: \tilde{X} \rightarrow X$  and  $\Pi_1(\tilde{X}) \approx \Pi_{i,j}^* \Phi_{ij} * F_s$  where  $s$  is determined as follows. Let  $\tilde{Y}$  be the complex obtained from  $\tilde{X}$  by collapsing each  $\tilde{X}_{ij}$  to a point. Then  $\Pi_1(\tilde{Y}) \approx F_s$ . Now  $\tilde{Y}$  may be considered as obtained from  $B_0$  by identifying the endpoints of  $d_{1j}$  edges with index 1,  $j=1, 2, \dots, r_1$ , then identifying the endpoints of  $d_{2j}$  edges with index 2,  $j=1, 2, \dots, r_2$  choosing the edges from *different* components as far as possible, and so on. In this process each identification of endpoints initially reduces the number of components by one, and until one obtains precisely one component the resulting complexes are unions of trees. After one has obtained precisely one component, any further identification introduces a loop and  $s$  is precisely the number of these latter identifications. So

$$(2.3) \quad 1 - \left\{ d - \sum_{i,j} (d_{ij} - 1) \right\} = s$$

or  $s = d(n-1) - \sum_{i=1}^n r_i + 1$  which equals  $r$  from condition (2).

Conversely, given the groups  $\Gamma_i$  and subgroups  $\Phi_{ij}$  of  $\Gamma_i$  of index  $d_{ij}$  and a subgroup  $\Phi \approx F_r * \Pi_{i,j} \Phi_{ij}$  of index  $d$  in  $\Gamma \approx \Pi^* \Gamma_i$ , construct a complex  $X$  as above with  $\Pi_1(X) \approx \Gamma$  and take the cover  $\tilde{X} \xrightarrow{p} X$ , corresponding to  $\Phi$ . Then  $p^{-1}(e_i)$  consists of  $d$  edges, and their distribution among the subspaces of  $\tilde{X}$  which are covering spaces of  $X_i$  corresponding to  $\Phi_{ij}$ 's gives the condition (1). Collapse  $\tilde{X}$  to  $\tilde{Y}$  as above.  $\tilde{Y}$  is a graph with  $dn$  edges. The argument in the last paragraph shows that  $d + \sum_{i=1}^n r_i - 1$  edges form a maximal tree so the difference  $dn - \{d + \sum_{i=1}^n r_i - 1\}$  is simply the rank of the free part.  $\square$

### 3. Proof of Theorem 2.

(3.1) *Necessity of  $(\alpha)$ ,  $(\beta)$ ,  $(\gamma)$ ,  $(\delta)$* : For definiteness consider  $F_l$  as a free product of  $\mathbf{Z}(i) \approx \mathbf{Z}$ ,  $i = k+1, \dots, k+t$  and thus  $\Gamma$  is a free product of  $k+t$  groups. Form the complex  $X$  as in the proof of Theorem 1 so that  $\prod_1(X) \approx \Gamma$ . For  $i = k+1, \dots, k+t$  we take  $X_i$  to be a circle. Let  $p: \tilde{X} \rightarrow X$  be the covering corresponding to  $\Phi$ .

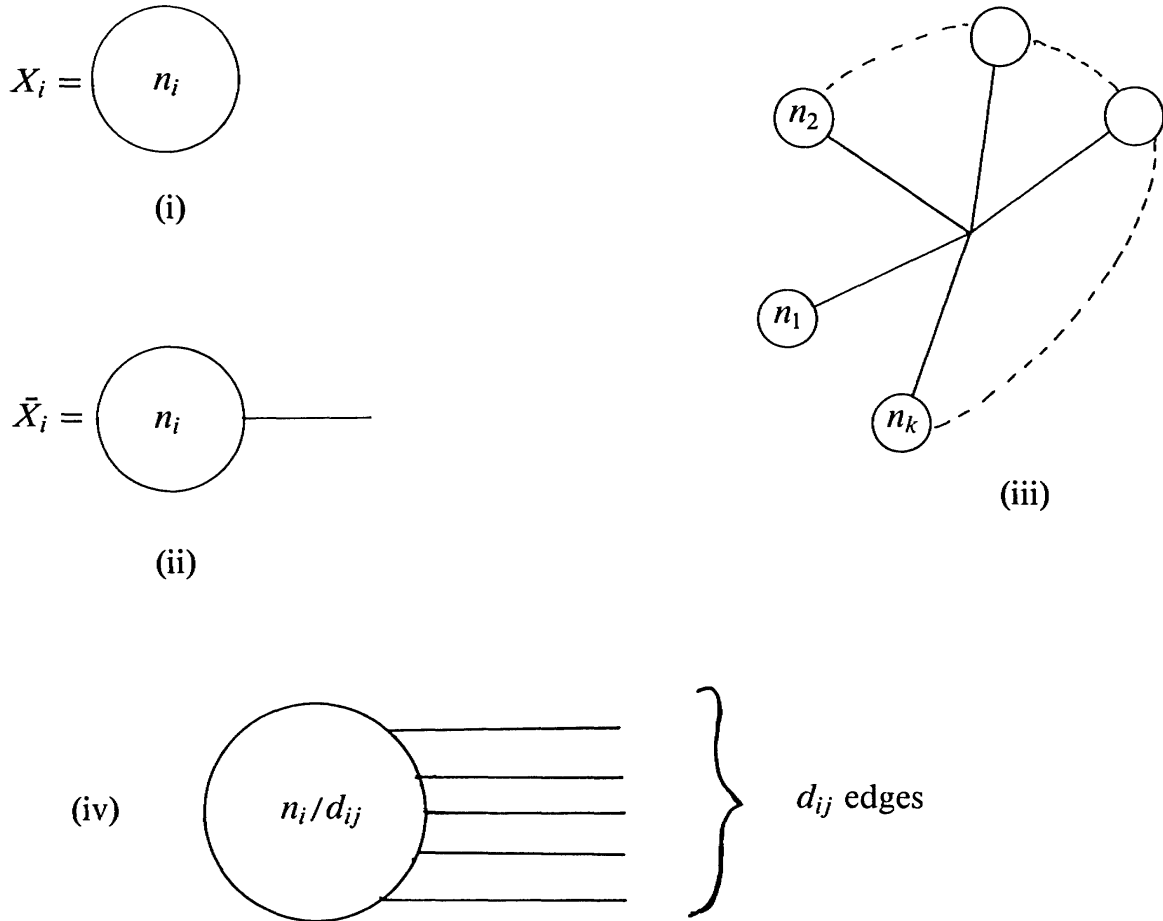
The necessity of the torsion condition  $(\alpha)$  is clear. The necessity of the R.H. condition and the end condition are also clear from the Riemann surface theory. (Strictly from the "1-dimensional" viewpoint the R.H. condition may be proved along the lines of [4]. As for the end condition note that each component of  $p^{-1}(X_i)$ ,  $i = k+1, \dots, k+t$ , is a circle which contributes at least one factor to the free part  $F_s$  of  $\Phi$ . So  $t \leq s$ .) Finally let  $x_{iq}$  be the number of components of  $p^{-1}(X_i)$ ,  $i = 1, 2, \dots, k$ , which have fundamental group isomorphic to  $\mathbf{Z}_{m_q}$ ,  $q = 0, 1, \dots, l$ . (For  $q = 0$ ,  $m_q = 1$  and  $\mathbf{Z}_{m_q} = (0)$ .) Condition (i) of  $(\delta)$  follows since by assumption  $m_q$ ,  $q > 0$  occurs  $b_q$  times. Now condition (ii) of  $(\delta)$  is simply condition (1) of Theorem 1.

(3.2) *Sufficiency of the conditions*: It suffices to reduce to the situation of Theorem 1. Let  $x_{iq} = x_{iq}^0$  be a nonnegative integral solution of the Diophantine system. Let  $n = k+t$ ,  $r_i = \sum_{q=0}^l \epsilon_{iq} x_{iq}^0$  for  $i = 1, 2, \dots, k$ . For  $i = k+1, \dots, k+t$  let  $r_i$  be any positive integers  $\leq d$  such that  $r = s - \sum_{i=k+1}^{k+t} r_i \geq 0$ . This is possible by condition  $(\gamma)$ , with at worst  $r_i = 1$ . For  $i = 1, 2, \dots, k$ ,  $j = 1, 2, \dots, r_i$   $d_{ij}$ 's are taken to be  $\delta_{iq}$ 's repeating  $x_{iq}^0$  times. For  $i = k+1, \dots, k+t$ ,  $j = 1, 2, \dots, r_i$ ,  $d = \sum_{j=1}^{r_i} d_{ij}$  are taken to be any partition of  $d$  with  $r_i$  positive terms. With these definitions of  $n, d, d_{ij}, r_i$ , condition (1) of Theorem 1 is a consequence of condition (ii) of  $(\delta)$  and the definitions of  $r_i$  and  $d_{ij}$ 's for  $i > k$ . It remains to show condition (2) of Theorem 1 for which, as is expected, condition  $(\beta)$  must play a crucial role. Notice first that by (ii) of  $(\delta)$

$$\begin{aligned}
 \sum_{i=1}^k x_{i0}^0 &= \sum_{i=1}^k \frac{1}{n_i} \left\{ d - \sum_{q=1}^l \delta_{iq} x_{iq}^0 \right\} = d \left\{ \sum_{i=1}^k \frac{1}{n_i} \right\} - \sum_{q=1}^l \frac{1}{m_q} \left\{ \sum_{i=1}^k \epsilon_{iq} x_{iq}^0 \right\} \\
 &= d \left\{ \sum_{i=1}^k \frac{1}{n_i} \right\} - \sum_{q=1}^l \frac{b_q}{m_q} \quad \text{by (i) of } (\delta) \\
 &= d \left\{ \sum_{i=1}^k \frac{1}{n_i} \right\} - \sum_{u=1}^L \frac{1}{m_u} \\
 &= d(k+t-1) - (L+s-1) \quad \text{by } (\beta).
 \end{aligned}
 \tag{3.2.1}$$

So the left-hand side of condition (2) of Theorem 1 is

$$\begin{aligned}
 d(k+t-1) - \sum_{i=1}^{k+t} r_i + 1 &= d(k+t-1) - \sum_{i=1}^k x_{i0}^0 - \sum_{q=1}^l \epsilon_{iq} x_{iq}^0 - \sum_{i=k+1}^{k+t} r_i + 1 \\
 &= d(k+t-1) - \sum_{i=1}^k x_{i0}^0 - \sum_{q=1}^l b_q + (r-s) + 1 \\
 &= d(k+t-1) - \sum_{i=1}^k x_{i0}^0 - (L+s-1) + r = r. \quad \square
 \end{aligned}
 \tag{3.2.2}$$



**4. Diagrams.** (4.1) Let  $\Gamma = \prod^* \mathbf{Z}_{n_i}$ ,  $1 \leq i \leq k$  where if  $n_i = 0$  then  $\mathbf{Z}_0$  stands for  $\mathbf{Z}$ . Let  $X_i$  be a space with fundamental group  $\mathbf{Z}_{n_i}$ , symbolically represented as in Figure (i). Let  $\bar{X}_i$  be  $X_i$  with an edge attached as in Figure (ii). The complex  $X$  in the proof of Theorem 1 may then be represented as in Figure (iii). If  $m_j$  divides  $n_i$  then the covering of  $\bar{X}_i$  with fundamental group  $\mathbf{Z}_{m_j}$  has degree  $d_{ij} = n_i/m_j$  and is represented as in Figure (iv). A covering of  $X$  corresponding to a subgroup  $\Phi$  of  $\Gamma$  is then built out of the spaces of type (iv).

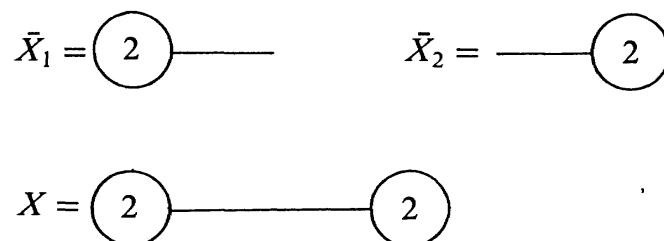
(4.2) EXAMPLE. Let  $\Gamma$  be the infinite dihedral group. So

$$\Gamma = \langle a, b | a^2 = b^2 = 1 \rangle = \langle c, a | a^2 = (ca)^2 = 1 \rangle, \quad c = ab.$$

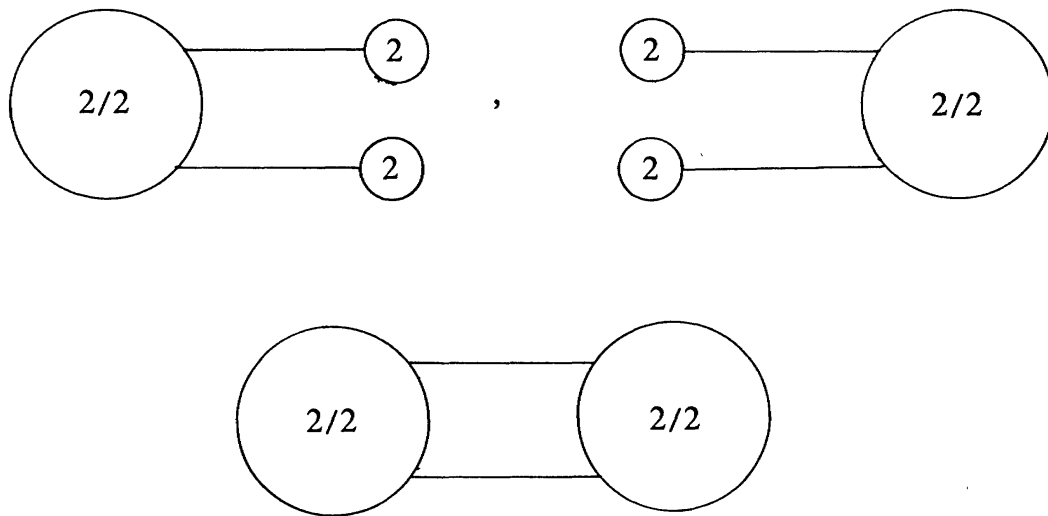
It has three index 2 subgroups, namely,

$$\langle c \rangle \approx \mathbf{Z}, \quad \langle b, aba \rangle = \langle b, c^2 \rangle \approx \Gamma, \quad \langle a, bab \rangle = \langle a, c^2 \rangle \approx \Gamma.$$

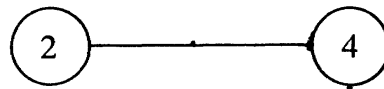
This information is readily read from the diagrams




The three degree 2 coverings of  $X$  are



(4.3) The independence of condition  $(\delta)$  from  $(\alpha)$ ,  $(\beta)$ ,  $(\gamma)$  in general can be easily seen from the diagrams. As an example take  $\Gamma = \mathbf{Z}_2 * \mathbf{Z}_4$ ,  $\Phi = \mathbf{Z}_4 * \mathbf{Z}_4 * \mathbf{Z}_4$ . Then  $\chi(\Phi) = -5/4 = 5\chi(\Gamma)$ . But  $\Phi$  does not embed as a subgroup of finite index in  $\Gamma$ . Indeed, if it does the index has to be 5. But in any 5-fold connected cover of



at least one  must occur which would contribute a factor  $\mathbf{Z}_2$  to the subgroup.

(4.4) REMARK. The reader may find it useful to work out the special cases of the theorems in the next section by means of these diagrams. While it will be difficult to give a satisfactorily complete proof based on diagrams alone, the special cases which can be treated easily by means of the diagrams lead to the heart of the matter.

In Appendix 1 we shall explain the 2-dimensional aspects of the diagrams.

## 5. Examples.

(5.1) THEOREM. Let  $p, q$  be distinct primes,  $\Gamma = \mathbf{Z}_p * \mathbf{Z}_q$  and  $\Phi$  a free product of  $s$  copies of  $\mathbf{Z}$ ,  $a$  copies of  $\mathbf{Z}_p$  and  $b$  copies of  $\mathbf{Z}_q$ . Then  $\Phi$  embeds in  $\Gamma$  as a subgroup of finite index if and only if  $\chi(\Phi)/\chi(\Gamma)$  is a positive integer.

*Proof.* Note that since  $p, q$  are distinct primes  $\chi(\Gamma) < 0$ . We have

(i)  $\chi(\Gamma) = (1/p) + (1/q) - 1$ .

(ii)  $\chi(\Phi) = (a/p) + (b/q) - (a + b + s - 1)$ .

Let  $\chi(\Phi)/\chi(\Gamma) = d$  which is a positive integer by hypothesis. The Diophantine system  $(\delta)$  of Theorem 2 in this case has the following form:

$$(5.1.1) \quad \begin{aligned} x_{11} &= a, & x_{22} &= b \\ px_{10} + x_{11} &= d = qx_{20} + x_{22}. \end{aligned}$$

So the problem amounts to whether  $(d-a)/p$ ,  $(d-b)/q$  are nonnegative integers. By symmetry we show this for  $(d-a)/p$  only. Now

$$\begin{aligned} d-a &= \left\{ \frac{a}{p} + \frac{b}{q} - (a+b+s-1) \right\} \left/ \left\{ \frac{1}{p} + \frac{1}{q} - 1 \right\} \right. - a \\ &= p\{a+qs+qb-b-q\}/pq-p-q \end{aligned}$$

from which the assertion follows. The result follows by Theorem 2.  $\square$

(5.2) COROLLARY. (Classification of subgroups of finite index in the non-homogeneous modular group). Let  $\Gamma = \text{PSL}_2(\mathbf{Z}) \approx \mathbf{Z}_2 * \mathbf{Z}_3$ , and  $\Phi = \Phi_{s,a,b}$  the free product of a free group of rank  $s$ ,  $a$  copies of  $\mathbf{Z}_2$  and  $b$  copies of  $\mathbf{Z}_3$ . Then  $\Phi$  is a subgroup of  $\Gamma$  of finite index if and only if  $\Phi \neq \mathbf{Z}, \mathbf{Z}_2, \mathbf{Z}_3, \mathbf{Z}_2 * \mathbf{Z}_2$ , i.e. if and only if  $6s+3a+4b-6 > 0$ .

*Proof.* Here  $\chi(\Gamma) = -1/6$ ,  $\chi(\Phi) = -(6s+3a+4b-6)/6$ . So  $\chi(\Phi)/\chi(\Gamma)$  is always an integer. The excluded cases are precisely the ones where this integer  $\leq 0$ .  $\square$

(5.3) COROLLARY. (Classification of subgroups of finite index in the homogeneous modular group). Let  $\Gamma = \text{SL}_2(\mathbf{Z})$  and  $\tilde{\Phi} = \tilde{\Phi}_{s,a,b}$  be the unique  $\mathbf{Z}_2$ -central extension of  $\Phi_{s,a,b}$  appearing in (5.2) which restricts to the nontrivial extension on each  $\mathbf{Z}_2$ -factor (if any) in  $\Phi_{s,a,b}$ . Every subgroup of finite index in  $\Gamma$  is isomorphic to  $\tilde{\Phi}_{s,a,b}$ ,  $6s+3a+4b-6 > 0$  or to  $\Phi_{s,0,b}$ ,  $6s+4b-6 > 0$ .

*Proof.*  $\text{SL}_2(\mathbf{Z})$  has a unique element of order 2 which is central. Let  $p: \text{SL}_2(\mathbf{Z}) \rightarrow \text{PSL}_2(\mathbf{Z})$  be the canonical projection. If  $\psi$  is a subgroup of finite index in  $\Gamma$  then  $\psi$  has index  $\leq 2$  in  $p^{-1}(p(\psi))$ . If  $p(\psi) = \Phi_{s,a,t}$  then  $p^{-1}(\psi) \approx \tilde{\Phi}_{s,a,b}$ . If  $a > 0$  the extension does not split so  $\psi = \tilde{\Phi}_{s,a,b}$ . If  $a = 0$  the extension splits so  $\psi \approx \tilde{\Phi}_{s,0,b} \cong \Phi_{s,0,b} \times \mathbf{Z}_2$  or  $\psi \approx \Phi_{s,0,b}$ .  $\square$

(5.4) THEOREM. Let  $\Gamma = \mathbf{Z} * \mathbf{Z}_n$ ,  $m_1, \dots, m_l$  distinct divisors of  $n$  different from 1 and  $d_q = n/m_q$ ,  $q = 1, 2, \dots, l$ . Let  $\Phi$  be a free product of  $s$  copies of  $\mathbf{Z}$  and  $a_q$  copies of  $\mathbf{Z}_{m_q}$ ,  $q = 1, 2, \dots, l$ . Then  $\Phi$  can be embedded as a subgroup of  $\Gamma$  of finite index if and only if

- (i)  $\chi(\Phi)/\chi(\Gamma) = d$  is a positive integer, and
- (ii)  $s \geq \sum_{q=1}^l (d_q - 1)a_q + 1$ .

*Proof.* Condition (i) is clear. The Diophantine system  $(\delta)$  of Theorem 2 in this case has the form

- (1)  $x_{1q} = a_q$ ,  $q = 1, 2, \dots, l$ ,
- (2)  $nx_{10} + \sum_{q=1}^l d_q a_q = d$ .

So a necessary and sufficient condition for  $\Phi$  to be a subgroup of  $\Gamma$  of finite index is just  $x_{10} \geq 0$ , i.e.

$$\begin{aligned}
0 &\leq d - \sum_{q=1}^l d_q a_q \\
&= \left\{ \sum_{q=1}^l \frac{a_q}{m_q} - \left( s + \sum_{q=1}^l a_q - 1 \right) \right\} \left/ \left\{ \frac{1}{n} - 1 \right\} \right. - \sum_{q=1}^l d_q a_q \\
&= \left\{ n \left( s + \sum_{q=1}^l a_q - 1 \right) - \sum_{q=1}^l d_q a_q \right\} \left/ (n-1) \right. - \sum_{q=1}^l d_q a_q \\
&= \frac{n}{n-1} \left\{ s - \sum_{q=1}^l (d_q - 1) a_q - 1 \right\}.
\end{aligned}$$

Hence condition (ii) holds.  $\square$

(5.5) COROLLARY. Let  $\Gamma = \mathbf{Z} * \mathbf{Z}_p$  where  $p$  is a prime. Let  $\Phi = \Phi_{s,a}$  denote a free product of  $s$  (resp.  $a$ ) copies of  $\mathbf{Z}$  (resp.  $\mathbf{Z}_p$ ). Then  $\Phi$  can be realized as a subgroup of finite index in  $\Gamma$  if and only if  $(s, a) \neq (1, 0)$ ,  $s \geq 1$  and  $(p-1)$  divides  $(s-1)$ .

*Proof.* Condition (ii) of (5.4) reduces to  $s \geq 1$ . Condition (i) becomes:

$$\left\{ \frac{a}{p} - (a+s-1) \right\} \left/ \left\{ \frac{1}{p} - 1 \right\} \right. = \frac{p(a+s-1) - a}{p-1} = a+s-1 + \frac{s-1}{p-1}$$

is a positive integer. Since  $s \geq 1$ , this is clearly equivalent to  $(s, a) \neq (1, 0)$  and  $(p-1)$  divides  $(s-1)$ .  $\square$

(5.6) THEOREM. Let  $\Gamma = \mathbf{Z}_p * \mathbf{Z}_p$ , where  $p$  is a prime  $\geq 3$ , and  $\Phi = \Phi_{s,a}$  a free product of  $s$  (resp.  $a$ ) copies of  $\mathbf{Z}$  (resp.  $\mathbf{Z}_p$ ). Then  $\Phi$  can be realized as a subgroup of finite index in  $\Gamma$  if and only if

- (i)  $(s, a) \neq (1, 0)$  or  $(0, 1)$ , and  $p-2$  divides  $a+2s-2$ , and
- (ii)  $a$  is not an odd integer less than  $p$ .

*Proof.* We have  $\chi(\Phi) = (a/p) - (a+s-1)$  and  $\chi(\Gamma) = (2/p) - 1$ . Condition (i) is equivalent to:  $\chi(\Phi)/\chi(\Gamma) = d$  is a positive integer. This condition can also be written as  $(2d-a)(1-(1/p)) = d+s-1$ . So  $a \leq 2d$ ,  $a \equiv 2d(p)$ . Set  $a = 2d - ep$ ,  $e \geq 0$ . System  $(\delta)$  becomes, writing  $x_1 = x_{11}$ ,  $x_2 = x_{21}$ ,  $y_1 = x_{10}$ ,  $y_2 = x_{20}$ ,

$$(5.6.1) \quad \begin{cases} x_1 + x_2 = a \\ py_1 + x_1 = d \\ py_2 + x_2 = d. \end{cases}$$

*Case 1.*  $a < p$ : A solution of (5.6.1) in nonnegative integers requires  $0 \leq x_i \leq a < p$ ,  $x_1 \equiv x_2(p)$  so  $x_1 = x_2$  and  $a$  is even. If  $a = 2b$  then  $2b = 2d - ep$ ,  $p$  divides  $(d-b)$ , so  $d-b = py$ , where  $y$  is a positive integer. Then  $x_1 = x_2 = b$ ,  $y_1 = y_2 = y$  is a solution.

*Case 2.*  $a \geq p$ : Let  $d \equiv d_0(p)$ ,  $0 \leq d_0 < p$ ,  $d = d_0 + gp$ ,  $g \geq 0$ . Then  $a = 2d - ep = 2d_0 + fp$  where  $f = 2g - e \geq 0$ , so  $f \leq 2g$ . Let  $f = f_1 + f_2$ ,  $0 \leq f_1, f_2 \leq g$ ,  $x_i = d_0 + f_i p$ ,  $y_i = g - f_i$ ; then



$$x_1 + x_2 = 2d_0 + p(f_1 + f_2) = 2d_0 + fp = a,$$

$$y_i p + x_i = (g - f_i)p + d_0 + f_i p = d_0 + gp = d, \quad i = 1, 2.$$

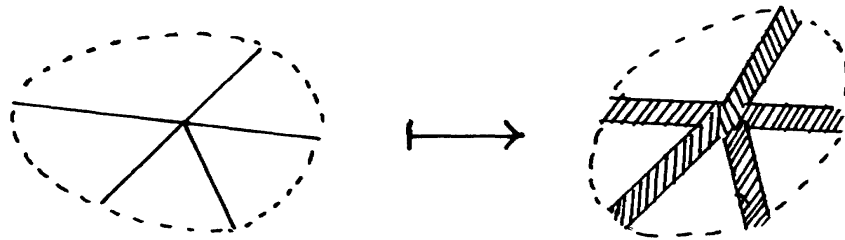
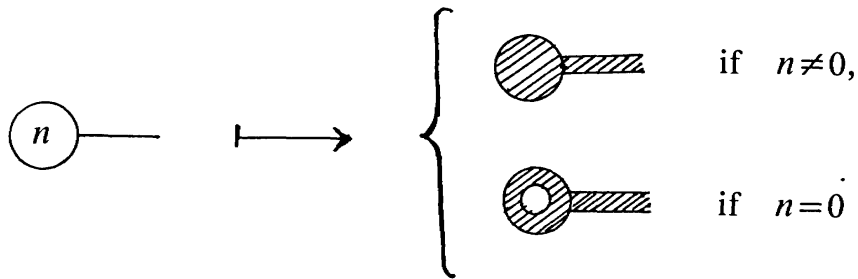
So (5.6.1) has a solution.

This finishes the proof.  $\square$

### Appendix 1: More on diagrams.

(A1.1) 2-DIMENSIONAL ASPECTS. Let  $\Gamma = F_t * \prod_{i=1}^k \mathbf{Z}_{n_i}$ . If  $\Gamma$  is realized as a Fuchsian group, it acts topologically as a properly discontinuous group on  $\mathbf{R}^2$ . Let  $\tilde{p}: \mathbf{R}^2 \rightarrow \Gamma \backslash \mathbf{R}^2 = N$  be the canonical projection which is a branched covering. Let  $N$  have genus  $g$  and  $\epsilon$  (necessarily  $\geq 1$ ) ends. Then  $t = 2g + \epsilon - 1$ . Moreover  $N$  has a set  $B$  of precisely  $k$  branch points,  $x_1, \dots, x_k$  of branching indices  $n_1, \dots, n_k$ . The invariants  $\{g; n_1, \dots, n_k; \epsilon\}$  are invariants of the topological action of  $\Gamma$ . If  $\Phi$  is a subgroup of finite index in  $\Gamma$ ,  $\Phi \backslash \mathbf{R}^2 = M$ , then the canonical projection  $p: M \rightarrow N$  is a branched covering which may be regarded as a subcovering of the universal branched covering  $\tilde{p}$ . The invariants of  $p: M \rightarrow N$  regarded as such a sub-branched covering include, in addition to those of  $N$ : the genus of  $M$ ; the branch data, i.e., local degrees of  $p$  at the points in  $p^{-1}(B)$ ; and the endsplits, i.e., the local degrees of  $p$  at the ends of  $M$  which all must lie over ends of  $N$ . (For  $\Gamma =$  the modular group there is only one end—which is geometrically a cusp—so one talks about a “cusp split” of a subgroup of the modular group. I am thankful to Raghavan and Rangachari for patiently explaining to me parts of the classical theory of the modular group.)

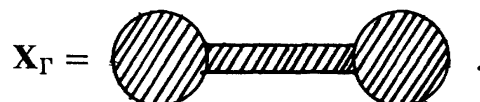
These 2-dimensional aspects can also be read from the diagrams provided we thicken them in an appropriate way. Indeed, for definiteness let  $\Gamma = F_t * \prod_{i=1}^k \mathbf{Z}_{n_i}$  be realized as a Fuchsian group with genus 0, and  $\Phi$  a subgroup of finite index in  $\Gamma$ . Thicken each subcomplex described in §4 as shown:



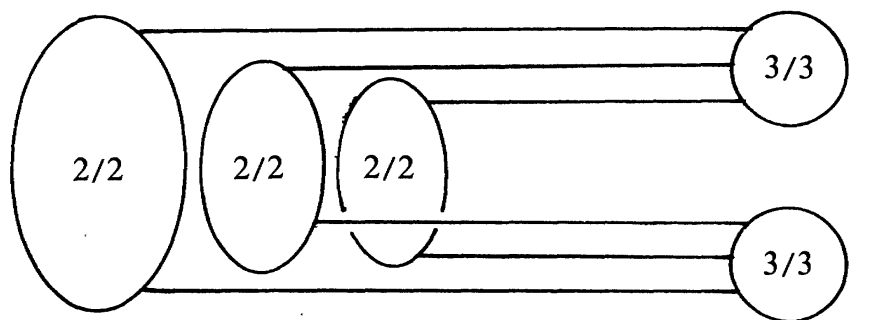
We then get compact surfaces with boundary which we denote by  $\mathbf{X}_\Gamma$  and  $\mathbf{X}_\Phi$ , respectively. Corresponding to  $\Gamma$  we have a sphere with  $t+1$  open disks removed. If we remove the boundaries in  $p: \mathbf{X}_\Phi \rightarrow \mathbf{X}_\Gamma$  this is just the branched covering  $p: M \rightarrow N$  considered above.

The number of “cusps” of a subgroup  $\Phi$  is evidently the number of boundary components of  $\mathbf{X}_\Phi$ . The “cusp split” can be determined by counting the number of times a boundary component of  $\mathbf{X}_\Phi$  wraps around a boundary component of  $\mathbf{X}_\Gamma$ .

(A1.2) EXAMPLE.  $\Gamma = \mathbf{Z}_2 * \mathbf{Z}_3 \approx \mathrm{PSL}_2(\mathbf{Z})$ . Then



A look at the diagrams shows that all subgroups of index  $\leq 5$  have genus 0. Among the 8 distinct conjugacy classes of subgroups of index 6 all but one have genus 0. The exception occurs for the diagram which has genus 1. It corresponds to the commutator subgroup:

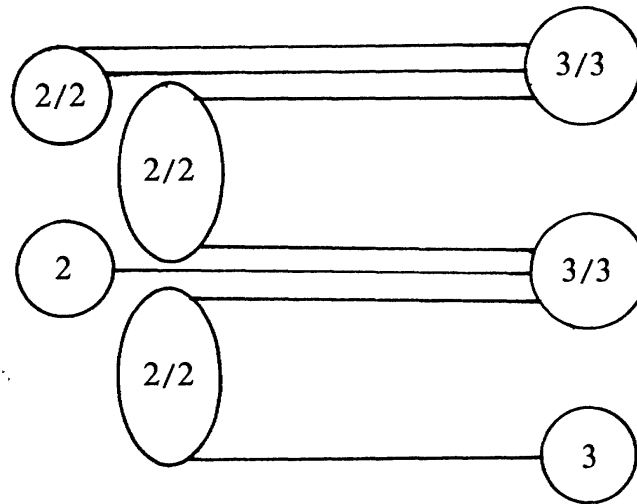


Its thickening clearly shows “the handle”.

(A1.3) CONGRUENCE SUBGROUPS OF  $\mathrm{PSL}_2(\mathbf{Z})$ . A subgroup  $\Phi$  of  $\Gamma = \mathrm{PSL}_2(\mathbf{Z})$  is called a *congruence subgroup* if it contains the kernel of the canonical map  $\rho_n: \mathrm{PSL}_2(\mathbf{Z}) \rightarrow \mathrm{PSL}_2(\mathbf{Z}_n)$  for some  $n$ . A theorem of Wohlfahrt [23] says that  $\Phi$  is a congruence subgroup if and only if  $\Phi \supseteq \ker \rho_n$  where  $n = \text{l.c.m. (cusp split)}$ .

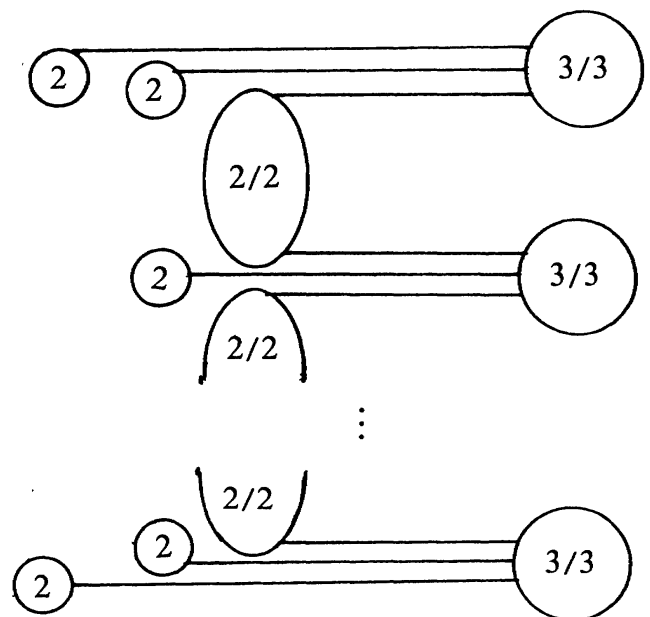
Given a diagram for a subgroup  $\Phi$  of finite index it is possible to determine whether  $\Phi$  is a congruence subgroup. Indeed one has only (i) to compute  $n = \text{l.c.m. (cusp split)}$ , and (ii) to check whether all the lifts of the loops in the diagram for  $\Gamma$  defined by the relations in the known presentations for  $\mathrm{PSL}_2(\mathbf{Z}_n)$  are again loops (cf. [5], and the references there for such presentations).

Here is a simple argument for the existence of noncongruence subgroups. Indeed, one may check from the diagrams using the above procedure that all subgroups of index  $\leq 6$  are congruence subgroups. Now consider any subgroup of index 7 with 2 cusps (in all there are four conjugacy classes of such subgroups); e.g., one defined by



Here the cusp split is  $(1, 6)$ . So  $n = \text{l.c.m.}(1, 6) = 6$ . If this corresponded to a congruence subgroup,  $\text{PSL}_2(\mathbb{Z}_6)$  would contain a subgroup of index 7. But  $7 \nmid |\text{PSL}_2(\mathbb{Z}_6)|$ , a contradiction.

(A1.4) CYCLOIDAL GROUPS. A subgroup of the modular group is called *cycloidal* if it has only one cusp. Petersson [17] proved that there are infinitely many cycloidal subgroups of genus 0. Without going into further refinements (cf. Millington [15]), let us prove Petersson's statement. Consider the infinite set of diagrams of which one is shown in the figure below. That is, construct diagrams without intertwining edges (as in the diagram in (A.2), for example) and without introducing internal loops. Clearly  $\mathbf{X}_\Phi$  has genus 0 and one boundary component, i.e.,  $\Phi$  is a cycloidal subgroup of genus 0.



I should remark that the diagrams can rarely be used to prove a general state-

ment about subgroups. But they are a useful visual aid for generating data and formulating guesses.

The diagrams in this paper deal only with free products. But similar techniques may be used for amalgamated products, HNN and similar constructions in combinatorial group theory.

**Appendix 2. A generating function for solutions of Diophantine systems in nonnegative integers.** It is difficult to describe the precise set of solutions of the Diophantine system  $(\delta)$  encountered in Theorem 2. The problem is not unlike that of enumerating all partitions of a positive integer which is indeed a special case of the problem considered below. Euler constructed generating functions for various types of partitions (cf. [1]). Here, briefly, we indicate that the same philosophy may be applied to our problem. *The recursive relations derived below from the generating functions may be used to tabulate systematically the solutions of  $(\delta)$  as well as (more easily) to decide the existence of solutions of  $(\delta)$ , at least with the aid of a computer.*

Consider

$$(*) \quad \sum_{j=1}^n a_{ij} x_j = b_i, \quad i = 1, 2, \dots, m,$$

where  $a_{ij}$  and  $b_i$  are nonnegative integers, and the problem is to investigate the solutions of  $(*)$  in nonnegative integers.

Write

$$x = (x_1, \dots, x_n), \quad s = (s_1, \dots, s_n), \quad b = (b_1, \dots, b_m), \quad t = (t_1, \dots, t_m),$$

$$s^x = \prod_{j=1}^n s_j^{x_j}, \quad t^b = \prod_{i=1}^m t_i^{b_i},$$

“ $x \geq 0$ ” or “ $b \geq 0$ ” means that the respective components are nonnegative.

Assume that each column in  $[a_{ij}]$  has a nonzero entry. This assumption ensures that  $(*)$  has at most *finitely many solutions*.

For  $x \geq 0$ ,  $b \geq 0$  set

$$N_x(b) = \begin{cases} 1 & \text{if } x \text{ is a solution of } (*), \\ 0 & \text{otherwise,} \end{cases}$$

$$N(b) = \text{the number of solutions of } (*),$$

$$\sigma(s, t) = \sum_{\substack{x \geq 0 \\ b \geq 0}} N_x(b) s^x t^b, \quad \tau(t) = \sum_{b \geq 0} N(b) t^b.$$

Here  $\sigma$  and  $\tau$  are considered as formal power series, and are called the *solution generating function* and the *solution counting function* respectively.

(A.2.1) MAIN ASSERTION.  $\sigma$  and  $\tau$  are rational functions. In fact,

$$(1) \quad \sigma(s, t) = \prod_{j=1}^n \left\{ \frac{1}{1 - s_j t_1^{a_{1j}}, \dots, t_m^{a_{mj}}} \right\},$$

$$(2) \quad \tau(t) = \prod_{j=1}^n \left\{ \frac{1}{1 - t_1^{a_{1j}}, \dots, t_m^{a_{mj}}} \right\}.$$

*Proof.* Expand the right-hand sides as products of geometric series. Observe also that  $\sigma(1, t) = \tau(t)$ .  $\square$

(A.2.2) RECURSIVE FORMULAS FOR  $N_x(b)$  AND  $N(b)$ .

(1) The  $N_x(b)$ 's are recursively determined as follows.

$$N_{0, \dots, 0}(0, \dots, 0) = 1, \quad N_{x_1, \dots, x_n}(b, \dots, b_m) = 0$$

if some  $x_j < 0$  or  $b_i < 0$ , and for  $x \geq 0$ ,  $b \geq 0$ ,

$$N_{x_1, \dots, x_n}(b_1, \dots, b_m) +$$

$$\sum_{1 \leq u_1 < \dots < u_k \leq n} (-1)^k N_{x_1, \dots, x_{u_1-1}, \dots, x_{u_k-1}, \dots, x_n} \left( b_1 - \sum_{l=1}^k a_{1u_l}, \dots, b_m - \sum_{l=1}^k a_{mu_l} \right) = 0.$$

(2) The  $N(b)$ 's are determined recursively as follows.  $N(0, \dots, 0) = 1$ ,  $N(b_1, \dots, b_m) = 0$  if some  $b_i < 0$ , and for  $b \geq 0$

$$N(b_1, \dots, b_m) + \sum_{1 \leq u_1 < \dots < u_k \leq n} (-1)^k N \left( b_1 - \sum_{l=1}^k a_{1u_l}, \dots, b_m - \sum_{l=1}^k a_{mu_l} \right) = 0.$$

*Proof.* (1) We have

$$\prod_{j=1}^m (1 - s_j t_1^{a_{1j}}, \dots, t_m^{a_{mj}}) \left\{ \sum_{\substack{x \geq 0 \\ b \geq 0}} N_x(b) s^x t^b \right\} = 1.$$

Now equate the coefficients of  $s^x t^b$  on both sides.

(2) Similar to (1).  $\square$

REMARKS. (1) We also know that  $N_x(b) = 0$  or 1. Hence one only needs to know the *parity* of  $N_x(b)$  in applying the recursion formulas.

(2) By the Cauchy integral formula one has

$$N(b) = \frac{1}{(2\pi i)^m} \int \frac{\tau(t)}{\sum_{i=1}^m t_i^{b_i+1}} dt$$

where the integral is taken over the boundary of a polydisk in  $\mathbb{C}^m$  of polyradius  $(r_1, \dots, r_m)$ ,  $\prod_{i=1}^m r_i \neq 1$ .

(3) Certain types of generating functions available in the literature sometimes can be derived quickly from the above algorithm. For example, the generating function of Gaussian polynomials (cf. [1, p. 36]) is the solution counting function of the system

$$(*) \quad \begin{cases} x_0 + x_1 + \dots + x_n = b_1 \\ x_1 + 2x_2 + \dots + nx_n = b_2. \end{cases}$$

## REFERENCES

1. G. E. Andrews, *The theory of partitions*, Addison-Wesley, Reading, 1976.
2. A. O. L. Atkin and H. P. F. Swinnerton-Dyer, *Modular forms on noncongruence subgroups*. Combinatorics (Los Angeles, Calif., 1968), 1–25, Proc. Sympos. Pure Math., XIX, Amer. Math. Soc., Providence, R.I., 1971.
3. H. Bass, *Euler characteristics and characters of discrete groups*, Invent. Math. 35 (1976), 155–196.
4. I. M. Chiswell, *Euler characteristics of groups*, Math. Z. 147 (1976), 1–11.
5. H. S. M. Coxeter and W. O. J. Moser, *Generators and relations for discrete groups*, 4th ed., Springer, Berlin, 1980.
6. A. Edmonds, J. Ewing and R. Kulkarni, *Regular tessellations of surfaces and  $(p, q, 2)$ -triangle groups*, Ann. of Math. 116 (1982), 113–132.
7. ———, *Torsion free subgroups of Fuchsian groups and tessellations of surfaces*, Invent. Math. 69 (1982), 331–346.
8. A. Edmonds, R. Kulkarni and R. E. Stong, *Realizability of branched coverings of surfaces*, Trans. Amer. Math. Soc., to appear.
9. R. Kulkarni, *Normal subgroups of Fuchsian groups*, to appear.
10. A. G. Kurosh, *The theory of groups*, Vol. II, Chelsea, New York, 1960.
11. J. Lehner, *Discontinuous groups and automorphic functions*, Amer. Math. Soc., Providence, R.I., 1964.
12. S. MacLane, *A proof of the subgroup theorem for free products*, Mathematika 5 (1958), 13–19.
13. W. Massey, *Algebraic topology: An introduction*, Harcourt, New York, 1964.
14. H. Maass, *Lectures on modular functions of one complex variable*, Tata Inst. Fund. Res., Bombay, 1964.
15. M. H. Millington, *On cycloidal subgroups of the modular group*, Proc. London Math. Soc. (3) 19 (1969), 164–176.
16. ———, *Subgroups of the classical modular group*, J. London Math. Soc. (2) 1 (1969), 351–357.
17. H. Petersson, *Über einen einfachen Typus von Untergruppen der Modulgruppe*, Arch. Math. 4 (1953), 308–315.
18. R. A. Rankin, *The modular group and its subgroups*, Ramanujan Institute, Madras, 1969.
19. D. Singerman, *Subgroups of Fuchsian groups and finite permutation groups*, Bull. London Math. Soc. 2 (1970), 319–323.
20. W. Wilson Stothers, *Subgroups of the modular group*, Proc. Cambridge Philos. Soc. 75 (1974), 139–153.
21. ———, *Impossible specifications for the modular group*, Manuscripta Math. 13 (1974), 415–428.
22. C. T. C. Wall, *Rational Euler characteristics*, Proc. Cambridge Philos. Soc. 57 (1961), 182–183.
23. K. Wohlfahrt, *An extension of F. Klein's level concept*, Illinois J. Math. 8 (1964), 529–535.

Department of Mathematics  
 Indiana University  
 Bloomington, Indiana 47401