# A DESCENT PRINCIPLE IN MODULAR SUBGROUP ARITHMETIC

PETER J. CAMERON AND THOMAS W. MÜLLER

## 1. Introduction

For a group $\Gamma$ and a positive integer $n$, denote by $s_n(\Gamma)$ the number of index $n$ subgroups in $\Gamma$.[1] We call $\Gamma$ an FSG-*group* if $s_n(\Gamma)$ is finite for all $n$. In particular, finitely generated groups have this property. Modular subgroup arithmetic, a chapter in the theory of subgroup growth, deals with divisibility properties of the sequence $\{s_n(\Gamma)\}_{n\geq 1}$ or related subgroup counting functions and their connection with the algebraic structure of the underlying group $\Gamma$; cf. the forthcoming book [11] 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 $\Gamma = \mathrm{PSL}_2(\mathbb{Z}) \cong C_2 * C_3$ 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. [18] and [12]. Moreover, by a theorem of Stothers [21],

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

On the other hand, it follows from M. Hall's recursion formula ([7, Theorem 5.2])

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

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 $\Gamma$, define the *p-pattern* $\Pi^{(p)}(\Gamma)$ of $\Gamma$ to be the family of sets

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

where

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

in particular, $\Pi_\Gamma := \Pi_1^{(2)}(\Gamma)$ is the *parity pattern* of $\Gamma$. The main result of this paper is the following.

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

**Theorem 1** (Descent Principle)**.** *Let $p$ be a prime, $\Gamma$ an* FSG*-group, and let $\Delta \trianglelefteq \Gamma$ be a normal subgroup of index $p^r$. Then*

$$\Pi_j^{(p)}(\Gamma) = p^r\,\Pi_j^{(p)}(\Delta)\ \cup \bigcup_{0\le\rho<r} p^\rho\Big(\Pi_j^{(p)}(\Delta)\cap(\mathbb{N}-p\,\mathbb{N})\Big),\quad 0<j<p. \tag{2}$$

*Equivalently, if $X_{\Gamma,p}(z)$ denotes the mod $p$ projection of the series $\sum_{n\ge0} s_{n+1}(\Gamma)z^n$, and if $X_{\Delta,p}(z)$ is the corresponding $GF(p)$-series for the group $\Delta$, then under our assumptions*

$$X_{\Gamma,p}(z) = \sum_{\rho=0}^{r} z^{p^\rho-1}\,X_{\Delta,p}(z^{p^\rho})\ +\ \sum_{\rho=0}^{r-1} z^{p^{\rho+1}-1}\,X_{\Delta,p}^{(p-1)}(z^{p^\rho}). \tag{3}$$

Theorem 1 generalizes the main result of [15], where the conclusions (2) and (3) are established under the extra hypothesis that $\Gamma/\Delta$ is cyclic. As the above example demonstrates, the assumption in Theorem 1 that $(\Gamma:\Delta)$ be a prime power cannot be weakened. Also, it is easy to see by examples that, in the context of this theorem, the subgroup $\Delta$ must be chosen as a normal subgroup.

A certain cohomological property of finite $p$-groups (to be of 'Frobenius type') plays a crucial role in the proof of the main theorem. This concept, whose definition will be given in the next section, is implicit in Frobenius' theorem concerning the equation $x^m = 1$ in finite groups[2] and P. Hall's twisted version [9, Theorem 1.6] of the latter result. It follows from Hall's theorem that every cyclic group of prime power order is of Frobenius type. The following generalization, to be established in Section 2, is a crucial ingredient in our proof of the main theorem.

**Proposition 1.** *Every group of prime power order is of Frobenius type.*

The relevance of this proposition in the present context stems from the following reduction result, whose proof occupies Section 3.

**Proposition 2.** *Let $p$ be a prime, $\Gamma$ an* FSG*-group, and let $\Delta\trianglelefteq\Gamma$ be a normal subgroup of index $p^r$ with $\Gamma/\Delta$ of Frobenius type. Then formulae* (2) *and* (3) *hold true.*

Our main result follows immediately from these two propositions.

In the remainder of the paper we present two applications. First, consider the fundamental group $\Gamma$ of a finite graph $(\Gamma(-), Y)$ of finite $p$-groups. If $\Gamma$ contains a free normal subgroup $\mathfrak{F}$ of index $m_\Gamma = \operatorname{lcm}\big\{|\Gamma(v)| : v\in V(Y)\big\}$, then $s_n(\Gamma)$ 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 normal subgroup $\mathfrak{F}$ is not guaranteed, and in Section 4 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 $\mathfrak{G}^{*q}$ of a finite group $\mathfrak{G}$ with $q$ a $p$-power to groups of the more general form $\mathfrak{H} * \mathfrak{G}^{*q}$, where $\mathfrak{H}$ is any finite $p$-group; cf. Theorem 3.

[2]See [4, §2, Theorem II] and [8].

## 2. Groups of Frobenius type

In what follows, a certain cohomological property of finite groups of prime power order (to be of 'Frobenius type') will play a crucial role. Recall the concept of a derivation (in a non-commutative setting): given groups $\mathfrak{G}$ and $\mathfrak{H}$, and a fixed action $\alpha : \mathfrak{G} \to \mathrm{Aut}(\mathfrak{H})$ by automorphisms of $\mathfrak{G}$ on $\mathfrak{H}$, a map $d : \mathfrak{G} \to \mathfrak{H}$ is called a *derivation* (with respect to the action $\alpha$), if

$$d(g_1 g_2) = \big(d(g_1)\big)^{\alpha(g_2)} d(g_2) \quad (g_1, g_2 \in \mathfrak{G}).$$

Note that, for a derivation $d : \mathfrak{G} \to \mathfrak{H}$ with respect to $\alpha$, we have $d(1) = 1$ and, consequently,

$$\big(d(g^{-1})\big)^{\alpha(g)} = (d(g))^{-1} \quad (g \in \mathfrak{G}).$$

**Definition 1.** *Let $p$ be a prime.*

(i) *A non-trivial finite $p$-group $\mathfrak{G}$ is termed* **admissible**, *if, for each finite group $\mathfrak{H}$ with $p \big| |\mathfrak{H}|$ and every action $\alpha : \mathfrak{G} \to \mathrm{Aut}(\mathfrak{H})$, the corresponding set $\mathrm{Der}_\alpha(\mathfrak{G}, \mathfrak{H})$ of derivations $d : \mathfrak{G} \to \mathfrak{H}$, formed with respect to this action $\alpha$, has cardinality a multiple of $p$.*

(ii) *A finite $p$-group $\mathfrak{G}$ is said to be of* **Frobenius type**, *if every subgroup $\mathfrak{U} > 1$ of $\mathfrak{G}$ is admissible.*

By a theorem of Philip Hall, cyclic groups of prime power order are of Frobenius type. Indeed, an equivalent way of stating Hall's original result [9, Theorem 1.6] is as follows.

*Let $\mathfrak{C}$ be a finite cyclic group, $\mathfrak{H}$ a finite group, and let $\alpha : \mathfrak{C} \to \mathrm{Aut}(\mathfrak{H})$ be an action by automorphisms of $\mathfrak{C}$ on $\mathfrak{H}$. Then*

$$|\mathrm{Der}_\alpha(\mathfrak{C}, \mathfrak{H})| \equiv 0 \mod \gcd(|\mathfrak{C}|, |\mathfrak{H}|).$$

For $\alpha = 1$, the trivial action of $\mathfrak{C}$ on $\mathfrak{H}$, Hall's theorem reduces to the well-known result of Frobenius concerning the equation $x^n = 1$ in finite groups. The problem to discern which finite groups of prime power order are of Frobenius type was raised in [17]. Proposition 1 provides a somewhat surprising solution of this problem. In order to establish this result, we first deal with the untwisted case ($\alpha = 1$).

**Lemma.** *Let $p$ be a prime, $\mathfrak{G}$ a non-trivial finite $p$-group, and let $\mathfrak{H}$ be a finite group of order divisible by $p$. Then $|\mathrm{Hom}(\mathfrak{G}, \mathfrak{H})| \equiv 0 \mod p$.*

*Proof.* Classifying homomorphisms by their kernel, and applying the isomorphism theorem, we find that

$$|\mathrm{Hom}(\mathfrak{G}, \mathfrak{H})| = \sum_{\mathfrak{V} \trianglelefteq \mathfrak{G}} |\mathrm{Inj}(\mathfrak{G}/\mathfrak{V}, \mathfrak{H})|. \tag{4}$$

We now make use of the facts that (i) every subgroup of index $p$ in a finite $p$-group is normal, (ii) the automorphism group of $\mathfrak{G}/\mathfrak{V}$ contains an element of order $p$, provided

$|\mathfrak{G}/\mathfrak{V}| > p$, and (iii) $\mathrm{Aut}(\mathfrak{G}/\mathfrak{V})$ acts freely on the set $\mathrm{Inj}(\mathfrak{G}/\mathfrak{V}, \mathfrak{H})$, provided the latter is non-empty. The second fact follows, for instance, from Gaschütz's theorem [6] asserting the existence of an outer automorphism of order $p$; however, since we only need to know that $p \big| |\mathrm{Aut}(\mathfrak{G}/\mathfrak{V})|$ for $|\mathfrak{G}/\mathfrak{V}| > p$, we can get by with a more elementary argument. Indeed, if $\mathfrak{G}/\mathfrak{V}$ is non-abelian, then it has an inner automorphism of order $p$. If, on the other hand, $\mathfrak{G}/\mathfrak{V}$ is abelian and $|\mathfrak{G}/\mathfrak{V}| > p$, then $\mathfrak{G}/\mathfrak{V}$ must contain a direct summand of one of the forms $\mathfrak{C}_{p^\sigma}$ or $\sigma\mathfrak{C}_p$ with $\sigma \geq 2$. In the first case, $|\mathrm{Aut}(\mathfrak{G}/\mathfrak{V})|$ is divisible by

$$|\mathrm{Aut}(\mathfrak{C}_{p^\sigma})| = \varphi(p^\sigma) = p^{\sigma-1}(p-1) \equiv 0 \mod p,$$

where $\varphi$ is Euler's totient function, while, in the second case, $|\mathrm{Aut}(\mathfrak{G}/\mathfrak{V})|$ must be divisible by

$$|\mathrm{Aut}(\sigma\mathfrak{C}_p)| = |\mathrm{GL}_\sigma(p)| = (p^\sigma - 1)(p^\sigma - p)\cdots(p^\sigma - p^{\sigma-1}) \equiv 0 \mod p.$$

Hence, evaluating (4) modulo $p$, we get

$$|\operatorname{Hom}(\mathfrak{G}, \mathfrak{H})| \equiv 1 + s_p(\mathfrak{G})|\mathrm{Inj}(\mathfrak{C}_p, \mathfrak{H})| \mod p.$$

We have $s_p(\mathfrak{G}) \equiv 1 \bmod p$ by Frobenius' generalization of Sylow's third theorem and the fact that $\mathfrak{G} \neq 1$. (Alternatively, one might compute

$$s_p(\mathfrak{G}) = \frac{p^{r(\overline{\mathfrak{G}})} - 1}{p-1} = 1 + p + p^2 + \cdots + p^{r(\overline{\mathfrak{G}})-1} \equiv 1 \mod p,$$

where $r(\overline{\mathfrak{G}})$ is the rank of the factor group $\overline{\mathfrak{G}} = \mathfrak{G}/\Phi(\mathfrak{G})$, since every subgroup of $\mathfrak{G}$ of index $p$ contains $\Phi(\mathfrak{G})$. Moreover, by Frobenius' theorem concerning the equation $x^m = 1$ in finite groups and the fact that $p \big| |\mathfrak{H}|$, we have

$$|\mathrm{Inj}(\mathfrak{C}_p, \mathfrak{H})| \equiv -1 \mod p,$$

whence the lemma. □

*Proof of Proposition* 1. Let $p$ be a prime, $\mathfrak{G}$ a non-trivial finite $p$-group, $\mathfrak{H}$ a finite group of order divisible by $p$, and let $\alpha : \mathfrak{G} \to \mathrm{Aut}(\mathfrak{H})$ be an action by automorphisms of $\mathfrak{G}$ on $\mathfrak{H}$, where multiplication in the group $\mathrm{Aut}(\mathfrak{H})$ is given by the rule

$$(\sigma_1 \cdot \sigma_2)(h) := \sigma_2(\sigma_1(h)) \quad (\sigma_1, \sigma_2 \in \mathrm{Aut}(\mathfrak{H}),\ h \in \mathfrak{H}).$$

We have to show that

$$|\mathrm{Der}_\alpha(\mathfrak{G}, \mathfrak{H})| \equiv 0 \mod p. \tag{5}$$

Let

$$\mathcal{F}(\mathfrak{G}, \mathfrak{H}) = \mathfrak{H}^{\mathfrak{G}}$$

be the set of all functions from $\mathfrak{G}$ to $\mathfrak{H}$. We make $\mathfrak{G}$ act (from the right) on $\mathcal{F}(\mathfrak{G}, \mathfrak{H})$ by setting

$$(\mathfrak{f} \circledast g)(x) := \big(\mathfrak{f}(gxg^{-1})\big)^{\alpha(g)} \quad \big(g, x \in \mathfrak{G},\ \mathfrak{f} \in \mathcal{F}(\mathfrak{G}, \mathfrak{H})\big).$$

For $g_1, g_2, x \in \mathfrak{G}$ and $\mathfrak{f} \in \mathcal{F}(\mathfrak{G}, \mathfrak{H})$,

$$\begin{aligned}\big((\mathfrak{f} \circledast g_1) \circledast g_2\big)(x) &= \big((\mathfrak{f} \circledast g_1)(g_2 x g_2^{-1})\big)^{\alpha(g_2)} \\ &= \big(\mathfrak{f}(g_1 g_2 x g_2^{-1} g_1^{-1})\big)^{\alpha(g_1 g_2)} \\ &= \big(\mathfrak{f} \circledast (g_1 g_2)\big)(x),\end{aligned}$$

as well as $\mathfrak{f} \circledast 1 = \mathfrak{f}$, and we have indeed defined an action of $\mathfrak{G}$ on $\mathcal{F}(\mathfrak{G}, \mathfrak{H})$. In what follows, two distinguished subsets of $\mathcal{F}(\mathfrak{G}, \mathfrak{H})$ will play a role: the set $\mathrm{Der}_\alpha(\mathfrak{G}, \mathfrak{H})$ of derivations $d : \mathfrak{G} \to \mathfrak{H}$ with respect to $\alpha$, and the set $\mathrm{Hom}^*(\mathfrak{G}, \mathfrak{H})$ of anti-homomorphisms from $\mathfrak{G}$ to $\mathfrak{H}$. Note that

$$|\,\mathrm{Hom}(\mathfrak{G}, \mathfrak{H})| = |\,\mathrm{Hom}^*(\mathfrak{G}, \mathfrak{H})|, \tag{6}$$

a bijection being given by the map

$$\psi \mapsto \psi^*, \quad \psi^*(g) := (\psi(g))^{-1} \quad \big(g \in \mathfrak{G},\ \psi \in \mathrm{Hom}(\mathfrak{G}, \mathfrak{H})\big).$$

We have to check that the action of $\mathfrak{G}$ on $\mathcal{F}(\mathfrak{G}, \mathfrak{H})$ defined above restricts to an action of $\mathfrak{G}$ on the subsets $\mathrm{Der}_\alpha(\mathfrak{G}, \mathfrak{H})$ and $\mathrm{Hom}^*(\mathfrak{G}, \mathfrak{H})$. Indeed, for $g, x, y \in \mathfrak{G}$ and $d \in \mathrm{Der}_\alpha(\mathfrak{G}, \mathfrak{H})$, we have

$$\begin{aligned}(d \circledast g)(xy) &= \big(d(gxyg^{-1})\big)^{\alpha(g)} \\ &= \big(d(gxg^{-1})\big)^{\alpha(gy)} \big(d(gyg^{-1})\big)^{\alpha(g)} \\ &= \big((d \circledast g)(x)\big)^{\alpha(y)} (d \circledast g)(y),\end{aligned}$$

that is, $d \circledast g : \mathfrak{G} \to \mathfrak{H}$ is again a derivation with respect to $\alpha$. Similarly, for $g, x, y \in \mathfrak{G}$ and $\psi^* \in \mathrm{Hom}^*(\mathfrak{G}, \mathfrak{H})$,

$$\begin{aligned}(\psi^* \circledast g)(xy) &= \big(\psi^*(gxyg^{-1})\big)^{\alpha(g)} \\ &= \big(\psi^*(gyg^{-1})\big)^{\alpha(g)} \big(\psi^*(gxg^{-1})\big)^{\alpha(g)} \\ &= (\psi^* \circledast g)(y)(\psi^* \circledast g)(x).\end{aligned}$$

Denote by $\mathrm{Der}_\alpha(\mathfrak{G}, \mathfrak{H})^{\mathfrak{G}}$ and $\mathrm{Hom}^*(\mathfrak{G}, \mathfrak{H})^{\mathfrak{G}}$ the fixed point sets of $\mathrm{Der}_\alpha(\mathfrak{G}, \mathfrak{H})$ and $\mathrm{Hom}^*(\mathfrak{G}, \mathfrak{H})$, respectively, under the respective $\mathfrak{G}$-action, so that

$$|\mathrm{Der}_\alpha(\mathfrak{G}, \mathfrak{H})| \equiv |\mathrm{Der}_\alpha(\mathfrak{G}, \mathfrak{H})^{\mathfrak{G}}| \mod p \tag{7}$$

and

$$|\,\mathrm{Hom}^*(\mathfrak{G}, \mathfrak{H})| \equiv |\,\mathrm{Hom}^*(\mathfrak{G}, \mathfrak{H})^{\mathfrak{G}}| \mod p. \tag{8}$$

The decisive point in the proof is the fact that

$$\mathrm{Der}_\alpha(\mathfrak{G}, \mathfrak{H})^{\mathfrak{G}} = \mathrm{Der}_\alpha(\mathfrak{G}, \mathfrak{H}) \cap \mathrm{Hom}^*(\mathfrak{G}, \mathfrak{H}) = \mathrm{Hom}^*(\mathfrak{G}, \mathfrak{H})^{\mathfrak{G}}. \tag{9}$$

Indeed, let $d \in \mathrm{Der}_\alpha(\mathfrak{G}, \mathfrak{H})$. Then

$$d \in \mathrm{Der}_\alpha(\mathfrak{G}, \mathfrak{H})^{\mathfrak{G}} \Longleftrightarrow \big(d(gxg^{-1})\big)^{\alpha(G)} = d(x) \quad (g, x \in \mathfrak{G}).$$

Now

$$\begin{aligned}\big(d(gxg^{-1})^{\alpha(g)} &= \Big(\big(d(gx)\big)^{\alpha(g^{-1})}d(g^{-1})\Big)^{\alpha(g)}\\ &= d(gx)\big(d(g^{-1})\big)^{\alpha(g)}\\ &= d(gx)\big(d(g)\big)^{-1},\end{aligned}$$

hence

$$d \in \mathrm{Der}_\alpha(\mathfrak{G},\mathfrak{H})^{\mathfrak{G}} \Longleftrightarrow d \in \mathrm{Hom}^*(\mathfrak{G},\mathfrak{H}), \quad d \in \mathrm{Der}_\alpha(\mathfrak{G},\mathfrak{H}).$$

Similarly, if $\psi^* \in \mathrm{Hom}^*(\mathfrak{G},\mathfrak{H})$, then

$$\begin{aligned}\psi^* \in \mathrm{Hom}^*(\mathfrak{G},\mathfrak{H})^{\mathfrak{G}} &\iff \psi^*(g^{-1}xg) = \big(\psi^*(x)\big)^{\alpha(g)} \quad (g,x \in \mathfrak{G})\\ &\iff \psi^*(xg)\psi^*(g^{-1}) = \big(\psi^*(x)\big)^{\alpha(g)} \quad (g,x \in \mathfrak{G})\\ &\iff \psi^* \in \mathrm{Der}_\alpha(\mathfrak{G},\mathfrak{H}),\end{aligned}$$

whence (9). In view of equations (6)–(9) and the lemma, we now find that, modulo $p$,

$$\begin{aligned}|\mathrm{Der}_\alpha(\mathfrak{G},\mathfrak{H})| &\equiv |\mathrm{Der}_\alpha(\mathfrak{G},\mathfrak{H})^{\mathfrak{G}}|\\ &= |\mathrm{Der}_\alpha(\mathfrak{G},\mathfrak{H}) \cap \mathrm{Hom}^*(\mathfrak{G},\mathfrak{H})|\\ &= |\,\mathrm{Hom}^*(\mathfrak{G},\mathfrak{H})^{\mathfrak{G}}|\\ &\equiv |\,\mathrm{Hom}^*(\mathfrak{G},\mathfrak{H})|\\ &= |\,\mathrm{Hom}(\mathfrak{G},\mathfrak{H})| \equiv 0,\end{aligned}$$

whence (5), and the proof of Proposition 1 is complete. □

## 3. Proof of Proposition 2

Put $\Gamma/\Delta = \mathfrak{G}$. A subgroup $\widetilde{\Gamma}$ of index $n$ in $\Gamma$, which is not contained in $\Delta$, projects onto a non-trivial subgroup $\widetilde{\Gamma}\Delta/\Delta = \widetilde{\mathfrak{G}}$ of $\mathfrak{G}$, say $|\widetilde{\mathfrak{G}}| = p^\rho$ with $0 < \rho \le r$, and intersects $\Delta$ in a subgroup $\widetilde{\Delta}$ with $(\Delta : \widetilde{\Delta}) = n/p^{r-\rho}$. Hence, each such $\widetilde{\Gamma}$ is a member of the set

$$\bigcup_{0<\rho\le r} \bigcup_{(\mathfrak{G}:\widetilde{\mathfrak{G}})=p^{r-\rho}} \bigcup_{(\Delta:\widetilde{\Delta})=n/p^{r-\rho}} \mathcal{S}(\widetilde{\mathfrak{G}},\widetilde{\Delta}), \tag{10}$$

where

$$\mathcal{S}(\widetilde{\mathfrak{G}},\widetilde{\Delta}) := \Big\{\widetilde{\Gamma} \le \Gamma :\ \widetilde{\Gamma} \cap \Delta = \widetilde{\Delta},\ \widetilde{\Gamma}\Delta/\Delta = \widetilde{\mathfrak{G}}\Big\},$$

and, conversely, each subgroup $\widetilde{\Gamma}$ contained in the set (10) is of index $n$ in $\Gamma$ and not contained in $\Delta$. It follows that

$$s_n(\Gamma) = \sum_{0<\rho\le r} \sum_{(\mathfrak{G}:\widetilde{\mathfrak{G}})=p^{r-\rho}} \sum_{(\Delta:\widetilde{\Delta})=n/p^{r-\rho}} |\mathcal{S}(\widetilde{\mathfrak{G}},\widetilde{\Delta})| + \begin{cases} s_{n/p^r}(\Delta), & p^r \mid n\\ 0, & p^r \nmid n.\end{cases} \tag{11}$$

Pick $\rho$, $\widetilde{\mathfrak{G}}$, and $\widetilde{\Delta}$ as in (11), and consider the corresponding set $\mathcal{S}(\widetilde{\mathfrak{G}},\widetilde{\Delta})$. We claim that

$$|\mathrm{Aut}(\widetilde{\mathfrak{G}})|\cdot|\mathcal{S}(\widetilde{\mathfrak{G}},\widetilde{\Delta})| = \big|\big\{\iota\in\mathrm{Hom}(\widetilde{\mathfrak{G}},N_\Gamma(\widetilde{\Delta})/\widetilde{\Delta}):\ \tau\iota(\widetilde{\mathfrak{G}})=\widetilde{\mathfrak{G}}\big\}\big|, \tag{12}$$

where $\tau : N_\Gamma(\widetilde{\Delta})/\widetilde{\Delta}\to\mathfrak{G}$ is the natural map with kernel $N_\Delta(\widetilde{\Delta})/\widetilde{\Delta}$ induced by the identity. Indeed, if we take $\widetilde{\Gamma}\in\mathcal{S}(\widetilde{\mathfrak{G}},\widetilde{\Delta})$, then combining the canonical isomorphism $\widetilde{\mathfrak{G}}\cong\widetilde{\Gamma}/\widetilde{\Delta}$ with the embedding $\widetilde{\Gamma}/\widetilde{\Delta}\hookrightarrow N_\Gamma(\widetilde{\Delta})/\widetilde{\Delta}$ induced by the inclusion map $\widetilde{\Gamma}\hookrightarrow N_\Gamma(\widetilde{\Delta})$ gives a homomorphism $\iota:\widetilde{\mathfrak{G}}\to N_\Gamma(\widetilde{\Delta})/\widetilde{\Delta}$, such that $\tau\iota=\mathrm{id}_{\widetilde{\mathfrak{G}}}$. Conversely, if $\iota:\widetilde{\mathfrak{G}}\to N_\Gamma(\widetilde{\Delta})/\widetilde{\Delta}$ is a homomorphism satisfying $\tau\iota=\mathrm{id}_{\widetilde{\mathfrak{G}}}$, then $\pi^{-1}(\iota(\widetilde{\mathfrak{G}}))$ is contained in the set $\mathcal{S}(\widetilde{\mathfrak{G}},\widetilde{\Delta})$. Here, $\pi : N_\Gamma(\widetilde{\Delta})\to N_\Gamma(\widetilde{\Delta})/\widetilde{\Delta}$ is the canonical projection map. It is straightforward to check that these two maps invert each other, whence the existence of a bijective correspondence between $\mathcal{S}(\widetilde{\mathfrak{G}},\widetilde{\Delta})$ and the set

$$\big\{\iota\in\mathrm{Hom}(\widetilde{\mathfrak{G}},N_\Gamma(\widetilde{\Delta})/\widetilde{\Delta}):\ \tau\iota=\mathrm{id}_{\widetilde{\mathfrak{G}}}\big\}.$$

It follows in particular, that our claim (12) holds if the set on its right-hand side is empty. If, on the other hand, this set is non-empty, then it decomposes into $|\mathrm{Aut}(\widetilde{\mathfrak{G}})|$ disjoint subsets of equal size according to the automorphism $\tau\iota\in\mathrm{Aut}(\widetilde{\mathfrak{G}})$ induced by $\iota$, whence (12). The set on the right-hand side of (12) is of cardinality

$$|\mathrm{Aut}(\widetilde{\mathfrak{G}})|\sum_{\mathfrak{V}}\big|\mathrm{Der}_{\alpha_{\mathfrak{V}}}(\widetilde{\mathfrak{G}},N_\Delta(\widetilde{\Delta})/\widetilde{\Delta})\big|,$$

where the summation extends over all subgroups $\mathfrak{V}\leq\tau^{-1}(\widetilde{\mathfrak{G}})$ which contain $N_\Delta(\widetilde{\Delta})/\widetilde{\Delta}$ and are split extensions of $N_\Delta(\widetilde{\Delta})/\widetilde{\Delta}$ by $\widetilde{\mathfrak{G}}$, and where, for each such $\mathfrak{V}$, the action $\alpha_{\mathfrak{V}}$ of $\widetilde{\mathfrak{G}}$ on $N_\Delta(\widetilde{\Delta})/\widetilde{\Delta}$ is by conjugation via a fixed chosen complement to $N_\Delta(\widetilde{\Delta})/\widetilde{\Delta}$ in $\mathfrak{V}$. Since $\mathfrak{G}$ is assumed to be of Frobenius type, we conclude that $|\mathcal{S}(\widetilde{\mathfrak{G}},\widetilde{\Delta})|\equiv 0 \bmod p$, unless $p\nmid|N_\Delta(\widetilde{\Delta})/\widetilde{\Delta}|$. Combining the latter observation with (12), we find that the triple sum occurring on the right-hand side of (11) is congruent modulo $p$ to

$$\sum_{0<\rho\leq r}\ \sum_{(\mathfrak{G}:\widetilde{\mathfrak{G}})=p^{r-\rho}}\ \sum\Big|\Big\{\widetilde{\Gamma}\leq\tau^{-1}(\widetilde{\mathfrak{G}}):\ \widetilde{\Gamma}\cong\widetilde{\mathfrak{G}}\Big\}\Big|, \tag{13}$$

where the innermost sum is extended over all subgroups $\widetilde{\Delta}$ of index $n/p^{r-\rho}$ in $\Delta$ satisfying $p\nmid(N_\Delta(\widetilde{\Delta}):\widetilde{\Delta})$ and $p^\rho\mid|\tau^{-1}(\widetilde{\mathfrak{G}})|$. Omitting the condition that $p^\rho\mid|\tau^{-1}(\widetilde{\mathfrak{G}})|$ (which is possible since this restriction only avoids zero summands), we can rewrite (13) by interchanging the second and third summation, to obtain

$$\sum_{0<\rho\leq r}\ \sum_{\substack{(\Delta:\widetilde{\Delta})=n/p^{r-\rho}\\ p\nmid(N_\Delta(\widetilde{\Delta}):\widetilde{\Delta})}}\ \sum_{(\mathfrak{G}:\widetilde{\mathfrak{G}})=p^{r-\rho}}\Big|\Big\{\widetilde{\Gamma}\leq\tau^{-1}(\widetilde{\mathfrak{G}}):\ \widetilde{\Gamma}\cong\widetilde{\mathfrak{G}}\Big\}\Big|. \tag{14}$$

Since $p\nmid(N_\Delta(\widetilde{\Delta}):\widetilde{\Delta})$, any $p$-subgroup of $N_\Gamma(\widetilde{\Delta})/\widetilde{\Delta}$ is mapped faithfully under $\tau$; hence, the inner sum in (14) precisely counts the number of subgroups of order $p^\rho$ in the group $N_\Gamma(\widetilde{\Delta})/\widetilde{\Delta}$, the latter number being congruent to 1 modulo $p$ (by Frobenius' generalization of Sylow's third theorem) provided that $p^\rho\big||N_\Gamma(\widetilde{\Delta})/\widetilde{\Delta}|$, and zero

otherwise. Consequently, we find that

$$s_n(\Gamma) \equiv \sum_{0<\rho\le r} |\Omega_{\rho,n}| \; + \; \begin{cases} s_{n/p^r}(\Delta), & p^r \mid n \\ 0, & p^r \nmid n \end{cases} \mod p, \tag{15}$$

where

$$\Omega_{\rho,n} := \Big\{ \widetilde{\Delta} \le \Delta : \; (\Delta : \widetilde{\Delta}) = n/p^{r-\rho},\, p \nmid (N_\Delta(\widetilde{\Delta}) : \widetilde{\Delta}),\, p^\rho \mid (N_\Gamma(\widetilde{\Delta}) : \widetilde{\Delta}) \Big\}.$$

Fix $\rho$ and $n$, and denote by $\mathcal{U}_{n/p^{r-\rho}}(\Delta)$ the set of subgroups of index $n/p^{r-\rho}$ in $\Delta$. Since $\Delta$ is normal in $\Gamma$, the group $\Gamma$ acts by conjugation on $\mathcal{U}_{n/p^{r-\rho}}(\Delta)$, and this action restricts to an action of $\Gamma$ (and hence of $\Delta$) on the sets $\Omega_{\rho,n}$. Therefore, if $p^{r-\rho+1} \mid n$ and $\widetilde{\Delta} \in \Omega_{\rho,n}$, then $(\Delta : N_\Delta(\widetilde{\Delta})) \equiv 0 \; (p)$, and $\Omega_{\rho,n}$ decomposes into orbits of length divisible by $p$ under $\Delta$. Suppose, on the other hand, that $p^{r-\rho} \mid\mid n$, and consider the action of $\Gamma$ on the set

$$\mathcal{U}_{n/p^{r-\rho}}(\Delta) - \Omega_{\rho,n} = \Big\{ \widetilde{\Delta} \le \Delta : \; (\Delta : \widetilde{\Delta}) = n/p^{r-\rho},\; p^\rho \nmid (N_\Gamma(\widetilde{\Delta}) : \widetilde{\Delta}) \Big\}.$$

Then, if $\widetilde{\Delta} \in \mathcal{U}_{n/p^{r-\rho}}(\Delta) - \Omega_{\rho,n}$, we have $(\Gamma : N_\Gamma(\widetilde{\Delta})) \equiv 0 \; (p)$; that is, $\mathcal{U}_{n/p^{r-\rho}}(\Delta) - \Omega_{\rho,n}$ decomposes into classes of length divisible by $p$ under $\Gamma$. Hence,

$$|\Omega_{\rho,n}| \equiv \begin{cases} s_{n/p^{r-\rho}}(\Delta), & p^{r-\rho} \mid\mid n \\ 0, & \text{otherwise} \end{cases} \mod p. \tag{16}$$

Analysing (15) by means of (16) gives

$$s_n(\Gamma) \equiv s_{n/p^r}(\Delta) \mod p, \quad p^r \mid n, \tag{17}$$

as well as

$$s_n(\Gamma) \equiv s_{n/p^{r-\rho}}(\Delta) \mod p, \quad p^{r-\rho} \parallel n,\; 0 < \rho \le r. \tag{18}$$

Statements (17) and (18) can be rephrased as

$$\Pi_j^{(p)}(\Gamma) \cap p^r\,\mathbb{N} = p^r\,\Pi_j^{(p)}(\Delta), \quad 0 < j < p, \tag{19}$$

and

$$\Pi_j^{(p)}(\Gamma) \cap p^{r-\rho}\,(\mathbb{N} - p\,\mathbb{N}) = p^{r-\rho}\big(\Pi_j^{(p)}(\Delta) \cap (\mathbb{N} - p\,\mathbb{N})\big), \quad 0 < \rho \le r,\; 0 < j < p, \tag{20}$$

respectively. Taking the union of (19) and (20) for every fixed $j$ now yields (2). It remains to establish equation (3) as an equivalent version of (2). Assuming (2), we have

$$X_{\Gamma,p}(z) = Y(z) \; + \sum_{0\le\rho<r} Y_\rho(z),$$

where

$$Y(z) := \sum_{0<j<p} \sum_{n\in\Pi_j^{(p)}(\Delta)} j\, z^{p^r n - 1}$$

and

$$Y_\rho(z) := \sum_{0<j<p} \sum_{n\in\Pi_j^{(p)}(\Delta)\cap(\mathbb{N}-p\,\mathbb{N})} j\, z^{p^\rho n - 1}, \quad 0 \le \rho < r.$$

Clearly,

$$Y(z) = z^{p^r-1}\, X_{\Delta,p}(z^{p^r}).$$

Moreover, by Wilson's theorem,

$$\begin{aligned} Y_\rho(z) &= z^{p^\rho-1}\, X_{\Delta,p}(z^{p^\rho}) \;+\; \sum_{0<j<p} \sum_{n\in\Pi_j^{(p)}(\Delta)} j\,(n-1)\,(n-2)\cdots(n-p+1)\, z^{p^\rho n-1} \\ &= z^{p^\rho-1}\, X_{\Delta,p}(z^{p^\rho}) \;+\; z^{p^{\rho+1}-1}\, X_{\Delta,p}^{(p-1)}(z^{p^\rho}), \end{aligned}$$

whence (3). The converse follows in a similar way.

## 4. Divisibility properties determined by free normal subgroups

The category of graphs used in this section is described in Serre's book [19]. Let $(\Gamma(-), Y)$ be a finite graph of finite groups with fundamental group $\Gamma = \pi_1(\Gamma(-), Y)$, 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 $m_\Gamma$ be the least common multiple of the orders of the finite subgroups in $\Gamma$, that is,

$$m_\Gamma = \operatorname{lcm}\Big\{|\Gamma(v)| :\; v \in V(Y)\Big\}.$$

The *free rank* $\mu(\Gamma)$ of $\Gamma$ is defined as the rank of a free subgroup in $\Gamma$ of index $m_\Gamma$. It is connected with the rational Euler characteristic $\chi(\Gamma)$ of $\Gamma$ via

$$\mu(\Gamma) \;+\; m_\Gamma\, \chi(\Gamma) = 1, \tag{21}$$

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

$$\chi(\Gamma) = \sum_{v\in V(Y)} \frac{1}{|\Gamma(v)|} \;-\; \sum_{e\in E(Y)} \frac{1}{|\Gamma(e)|}; \tag{22}$$

cf. [1, Chap. IX, Prop. 7.3] or [20, Prop. 14]. If $\Gamma$ has a free normal subgroup $\mathfrak{F}$ of index $m_\Gamma$ and with quotient $\Gamma/\mathfrak{F}$ a $p$-group, then every vertex group $\Gamma(v)$ must be of $p$-power order; and if $\chi(\Gamma) \le 0$, then any free normal subgroup $\mathfrak{F}$ of index $m_\Gamma$ has rank $\operatorname{rk}(\mathfrak{F}) = \mu(\Gamma) \ge 1$, and, by Theorem 1, the $p$-pattern of $\Gamma$ is determined via (2) 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, $(\Gamma(-), Y)$ a finite graph of groups all of whose vertex groups are of $p$-power order, and let $\Gamma$ be its fundamental group. Let $m_\Gamma = p^r$, and suppose that $\Gamma$ contains a normal free subgroup of index $m_\Gamma$, and that $\chi(\Gamma) \le 0$. Then*

(i) *the function $s_n(\Gamma)$ is periodic modulo $p$,*

(ii) *for $p = 2$ we have $\Pi_\Gamma = \mathbb{N}$,*

(iii) *for $p = 3$ and $\mu(\Gamma)$ odd we have $\Pi_1^{(3)}(\Gamma) = \mathbb{N}$,*

(iv) *for $p = 3$ and $\mu(\Gamma)$ even, $s_n(\Gamma)$ is periodic modulo 3 with period $8\cdot 3^r$. More precisely, in this case $s_n(\Gamma) \equiv 1 \bmod 3$ if and only if $n$ is congruent $\bmod 8\cdot 3^r$ 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* $0 \le \rho < r-1$ *and* $0 \le \lambda < 3^{r-\rho-1}$;
*and* $s_n(\Gamma) \equiv 2 \bmod 3$ *if and only if* $n$ *is congruent* $\bmod 8 \cdot 3^r$ *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* $0 \le \rho < r-1$ *and* $0 \le \lambda < 3^{r-\rho-1}$.

The usefulness of Theorem 2 depends on our being able to verify the hypothesis that $\Gamma$ contains a normal free subgroup of index $m_\Gamma$. The remainder of this section is devoted to the latter problem.

**Proposition 3.** *Let $p$ be a prime, $(\Gamma(-), Y)$ a finite tree of groups all of whose vertex groups are of $p$-power order, $\Gamma \cong \pi_1(\Gamma(-), Y)$, and let $m_\Gamma = p^r$.*

(i) *If all vertex groups $\Gamma(v)$ are cyclic, then $\Gamma$ contains precisely*

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

*free normal subgroups of index $m_\Gamma$, where $\varphi$ is Euler's totient function.*

(ii) *If all vertex groups $\Gamma(v)$ are elementary abelian, then $\Gamma$ contains exactly*

$$\frac{\prod_{e \in E(Y)} \left[ |\Gamma(e)|^{r-d_e} \, |GL_{r-d_e}(p)| \right]}{\prod_{v \in V(Y)} \left[ |\Gamma(v)|^{r-d_v} \, |GL_{r-d_v}(p)| \right]}$$

*free normal subgroups of index $m_\Gamma$, where $d_\sigma = \dim_p \Gamma(\sigma)$, $\sigma \in V(Y) \cup E(Y)$.*

*Proof.* (i) This is [15, Lemma 1].

(ii) Let $\mathfrak{G}$ be an elementary abelian $p$-group of rank $r$. The number of free normal subgroups in $\Gamma$ of index $m_\Gamma$ is obtained by dividing by

$$|\mathrm{Aut}(\mathfrak{G})| = |GL_r(p)| = (p^r - 1)(p^r - p) \cdots (p^r - p^{r-1})$$

the number of homomorphisms $\psi : \Gamma \to \mathfrak{G}$ with the property that

$$\psi_{|\Gamma(v)} : \Gamma(v) \to \mathfrak{G} \text{ is an embedding} \tag{23}$$

for every vertex $v \in V(Y)$. We will show by induction on $|V(Y)|$ that there are precisely

$$|GL_r(p)| \, \frac{\prod_{e \in E(Y)} \left[ |\Gamma(e)|^{r-d_e} \, |GL_{r-d_e}(p)| \right]}{\prod_{v \in V(Y)} \left[ |\Gamma(v)|^{r-d_v} \, |GL_{r-d_v}(p)| \right]}$$

such homomorphisms $\psi$. This is true if $|V(Y)| = 1$. So suppose that $|V(Y)| \ge 2$, let $v_0$ be a terminal vertex of $Y$ such that

$$\max \left\{ |\Gamma(v)| : \ v \in V(Y) \backslash \{v_0\} \right\} = p^r,$$

and let $Y'$ be the subtree of $Y$ obtained by clipping the edge $e_0 \in E(Y)$ with $v_0 \in \partial e_0$. Let $\partial e_0 = \{v_0, v_0'\}$. We have $\Gamma = \Gamma' \underset{\Gamma(e_0)}{*} \Gamma(v_0)$, where $\Gamma' := \pi_1(\Gamma(-), Y')$, the

amalgamation being with respect to the canonical embeddings $\iota_{e_0}$, $\iota'_{e_0}$ of $\Gamma(e_0)$ in $\Gamma(v_0)$ respectively $\Gamma(v'_0)$. By our inductive hypothesis there are exactly

$$|GL_r(p)| \prod_{e\in E(Y')} \left[|\Gamma(e)|^{r-d_e}\,|GL_{r-d_e}(p)|\right] \Big/ \prod_{v\in V(Y')} \left[|\Gamma(v)|^{r-d_v}\,|GL_{r-d_v}(p)|\right]$$

homomorphisms $\psi' : \Gamma' \to \mathfrak{G}$ satisfying (23) for every $v \in V(Y')$. In order to extend a given such map $\psi'$ to a homomorphism $\psi$ on $\Gamma$ satisfying (23) for all $v \in V(Y)$, we have to find an embedding $j : \Gamma(v_0) \to \mathfrak{G}$ such that the diagram

$$\begin{array}{ccc} \Gamma(e_0) & \xrightarrow{\iota_{e_0}} & \Gamma(v_0) \\ {\scriptstyle \psi'_{|\Gamma(v'_0)}\circ\iota'_{e_0}}\big\downarrow & & \big\downarrow{\scriptstyle j} \\ \mathfrak{G} & = & \mathfrak{G} \end{array}$$

commutes. Let $\dim_p\Gamma(v_0) = r_0$ and $\dim_p\Gamma(e_0) = \rho_0$ with $0 \le \rho_0 \le r_0 \le r$. Moreover, let $C_0$ be a complement to $\iota_{e_0}(\Gamma(e_0))$ in $\Gamma(v_0)$, that is, $\Gamma(v_0) = \iota_{e_0}(\Gamma(e_0)) \oplus C_0$ and $\dim_p C_0 = r_0 - \rho_0$. Then our task is to find embeddings $j_{C_0} : C_0 \to \mathfrak{G}$ such that

$$\psi'(\iota'_{e_0}(\Gamma(e_0))) \cap j_{C_0}(C_0) = 0. \tag{24}$$

To this end, we first run through all $r_0$-dimensional subspaces $\mathfrak{G}'_0$ of $\mathfrak{G}$ containing $\psi'(\iota'_{e_0}(\Gamma(e_0)))$, then seek complements $C'_0$ to $\psi'(\iota'_{e_0}(\Gamma(e_0)))$ in each such $\mathfrak{G}'_0$, and finally identify $C_0$ with each such $C'_0$ via an isomorphism, which can be done in $|GL_{r_0-\rho_0}(p)|$ possible ways. There are $\binom{r-\rho_0}{r_0-\rho_0}_p$ $r_0$-dimensional subspaces $\mathfrak{G}'_0$ in $\mathfrak{G}$ containing $\psi'(\iota'_{e_0}(\Gamma(e_0)))$, and, given such a subspace $\mathfrak{G}'_0$, there are

$$|\mathrm{Hom}(\mathfrak{G}'_0/\psi'(\iota'_{e_0}(\Gamma(e_0))), \psi'(\iota'_{e_0}(\Gamma(e_0))))| = p^{\rho_0(r_0-\rho_0)}$$

complements $C'_0$ to $\psi'(\iota'_{e_0}(\Gamma(e_0)))$ in $\mathfrak{G}'_0$. Hence, the total number of embeddings $j_{C_0}$ satisfying (24) equals

$$\binom{r-\rho_0}{r_0-\rho_0}_p p^{\rho_0(r_0-\rho_0)}\,|GL_{r_0-\rho_0}(p)| = \frac{|\Gamma(e_0)|^{r-d_{e_0}}\,|GL_{r-d_{e_0}}(p)|}{|\Gamma(v_0)|^{r-d_{v_0}}\,|GL_{r-d_{v_0}}(p)|},$$

giving rise to the same number of extensions of a given map $\psi'$ on $\Gamma'$, whence (ii). □

A group $\mathfrak{G}$ is termed *homogeneous*, if every isomorphism between finitely generated subgroups is induced by an automorphism of $\mathfrak{G}$. This concept arouse (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. [10, 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 $\mathfrak{G}$ is homogeneous if and only if one of the following holds:

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

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

(iii) $\mathfrak{G} \cong \mathfrak{Q}^*$.

Here, $\mathfrak{Q}^*$ 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.

**Definition 2.** *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*

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

**Proposition 4.** *Let $p$ be a prime, let $(\Gamma(-), Y)$ be a finite tree of groups, $\Gamma \cong \pi_1(\Gamma(-), Y)$, and suppose that all vertex groups $\Gamma(v)$ are isomorphic to $\mathfrak{G}$, where $\mathfrak{G}$ is a finite homogeneous $p$-group. Then $\Gamma$ contains precisely*

$$\prod_{e \in E(Y)} |C_{\mathrm{Aut}(\mathfrak{G})}(\Gamma(e)^e)|$$

*free normal subgroups of index $m_\Gamma = |\mathfrak{G}|$.*

The proof of Proposition 4 is similar to that of Proposition 3 (ii), making use of the fact that $|C_{\mathrm{Aut}(\mathfrak{G})}(\Gamma(e)^e)|$ exactly equals the number of ways in which to extend any embedding of the edge group $\Gamma(e_0)$ into $\mathfrak{G}$ to an automorphism of $\mathfrak{G}$.

**Corollary 1.** (i) *If, in Proposition 4, we take $\mathfrak{G} = \mathfrak{Q}$, then $\Gamma$ contains precisely $24^{a(\Gamma)} \cdot 4^{b(\Gamma)}$ free normal subgroups of index $m_\Gamma = 8$, where*

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

(ii) *For $\mathfrak{G} = \mathfrak{Q}^*$, the number of free normal subgroups in $\Gamma$ of index $m_\Gamma = 64$ equals*

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

*where*

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

*Here, $\mathfrak{H}_{16}$ is the split extension*

$$\mathfrak{H}_{16} = \Big\langle a, b \mid a^4 = b^4 = 1,\ a^b = a^{-1} \Big\rangle.$$

The assertions of the corollary follow immediately from Proposition 4, once the orders of the corresponding centralizers are known. For the second part these have been found with the help of the computer algebra system GAP [5].

**Remark.** A finite group $\mathfrak{G}$ is homogeneous if and only if, for every tree of groups $(\Gamma(-), Y)$ with all vertex stabilizers isomorphic to $\mathfrak{G}$, $\Gamma = \pi_1(\Gamma(-), Y)$ contains a free normal subgroup of index $m_\Gamma$. Indeed, the forward implication follows immediately from Proposition 4. If, on the other hand, $\mathfrak{G}$ is not homogeneous, then there exists an isomorphism between two subgroups $\mathfrak{H}_1, \mathfrak{H}_2$ of $\mathfrak{G}$, which is not induced by an automorphism. We can then form the amalgam $\Gamma = \mathfrak{G} \underset{\mathfrak{H}}{*} \mathfrak{G}$, where the abstract group $\mathfrak{H}$ is identified with $\mathfrak{H}_1$ in the left factor and with $\mathfrak{H}_2$ in the right factor, in such a way that the isomorphism between $\mathfrak{H}_1$ and $\mathfrak{H}_2$ induced by these embeddings is the given isomorphism. Then $\Gamma$ does not possess a free normal subgroup of index $m_\Gamma = |\mathfrak{G}|$.

Now let $(\Gamma(-), Y)$ be a tree of groups all of whose vertex groups are isomorphic to $D_4$, the dihedral group of order 8, and let $\Gamma$ be its fundamental group. Call an edge $e \in E(Y)$ *wild*, if $\Gamma(e)$ 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.

**Proposition 5.** *Let $\Gamma$ be as above. Then $\Gamma$ has a free normal subgroup of index $m_\Gamma = 8$ if and only if the tree of groups $(\Gamma(-), Y)$ does not contain a wild edge. In the latter case, the number of free normal subgroups of index $m_\Gamma$ equals*

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

*where*

$$o(\Gamma) := \left|\left\{e \in E(Y) : \Gamma(e) \text{ outer}\right\}\right|,$$

*and an edge $e \in E(Y)$ is termed* inner *respectively* outer*, depending on whether or not $\Gamma(e)$ is embedded into the cyclic subgroup of order 4 of $\Gamma(\tau(e))$.*

*Proof.* Necessity of the stated existence criterion is clear. In the positive direction, one argues along lines similar to the proof of Proposition 3 (ii), distinguishing cases according to how the group associated with the relevant terminal edge $e$ is embedded into $\Gamma(\sigma(e))$ in the induction step. □

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

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

where the $\zeta_\kappa(\Gamma)$ are integers indexed by the divisors of $m_\Gamma$, given by

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

with $V(Y)$ and $E(Y)$ as above. We have $\zeta_\kappa(\Gamma) \geq 0$ for $\kappa < m_\Gamma$ and $\zeta_{m_\Gamma}(\Gamma) \geq -1$ with equality occurring in the latter inequality if and only if $Y$ is a tree; cf. [13, Lemma 2] and [14, Proposition 1]. It can be shown that the type $\tau(\Gamma)$ is in fact an invariant of the group $\Gamma$, that is, independent of the particular decomposition of $\Gamma$ in terms of a graph of groups $(\Gamma(-), Y)$, and that two virtually free groups $\Gamma_1$ and $\Gamma_2$ contain the same number of free subgroups of index $n$ for each positive integer $n$ if and only if

$\tau(\Gamma_1) = \tau(\Gamma_2)$; cf. [13, Theorem 2]. It follows from (22) that the Euler characteristic of $\Gamma$ can be expressed in terms of the type via

$$\chi(\Gamma) = -m_\Gamma^{-1} \sum_{\kappa | m_\Gamma} \varphi(m_\Gamma/\kappa)\zeta_\kappa(\Gamma). \tag{25}$$

Equations (21) and (25) 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 $\Gamma$ and a prime $p$ define the *p-rank* $\mu_p(\Gamma)$ of $\Gamma$ by means of the formula

$$\mu_p(\Gamma) = 1 + \sum_{p|\kappa|m_\Gamma} \varphi(m_\Gamma/\kappa)\zeta_\kappa(\Gamma).$$

Moreover, denote by $f_\lambda(\Gamma)$ the number of free subgroups in $\Gamma$ of index $\lambda m_\Gamma$.

**Proposition 6.** *Let $p$ be a prime, $(\Gamma(-), Y)$ a finite graph of groups all of whose vertex groups are non-trivial finite $p$-groups, and let $\Gamma = \pi_1(\Gamma(-), Y)$. Then the following assertions are equivalent:*

(i) $f_1(\Gamma) \not\equiv 0 \mod p$,

(ii) $\mu_p(\Gamma) = 0$,

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

**Corollary 2.** *Let $p$ be a prime, and let $\Gamma = \mathfrak{H} * C_p^{*s}$ be a free product of $s \geq 0$ copies of the cyclic group of order $p$ and a finite $p$-group $\mathfrak{H}$. Then $\Gamma$ contains a normal free subgroup of index $m_\Gamma$.*

*Proof.* This follows from the action by conjugation of $\Gamma$ on the set of free subgroups of index $m_\Gamma$, together with the implication (iii) $\Rightarrow$ (i) of Proposition 6. □

*Proof of Proposition* 6. The equivalence of (i) and (ii) follows from a discussion of the formula[3]

$$f_1(\Gamma) = m_\Gamma \prod_{\kappa | m_\Gamma} \prod_{\substack{1 \leq k \leq m_\Gamma \\ (m_\Gamma, k) = \kappa}} k^{\zeta_\kappa(\Gamma)},$$

making use of facts concerning $\tau(\Gamma)$ mentioned above. Suppose now that $\mu_p(\Gamma) = 0$. Then $Y$ is a tree, and, after contracting edges of $Y$ corresponding to trivial amalgamations if necessary, we may assume that $(\Gamma(-), Y)$ is *normalized*, that is, $|\Gamma(e)| \neq |\Gamma(v)|$ 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 $\Gamma(e)$ respectively $\Gamma(v)$ has order $n$, define an arithmetic function $f(n)$ via

$$f(n) = \sum_{\nu | n} (e_\nu - v_\nu), \quad n \geq 1,$$

[3]Cf. formulae (3) and (11) in [13].

and let $m_\Gamma = p^r$. Then, for $0 \le \rho \le r$,

$$f(p^\rho) = \begin{cases} e_1, & \rho = 0 \\ -1, & \rho = r \\ 0, & \text{otherwise,} \end{cases} \tag{26}$$

and, by Möbius inversion,

$$e_n - v_n = \sum_{\nu | n} \mu(\nu)\, f(n/\nu), \quad n \ge 1, \tag{27}$$

where $\mu$ is the classical Möbius function. Since our claim (iii) holds for $r \le 1$, we may assume that $r \ge 2$. In the latter case, we find from (26) and (27) that

$$e_{p^\rho} - v_{p^\rho} = \begin{cases} -e_1, & \rho = 1 \\ 0, & 1 < \rho < r \\ -1, & \rho = r. \end{cases} \tag{28}$$

Using the facts that $(\Gamma(-), Y)$ is normalized and that $Y$ is a tree (hence, in particular, does not contain loops), we find from (28) 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, $\Gamma$ is the free product of its vertex groups, and that $V(Y)$ contains precisely one vertex $v_0$ with $|\Gamma(v_0)| = p^r$ and $e_1 \ge 0$ vertices $v$ satisfying $\Gamma(v) \cong C_p$, whence (iii). Since the implication (iii) $\Rightarrow$ (ii) is trivial, the proof of Proposition 6 is complete. □

## 5. The groups $\Gamma(\mathfrak{G}, \mathfrak{H}, q)$

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

$$\Gamma = \Gamma(\mathfrak{G}, \mathfrak{H}, q) = \mathfrak{H} * \underbrace{\mathfrak{G} * \cdots * \mathfrak{G}}_{q \text{ copies}}, \tag{29}$$

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

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

by $\mathfrak{H}$; in particular, the groups $\Gamma$ and $\Delta$ satisfy the hypotheses of Theorem 1, and (2) yields the reduction formula

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

$$0<j<p. \quad (30)$$

Formula (30) allows us to translate results concerning the groups $\Gamma(\mathfrak{G},1,q)$ obtained in [16] into results for groups of the more general form (29). 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 $\Pi^{(p)}(\Gamma(\mathfrak{G},\mathfrak{H},q))$ under a certain assumption on $\mathfrak{G}$.

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

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

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

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

*is congruent to $j$ modulo $p$.*

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

$$\underline{d}_{\mathfrak{G},p} := \Big(\frac{d_1-1}{p},\frac{d_2-1}{p},\dots,\frac{d_r-1}{p}\Big),$$

where $1=d_0<d_1<\cdots<d_r=|\mathfrak{G}|$ is the collection in increasing order of those positive integers $d$ for which $s_d(\mathfrak{G})\not\equiv 0\ (p)$.

## 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] G. Frobenius, Verallgemeinerung des Sylow'schen Satzes, *Berliner Sitzungsber.* (1895), 981–993.

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

[6] W. Gaschütz, Nichtabelsche $p$-Gruppen besitzen äußere $p$-Automorphismen, *J. Algebra* **4** (1966), 1–2.

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

[8] I. M. Isaacs and G. R. Robinson, On a theorem of Frobenius: solutions of $x^n = 1$ in finite groups, *Am. Math. Monthly* **99** (1992), 352–354.
[9] P. Hall, On a theorem of Frobenius, *Proc. London Math. Soc.* **40** (1936), 468–501.
[10] W. Hodges, *Model Theory*, Encyclopedia of Mathematics and its Applications Vol. 42, Cambridge University Press, Cambridge, 1993.
[11] A. Lubotzky and D. Segal, *Subgroup Growth*, Progress in Mathematics, Birkhäuser, Basel, 2003.
[12] R. Lyndon, Two notes on Rankin's book on the modular group, *J. Austral. Math. Soc.* **16** (1973), 454–457.
[13] T. Müller, Combinatorial aspects of finitely generated virtually free groups, *J. London Math. Soc.* (2) **44** (1991), 75–94.
[14] T. Müller, A group-theoretical generalization of Pascal's triangle, *Europ. J. Combin.* **12** (1991), 43–49.
[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.*, to appear.
[17] T. Müller, Modular subgroup arithmetic, in: Proc. 2001 Durham Symposium on Groups, Geometries, and Combinatorics (A. Ivanov, M. Liebeck, and J. Saxl eds.), World Scientific, to appear.
[18] J. Nielsen, The commutator group of the free product of cyclic groups, *Mat. Tidsskr.* **B** (1948), 49–56.
[19] J.-P. Serre, *Trees*, Springer, Berlin, 1980.
[20] J.-P. Serre, *Cohomologie des groupes discrets*, Ann. Math. Studies vol. 70, Princeton University Press, 1971.
[21] 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