A DESCENT PRINCIPLE IN MODULAR SUBGROUP ARITHMETIC

PETER J. CAMERON AND THOMAS W. MÜLLER

ABSTRACT. We establish and comment on a surprising relationship between the behaviour modulo a prime p of the number $s_n(\mathfrak{G})$ of index n subgroups in a group $\mathfrak{G}$, and that of the corresponding subgroup numbers for a subnormal subgroup of p-power index in $\mathfrak{G}$. One of the applications of this result presented here concerns the explicit determination modulo p of $s_n(\mathfrak{G})$ in the case when $\mathfrak{G}$ is the fundamental group of a finite graph of finite p-groups. As another application, we extend one of the main results of the second author's paper [16] concerning the p-patterns of free powers G^{*q} of a finite group G with q a p-power to groups of the more general form $H * G^{*q}$, where H is any finite p-group.

1. INTRODUCTION

For a group $\mathfrak{G}$ and a positive integer n, denote by $s_n(\mathfrak{G})$ the number of index n subgroups in $\mathfrak{G}$.[1] We call $\mathfrak{G}$ an FSG-*group* if $s_n(\mathfrak{G})$ is finite for all n; for instance, finitely generated groups and groups of finite subgroup rank have this property. Modular subgroup arithmetic, a chapter in the theory of subgroup growth, deals with divisibility properties of the sequence $\{s_n(\mathfrak{G})\}_{n\geq 1}$ or related subgroup counting functions and their connection with the algebraic structure of the underlying group $\mathfrak{G}$; cf. the recent book [10] by Lubotzky and Segal for more background information.

In general, divisibility properties of subgroup counting functions appear to be rather peculiar to the particular group under investigation, and (unlike their growth behaviour) tend to be severely distorted when passing to a subgroup of finite index.

Example. Consider the cartesian map from the modular group $\mathfrak{G} = \mathrm{PSL}_2(\mathbb{Z}) \cong C_2 * C_3$ onto $C_2 \times C_3 \cong C_6$. By a theorem of Nielsen, the kernel of this map is free of rank 2; cf. [11] and [17]. Moreover, by a theorem of Stothers [20],

$$s_n(\mathrm{PSL}_2(\mathbb{Z})) \equiv 1 \bmod 2 \iff n = 2^{\sigma+1} - 3 \text{ or } n = 2(2^{\sigma+1} - 3) \text{ for some } \sigma \geq 1.$$

On the other hand, it follows from M. Hall's recursion formula ([8, Theorem 5.2])

$$s_n(F_r) = n\,(n!)^{r-1} - \sum_{0<\mu<n} \big((n-\mu)!\big)^{r-1} s_\mu(F_r), \quad (n \geq 2, s_1(F_r) = 1)$$

that $s_n(F_2)$ is always odd.

Against this background it is rather surprising that a non-trivial positive result in this direction does in fact exist (see Theorem 1 below). Given a prime p and an FSG-group $\mathfrak{G}$, define the

[1] The reader should be warned that, in the literature on subgroup growth, $s_n(\mathfrak{G})$ often denotes the number of subgroups in $\mathfrak{G}$ of index at most n, that is, the summatory function of $s_n(\mathfrak{G})$ in our notation.

p-pattern $\Pi^{(p)}(\mathfrak{G})$ of $\mathfrak{G}$ to be the family of sets

$$\Pi^{(p)}(\mathfrak{G}) = \Big\{\Pi_1^{(p)}(\mathfrak{G}), \Pi_2^{(p)}(\mathfrak{G}), \ldots, \Pi_{p-1}^{(p)}(\mathfrak{G})\Big\},$$

where

$$\Pi_j^{(p)}(\mathfrak{G}) := \Big\{n \in \mathbb{N} : \ s_n(\mathfrak{G}) \equiv j \bmod p\Big\}, \quad 0 < j < p;$$

in particular, $\Pi_{\mathfrak{G}} := \Pi_1^{(2)}(\mathfrak{G})$ is the *parity pattern* of $\mathfrak{G}$. The main purpose of this paper is to draw attention to the following remarkable result.

Theorem 1 (Descent Principle)**.** *Let p be a prime, $\mathfrak{G}$ an* FSG*-group, and let $\mathfrak{H} \lhd\lhd \mathfrak{G}$ be a subnormal subgroup of index p^r. Then*

$$\Pi_j^{(p)}(\mathfrak{G}) = p^r\, \Pi_j^{(p)}(\mathfrak{H}) \ \cup \bigcup_{0 \le \rho < r} p^\rho \Big(\Pi_j^{(p)}(\mathfrak{H}) \cap (\mathbb{N} - p\,\mathbb{N})\Big), \quad 0 < j < p. \tag{1}$$

Equivalently, if $X_{\mathfrak{G},p}(z)$ denotes the mod p projection of the series $\sum_{n\ge 0} s_{n+1}(\mathfrak{G}) z^n$, and if $X_{\mathfrak{H},p}(z)$ is the corresponding GF(p)-series for the group $\mathfrak{H}$, then, under our assumptions,

$$X_{\mathfrak{G},p}(z) = \sum_{\rho=0}^{r} z^{p^\rho - 1}\, X_{\mathfrak{H},p}(z^{p^\rho}) \ + \sum_{\rho=0}^{r-1} z^{p^{\rho+1}-1}\, X_{\mathfrak{H},p}^{(p-1)}(z^{p^\rho}). \tag{2}$$

Theorem 1 follows quickly from the main result of [15], where the conclusions (1) and (2) are established under the extra hypotheses that $\mathfrak{H}$ is normal in $\mathfrak{G}$, and that $\mathfrak{G}/\mathfrak{H}$ is cyclic; cf. Section 2 for more details. As the above example demonstrates, the assumption in Theorem 1 that $(\mathfrak{G} : \mathfrak{H})$ be a prime power cannot be weakened.

In Sections 3 and 4, we present two applications of Theorem 1. First, consider the fundamental group $\mathfrak{G}$ of a finite graph $(\mathfrak{G}(-), Y)$ of finite p-groups. If $\mathfrak{G}$ contains a free subnormal subgroup $\mathfrak{F}$ of index $m_{\mathfrak{G}} = \operatorname{lcm}\big\{|\mathfrak{G}(v)| : v \in V(Y)\big\}$, then $s_n(\mathfrak{G})$ is periodic modulo p, and its p-pattern is determined completely by that of $s_n(\mathfrak{F})$; cf. Theorem 2. Existence of such a free subnormal subgroup $\mathfrak{F}$ is not guaranteed, and we provide various sufficient conditions, one of which involves homogeneity; we use the classification of finite homogeneous groups due to Cherlin and Felgner [3]. As another application, we extend one of the main results of [16] concerning the p-patterns of free powers G^{*q} of a finite group G with q a p-power to groups of the more general form $H * G^{*q}$, where H is any finite p-group; cf. Theorem 3.

We thank the referee, whose comments have improved both the substance and the presentation of the material in Section 3.

2. Remarks on the proof of Theorem 1

We concentrate on Equation (1); the equivalence of (1) and (2) was already established in [15] (see the end of Section 2 in that paper). First note that Theorem 1 has a straightforward reduction to the case of prime index. Indeed, suppose that for an *FSG*-group $\mathfrak{G}$ and a normal subgroup $\mathfrak{H} \trianglelefteq \mathfrak{G}$ of index p (a prime), we know that

$$\Pi_j^{(p)}(\mathfrak{G}) = p\,\Pi_j^{(p)}(\mathfrak{H}) \cup \big(\Pi_j^{(p)}(\mathfrak{H}) \cap (\mathbb{N} - p\mathbb{N})\big), \quad 0 < j < p. \tag{3}$$

Let

$$\mathfrak{H} = \mathfrak{H}_0 \trianglelefteq \mathfrak{H}_1 \trianglelefteq \cdots \trianglelefteq \mathfrak{H}_r = \mathfrak{G}$$

be a normal series for $\mathfrak{H}$ with $(\mathfrak{H}_i : \mathfrak{H}_{i-1}) = p$ for all $1 \leq i \leq r$ (such a normal series exists since, by Frobenius' generalization of Sylow's third theorem [5, § 4, Theorem I], every non-trivial finite p-group contains a normal subgroup of index p). Then, by (3), we have

$$\Pi_j^{(p)}(\mathfrak{H}_i) = p\Pi_j^{(p)}(\mathfrak{H}_{i-1}) \cup \left(\Pi_j^{(p)}(\mathfrak{H}_{i-1}) \cap (\mathbb{N} - p\mathbb{N})\right) \quad (1 \leq i \leq r, 0 < j < p), \tag{4}$$

and, using (4), an immediate induction on i shows that, for $1 \leq i \leq r$ and $0 < j < p$,

$$\Pi_j^{(p)}(\mathfrak{H}_i) = p^i\, \Pi_j^{(p)}(\mathfrak{H}) \cup \bigcup_{0 \leq \rho < i} p^\rho \left(\Pi_j^{(p)}(\mathfrak{H}) \cap (\mathbb{N} - p\,\mathbb{N})\right),$$

whence (1).

Validity of Equation (1) in the case where $\mathfrak{H} \trianglelefteq \mathfrak{G}$ and $(\mathfrak{G} : \mathfrak{H}) = p$ follows immediately from [15, Theorem 1]. Here, we briefly sketch an alternative proof of (3) generalizing an argument in [14]. As in the proof of [14, Prop. 4] one observes that a subgroup $\tilde{\mathfrak{G}} \leq \mathfrak{G}$ is of index n in $\mathfrak{G}$ and not contained in $\mathfrak{H}$ if, and only if,

$$\tilde{\mathfrak{G}} \in \bigcup_{(\mathfrak{H}:\tilde{\mathfrak{H}})=n} \mathfrak{S}(\tilde{\mathfrak{H}}),$$

where

$$\mathfrak{S}(\tilde{\mathfrak{H}}) := \left\{\tilde{\mathfrak{G}} \leq \mathfrak{G} :\ \tilde{\mathfrak{G}} \cap \mathfrak{H} = \tilde{\mathfrak{H}} \ \text{ and } \ \tilde{\mathfrak{G}}\mathfrak{H} = \mathfrak{G}\right\}.$$

It follows that

$$s_n(\mathfrak{G}) = \sum_{(\mathfrak{H}:\tilde{\mathfrak{H}})=n} |\mathfrak{S}(\tilde{\mathfrak{H}})| + \begin{cases} s_{n/p}(\tilde{\mathfrak{H}}), & p \mid n \\ 0, & p \nmid n. \end{cases} \tag{5}$$

Fix an element ζ with $\mathfrak{G} = \langle \mathfrak{H}, \zeta \rangle$. Given a subgroup $\tilde{\mathfrak{H}}$ of index n in $\mathfrak{H}$ and a right transversal $1 = \mathfrak{h}_0, \mathfrak{h}_1, \ldots, \mathfrak{h}_{n-1}$ for $\tilde{\mathfrak{H}}$ in $\mathfrak{H}$, then the elements

$$\mathfrak{g}_{\mu,\nu} := \mathfrak{h}_\mu\, \zeta^\nu, \quad (0 \leq \mu < n, 0 \leq \nu < p)$$

form a right transversal for $\tilde{\mathfrak{H}}$ in $\mathfrak{G}$. A subgroup $\tilde{\mathfrak{G}} \in \mathfrak{S}(\tilde{\mathfrak{H}})$ must be of the form

$$\tilde{\mathfrak{G}} = \tilde{\mathfrak{G}}_{\underline{\mu}} = \tilde{\mathfrak{H}}\,\mathfrak{g}_{0,0} \cup \bigcup_{0<j<p} \tilde{\mathfrak{H}}\,\mathfrak{g}_{\mu_j,j}$$

with some vector

$$\underline{\mu} = (\mu_1, \mu_2, \ldots, \mu_{p-1}) \in \{0, 1, \ldots, n-1\}^{p-1},$$

and such a set $\tilde{\mathfrak{G}}_{\underline{\mu}} \subseteq \mathfrak{G}$ is a member of $\mathfrak{S}(\tilde{\mathfrak{H}})$ if, and only if, $\tilde{\mathfrak{G}}_{\underline{\mu}}$ is a subgroup of $\mathfrak{G}$. The necessary and sufficient condition for the last assertion to hold is that

$$\mathfrak{g}_{\mu_j,j}\tilde{\mathfrak{H}}\,\mathfrak{g}_{\mu_k,k} = \tilde{\mathfrak{H}}\,\mathfrak{g}_{\mu_{\overline{j+k}},\overline{j+k}}, \quad 0 \leq j,k < p$$

with $\mu_0 := 0$ and reduction (indicated by an overstroke) being modulo p. It follows from this analysis that the cardinality of the set $\mathfrak{S}(\tilde{\mathfrak{H}})$ equals the number of subgroups in $N_{\mathfrak{G}}(\tilde{\mathfrak{H}})/\tilde{\mathfrak{H}}$ of order p, which are not contained in $N_{\mathfrak{H}}(\tilde{\mathfrak{H}})/\tilde{\mathfrak{H}}$. Applying Frobenius' theorem[2] concerning the

[2]Cf. [5, pp. 984–985] and [6].

number of solutions of the equation $X^m = 1$ in a finite group G in the case when $m = p$ and $G = N_{\mathfrak{G}}(\tilde{\mathfrak{H}})/\tilde{\mathfrak{H}}$ or $G = N_{\mathfrak{H}}(\tilde{\mathfrak{H}})/\tilde{\mathfrak{H}}$, we deduce that

$$|\mathfrak{S}(\tilde{\mathfrak{H}})| \equiv \begin{cases} 1, & p \mid (N_{\mathfrak{G}}(\tilde{\mathfrak{H}}) : \tilde{\mathfrak{H}}) \text{ and } p \nmid (N_{\mathfrak{H}}(\tilde{\mathfrak{H}}) : \tilde{\mathfrak{H}}) \\ 0, & \text{otherwise} \end{cases} \mod p,$$

which, in conjunction with (5), yields

$$s_n(\mathfrak{G}) \equiv |\Omega_n| + \begin{cases} s_{n/p}(\mathfrak{H}), & p \mid n \\ 0, & p \nmid n \end{cases} \mod p, \tag{6}$$

where

$$\Omega_n := \Big\{ \tilde{\mathfrak{H}} \leq \mathfrak{H} : \ (\mathfrak{H} : \tilde{\mathfrak{H}}) = n,\, p \mid (N_{\mathfrak{G}}(\tilde{\mathfrak{H}}) : \tilde{\mathfrak{H}}),\, p \nmid (N_{\mathfrak{H}}(\tilde{\mathfrak{H}}) : \tilde{\mathfrak{H}}) \Big\}.$$

Denote by $\mathfrak{U}_n(\mathfrak{H})$ the set of subgroups of index n in $\mathfrak{H}$. Then, making use of the action by conjugation of $\mathfrak{H}$ on Ω_n and that of $\mathfrak{G}$ on $\mathfrak{U}_n(\mathfrak{H}) \setminus \Omega_n$, we find that

$$|\Omega_n| \equiv \begin{cases} s_n(\mathfrak{H}), & p \nmid n \\ 0, & p \mid n \end{cases} \mod p,$$

which, when combined with (6), gives

$$s_n(\mathfrak{G}) \equiv s_{n/(n,p)}(\mathfrak{H}) \mod p,$$

whence (3).

3. Divisibility properties determined by free normal subgroups

The category of graphs used in this section is described in Serre's book [18]. Let $(\mathfrak{G}(-), Y)$ be a finite graph of finite groups with fundamental group $\mathfrak{G} = \pi_1(\mathfrak{G}(-), Y)$, and let p be a prime. Moreover, denote by $V(Y)$ and $E(Y)$ the set of vertices respectively (geometric) edges of Y, and let $m_{\mathfrak{G}}$ be the least common multiple of the orders of the finite subgroups in $\mathfrak{G}$, that is,

$$m_{\mathfrak{G}} = \operatorname{lcm}\big\{ |\mathfrak{G}(v)| : \ v \in V(Y) \big\}.$$

The *free rank* $\mu(\mathfrak{G})$ of $\mathfrak{G}$ is defined as the rank of a free subgroup in $\mathfrak{G}$ of index $m_{\mathfrak{G}}$ (such subgroups always exist; cf., for instance, [18, Lemmas 8 and 10]). It is connected with the rational Euler characteristic $\chi(\mathfrak{G})$ of $\mathfrak{G}$ via

$$\mu(\mathfrak{G}) + m_{\mathfrak{G}}\, \chi(\mathfrak{G}) = 1, \tag{7}$$

and the latter quantity can be computed in terms of the graph of groups $(\mathfrak{G}(-), Y)$ by means of the formula

$$\chi(\mathfrak{G}) = \sum_{v \in V(Y)} \frac{1}{|\mathfrak{G}(v)|} - \sum_{e \in E(Y)} \frac{1}{|\mathfrak{G}(e)|}; \tag{8}$$

cf. [1, Chap. IX, Prop. 7.3] or [19, Prop. 14]. If $\mathfrak{G}$ has a free subnormal subgroup $\mathfrak{F}$ of index $m_{\mathfrak{G}}$ a p-power, then every vertex group $\mathfrak{G}(v)$ must be of p-power order; and if $\chi(\mathfrak{G}) \leq 0$, then any free subnormal subgroup $\mathfrak{F}$ of index $m_{\mathfrak{G}}$ has rank $\operatorname{rk}(\mathfrak{F}) = \mu(\mathfrak{G}) \geq 1$, and, by Theorem 1,

the p-pattern of $\mathfrak{G}$ is determined via (1) by the p-pattern of $\mathfrak{F}$. Consequently, all conclusions of [15, Theorem 2] remain valid in this more general situation, and we obtain the following.

Theorem 2. *Let p be a prime, $(\mathfrak{G}(-),Y)$ a finite graph of groups all of whose vertex groups are of p-power order, and let $\mathfrak{G}$ be its fundamental group. Let $m_{\mathfrak{G}} = p^r$, and suppose that $\mathfrak{G}$ contains a subnormal free subgroup of index $m_{\mathfrak{G}}$, and that $\chi(\mathfrak{G}) \leq 0$. Then*

(i) *the function $s_n(\mathfrak{G})$ is periodic modulo p,*
(ii) *for $p = 2$ we have $\Pi_{\mathfrak{G}} = \mathbb{N}$,*
(iii) *for $p = 3$ and $\mu(\mathfrak{G})$ odd we have $\Pi_1^{(3)}(\mathfrak{G}) = \mathbb{N}$,*
(iv) *for $p = 3$ and $\mu(\mathfrak{G})$ even, $s_n(\mathfrak{G})$ is periodic modulo 3 with period $8 \cdot 3^r$. More precisely, in this case $s_n(\mathfrak{G}) \equiv 1 \mod 3$ if and only if n is congruent $\mod 8 \cdot 3^r$ to one of the 3^{r+1} numbers*
$0, 3^{r-1}, 3^r, 8 \cdot 3^{r-1}, 3^{r+1}, 11 \cdot 3^{r-1}, 16 \cdot 3^{r-1}, 17 \cdot 3^{r-1}, 19 \cdot 3^{r-1}, 3^\rho(1+24\lambda), 8 \cdot 3^\rho(1+3\lambda), 3^\rho(11+24\lambda), 8 \cdot 3^\rho(2+3\lambda), 3^\rho(17+24\lambda), 3^\rho(19+24\lambda)$
with $0 \leq \rho < r-1$ and $0 \leq \lambda < 3^{r-\rho-1}$;
and $s_n(\mathfrak{G}) \equiv 2 \mod 3$ if and only if n is congruent $\mod 8 \cdot 3^r$ to one of the 3^{r+1} numbers
$4 \cdot 3^{r-1}, 5 \cdot 3^{r-1}, 7 \cdot 3^{r-1}, 4 \cdot 3^r, 13 \cdot 3^{r-1}, 5 \cdot 3^r, 20 \cdot 3^{r-1}, 7 \cdot 3^r, 23 \cdot 3^{r-1}, 4 \cdot 3^\rho(1+6\lambda), 4 \cdot 3^\rho(5+6\lambda), 3^\rho(5+24\lambda), 3^\rho(7+24\lambda), 3^\rho(13+24\lambda), 3^\rho(23+24\lambda)$
with $0 \leq \rho < r-1$ and $0 \leq \lambda < 3^{r-\rho-1}$.

The usefulness of Theorem 2 depends on our being able to verify the hypothesis that $\mathfrak{G}$ contains a subnormal free subgroup of index $m_{\mathfrak{G}}$. The remainder of this section is devoted to this last problem. Rather than attempt to state a very general result here, we isolate the essential part of the argument in the next two lemmas, followed by several applications.

Lemma 1. *Let $(\mathfrak{G}(-),Y)$ be a finite tree of finite groups, and set $\mathfrak{G} = \pi_1(\mathfrak{G}(-),Y)$ and $m = m_{\mathfrak{G}}$. For $e \in E(Y)$, and a vertex v in the boundary of e, let $\alpha_{(e,v)}$ be the embedding of $\mathfrak{G}(e)$ into $\mathfrak{G}(v)$ given by the tree of groups $(\mathfrak{G}(-),Y)$. Assume that there is a vertex $v_0 \in V(Y)$ with the property that $|\mathfrak{G}(v_0)| = m$. Set $G = \mathfrak{G}(v_0)$, and denote by $\Psi = \Psi(\mathfrak{G}(-),Y)$ the set of all homomorphisms $\psi : \mathfrak{G} \to G$ such that the restriction of ψ to any vertex-group is injective. Then the following hold:*

(i) *Ψ is non-empty if and only if there is a family $\{\psi_v : \mathfrak{G}(v) \to G\}_{v \in V(Y)}$ of injective homomorphisms such that, for every $e \in E(Y)$, we have*

$$\psi_v|_{\alpha(e,v)\mathfrak{G}(e)} = \psi_{v'}|_{\alpha(e,v')\mathfrak{G}(e)}, \tag{9}$$

where v and v' are the two vertices bounding e.
(ii) *The number of free normal subgroups having index m in $\mathfrak{G}$ is $|\Psi|/|\operatorname{Aut}(G)|$.*

Proof. (i) For $v \in V(Y)$, define ψ_v to be $\psi|_{\mathfrak{G}(v)}$, for all $v \in V(Y)$. Then Equation (9) follows from the definition of a tree of groups.

Conversely, if the homomorphisms ψ_v exist and satisfy Equation (9), then there is a homomorphism $\psi : \mathfrak{G} \to G$ whose restriction to $\mathfrak{G}(v)$ is ψ_v; by definition, $\psi \in \Psi$.

(ii) $\mathrm{Aut}(G)$ acts naturally on Ψ via

$$\psi \cdot \alpha := \alpha \circ \psi \quad (\psi \in \Psi, \alpha \in \mathrm{Aut}(G)),$$

and, since each $\psi \in \Psi$ is surjective, this action is free; thus

$$|\Psi/\mathrm{Aut}(G)| = |\Psi|/|\mathrm{Aut}(G)|.$$

Now let $\mathfrak{F}$ be a free normal subgroup of $\mathfrak{G}$ of index m. Then $\mathfrak{G}(v_0) \cap \mathfrak{F} = 1$ and $\mathfrak{G}(v_0)\mathfrak{F} = \mathfrak{G}$, so $\mathfrak{G}/\mathfrak{F} \cong G$, and the canonical projection map π from $\mathfrak{G}$ to G belongs to Ψ. Sending $\mathfrak{F}$ to $[\pi]$, the orbit of π under $\mathrm{Aut}(G)$, gives a well-defined map

$$\varphi : \{\mathfrak{F} \trianglelefteq \mathfrak{G} : \mathfrak{F} \text{ free}, (\mathfrak{G} : \mathfrak{F}) = m\} \to \Psi/\mathrm{Aut}(G).$$

Moreover, the kernel of any member ψ of Ψ is a free normal subgroup of $\mathfrak{G}$ of index m (see, for instance, [4, Chapter II, Theorem 1.3]), and the projection map $\pi : \mathfrak{G} \to \mathfrak{G}/\ker(\psi) \cong G$ differs from ψ only by an automorphism of G, so $[\pi] = [\psi]$, and φ is surjective. Finally, if two free normal subgroups $\mathfrak{F}_1, \mathfrak{F}_2$ of $\mathfrak{G}$ of index m have projections $\pi : \mathfrak{G} \to \mathfrak{G}/\mathfrak{F}_i \cong G$ only differing by an automorphism of G, then $\mathfrak{F}_1 = \mathfrak{F}_2$, so φ is a bijection. □

Definition. *For a group $\mathfrak{G}$ and a subgroup $\mathfrak{H} \leq \mathfrak{G}$, we define the centralizer $C_{\mathrm{Aut}(\mathfrak{G})}(\mathfrak{H})$ of $\mathfrak{H}$ in* $\mathrm{Aut}(\mathfrak{G})$ *to be*

$$C_{\mathrm{Aut}(\mathfrak{G})}(\mathfrak{H}) := \{\alpha \in \mathrm{Aut}(\mathfrak{G}) : \ \alpha(h) = h \ \text{ for all } \ h \in \mathfrak{H}\}.$$

Lemma 2. *Let the hypotheses and notation be as in Lemma* 1. *Suppose that $E(Y)$ is non-empty and that the set Ψ in Lemma* 1 *is also non-empty. Choose v' to be a terminal vertex of Y different from v_0. Let Y_0 be the subtree of Y induced on $V(Y) - \{v'\}$, and let $\Psi_0 = \Psi(\mathfrak{G}(-)|_{Y_0}, Y_0)$. Let e' be the edge containing v', and let $v'' \in V(Y_0)$ be the other vertex bounding e'. For $\psi_0 \in \Psi_0$, let $S(\psi_0)$ be the set of injective homomorphisms $\psi_{v'} : \mathfrak{G}(v') \to G$ for which $\psi|_{\alpha(e',v')\mathfrak{G}(e')} = \psi_0|_{\alpha(e',v'')\mathfrak{G}(e')}$. (This set may be empty). Then*

$$|\Psi| = \sum_{\psi_0 \in \Psi_0} |S(\psi_0)|.$$

Proof. Let $\mathfrak{G}_0 = \pi_1(\mathfrak{G}(-)|_{Y_0}, Y_0)$. We have $\mathfrak{G} = \mathfrak{G}_0 *_{\mathfrak{G}(e')} \mathfrak{G}(v')$, the amalgamation being with respect to the canonical embeddings of $\mathfrak{G}(e')$ in $\mathfrak{G}_0$ and $\mathfrak{G}(v')$ respectively. The number of elements of Ψ which restrict to ψ_0 is equal to $|S(\psi_0)|$. □

The results of these two lemmas are most easily applied when the vertex groups are homogeneous, a concept we discuss next.

A group $\mathfrak{G}$ is termed *homogeneous* if every isomorphism between finitely generated subgroups is induced by an automorphism of $\mathfrak{G}$. This concept arose (for arbitrary first order structures) in model theory in connection with quantifier elimination. For instance, it is known that a finite group is homogeneous if and only if its first order theory has quantifier elimination; cf. [9, Cor. 8.4.2]. The finite homogeneous groups have been classified by Cherlin and Felgner; cf. [2] and [3]. In particular, a finite p-group G is homogeneous if and only if one of the following holds:

(i) $G \cong \underbrace{C_{p^r} \oplus \cdots \oplus C_{p^r}}_{s \text{ copies}}$ for some $r,s \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}$;

(ii) $G \cong Q$, the quaternion group of order 8;

(iii) $G \cong Q^*$.

Here, Q^* is a certain group of order 64, class 2, and exponent 4, which arises for instance as the Sylow 2-subgroup of $\mathrm{PSU}_3(4^2)$; cf. [2, Sect. 2] for more details.

Proposition 1. *Let p be a prime. Let $(\mathfrak{G}(-),Y)$ be a finite tree of groups such that*

(i) *every vertex group $\mathfrak{G}(v)$ is a finite homogeneous p-group; and*
(ii) *there is a vertex $v_0 \in V(Y)$ such that every vertex group is isomorphic to a subgroup of $G = \mathfrak{G}(v_0)$.*

Set $\mathfrak{G} \cong \pi_1(\mathfrak{G}(-),Y)$. Then the number of free normal subgroups of index $m_{\mathfrak{G}} = |G|$ in $\mathfrak{G}$ is

$$\prod_{e \in E(Y)} |C_{\mathrm{Aut}(G)}(G_e)| \Big/ \prod_{v \in V(Y)} |C_{\mathrm{Aut}(G)}(G_v)|,$$

where G_v and G_e are subgroups of G isomorphic to $\mathfrak{G}(v)$ and $\mathfrak{G}(e)$ respectively, for $v \in V(Y)$ and $e \in E(Y)$.

Proof. The proof is by induction on $|E(Y)|$. (The induction hypothesis, in conjunction with Lemma 1, asserts that $|\Psi|$ is equal to $|\mathrm{Aut}(G)|$ times the quantity in the Proposition.)

If $E(Y) = \emptyset$, then $V(Y) = \{v_0\}$, and the formula gives $1/|C_{\mathrm{Aut}(G)}(G)| = 1$, which is correct; so $|\Psi| = |\mathrm{Aut}(G)|$ in this case.

Suppose that $|E(Y) \neq \emptyset$. Choose v' to be a terminal vertex of Y not equal to v_0, let e' be the edge containing v' and let v'' be the other vertex in the boundary of e'. Since $\alpha(e',v')\mathfrak{G}(e') \cong \alpha(e',v'')\mathfrak{G}(e')$, the sets $S(\psi_0)$ appearing in Lemma 2 are all non-empty.

Let G be a finite homogeneous group. If $H \leq G$, then the number of extensions of a given embedding $H \to G$ to an automorphism of G is $|C_{\mathrm{Aut}(G)}(H)|$. Hence, if $K \leq H \leq G$, then the number of extensions of an embedding $K \to G$ to an embedding $H \to G$ is $|C_{\mathrm{Aut}(G)}(K)|/|C_{\mathrm{Aut}(G)}(H)|$. Hence, in Lemma 2, we have

$$S(\psi_0)| = |C_{\mathrm{Aut}(G)}(G_{e'})|/|C_{\mathrm{Aut}(G)}(G_{v'}),$$

independent of ψ_0, and so

$$|\Psi| = |\Psi_0| \cdot |C_{\mathrm{Aut}(G)}(G_{e'})|/|C_{\mathrm{Aut}(G)}(G_{v'}).$$

On the other hand, the induction hypothesis asserts that

$$|\Psi_0| = |\mathrm{Aut}(G)| \cdot \prod_{e \in E(Y_0)} |C_{\mathrm{Aut}(G)}(G_e)| \Big/ \prod_{v \in V(Y_0)} |C_{\mathrm{Aut}(G)}(G_v)|,$$

and combining the last two equations, and applying Lemma 1 again, gives the desired result, since $V(Y) = V(Y_0) \cup \{v'\}$ and $E(Y) = E(Y_0) \cup \{e'\}$. □

Corollary 1. *Let p be a prime, $(\mathfrak{G}(-),Y)$ a finite tree of groups all of whose vertex groups are of p-power order, $\mathfrak{G} \cong \pi_1(\mathfrak{G}(-),Y)$, and let $m_{\mathfrak{G}} = p^r$.*

(i) *If all vertex groups $\mathfrak{G}(v)$ are cyclic, then $\mathfrak{G}$ contains precisely*

$$\frac{\prod_{v\in V(Y)} \varphi(|\mathfrak{G}(v)|)}{\prod_{e\in E(Y)} \varphi(|\mathfrak{G}(e)|)} \Big/ \varphi(m_{\mathfrak{G}})$$

free normal subgroups of index $m_{\mathfrak{G}}$, where φ is Euler's totient function.

(ii) *If all vertex groups $\mathfrak{G}(v)$ are elementary abelian, then $\mathfrak{G}$ contains exactly*

$$\frac{\prod_{e\in E(Y)} \left[|\mathfrak{G}(e)|^{r-d_e} \,|\mathrm{GL}_{r-d_e}(p)|\right]}{\prod_{v\in V(Y)} \left[|\mathfrak{G}(v)|^{r-d_v} \,|\mathrm{GL}_{r-d_v}(p)|\right]}$$

free normal subgroups of index $m_{\mathfrak{G}}$, where $d_\sigma = \dim_p \mathfrak{G}(\sigma)$, $\sigma \in V(Y)\cup E(Y)$.

Proof. The hypotheses of Proposition 1 are satisfied in both cases.

Note that, if G is a finite homogeneous group and H a subgroup of G, then we have $N_{\mathrm{Aut}\,G}(H)/C_{\mathrm{Aut}\,G}(H) \cong \mathrm{Aut}(H)$, and hence

$$|C_{\mathrm{Aut}(G)}(H)| = \frac{|\,\mathrm{Aut}(G)|}{\#(G,H)\cdot|\mathrm{Aut}(H)|},$$

where

$$N_{\mathrm{Aut}(G)}(H) := \big\{\alpha \in \mathrm{Aut}(G) : \alpha(H) = H\big\},$$

and with $\#(G,H) = |\,\mathrm{Aut}(G)|/|N_{\mathrm{Aut}(G)}(H)|$ the number of subgroups of G isomorphic to H.

For (i), we have $|\,\mathrm{Aut}(G)| = \varphi(|G|)$ and $\#(G,H) = 1$ whenever G is a cyclic group and $H \le G$. Proposition 1 shows that the number of free subgroups of $\mathfrak{G}$ of index $m_{\mathfrak{G}}$ is

$$\frac{\prod_{e\in E(Y)} \varphi(m_{\mathfrak{G}})/\varphi(|\mathfrak{G}(e)|)}{\prod_{v\in V(Y)} \varphi(m_{\mathfrak{G}})/\varphi(|\mathfrak{G}(v)|)},$$

which is equal to the value claimed, since $|V(Y)| = |E(Y)| + 1$. (Note that this result is also proved in [15, Lemma 1].)

For (ii), if G is elementary abelian of order p^r, and H is a subgroup of order p^s, then we have

$$|\,\mathrm{Aut}(G)| = |\mathrm{GL}_r(p)| = (p^r-1)(p^r-p)\cdots(p^r-p^{r-1})$$

and

$$\#(G,H) = \begin{bmatrix} r \\ s \end{bmatrix}_p = \frac{(p^r-1)(p^r-p)\cdots(p^r-p^{s-1})}{(p^s-1)(p^s-p)\cdots(p^s-p^{s-1})}.$$

Hence, if $|G| = p^r$, $H \le G$, and $|H| = p^s$, then

$$|C_{\mathrm{Aut}(G)}(H)| = |\mathrm{GL}_{r-s}(p)|\cdot p^{s(r-s)} = |\mathrm{GL}_{r-s}(p)|\cdot|H|^{r-s}.$$

Hence, the result follows from Proposition 1. □

Corollary 2. (i) *If, in Proposition* 1*, all the vertex groups are isomorphic to $G = Q$ then $\mathfrak{G}$ contains precisely $24^{a(\mathfrak{G})} \cdot 4^{b(\mathfrak{G})}$ free normal subgroups of index $m_{\mathfrak{G}} = 8$, where*

$$a(\mathfrak{G}) := |\{e \in E(Y) : \ |\mathfrak{G}(e)| < 4\}| \ \text{ and } \ b(\mathfrak{G}) := |\{e \in E(Y) : \ |\mathfrak{G}(e)| = 4\}|.$$

(ii) *If, in Proposition* 1*, all the vertex groups are isomorphic to $G = Q^*$, the number of free normal subgroups in $\mathfrak{G}$ of index $m_{\mathfrak{G}} = 64$ equals*

$$15360^{a(\mathfrak{G})} \cdot 5120^{b(\mathfrak{G})} \cdot 2560^{c(\mathfrak{G})} \cdot 256^{d(\mathfrak{G})} \cdot 128^{e(\mathfrak{G})} \cdot 32^{f(\mathfrak{G})} \cdot 16^{g(\mathfrak{G})} \cdot 4^{h(\mathfrak{G})},$$

where

$$\begin{aligned}
a(\mathfrak{G}) &:= |\{e \in E(Y) : \ \mathfrak{G}(e) = 1\}|,\\
b(\mathfrak{G}) &:= |\{e \in E(Y) : \ |\mathfrak{G}(e)| = 2\}|,\\
c(\mathfrak{G}) &:= |\{e \in E(Y) : \ \mathfrak{G}(e) \cong C_2 \times C_2\}|,\\
d(\mathfrak{G}) &:= |\{e \in E(Y) : \ \mathfrak{G}(e) \cong C_4\}|,\\
e(\mathfrak{G}) &:= |\{e \in E(Y) : \ |\mathfrak{G}(e)| = 8\}|,\\
f(\mathfrak{G}) &:= |\{e \in E(Y) : \ \mathfrak{G}(e) \cong C_4 \times C_4\}|,\\
g(\mathfrak{G}) &:= |\{e \in E(Y) : \ \mathfrak{G}(e) \cong H_{16}\}|,\\
h(\mathfrak{G}) &:= |\{e \in E(Y) : \ |\mathfrak{G}(e)| = 32\}|.
\end{aligned}$$

Here, $H_{16} = \langle a, b \mid a^4 = b^4 = 1, \ a^b = a^{-1} \rangle$.

Proof. Since all vertex groups are isomorphic to G, we have $C_{\mathrm{Aut}(G)}(G_v) = 1$ for all $v \in V(Y)$. The assertions of the corollary follow immediately from Proposition 1, once the orders of the corresponding centralizers $C_{\mathrm{Aut}(G)}(G_e)$ are known. For the second part, these have been found with the help of the computer algebra system GAP [7]. □

Remark. A finite group G is homogeneous if and only if, for every finite tree of groups $(\mathfrak{G}(-), Y)$ with all vertex stabilizers isomorphic to G, $\mathfrak{G} = \pi_1(\mathfrak{G}(-), Y)$ contains a free normal subgroup of index $m_{\mathfrak{G}}$. Indeed, the forward implication follows immediately from Lemma 1. If, on the other hand, G is not homogeneous, then there exists an isomorphism between two subgroups H_1, H_2 of $\mathfrak{G}$, which is not induced by an automorphism. We can then form the amalgam $\mathfrak{G} = G *_H G$, where the abstract group H is identified with H_1 in the left factor and with H_2 in the right factor, in such a way that the isomorphism between H_1 and H_2 induced by these embeddings is the given isomorphism. Then $\mathfrak{G}$ does not possess a free normal subgroup of index $m_{\mathfrak{G}} = |G|$. For, if $\mathfrak{F}$ were such a subgroup, then $\mathfrak{G}/\mathfrak{F} \cong G$, and the two embeddings of H in $\mathfrak{G}$ would coincide in this quotient, which (by assumption) is not the case.

We now describe a simple example to illustrate that, even if the vertex groups are not homogeneous, the counting may still be possible. Let $(\mathfrak{G}(-), Y)$ be a tree of groups all of whose vertex groups are isomorphic to D_4, the dihedral group of order 8, and let $\mathfrak{G}$ be its fundamental group. Call an edge $e \in E(Y)$ *wild*, if $\mathfrak{G}(e)$ contains an involution which is identified with the central involution in one of its corresponding vertex groups, and a non-central involution

in the other. If e is not wild, we call it *inner* if $\mathfrak{G}(e)$ is embedded in the cyclic subgroup of order 4 of $\mathfrak{G}(v)$ for v on e, and *outer* otherwise.

Proposition 2. *Let $\mathfrak{G}$ be as above. Then $\mathfrak{G}$ has a free normal subgroup of index $m_{\mathfrak{G}} = 8$ if and only if the tree of groups $(\mathfrak{G}(-), Y)$ does not contain a wild edge. In the latter case, the number of free normal subgroups of index $m_{\mathfrak{G}}$ equals*

$$2^{o(\mathfrak{G})} \prod_{\substack{e \in E(Y) \\ \mathfrak{G}(e) \text{ inner}}} \frac{8}{\varphi\left(|\mathfrak{G}(e)|\right)},$$

where

$$o(\mathfrak{G}) := \left|\left\{e \in E(Y) : \ \mathfrak{G}(e) \text{ outer}\right\}\right|.$$

Proof. Necessity of the stated existence criterion is clear. In the positive direction, the condition that no edge is wild guarantees that, in the notation of Lemma 2, the sets $S(\psi_0)$ are all non-empty, and have cardinality 2 if e is outer and $8/\varphi(|\mathfrak{G}(e)|)$ if e is inner. □

Define the *type* $\tau(\mathfrak{G})$ of a finitely generated virtually free group $\mathfrak{G} \cong \pi_1(\mathfrak{G}(-), Y)$ as the tuple

$$\tau(\mathfrak{G}) = \big(m_{\mathfrak{G}}; \zeta_1(\mathfrak{G}), \ldots, \zeta_\kappa(\mathfrak{G}), \ldots, \zeta_{m_{\mathfrak{G}}}(\mathfrak{G})\big),$$

where the $\zeta_\kappa(\mathfrak{G})$ are integers indexed by the divisors of $m_{\mathfrak{G}}$, given by

$$\zeta_\kappa(\mathfrak{G}) = \left|\left\{e \in E(Y) : \ |\mathfrak{G}(e)| \,\middle|\, \kappa\right\}\right| \ - \ \left|\left\{v \in V(Y) : \ |\mathfrak{G}(v)| \,\middle|\, \kappa\right\}\right|$$

with $V(Y)$ and $E(Y)$ as above. We have $\zeta_\kappa(\mathfrak{G}) \geq 0$ for $\kappa < m_{\mathfrak{G}}$ and $\zeta_{m_{\mathfrak{G}}}(\mathfrak{G}) \geq -1$ with equality occurring in the latter inequality if and only if Y is a tree; cf. [12, Lemma 2] and [13, Proposition 1]. It can be shown that the type $\tau(\mathfrak{G})$ is in fact an invariant of the group $\mathfrak{G}$, that is, independent of the particular decomposition of $\mathfrak{G}$ in terms of a graph of groups $(\mathfrak{G}(-), Y)$, and that two virtually free groups $\mathfrak{G}_1$ and $\mathfrak{G}_2$ contain the same number of free subgroups of index n for each positive integer n if and only if $\tau(\mathfrak{G}_1) = \tau(\mathfrak{G}_2)$; cf. [12, Theorem 2]. It follows from (8) that the Euler characteristic of $\mathfrak{G}$ can be expressed in terms of the type via

$$\chi(\mathfrak{G}) = -m_{\mathfrak{G}}^{-1} \sum_{\kappa \mid m_{\mathfrak{G}}} \varphi(m_{\mathfrak{G}}/\kappa)\, \zeta_\kappa(\mathfrak{G}). \tag{10}$$

Equations (7) and (10) imply in particular that, if two virtually free groups have the same number of free index n subgroups for each n, then their Euler characteristics respectively free ranks must coincide. For a finitely generated virtually free group $\mathfrak{G}$ and a prime p define the *p-rank* $\mu_p(\mathfrak{G})$ of $\mathfrak{G}$ by means of the formula

$$\mu_p(\mathfrak{G}) = 1 + \sum_{p \mid \kappa \mid m_{\mathfrak{G}}} \varphi(m_{\mathfrak{G}}/\kappa)\, \zeta_\kappa(\mathfrak{G}).$$

Moreover, denote by $f_\lambda(\mathfrak{G})$ the number of free subgroups in $\mathfrak{G}$ of index $\lambda m_{\mathfrak{G}}$.

Proposition 3. *Let p be a prime, $(\mathfrak{G}(-), Y)$ a finite graph of groups all of whose vertex groups are non-trivial finite p-groups, and let $\mathfrak{G} = \pi_1(\mathfrak{G}(-), Y)$. Then the following assertions are equivalent:*

(i) $f_1(\mathfrak{G}) \not\equiv 0 \mod p$,

(ii) $\mu_p(\mathfrak{G}) = 0$,

(iii) $\mathfrak{G}$ *is a free product of the form* $\mathfrak{G} \cong H * \underbrace{C_p * \cdots * C_p}_{s \text{ copies}}$ *with* $s \geq 0$

and a group H *of order* $m_{\mathfrak{G}}$.

Corollary 3. *Let* p *be a prime, and let* $\mathfrak{G} = H * C_p^{*s}$ *be a free product of* $s \geq 0$ *copies of the cyclic group of order* p *and a finite* p*-group* H. *Then* $\mathfrak{G}$ *contains a normal free subgroup of index* $m_{\mathfrak{G}}$.

Proof. This follows from the action by conjugation of $\mathfrak{G}$ on the set of free subgroups of index $m_{\mathfrak{G}}$, together with the implication (iii) $\Rightarrow$ (i) of Proposition 3. It also follows immediately from Lemma 1. □

Proof of Proposition 3. The equivalence of (i) and (ii) follows from a discussion of the formula[3]

$$f_1(\mathfrak{G}) = m_{\mathfrak{G}} \prod_{\kappa \mid m_{\mathfrak{G}}} \prod_{\substack{1 \leq k \leq m_{\mathfrak{G}} \\ (m_{\mathfrak{G}}, k) = \kappa}} k^{\zeta_\kappa(\mathfrak{G})},$$

making use of facts concerning $\tau(\mathfrak{G})$ mentioned above. Suppose now that $\mu_p(\mathfrak{G}) = 0$. Then Y is a tree, and, after contracting edges of Y corresponding to trivial amalgamations if necessary, we may assume that $(\mathfrak{G}(-), Y)$ is *normalized*, that is, $|\mathfrak{G}(e)| \neq |\mathfrak{G}(v)|$ for all $e \in E(Y)$ and $v \in \partial e$. For a positive integer n, denote by e_n, v_n the number of edges $e \in E(Y)$ respectively vertices $v \in V(Y)$ whose associated group $\mathfrak{G}(e)$ respectively $\mathfrak{G}(v)$ has order n, define an arithmetic function $f(n)$ via

$$f(n) = \sum_{v \mid n} (e_v - v_v), \quad n \geq 1,$$

and let $m_{\mathfrak{G}} = p^r$. Then, for $0 \leq \rho \leq r$,

$$f(p^\rho) = \begin{cases} e_1, & \rho = 0 \\ -1, & \rho = r \\ 0, & \text{otherwise,} \end{cases} \tag{11}$$

and, by Möbius inversion,

$$e_n - v_n = \sum_{v \mid n} \mu(v)\, f(n/v), \quad n \geq 1, \tag{12}$$

where μ is the classical Möbius function. Since our claim (iii) holds for $r \leq 1$, we may assume that $r \geq 2$. In the latter case, we find from (11) and (12) that

$$e_{p^\rho} - v_{p^\rho} = \begin{cases} -e_1, & \rho = 1 \\ 0, & 1 < \rho < r \\ -1, & \rho = r. \end{cases} \tag{13}$$

[3]Cf. formulae (3) and (11) in [12].

Using the facts that $(\mathfrak{G}(-),Y)$ is normalized and that Y is a tree (hence, in particular, does not contain loops), we find from (13) that

$$\begin{aligned} e_{p^r} = 0, &\quad \text{therefore} \quad v_{p^r} = 1 \\ e_{p^{r-1}} = 0, &\quad \text{therefore} \quad v_{p^{r-1}} = 0 \\ &\vdots \\ e_{p^2} = 0, &\quad \text{therefore} \quad v_{p^2} = 0 \\ e_p = 0, &\quad \text{therefore} \quad v_p = e_1. \end{aligned}$$

It follows that all edge groups are trivial, that is, $\mathfrak{G}$ is the free product of its vertex groups, and that $V(Y)$ contains precisely one vertex v_0 with $|\mathfrak{G}(v_0)| = p^r$ and $e_1 \geq 0$ vertices v satisfying $\mathfrak{G}(v) \cong C_p$, whence (iii). Since the implication (iii) $\Rightarrow$ (ii) is trivial, the proof of Proposition 3 is complete. □

4. The groups $\mathfrak{G}(G,H,q)$

For a finite group G, a prime p, and p-powers $q, \bar{q}$ with $q\bar{q} > 1$, let

$$\mathfrak{G} = \mathfrak{G}(G,H,q) = H * \underbrace{G * \cdots * G}_{q \text{ copies}}, \tag{14}$$

where H is of order $\bar{q}$. Put $\widetilde{\mathfrak{G}} := \mathfrak{G}(G,1,q) \cong G^{*q}$. It follows from the normal form theorem applied to the free product $H * \widetilde{\mathfrak{G}}$ that $\mathfrak{G}(G,H,q)$ is a split extension of the group

$$\mathfrak{H} = \left\langle \widetilde{\mathfrak{G}}^h : h \in H \right\rangle \cong G^{*q\bar{q}} = \mathfrak{G}(G,1,q\bar{q})$$

by H; in particular, the groups $\mathfrak{G}$ and $\mathfrak{H}$ satisfy the hypotheses of Theorem 1, and (1) yields the reduction formula

$$\Pi_j^{(p)}(\mathfrak{G}(G,H,q)) = \bar{q}\Pi_j^{(p)}(\mathfrak{G}(G,1,q\bar{q})) \cup \bigcup_{\substack{\sigma \mid \bar{q} \\ \sigma < \bar{q}}} \sigma\big(\Pi_j^{(p)}(\mathfrak{G}(G,1,q\bar{q})) \cap (\mathbb{N} - p\mathbb{N})\big),$$

$$0 < j < p. \tag{15}$$

Formula (15) allows us to translate results concerning the groups $\mathfrak{G}(G,1,q)$ obtained in [16] into results for groups of the more general form (14). Since, for the most part, this translation process is entirely straightforward, and whatever extra arguments are needed can be found in [16, Sect. 8], we shall leave this task to the reader. As an example, we state the generalization of [16, Theorem 12], which provides a remarkably explicit combinatorial description of the p-pattern $\Pi^{(p)}(\mathfrak{G}(G,H,q))$ under a certain assumption on G.

Theorem 3. *Let G be a finite group, p a prime, let q and $\bar{q}$ be p-powers such that $q\bar{q} > 1$, and let H be a group of order $\bar{q}$. Assume that $s_d(G) \equiv 0\ (p)$ for all $d \in \mathbb{N}$ with $d \not\equiv 1\ (p)$ (that is, $G \in \mathbf{Fin}(p)$ in the notation of* [16]*). Then we have*

$$\Pi_j^{(p)}(\mathfrak{G}(G,H,q)) = \bigcup_{\sigma \mid \bar{q}} \sigma\, \Theta^{(j)}_{G,q,\bar{q}}, \quad 0 < j < p,$$

where $\Theta^{(j)}_{G,q,\bar{q}}$ *consists of all positive integers* $n \equiv 1 \bmod pq\bar{q}$ *such that the sum*

$$\sum_{\substack{\underline{n}\in\mathbb{N}_0^r \\ \underline{d}_{G,p}\cdot\underline{n}=\frac{n-1}{pq\bar{q}}}} \binom{1+(q\bar{q}-1)(n-1)/(q\bar{q})}{\underline{n}, 1+(q\bar{q}-1)(n-1)/(q\bar{q})-\|\underline{n}\|} \prod_{i=1}^{r} \left(s_{d_i}(G)\right)^{n_i}$$

is congruent to j *modulo* p.

Here, the vector $\underline{d}_{G,p} \in \mathbb{N}^r$ attached to the group G and prime p is defined as

$$\underline{d}_{G,p} := \left(\frac{d_1-1}{p}, \frac{d_2-1}{p}, \ldots, \frac{d_r-1}{p}\right),$$

where $1 = d_0 < d_1 < \cdots < d_r = |G|$ is the collection in increasing order of those positive integers d for which $s_d(G) \not\equiv 0\ (p)$. Also, if $\underline{n} = (n_1, \ldots, n_r)$ is a vector of positive integers with sum $\|\underline{n}\|$, and $N \geq \|\underline{n}\|$, then

$$\binom{N}{\underline{n}, N-\|\underline{n}\|}$$

denotes the multinomial coefficient

$$\frac{N!}{n_1!\, n_2! \cdots n_r!\, (N-\|\underline{n}\|)!}.$$

REFERENCES

[1] K. S. Brown, *Cohomology of groups*, Springer, New York, 1982.

[2] G. L. Cherlin and U. Felgner, Homogeneous solvable groups, *J. London Math. Soc.* (2) **44** (1991), 102–120.

[3] G. L. Cherlin and U. Felgner, Homogeneous finite groups, *J. London Math. Soc.* (2) **62** (2000), 784–794.

[4] W. Dicks, *Groups, Trees, and Projective Modules*, Lecture Notes in Mathematics vol 790, Springer, Berlin, 1980.

[5] G. Frobenius, Verallgemeinerung des Sylow'schen Satzes, *Berliner Sitzungsberichte* (1895), 981–993.

[6] G. Frobenius, Über einen Fundamentalsatz der Gruppentheorie, *Berliner Sitzungsberichte* (1903), 987–991.

[7] The GAP Group, GAP — Groups, Algorithms, and Programming, Version 4.3; Aachen, St Andrews, 2002, `http://www-gap.dcs.st-and.ac.uk/~gap`.

[8] M. Hall, Subgroups of finite index in free groups, *Can. J. Math.* **1** (1949), 187–190.

[9] W. Hodges, *Model Theory*, Encyclopedia of Mathematics and its Applications Vol. 42, Cambridge University Press, Cambridge, 1993.

[10] A. Lubotzky and D. Segal, *Subgroup Growth*, Progress in Mathematics, Birkhäuser, Basel, 2003.

[11] R. Lyndon, Two notes on Rankin's book on the modular group, *J. Austral. Math. Soc.* **16** (1973), 454–457.

[12] T. Müller, Combinatorial aspects of finitely generated virtually free groups, *J. London Math. Soc.* (2) **44** (1991), 75–94.

[13] T. Müller, A group-theoretical generalization of Pascal's triangle, *Europ. J. Combin.* **12** (1991), 43–49.

[14] T. Müller, Parity patterns in Hecke groups and Fermat primes, in: *Groups: Topological, Combinatorial and Arithmetic Aspects* (T. W. Müller editor), LMS Lecture Note Series, Cambridge University Press, to appear.

[15] T. Müller, Modular subgroup arithmetic and a theorem of Philip Hall, *Bull. London Math. Soc.* **34** (2002), 587–598.

[16] T. Müller, Modular subgroup arithmetic in free products, *Forum Math.*, in press.

[17] J. Nielsen, The commutator group of the free product of cyclic groups, *Mat. Tidsskr.* **B** (1948), 49–56.

[18] J.-P. Serre, *Trees*, Springer, Berlin, 1980.
[19] J.-P. Serre, *Cohomologie des groupes discrets*, Ann. Math. Studies vol. 70, Princeton University Press, 1971.
[20] W. Stothers, The number of subgroups of given index in the modular group, *Proc. Royal Soc. Edinburgh* **78A** (1977), 105–112.

SCHOOL OF MATHEMATICAL SCIENCES
QUEEN MARY, UNIVERSITY OF LONDON
MILE END ROAD
LONDON E1 4NS
UNITED KINGDOM
E-mail: P.J.Cameron@qmul.ac.uk
and T.W.Muller@qmul.ac.uk