CLASSIFICATION AND STATISTICS OF FINITE INDEX SUBGROUPS IN FREE PRODUCTS

Thomas W. Müller and Jan-Christoph Schlage-Puchta

1. introduction

For positive integers e and m denote by C_m^{*e} the free product of e copies of the cyclic group of order m, and let F_r be the free group of rank r. Given integers $r, t \geq 0$, distinct primes $p_1, \ldots, p_t$, and positive integers $e_1, \ldots, e_t$, let

$$\Gamma = C_{p_1}^{*e_1} * \cdots * C_{p_t}^{*e_t} * F_r. \tag{1}$$

By the Kurosh subgroup theorem, a finite index subgroup $\Delta \leq \Gamma$ is again of the same form, that is, $\Delta \cong C_{p_1}^{*\lambda_1} * \cdots * C_{p_t}^{*\lambda_t} * F_\mu$ with non-negative integers $\lambda_1, \ldots, \lambda_t, \mu$. An Euler characteristic computation shows that the latter parameters are related to the index $(\Gamma : \Delta)$ via the relation

$$\sum_j \lambda_j \Big(1 - \frac{1}{p_j}\Big) + \mu - 1 = (\Gamma : \Delta) \Big[\sum_j \Big(1 - \frac{1}{p_j}\Big) + r - 1\Big]. \tag{2}$$

The tuple $\tau(\Delta) := (\lambda_1, \ldots, \lambda_t; \mu)$ is called the *(isomorphism) type* of Δ. The principal theme of the present paper is the enumeration of finite index subgroups Δ in Γ under restrictions on $\tau(\Delta)$. In particular, we shall discuss, for Γ as above, the following three basic problems.

(I) (Realization) Which abstract groups admitted by the Kurosh subgroup theorem are realized as finite index subgroups of Γ?

(II) (Asymptotics) Find natural deformation conditions on $\tau \in \mathbb{R}^{t+1}$ implying an interesting asymptotic behaviour of the function $s_\tau(\Gamma)$ counting the number of finite index subgroups in Γ of type τ.

(III) (Distribution) What can we say about the distribution of isomorphism types for subgroups of index n in Γ (with respect to various weight distributions) as n tends to infinity?

The motivation for these questions comes from three main sources: number theory, geometric function theory, and the theory of subgroup growth. As is well known, many important number–theoretic functions are invariant under the modular group $\mathrm{PSL}_2(\mathbb{Z})$ or certain other free products Γ of the form (1); a phenomenon leading for instance to functional equations for L-series and Dedekind zeta functions. It is in this way that the modular group and, more generally, subgroups of finite index in Hecke groups $\mathfrak{H}(q) \cong C_2 * C_q$ for $q \geq 3$ made their first significant appearance; cf. for example [1], [7], and [35, Chap. VII]. As Fuchsian groups, these groups also have intimate connections with the theory of Riemann surfaces; cf. for instance [43], in particular Chapter 3.9. Around 1880, both Klein and Poincaré independently realized the importance of group-theoretic information of the above mentioned kind for the construction and investigation of automorphic functions. This point of view is already present in [8] and [9]; in particular, the enumeration and classification of subgroups in the modular group is singled out in [8] as a group-theoretic problem of fundamental importance, situated at the crossroads of various branches of mathematics. Since the early 1960's the general point of view has shifted even more in that direction, so that (I) – (III) have become to be regarded as purely algebraic problems in their own right; cf. for instance [16], [17], [39], [40], [41], [44], as well as Newman's monograph [36]. From a recent perspective, a natural context for the research reported in this paper is the theory of *subgroup growth*, an exciting and fast developing part of what has in recent years become known as 'asymptotic group theory', which has evolved over the last two decades in the work of Grunewald, Lubotzky, Mann, Segal, and others including the first named author. The principal objects of study in the theory of subgroup growth are arithmetic properties of subgroup counting functions and their connection with the algebraic structure of the underlying group. An account of some of the major results in this area obtained prior to 1992 can be found in Lubotzky's Galway notes [10] and [11]. More recent contributions include (in rough chronological order) [4], [12], [13], [22], [23], [25], [5], [28], [30], [31], [32], and [33]; cf. also the forthcoming monograph [14].

As is well known, counting finite index subgroups in a group Γ is intimately related to the enumeration of Γ-actions on finite sets, that is, permutation representations of Γ; cf. for instance [3, Prop. 1]. Our present results depend on a powerful and surprisingly explicit refinement of this relationship. Let $\Gamma = G_1 * \cdots * G_s * F_r$ be a free product of finite groups G_σ and a free group of rank r. Restricting the action of Γ by right multiplication on the coset space $\Delta\backslash\Gamma$ to the free factors of Γ gives rise to representations $\varphi_\sigma : G_\sigma \to \mathrm{Sym}(\Delta\backslash\Gamma)$. Each representation φ_σ in turn decomposes as direct sum $\varphi_\sigma = \bigoplus_\kappa m_{\sigma\kappa}\rho_{\sigma\kappa}$ of the transitive G_σ-representations $\rho_{\sigma 1}, \rho_{\sigma 2}, \ldots, \rho_{\sigma k_\sigma}$ with certain non-negative multiplicities $m_{\sigma\kappa}$. The collection of these data $m_{\sigma\kappa}$ is referred to as the *representation type* of Δ, denoted $m(\Delta)$. The key observation underlying all our results is an explicit identity relating $m(\Delta)$ and $\tau(\Delta)$; see Proposition 1 below. The proof of this identity, which occupies the next section, relies on ideas and techniques from a recently developed enumerative theory of representations in wreath products; cf. [25], [34], and [29]. An introduction to and survey of the latter theory from two somewhat different points of view can be found in [26] and [27]. We now turn to the contents of this paper, explaining our main results under the headings of the problems listed above.

(I) Let Γ be as in (1), and for $i = 1, \ldots, t$ and $j = 1, \ldots, e_i$ let x_{ij} be a generator of the corresponding cyclic free factor of Γ. Given a transitive permutation representation $\varphi : \Gamma \to S_n$, we have $\varphi\,|_{\langle x_{ij}\rangle} = \rho_i^{m_{ij}} \oplus 1^{n-p_i m_{ij}}$, where ρ_i denotes the regular and 1 the trivial representation of C_{p_i}, and where m_{ij} is the number of p_i-cycles occurring in $\varphi(x_{ij})$. Hence, if Δ is a subgroup of index n in Γ, and if φ is the permutation representation describing the natural action of Γ on $\Delta\backslash\Gamma$, then the numbers m_{ij} together with the numbers $n - p_i m_{ij}$ correspond precisely to the multiplicities constituting the representation type of Δ. Set

$$M_i(\Delta) := \sum_{j=1}^{e_i} m_{ij}, \quad 1 \leq i \leq t.$$

As we shall see, the representation type does not in general determine the original representation up to equivalence; cf. Remark 1. Nevertheless, as a consequence of the above mentioned identity relating representation and isomorphism type of a finite index subgroup, the following is proved in Section 3.

Theorem A. *Let Γ be as in* (1)*, and let Δ be a subgroup of index n in Γ. Then the type $\tau(\Delta) = (\lambda_1, \ldots, \lambda_t; \mu)$ of Δ is determined in terms of n and the $M_i(\Delta)$ by means of the equations*

$$\lambda_k = e_k n \,-\, p_k M_k(\Delta), \quad 1 \leq k \leq t$$

$$\mu = \sum_{i=1}^{t} (p_i - 1) M_i(\Delta) \,+\, n(r-1) \,+\, 1.$$

Using Proposition 1 we also obtain a partial reconstruction of $\tau(\Delta)$ from $m(\Delta)$ for groups Γ of the more general form $\Gamma = G_1 * \ldots * G_s * F_r$. This aspect leads for instance to a far reaching generalization of a well-known theorem of Lyndon concerning the kernels of cartesian maps; cf. Corollary 1. Theorem A in turn allows us to completely resolve the realization problem for groups Γ of the form (1).

Theorem B. *A tuple $\tau = (\lambda_1, \ldots, \lambda_t; \mu)$ of non-negative integers is the isomorphism type of a finite index subgroup in Γ if and only if*

(i) *the quantity*

$$n = \frac{\sum_i \lambda_i (1 - \frac{1}{p_i}) + \mu - 1}{\sum_i e_i (1 - \frac{1}{p_i}) + r - 1}$$

is a positive integer,

(ii) *we have $\lambda_k \leq e_k n$ for $1 \leq k \leq t$, and with n as in* (i).

Specializing Theorem B to the modular group, we find that $\mathrm{PSL}_2(\mathbb{Z})$ contains a finite index subgroup isomorphic to $\Delta = C_2^{*\alpha} * C_3^{*\beta} * F_\gamma$ if and only if $\chi(\Delta) < 0$, that is, if and only if $\Delta \not\cong C_2, C_3, F_1, C_2 * C_2$. In Section 4, with the help of Theorem B, sufficient conditions for the realizability of types by non-maximal subgroups are found, and we derive properties of types realized by, as well as existence theorems for normal subgroups. In this context it should be noted that 'almost all' subgroups of finite index in a group Γ of the form (1) are maximal. This is shown among other things in Section 5.

(II) It is more difficult to give an un-technical account of our results concerning the asymptotic enumeration of subgroups with given type. Roughly speaking, for Γ large ($\chi(\Gamma) < 0$) and of the form (1), our main result in this direction (Section 5, Theorem 3) associates with Γ certain infinite domains $\Omega_\Gamma \subseteq \mathbb{R}^{e_1 + \cdots + e_t}$ such that

$$s_n(m_{11}, \ldots, m_{te_t}) \sim h_n(m_{11}, \ldots, m_{te_t})/(n-1)! \quad (n \to \infty),$$

subject to the condition that $(m_{11}, \ldots, m_{te_t}) \in \Omega_\Gamma$. Here, $s_n(m_{11}, \ldots, m_{te_t})$ denotes the number of index n subgroups Δ in Γ such that, for all i and j, the group $\langle x_{ij} \rangle$ acts on $\Delta\backslash\Gamma$ as a product of precisely m_{ij} p_i-cycles, and $h_n(m_{11}, \ldots, m_{te_t})$, which is explicitly computed in Proposition 7 (iv), counts the number of permutation representations of Γ of degree n enjoying the analogous property. The condition that $(m_{11}, \ldots, m_{te_t}) \in \Omega_\Gamma$ can be translated into deformation conditions for τ by means of Theorem A. As an illustration of the power of Theorem 3, here is a consequence for the modular group.

Theorem C. *Let $\tau_i = (\alpha_i, \beta_i, ; \gamma_i)$ be a sequence of types in $\mathbb{N}_0^3$ such that $n_i := 3\alpha_i + 4\beta_i + 6(\gamma_i - 1)$ tends to infinity with i. Assume that for all i we have $\alpha_i < n_i^{\frac{2}{3}-\varepsilon}$, $\beta_i < n_i^{\frac{1}{2}-\varepsilon}$, and $\alpha_i\beta_i < n_i^{1-\varepsilon}$ with some fixed $\varepsilon > 0$. Then the number $s_{\tau_i}(PSL_2(\mathbb{Z}))$ of finite index subgroups in the modular group of type τ_i satisfies*

$$s_{\tau_i}(\mathrm{PSL}_2(\mathbb{Z})) \sim \frac{n_i \cdot n_i!}{\alpha_i!\,\beta_i!\,(\frac{n_i-\alpha_i}{2})!\,(\frac{n_i-\beta_i}{3})!\,2^{\frac{n_i-\alpha_i}{2}}\,3^{\frac{n_i-\beta_i}{3}}} \quad (i \to \infty).$$

In connection with the construction of automorphic functions, Poincaré raised the question whether 'almost all' finite index subgroups of the modular group are free. If subgroups are enumerated by index, a negative answer was given in [22, Prop. 3] for a larger class of free products including the modular group. As an application of Theorems 1 and 3, we show in Section 5 that, if subgroups are enumerated by rank, then a positive proportion of all finite index subgroups in a group of the form (1) is in fact free.

In the special case of the modular group we are able to establish an asymptotic expansion for $s_\tau(\mathrm{PSL}_2(\mathbb{Z}))$ considerably refining Theorem C under similar hypotheses on τ; cf. Section 8, Proposition 10.

(III) Every statement on probability distributions depends on the choice of a weight function. In the present context, apart from uniform weights, the weight distributions on finite index subgroups Δ of groups of the form (1) given by $w(\Delta) := |\mathrm{Hom}(\Delta, H)|$ with some fixed finite group H, appear to be the most natural ones. For $1 \leq i \leq t$ and a positive integer n define random variables ξ_{in} by choosing a subgroup Δ of index n in Γ at random (with respect to uniform weights), and putting $\xi_{in} = \lambda_i$, where $\tau(\Delta) = (\lambda_1, \ldots, \lambda_t; \mu)$. Furthermore, for a prime q define random variables $\xi_{in}^{(q)}$ by choosing a transitive representation $\psi : \Gamma \to C_q \wr S_n$ (with respect to uniform weights), putting $\Delta = \mathrm{stab}_{\epsilon\psi}(1)$, and setting $\xi_{in}^{(q)} = \lambda_i$, with λ_i as above. Here, $\epsilon\psi$ is the permutation part of ψ. It is shown in Section 7 that the variables $\xi_{1n}, \ldots, \xi_{tn}$ are asymptotically independent, as are the variables $\xi_{1n}^{(q)}, \ldots, \xi_{tn}^{(q)}$ for fixed q, and that each of these variables converges to a normal distribution. More specifically, we obtain the following.

Theorem D. *Suppose that $\chi(\Gamma) < 0$. Then, as $n \to \infty$, the variables $\xi_{1n}, \ldots, \xi_{tn}$ are asymptotically independent. Moreover, for each $i \in [t]$ and real x,*

$$P\big(\xi_{in} \leq e_i n^{1/p_i} + x\sqrt{e_i}\, n^{1/(2p_i)}\big) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-s^2/2}\, ds \,+\, \mathcal{O}\big(n^{-\delta(\Gamma)}\big),$$

where $\delta(\Gamma) := \frac{1}{5} \min\big(\frac{1}{p_1}, \ldots, \frac{1}{p_t}\big)$; in particular, the distribution of ξ_{in} converges weakly to a normal distribution with mean $e_i n^{1/p_i}$ and standard deviation $\sqrt{e_i}\, n^{1/(2p_i)}$.

Theorem E. *Let* Γ *be as in Theorem* D, *and let* q *be a prime. Then, as* $n \to \infty$, *the variables* $\xi_{1n}^{(q)}, \dots, \xi_{tn}^{(q)}$ *are asymptotically independent. Moreover,*

(i) *if* $q \neq p_i$, *then the distribution of* $\xi_{in}^{(q)}$ *converges weakly to a normal distribution with mean* $\frac{e_i}{q^{1-1/p_i}} n^{1/p_i}$ *and standard deviation* $\frac{\sqrt{e_i}}{q^{1/2-1/(2p_i)}} n^{1/(2p_i)}$,

(ii) *the distribution of* $\xi_{in}^{(p_i)}$ *converges weakly to a normal distribution with mean* $e_i(p_i n)^{1/p_i}$ *and standard deviation* $\sqrt{e_i}(p_i n)^{1/(2p_i)}$.

In both cases, the error term is as in Theorem D.

The final section studies the impact of the theory developed here towards the solution of the Poincaré-Klein problem for the modular group. Here, the rather simple structure of $\mathrm{PSL}_2(\mathbb{Z})$ also allows us to obtain improved versions, and we demonstrate that some of the seemingly technical hypotheses introduced in Sections 4 and 5 are indeed necessary.

2. Isomorphism versus representation type

Given finite groups $G_1, \dots, G_s$ and an integer $r \geq 0$, consider the group

$$\Gamma = G_1 * \cdots * G_s * F_r. \tag{3}$$

Let $U_1, U_2, \dots, U_\ell$ be a complete list of the isomorphism types of subgroups occurring in the groups $G_1, \dots, G_s$ (excluding the trivial group), and let $\Delta \leq \Gamma$ be a subgroup of finite index. By Kurosh's subgroup theorem, Δ is of the form

$$\Delta \cong U_1^{*\lambda_1} * U_2^{*\lambda_2} * \cdots * U_\ell^{*\lambda_\ell} * F_\mu$$

with non–negative integers $\lambda_1, \lambda_2, \dots, \lambda_\ell$, and μ. The tuple $\tau(\Delta) := (\lambda_1, \dots, \lambda_\ell; \mu)$ is called the *(isomorphism) type* of Δ. Computation of the rational Euler characteristic shows that $\tau(\Delta)$ is related to the index $(\Gamma : \Delta) = n$ via

$$\sum_{j=1}^{\ell} \lambda_j \Big(1 - \frac{1}{|U_j|}\Big) + \mu - 1 = n \Big[\sum_{\sigma=1}^{s} \Big(1 - \frac{1}{|G_\sigma|}\Big) + r - 1 \Big]. \tag{4}$$

As is well known, the problem of counting finite index subgroups in a group Γ is intimately connected with the enumeration of Γ–actions on finite sets (that is permutation representations of Γ). Restricting the action of Γ by right multiplication on the coset space $\Delta \backslash \Gamma$ to the factors G_σ respectively F_r gives rise to representations $\varphi_\sigma : G_\sigma \to \mathrm{Sym}(\Delta \backslash \Gamma)$. Each representation φ_σ in turn decomposes as direct sum $\varphi_\sigma = \bigoplus_\kappa m_{\sigma\kappa} \rho_{\sigma\kappa}$ of the transitive G_σ–representations $\rho_{\sigma 1}, \dots, \rho_{\sigma k_\sigma}$ with certain non–negative multiplicities $m_{\sigma\kappa}$. Let $d_{\sigma\kappa}$ be the degree of $\rho_{\sigma\kappa}$. Our first result relates the set of data (the representation type of Δ)

$$m(\Delta) = (m_{\sigma\kappa})_{\substack{\sigma=1,\dots,s \\ \kappa=1,\dots k_\sigma}}$$

to $\tau(\Delta)$. For a group H and a permutation group Π denote by ϵ the canonical projection $H \wr \Pi \to \Pi$. We will choose algebraic multiplication in permutation groups, that is,

$$(\pi_1 \cdot \pi_2)(\omega) = \pi_2(\pi_1(\omega)) \quad (\pi_1, \pi_2 \in \Pi(\Omega),\ \omega \in \Omega).$$

Consequently, group actions will always be right actions, and multiplication in the wreath product $H \wr \Pi(\Omega)$ is given by the formulae

$$\begin{aligned}(f_1, \pi_1) \cdot (f_2, \pi_2) &= (f, \pi_1 \cdot \pi_2)\\ f(\omega) &= f_1(\omega) f_2(\pi_1(\omega)).\end{aligned}$$

Proposition 1. *Let Γ be as in* (3)*, let $U_1, \dots, U_\ell$ be as above, and let H be a fixed finite group. Then isomorphism and representation type of a subgroup Δ of index n in Γ are related via the equation*

$$|H|^{nr} \prod_{\sigma=1}^{s} \prod_{\kappa=1}^{k_\sigma} \Big|\Big\{\psi \in \operatorname{Hom}(G_\sigma, H \wr S_{d_{\sigma\kappa}}) : \epsilon\psi = \rho_{\sigma\kappa}\Big\}\Big|^{m_{\sigma\kappa}} = |H|^{n+\mu-1} \times \prod_{j=1}^{\ell} |\operatorname{Hom}(U_j, H)|^{\lambda_j}. \tag{5}$$

Proof. Fix some representation φ obtained from the action of Γ on $\Delta\backslash\Gamma$ by numbering the cosets in such a way that $\Delta \cdot 1 \mapsto 1$, and let φ_σ be the restriction of φ to G_σ. Consider the following four quantities:

$$|H|^{nr} \prod_{\sigma=1}^{s} \prod_{\kappa=1}^{k_\sigma} \Big|\Big\{\psi \in \operatorname{Hom}(G_\sigma, H \wr S_{d_{\sigma\kappa}}) : \epsilon\psi = \rho_{\sigma\kappa}\Big\}\Big|^{m_{\sigma\kappa}}, \tag{6}$$

$$\Big|\Big\{\psi \in \operatorname{Hom}(\Gamma, H \wr S_n) : \epsilon\psi = \varphi\Big\}\Big|, \tag{7}$$

$$|H|^{n-1} |\operatorname{Hom}(\Delta, H)|, \tag{8}$$

and

$$|H|^{n+\mu-1} \prod_{n=1}^{\ell} |\operatorname{Hom}(U_j, H)|^{\lambda_j}. \tag{9}$$

We will show that (i) (8)=(9), (ii) (6)=(7), and (iii) (7)=(8).

(i) By definition of the type and the mapping property of free products,

$$|\operatorname{Hom}(\Delta, H)| = \big|\operatorname{Hom}(U_1^{*\lambda_1} * \cdots * U_\ell^{*\lambda_\ell} * F_\mu, H)\big| = |\operatorname{Hom}(F_\mu, H)| \prod_{j=1}^{\ell} |\operatorname{Hom}(U_j, H)|^{\lambda_j}.$$

Multiplication by $|H|^{n-1}$ now gives (8) = (9).

(ii) For $\Gamma' := G_1 * \cdots * G_s$, we have

$$\big|\big\{\psi \in \operatorname{Hom}(\Gamma, H \wr S_n : \epsilon\psi = \varphi\big\}\big| = \big|\big\{\psi \in \operatorname{Hom}(\Gamma', H \wr S_n : \epsilon\psi = \varphi\,|_{\Gamma'}\,\big\}\big| \times \big|\big\{\psi \in \operatorname{Hom}(F_r, H \wr S_n) : \epsilon\psi = \varphi\,|_{F_r}\,\big\}\big|.$$

A homomorphism $\psi : F_r \to H \wr S_n$ is determined by r arbitrary elements of H^n and r permutations. Thus, with $\epsilon\psi = \varphi\,|_{F_r}$ prescribed, there are exactly $|H|^{nr}$ choices for

ψ lifting $\varphi\,|_{F_r}$. Hence, it suffices to consider the case where $r = 0$. By the mapping property of Γ, it is enough to check that

$$\Big|\big\{\psi \in \mathrm{Hom}(G_\sigma, H \wr S_n) :\ \epsilon\psi = \varphi_\sigma\big\}\Big| = \prod_{\kappa=1}^{k_\sigma} \Big|\big\{\psi \in \mathrm{Hom}(G_\sigma, H \wr S_{d_{\sigma\kappa}}) :\ \epsilon\psi = \rho_{\sigma\kappa}\big\}\Big|^{m_{\sigma\kappa}}. \tag{10}$$

Consider an element ψ of the left–hand set. By the condition that $\epsilon\psi = \varphi_\sigma$ and the definition of the multiplicities $m_{\sigma\kappa}$, the image $\psi(G_\sigma)$ is contained in a subgroup of $H \wr S_n$ which is independent of ψ and isomorphic to $\prod_{\kappa=1}^{k_\sigma}(H \wr S_{d_{\sigma\kappa}})^{m_{\sigma\kappa}}$, and, on a component of the κ–th factor, $\epsilon(\psi(G_\sigma))$ acts like $\rho_{\sigma\kappa}$. Since for arbitrary groups G, H_1, H_2

$$|\mathrm{Hom}(G, H_1 \times H_2)| = |\mathrm{Hom}(G, H_1)| \cdot |\mathrm{Hom}(G, H_2)|, \tag{11}$$

we obtain (10).

(iii) Let

$$L(\Delta) := \Big\{\psi \in \mathrm{Hom}(\Gamma, H \wr S_n) :\ \mathrm{stab}_{\epsilon\psi}(1) = \Delta\Big\}.$$

Then

$$|L(\Delta)| = (n-1)! \cdot \Big|\big\{\psi \in \mathrm{Hom}(\Gamma, H \wr S_n) :\ \epsilon\psi = \varphi\big\}\Big|. \tag{12}$$

For $\gamma \in \Gamma$ and $\psi \in \mathrm{Hom}(\Gamma, H \wr S_n)$ write $\psi(\gamma) = (f_\gamma, \pi_\gamma)$, and for $\psi \in L(\Delta)$ define a map $\chi_\psi : \Delta \to H$ by

$$\chi_\psi(\delta) = f_\delta(1), \quad \delta \in \Delta.$$

With this notation, we claim: firstly, that χ_ψ is a homomorphism, secondly, that the map $L(\Delta) \to \mathrm{Hom}(\Delta, H)$ given by $\psi \mapsto \chi_\psi$ is surjective, and thirdly, that each fibre of this map has cardinality $(n-1)!|H|^{n-1}$. In view of (12), these claims imply that (7) = (8).

Let $\delta_1, \delta_2 \in \Delta$, and let (f_1, π_1) respectively (f_2, π_2) be the images under ψ. Then $\chi_\psi(\delta_1) = f_1(1)$, $\chi_\psi(\delta_2) = f_2(1)$, and $\chi_\psi(\delta_1\delta_2) = f(1)$, where

$$(f_1, \pi_1)(f_2, \pi_2) = (f, \pi_1\pi_2).$$

Hence,

$$\chi_\psi(\delta_1\delta_2) = f_1(1)\, f_2(\pi_1(1)) = \chi_\psi(\delta_1)\, \chi_\psi(\delta_2),$$

since $\pi_1(1) = 1$. This proves our first claim.

In order to prove surjectivity of the map $\psi \mapsto \chi_\psi$, we will exhibit, for every homomorphism $\chi : \Delta \to H$, a representation $\psi : \Gamma \to H \wr S_n$ with $\epsilon\psi = \varphi$ and $\chi_\psi = \chi$. The latter task is equivalent to finding a map $f : \Gamma \times [n] \to H$ such that [1]

$$f(\gamma_1\gamma_2, i) = f(\gamma_1, i)\, f(\gamma_2, \varphi(\gamma_1)(i)) \quad (\gamma_1, \gamma_2 \in \Gamma,\ i \in [n]) \tag{13}$$

and

$$f(\gamma, 1) = \chi(\gamma), \quad \gamma \in \Delta. \tag{14}$$

By the transitivity of φ, we can find elements $\gamma^{(i)} \in \Gamma$ for $i \in [n]$ such that

$$\begin{gathered} \varphi(\gamma^{(i)})(1) = i, \quad i \in [n] \\ \gamma^{(1)} = 1. \end{gathered} \tag{15}$$

[1] $[n]$ denotes the standard n–set, that is, the set consisting of the integers $1, 2, \ldots, n$.

Moreover, choose elements $h_i \in H$ for $i \in [n]$, $h_1 = 1$, and define a function $f : \Gamma \times [n] \to H$ via

$$f(\gamma, i) := h_i^{-1}\,\chi(\delta)\,h_j,$$

where $\gamma^{(i)}\gamma = \delta\,\gamma^{(j)}$ with $\delta \in \Delta$ and $j \in [n]$. If $\gamma \in \Delta$ and $i = 1$, then $\delta = \gamma$ and $j = 1$, and hence

$$f(\gamma, 1) = h_1^{-1}\,\chi(\gamma)\,h_1 = \chi(\gamma),$$

which proves (14). In proving (13), we first consider the case where $i = 1$. Let $\gamma_1, \gamma_2 \in \Gamma$, and suppose that $\gamma_1 = \delta_1\,\gamma^{(j)}$, that is, $\varphi(\gamma_1)(1) = j$, and that $\gamma^{(j)}\gamma_2 = \delta_2\,\gamma^{(k)}$, where $\delta_1, \delta_2 \in \Delta$ and $j, k \in [n]$. Then we have

$$\gamma_1\gamma_2 = \delta_1\,\gamma^{(j)}\,(\gamma^{(j)})^{-1}\,\delta_2\,\gamma^{(k)} = \delta_1\,\delta_2\,\gamma^{(k)},$$

and, since χ is a homomorphism,

$$\begin{aligned} f(\gamma_1\gamma_2, 1) &= h_1^{-1}\,\chi(\delta_1\delta_2)\,h_k \\ &= h_1^{-1}\,\chi(\delta_1)\,h_j\,h_j^{-1}\,\chi(\delta_2)\,h_k \\ &= f(\gamma_1, 1)\,f(\gamma_2, \varphi(\gamma_1)(1)). \end{aligned}$$

Now let $\gamma_1, \gamma_2 \in \Gamma$ and $i \in [n]$. Let $\gamma^{(i)}\,\gamma_1 = \delta_1\,\gamma^{(j)}$ and $\gamma^{(j)}\,\gamma_2 = \delta_2\,\gamma^{(k)}$ with $\delta_1, \delta_2 \in \Delta$. Then

$$\gamma^{(i)}\,\gamma_1\,\gamma_2 = \delta_1\,\gamma^{(j)}\,(\gamma^{(j)})^{-1}\,\delta_2\,\gamma^{(k)} = \delta_1\,\delta_2\,\gamma^{(k)},$$

and we find that

$$\begin{aligned} f(\gamma_1\gamma_2, i) &= h_i^{-1}\,\chi(\delta_1\delta_2)\,h_k \\ &= h_i^{-1}\,\chi(\delta_1)\,h_j \cdot h_j^{-1}\,(\chi(\delta_1))^{-1}\,h_1 \cdot h_1^{-1}\,\chi(\delta_1\delta_2)\,h_k \\ &= f(\gamma_1, i)\,(f(\gamma^{(i)}\gamma_1, 1))^{-1}\,f(\gamma^{(i)}\gamma_1\gamma_2, 1) \\ &= f(\gamma_1, i)\,f(\gamma_2, \varphi(\gamma^{(i)}\gamma_1)(1)) \\ &= f(\gamma_1, i)\,f(\gamma_2, \varphi(\gamma_1)(i)), \end{aligned}$$

where we have made use of the case $i = 1$ of (13) to rewrite $f(\gamma^{(i)}\gamma_1\gamma_2, 1)$. This proves our second claim.

In order to establish our last claim, consider the action by conjugation of the group

$$U := \Big\{(f, \pi) \in H \wr S_n :\ f(1) = 1 \text{ and } \pi(1) = 1\Big\}$$

on the set $L(\Delta)$. Since $U \cong H \wr S_{n-1}$, we have $|U| = |H|^{n-1}\,(n-1)!$. We show next that this action of U on $L(\Delta)$ is in fact free. Assume that $\psi^u = \psi$ for some $\psi \in L(\Delta)$ and $u \in U$, that is, $[\psi(\gamma), u] = 1$ for all $\gamma \in \Gamma$. Setting $u = (g, \tau)$, this property is equivalent to the two assertions that

$$\pi_\gamma\,\tau = \tau\,\pi_\gamma \quad (\gamma \in \Gamma)$$

and

$$f_\gamma(i)\,g(\pi_\gamma(i)) = g(i)\,f_\gamma(\tau(i)) \quad (\gamma \in \Gamma,\ i \in [n]).$$

Since $\epsilon\psi$ is transitive and $\tau(1) = 1$, the first of these equations immediately implies $\tau = \mathrm{id}$, and the second equation simplifies to

$$f_\gamma(i)\,g(\pi_\gamma(i)) = g(i)\,f_\gamma(i) \quad (\gamma \in \Gamma,\ i \in [n]).$$

Setting $i = 1$ and using the facts that $g(1) = 1$ and that $\epsilon\psi$ is transitive, we now find that $g(j) = 1$ for all $j \in [n]$, that is, $u = 1$. Hence, $L(\Delta)$ decomposes into

$$|L(\Delta)|/|U| = |L(\Delta)|/(|H|^{n-1}(n-1)!)$$

orbits under U, and any two elements in the same orbit correspond to the same homomorphism in $\mathrm{Hom}(\Delta, H)$. Thus, it only remains to show that two elements not equivalent under U have different images in $\mathrm{Hom}(\Delta, H)$.

Let $\psi_1, \psi_2 \in L(\Delta)$ be elements such that $\chi_{\psi_1} = \chi_{\psi_2}$. After conjugation with appropriate elements of U we can assume that $\epsilon\psi_1 = \epsilon\psi_2 = \varphi$. Define a map $\partial : \Gamma \to H$ via $\partial(\gamma) := (f_\gamma^{(2)}(1))^{-1} f_\gamma^{(1)}(1)$, where $\psi_i(\gamma) = (f_\gamma^{(i)}, \pi_\gamma)$. By assumption $\partial(\gamma) = 1$ for $\gamma \in \Delta$. An immediate calculation yields the multiplication rule

$$\partial(\gamma\gamma') = (f_{\gamma'}^{(2)}(\pi_\gamma(1)))^{-1}\,\partial(\gamma)\,f_{\gamma'}^{(1)}(\pi_\gamma(1)) \quad (\gamma, \gamma' \in \Gamma). \tag{16}$$

If $\gamma \in \Delta$, we see from (16) that $\partial(\gamma\gamma') = \partial(\gamma')$, that is, ∂ is a class function for Γ modulo Δ. Define a map $f : [n] \to H$ via $f(i) := \partial(\gamma^{(i)})$, where $\gamma^{(i)}$ is as in (15); in particular $f(1) = 1$. We can now finish the proof by showing that

$$f(i)\,f_\gamma^{(1)}(i) = f_\gamma^{(2)}(i)\,f(\pi_\gamma(i)) \quad (\gamma \in \Gamma,\ i \in [n]), \tag{17}$$

since this implies that

$$\psi_2(\gamma)^{(f,\mathrm{id})} = \psi_1(\gamma), \quad \gamma \in \Gamma.$$

We compute $f(\pi_\gamma(i))$:

$$\begin{aligned} f(\pi_\gamma(i)) &= f(\pi_\gamma(\pi_{\gamma^{(i)}}(1))) \\ &= f(\pi_{\gamma^{(i)}\gamma}(1)) \\ &= \partial(\gamma^{(\pi_{\gamma^{(i)}\gamma}(1))}) \\ &= \partial(\gamma^{(i)}\gamma) \\ &= (f_\gamma^{(2)}(\pi_{\gamma^{(i)}}(1)))^{-1}\,\partial(\gamma^{(i)})\,f_\gamma^{(1)}(\pi_{\gamma^{(i)}}(1)) \\ &= (f_\gamma^{(2)}(i))^{-1}\,f(i)\,f_\gamma^{(1)}(i), \end{aligned}$$

where we have used the multiplication rule (16) and the facts that $\gamma^{(\pi_{\gamma^{(i)}\gamma}(1))} \sim_\Delta \gamma^{(i)}\gamma$ and that ∂ is a class function. The desired result (17) follows now upon multiplication from the left with $f_\gamma^{(2)}(i)$. □

3. The realization problem for isomorphism types

From now on, with the exception of Subsection 3.2, we shall restrict our attention to groups Γ of the form (1).

3.1. **Explicit determination of isomorphism types.** For $i = 1, \dots, t$ and $j = 1, \dots, e_i$ let x_{ij} be a generator of the corresponding cyclic factor of Γ. Given a transitive permutation representation $\varphi : \Gamma \to S_n$, the restriction of φ to $\langle x_{ij} \rangle$ is determined up to equivalence by the number m_{ij} of p_i–cycles occurring in $\varphi(x_{ij})$. More precisely, $\varphi\,|_{\langle x_{ij}\rangle}$ is equivalent to $\rho_i^{m_{ij}} \oplus 1^{n-p_i m_{ij}}$, where ρ_i denotes the regular and 1 the trivial representation of C_{p_i}, that is, up to renumbering, the numbers m_{ij} together with the numbers $n-p_im_{ij}$ correspond exactly to the multiplicities introduced in the previous section. Given a subgroup Δ of index n in Γ, let $M_i(\Delta)=\sum_j m_{ij}$, where the multiplicities m_{ij} pertain to the natural action of Γ on $\Delta\backslash\Gamma$.

Theorem 1. *Let $\Gamma = C_{p_1}^{*e_1} * \cdots * C_{p^t}^{*e_t} * F_r$ with distinct primes $p_1, \ldots p_t$, and let Δ be a subgroup of index n in Γ, with invariants $M_i(\Delta)$ as defined above. Then the type $\tau(\Delta)=(\lambda_1,\ldots,\lambda_t;\mu)$ of Δ is determined in terms of n and the $M_i(\Delta)$ by means of the equations*

$$\lambda_k = e_k n \,-\, p_k M_k(\Delta), \quad 1\le k\le t$$

$$\mu = \sum_{i=1}^{t}(p_i-1)\,M_i(\Delta) \,+\, n(r-1)\,+\,1.$$

Proof. In Proposition 1 put $H = C_p$, where p is prime. We have to compute the quantities

$$|\mathrm{Hom}(C_{p_i}, C_p)| \quad\text{and}\quad \left|\left\{\psi\in \mathrm{Hom}(C_{p_i}, C_p\wr S_{p_i}):\ \epsilon\psi=\rho_i\right\}\right|.$$

The first expression equals p_i if $p=p_i$, and 1 otherwise. In order to compute the second expression we have to count elements (f,π) in $C_p\wr S_{p_i}$ of order p_i, which are mapped via ϵ onto a given p_i–cycle, say $\pi=(1\ldots p_i)$. The condition that $(f,\pi)^{p_i}=1$ is equivalent to the equation

$$f(1)\,f(2)\,\ldots\,f(p_i)=1$$

in C_p, which is satisfied by exactly p^{p_i-1} such functions f. We first choose p to be different from all the p_i. Then, on the left–hand side of (5), the first factor is p^{nr}, while the contribution of the trivial representations is 1, and the regular representations contribute a total of

$$\prod_{i=1}^{t}\prod_{j=1}^{e_i} p^{(p_i-1)m_{ij}} = \prod_{i=1}^{t} p^{(p_i-1)M_i(\Delta)}.$$

The right–hand side in this case becomes $p^{n+\mu-1}$. Comparing exponents, we obtain the last equation of Theorem 1. Next, we take $p=p_k$ for some $1\le k\le t$. The same computation as above now shows that in this case the first factor on the right–hand side is p_k^{nr}, while the regular representations contribute $\prod_{i=1}^t p_k^{(p_i-1)M_i(\Delta)}$, so that, by the equation just verified, the product of these two terms equals $p_k^{n+\mu-1}$. The trivial representations contribute 1 to the left–hand side, except for σ such that $G_\sigma\cong C_{p_k}$, in which case the contribution is $p_k^{n-p_km_{kj}}$. Hence, for $p=p_k$, the left–hand side equals

$$p_k^{n+\mu-1}\prod_{j=1}^{e_k} p_k^{n-p_km_{kj}} = p_k^{n+\mu-1+e_kn-p_kM_k(\Delta)}.$$

The right–hand side in this case equals $p_k^{n+\mu-1+\lambda_k}$. Comparing exponents gives rise to the first equation of Theorem 1. □

Remark 1. *Let $\Gamma=\langle x,y\mid x^2=y^3=1\rangle$ be the modular group, and define representations φ_1,φ_2 of degree 6 via*

$$\varphi_1(x)=(12)(34)(56),\quad \varphi_2(x)=(15)(26)(34)$$

and

$$\varphi_1(y) = \varphi_2(y) = (123)(456).$$

Then, by Theorem 1*, the associated subgroups* $\Delta_i = \mathrm{stab}_{\varphi_i}(1)$ *are isomorphic. However, since*

$$|\varphi_1(\Gamma)| = |S_2 \wr S_3| = 48 \quad \textit{and} \quad |\varphi_2(\Gamma)| = |C_6| = 6,$$

the core of Δ_1 *has index* 8 *in* Δ_1*, whereas* Δ_2 *is normal in* Γ (*in fact* Δ_1 *has class number* 3)*. This shows in particular that* Δ_1 *and* Δ_2 *are not conjugate, not even under an outer automorphism, although they have the same representation type.*

3.2. **Some remarks on Theorem 1.** In this subsection we shall consider the question how far Theorem 1 can be generalized towards free products Γ of the form (3). The proof of our next result demonstrates that, while it may be true that the isomorphism type of a finite index subgroup in such a group Γ is determined by its representation type, the proof strategy of Theorem 1 becomes problematic, since the correct choice of the auxiliary groups H turns out to be difficult.

Proposition 2. *Let* $\Gamma = C_4 * C_6$*, and let* Δ_1 *and* Δ_2 *be subgroups of index* n*. Then* $\Delta_1 \cong \Delta_2$ *if* Δ_1 *and* Δ_2 *have the same representation type.*

Proof. As in the proof of Theorem 1, we have to solve the system of equations (5) for $\lambda_1, \dots, \lambda_\ell$, and μ. The non-trivial subgroups of C_4 and C_6 are C_2, C_3, C_4, and C_6. As H runs over all cyclic groups of finite order, we obtain equations for

$$(2, |H|)^{\lambda_1}(3, |H|)^{\lambda_2}(4, |H|)^{\lambda_3}(6, |H|)^{\lambda_4}|H|^{\mu}.$$

Choosing for instance $|H| = 5$, one can easily determine μ. The remaining parts of this expression depend on $(12, |H|)$ only, thus choosing for $|H|$ all divisors $\neq 1$ of 12, we obtain 5 exponential equations in $\lambda_1, \dots, \lambda_4$, which can be transformed into seven linear equations by considering powers of 2 and 3 separately. The resulting system has the following form:

$$\begin{array}{cccccccc}
\lambda_1 & & + & \lambda_3 & + & \lambda_4 & = & c_1 \\
& \lambda_2 & & & + & \lambda_4 & = & c_2 \\
\lambda_1 & & + & 2\lambda_3 & + & \lambda_4 & = & c_3 \\
\lambda_1 & & + & \lambda_3 & + & \lambda_4 & = & c_4 \\
& \lambda_2 & & & + & \lambda_4 & = & c_5 \\
\lambda_1 & & + & 2\lambda_3 & + & \lambda_4 & = & c_6 \\
& \lambda_2 & & & + & \lambda_4 & = & c_7.
\end{array}$$

Obviously, among these equations there are only three independent ones, hence it is impossible to determine the four variables. Moreover, in view of (11), choosing H as an arbitrary abelian group yields no further information. However, if we take $H = S_3$, and consider the 2-part of the exponential equation, we obtain the linear equation

$$2\lambda_1 + 2\lambda_3 + \lambda_4 = c_8.$$

Since this new equation is independent of the three former ones, the enlarged system is uniquely solvable. This shows that the representation type of a finite index subgroup in Γ determines its isomorphism type. □

It is interesting to observe however that, even in the general setting of (3), we can still compute the free part of finite index subgroups. In order to exploit Proposition 1 for such groups, we first have to study the factors on the left–hand side of equation (5).

Lemma 1. *Let G be a finite group, p a prime such that $p \nmid |G|$, and let ρ be a transitive permutation representation of G of degree d. Then*

$$\left|\left\{\psi \in \mathrm{Hom}(G, C_p \wr S_d):\ \epsilon\psi = \rho\right\}\right| = p^{d-1}. \tag{18}$$

Proof. In Proposition 1 put $\Gamma = G$ and $\Delta = \mathrm{stab}_\rho(1)$. Then $s = 1$ and

$$m_{1\kappa} = \begin{cases} 1, & \rho_{1\kappa} = \rho \\ 0, & \text{otherwise,} \end{cases}$$

hence, in this situation equation (5) coincides with (18). □

Proposition 3. *Let Γ be as in* (3)*, and let Δ be a subgroup of index n in Γ of type $\tau(\Delta) = (\lambda_1, \dots, \lambda_\ell; \mu)$ and representation type $m(\Delta) = (m_{\sigma\kappa})$.*

(i) *We have*

$$\mu = (r + s - 1)n - \sum_{\sigma=1}^{s} \sum_{\kappa=1}^{k_\sigma} m_{\sigma\kappa} + 1.$$

(ii) Δ *is free if and only if*

$$m_{\sigma\kappa} = \begin{cases} \dfrac{n}{|G_\sigma|}, & \rho_{\sigma\kappa} \text{ regular} \\ 0, & \text{otherwise.} \end{cases} \tag{19}$$

Proof. (i) Let p be a prime such that $p \nmid |G_\sigma|$ for all σ, and put $H = C_p$. Combining Proposition 1 with the previous lemma yields

$$p^{nr} \prod_{\sigma=1}^{s} \prod_{\kappa=1}^{k_\sigma} p^{m_{\sigma\kappa}(d_{\sigma\kappa}-1)} = p^{n+\mu-1}.$$

Taking logarithms, solving the resulting equation for μ, and using the fact that $\sum_\kappa d_{\sigma\kappa} m_{\sigma\kappa} = n$ now gives (i).

(ii) According to (4), Δ is free if and only if

$$\mu = (r-1)n + n\sum_{\sigma=1}^{s}\left(1 - \frac{1}{|G_\sigma|}\right) + 1,$$

that is, in view of (i), if and only if

$$\sum_{\sigma=1}^{s} \sum_{\kappa=1}^{k_\sigma} m_{\sigma\kappa} = \sum_{\sigma=1}^{s} \frac{n}{|G_\sigma|}.$$

It follows that condition (19) on the representation type is sufficient to ensure that Δ is free. Conversely, since $\sum_\kappa d_{\sigma\kappa} m_{\sigma\kappa} = n$, and since all but the regular representations of the G_σ have degrees strictly less than $|G_\sigma|$, Δ free implies (19). □

Proposition 3 allows us to decide with reasonable effort whether or not a given subgroup is free. Note in this context that, since a common way of representing finite index subgroups within a computer algebra system like GAP is via the associated coset representation, the representation type $m(\Delta)$ of a subgroup Δ can be computed at negligible cost. Hence, any method allowing to deduce from $m(\Delta)$ further information on Δ, is of potential interest from an algorithmic point of view. As an example of a more theoretical application, we derive a result generalizing the well–known theorem of Lyndon concerning the kernels of cartesian maps.[2]

Corollary 1. *Let Γ be as in* (3), *G a finite group, $\psi_\sigma : G_\sigma \to G$ monomorphisms for $1 \leq \sigma \leq s$, and let $\psi : \Gamma \to G$ be an epimorphism simultaneously extending every ψ_σ. Then the kernel of ψ is free. In particular, the kernel of the cartesian map $G_1 * \cdots * G_s \to G_1 \times \cdots \times G_s$ is free of rank*

$$\mathrm{rk}(K) = |G_1| \cdots |G_s| \bigg[\sum_\sigma \Big(1 - \frac{1}{|G_\sigma|}\Big) - 1 \bigg] + 1.$$

Proof. Let K be the kernel of ψ. Then the canonical action of G_σ on $K\backslash\Gamma$ is equivalent to the action of $\psi_\sigma(G_\sigma)$ on G by right multiplication. The latter action is the direct sum of $|G|/|G_\sigma|$ regular actions of G_σ. Hence, condition (19) is satisfied, and K is free by the second part of Proposition 3. The particular statement follows from this and formula (4). □

3.3. **Solution of the realization problem.** We now come to the main result of Section 3, characterizing those $(t+1)$–tuples $\tau = (\lambda_1, \ldots, \lambda_t; \mu) \in \mathbb{N}_0^{t+1}$, which are *realized*, that is, occur as the isomorphism type of a finite index subgroup in $\Gamma = \mathop{*}\limits_{i=1}^{t} C_{p_i}^{*e_i} * F_r$.

Theorem 2. *Let Γ be as in* (1). *Then a tuple $\tau = (\lambda_1, \ldots, \lambda_t; \mu)$ of non–negative integers is the isomorphism type of a finite index subgroup in Γ if and only if*

(i) *the quantity*

$$n = \frac{\sum_{i=1}^t \lambda_i (1 - \frac{1}{p_i}) + \mu - 1}{\sum_{i=1}^t e_i (1 - \frac{1}{p_i}) + r - 1}$$

is a positive integer,

(ii) *we have $\lambda_k \leq e_k n$ for $1 \leq k \leq t$, and with n as in* (i).

If (i) *and* (ii) *hold, then n is the index of any subgroup in Γ realizing τ.*

Proof. By Theorem 1, a tuple $\tau \in \mathbb{N}_0^{t+1}$ is the type of a finite index subgroup in Γ if and only if there exists a transitive permutation representation of Γ of degree n such

[2] Cf. [15]. The basic idea of Lyndon's theorem goes back to Nielsen [38].

that

$$M_k = \frac{e_k n - \lambda_k}{p_k} \tag{20}$$

and with n as given in the theorem. Solving (20) for λ_k, and substituting the resulting expression into the definition of n in (i), we find that

$$\sum_{i=1}^{t}(p_i - 1)M_i + n(r-1) + 1 = \mu, \tag{21}$$

that is, the second equation in Theorem 1 holds as a consequence of (20) and the definition of n.

We first show that our hypothesis (i) is equivalent to the assertions that the numbers $M_1, \dots M_t, n$, as given by the equations above, are in fact integral, and that $n > 0$. For n there is nothing to show. We have

$$n\Bigg[\sum_{i=1}^{t} e_i(p_i-1)\prod_{j\neq i} p_j + (r-1)\prod_j p_j\Bigg] = \sum_{i=1}^{t}\lambda_i(p_i-1)\prod_{j\neq i}p_j + (\mu-1)\prod_j p_j.$$

Reducing modulo p_k for some $k \in [t]$, this equation becomes

$$ne_k(p_k-1)\prod_{j\neq k}p_j \equiv \lambda_k(p_k-1)\prod_{j\neq k}p_j \mod p_k,$$

implying $ne_k \equiv \lambda_k\ (p_k)$, since the factor $(p_k-1)\prod_{j\neq k}p_j$ is invertible modulo p_k. This shows that all M_k as defined above are indeed integral.

Clearly, condition (ii) is equivalent to the assertion that the quantities M_k as defined above are non–negative. Moreover, for $1 \leq k \leq t$, the trivial inequalities $\lambda_k \geq 0$ correspond to the inequalities $p_k M_k \leq e_k n$, while $\mu \geq 0$ corresponds to the inequality $\sum_{i=1}^t (p_i - 1)M_i \geq n(1-r) - 1$. For each $i = 1, \dots, t$ choose integers $m_{i1}, \dots, m_{ie_i} \geq 0$ such that $p_i m_{ij} \leq n$ and $\sum_j m_{ij} = M_i$. We shall construct a transitive permutation representation φ of Γ of degree n such that $\varphi(x_{ij})$ has precisely m_{ij} cycles of length p_i and $n - p_i m_{ij}$ fixed points.

If $r > 0$, then we can choose $\varphi(x_{ij})$ in S_n subject only to the above condition on the cycle structure, and map the r generators of the free part of Γ to the n–cycle $(1, \dots, n)$, in this way ensuring transitivity of the image. Hence, we can assume from now on that $r = 0$, which means that the inequality corresponding to $\mu \geq 0$ becomes non–trivial. Without loss of generality we may further assume that $p_1 m_{11} \geq p_i m_{ij}$ for all i and j. In order to define $\varphi(x_{11})$ we choose m_{11} disjoint cycles of length p_1 in $[n]$. The image of the (lexicographically) next generator x_{ij} (that is, x_{12} or x_{21} at this stage) is then constructed as follows: we choose the first point from each of the first p_i cycles of $\varphi(x_{11})$ to form the first p_i–cycle of $\varphi(x_{ij})$; then we choose a second point in the p_i–th cycle of $\varphi(x_{11})$ and one point from each of the next $p_i - 1$ cycles of $\varphi(x_{11})$. We continue in this way until we have constructed m_{ij} cycles of length p_i (which then define $\varphi(x_{ij})$), or until not enough free p_1–cycles are left to continue (that is, less than p_i for the first step, respectively less than $p_i - 1$ if the first step occurs). In the latter case we proceed as follows: going through the p_1–cycles of $\varphi(x_{11})$ from left to right, we choose the first free point (that is the first or the second point in the first p_1–cycle at this stage), the first point in each of the remaining free p_1–cycles, and enough fixed points (from left to right) of $\varphi(x_{11})$ to fill up another p_i–cycle. We iterate this second procedure until we have constructed m_{ij} cycles of length p_i, or until there are less than $p_i - 1$ fixed points of $\varphi(x_{11})$ left. In the first case we have completed the construction of $\varphi(x_{ij})$, in the second case we combine the remaining fixed points of $\varphi(x_{11})$ with the correct number of free points in the p_1–cycles to form a further p_i–cycle. If this last step occurs we construct the missing number of p_i–cycles arbitrarily from remaining free points.

We have to check that at each stage we have a sufficient supply of free points. Assume that this is not the case. When starting the second procedure, the first p_1–cycle of $\varphi(x_{11})$ contains at least one free point, thus we can at least link all the p_1–cycles. Since all points not free are moved by $\varphi(x_{ij})$, and at least one fixed point of $\varphi(x_{11})$ is moved by $\varphi(x_{ij})$, the permutation $\varphi(x_{ij})$ has less fixed points than $\varphi(x_{11})$, that is, $p_i m_{ij} > p_1 m_{11}$, contradicting the maximality of $p_1 m_{11}$.

The image of the next generator is chosen by repeating the procedure leading to $\varphi(x_{ij})$, now linking orbits of $\langle \varphi(x_{11}), \varphi(x_{ij}) \rangle$ instead of cycles. Since the number of free points at our disposal increases with each step, we can define the action in this way for all the remaining generators.

Finally, it remains to show that the action obtained is transitive. Clearly, this is the case if we are running out of fixed points while performing the second procedure. Hence assume that this situation never occurs. Then, in every step of the construction, a newly formed p_k–cycle links $p_k - 1$ orbits previously disconnected, thus the number of orbits after the construction of m_{11} cycles of length $p_1, \ldots,$ m_{te_t} cycles of length p_t equals

$$n - \sum_{i=1}^{t} \sum_{j=1}^{e_t} m_{ij}\,(p_i - 1) = n - \sum_{i=1}^{t} M_i\,(p_i - 1) = 1 - \mu \leq 1$$

by equation (21) and the fact that $r = 0$. Hence, there is exactly one orbit, that is, we have obtained a transitive action. The last assertion of the theorem follows from Equation (4). □

Remark 2. *Consider the group $\Gamma = C_2 * C_3 * C_5$. Then the quantity n defined in condition* (i) *of Theorem* 2 *satisfies*

$$29n = 15\lambda_1 + 20\lambda_2 + 24\lambda_3 + 30(\mu - 1).$$

We can find a solution $(\lambda_1, \lambda_2, \lambda_3, \mu, n)$ of this equation such that $\lambda_1 > n$; for instance

$$\lambda_1 = 29m,\ \lambda_2 = \lambda_3 = 0,\ \mu = 1,\ n = 15m.$$

This shows that conditions (i) *and* (ii) *in Theorem* 2 *are independent.*

Remark 3. *Note that, for every tuple $\tau = (\lambda_1, \ldots, \lambda_t; \mu) \in \mathbb{N}_0^{t+1}$ satisfying conditions* (i) *and* (ii), *the proof of Theorem* 2 *effectively supplies a finite index subgroup realizing τ.*

4. The realization problem for isomorphism types, II: Normal and non–maximal subgroups

Let Γ be as in (1). In this section, we shall be concerned with the isomorphism types of normal and non–maximal subgroups in Γ. More specifically, we shall obtain sufficient conditions for a type realizable in Γ to be realized by a non–maximal subgroup, and we shall derive properties of types realized by, as well as some existence results for normal subgroups.

4.1. **Non–maximal subgroups.** As we shall see (among other things) in Section 5, almost all subgroups of finite index in Γ are in fact maximal; hence, we have to expect further non-trivial restrictions, when trying to realize types via non-maximal subgroups. Here, we shall prove the following.

Proposition 4. *Let Γ be as in* (1), *let $\tau = (\lambda_1, \dots, \lambda_t; \mu)$ be a realizable type for Γ, and let n be as given in Theorem* 2. *Suppose that $n > 1$ is not prime, and that*

$$\mu > \Big(\sum_i p_i - t - 1\Big) \min_{p \mid n} p.$$

Then there exists a non–maximal subgroup of finite index in Γ of isomorphism type τ.

Proof. Let d be a proper divisor of n, $1 < d < n$. Suppose there exists a subgroup Δ' of index d in Γ such that $\tau(\Delta') = (\lambda_1', \dots, \lambda_t'; \mu')$ satisfies

$$n\,\lambda_j' \geq d\,\lambda_j, \quad 1 \leq j \leq t. \tag{22}$$

Then we can apply Theorem 2 to see that Δ' has a subgroup of index n/d realizing τ, that is, τ can be realized by a non–maximal subgroup of finite index in Γ. Indeed, condition (i) is satisfied since τ is realizable and the Euler characteristic is multiplicative on subgroup chains, while condition (ii) of Theorem 2 corresponds precisely to (22). Define λ_j' to be the least integer satisfying both (22) and the congruence $\lambda_j' \equiv d\,e_j\ (p_j)$. We claim that there exists $\mu' \geq 0$ such that $(\lambda_1', \dots, \lambda_t'; \mu')$ is realizable in Γ, which implies Proposition 4 by the argument above. Clearly, an integer $\mu' \geq 0$ satisfying

$$\sum_i \lambda_i' \big(1 - \frac{1}{p_i}\big) + \mu' - 1 = -d\,\chi(\Gamma)$$

exists if and only if the quantity

$$\sum_i \big(de_i - \lambda_i'\big)\big(1 - \frac{1}{p_i}\big) + (r-1)d + 1 \tag{23}$$

is integral and non–negative. Integrality of (23) is clear by the definition of the numbers $\lambda_1', \dots, \lambda_t'$. Since $d\lambda_i/n \leq \lambda_i' < d\lambda_i/n + p_i$, the expression (23) is bounded below by

$$\begin{aligned}
&\sum_i \big(de_i - d\lambda_i/n - p_i\big)\big(1 - \frac{1}{p_i}\big) + d(r-1) + 1\\
&= d\Big(\sum_i e_i\big(1 - \frac{1}{p_i}\big) + r - 1\Big) - \frac{d}{n}\sum_i \lambda_i\big(1 - \frac{1}{p_i}\big) - \sum_i (p_i - 1) + 1\\
&= -d\chi(\Gamma) - \frac{d}{n}\big(-\chi(\tau) - \mu + 1\big) - \sum_i (p_i - 1) + 1\\
&= d(\mu - 1)/n - \sum_i (p_i - 1) + 1.
\end{aligned}$$

Now we choose d to be the largest proper divisor of n, that is, $n/d = \min_{p|n} p$. Then we find that (23) is certainly non–negative, provided that

$$\mu > \left(\sum_i p_i - t - 1\right) \min_{p|n} p.$$

In order to see that the tuple $(\lambda_1', \ldots, \lambda_t'; \mu')$ defined under the latter condition is realizable in Γ, it remains to check that $\lambda_i' \leq de_i$. Since $\tau = (\lambda_1, \ldots, \lambda_t; \mu)$ can by realized by assumption, we have $\lambda_i \leq ne_i$, and hence by definition of λ_i' that $\lambda_i' < de_i + p_i$. However, the construction of λ_i' also implies that $\lambda_i' \equiv de_i\ (p_i)$, and we conclude that indeed $\lambda_i' \leq de_i$, as required. □

Remark 4. *As we shall see in Section* 7*, most finite index subgroups have a free part of rather large rank* μ*, in particular, the condition on* μ *in Proposition* 4 *becomes weaker as* n *increases. On the other hand, while condition* (ii) *of Theorem* 2 *becomes vacuous for* $\Gamma = \mathrm{PSL}_2(\mathbb{Z})$*, we shall see in Section* 8 *that the assertion of Proposition* 4 *does in fact not hold in the modular group without some assumption on the size of* μ*.*

4.2. Normal subgroups.

Let Γ be as above, and let $\Delta \leq \Gamma$ be a subgroup of finite index in Γ. Then Δ is normal in Γ if and only if the induced action of Γ on Γ/Δ is regular. Concerning the type of a normal subgroup in Γ we have the following.

Proposition 5. *Let* Δ *be a normal subgroup of index* n *in* Γ *of type* $\tau(\Delta) = (\lambda_1, \ldots, \lambda_t; \mu)$*. Then we have* $n \mid \lambda_i$ *and* $\lambda_i \leq ne_i$ *for* $1 \leq i \leq t$*. Moreover, either* $n = 1$ *or* $n = p_i$ *for some* $i \in [t]$*, or* $\sum_i \left(e_i - \frac{\lambda_i}{n}\right) \geq 2$*.*

Proof. In the notation of Section 3, we see that for $i \in [t]$ and $j \in [e_i]$ the multiplicity m_{ij} is either 0 or n/p_i. The divisibility property follows from this observation and Theorem 1. The upper bound for λ_i is already contained in Theorem 2. Now assume that $\sum_i \left(e_i - \frac{\lambda_i}{n}\right) \leq 1$. By Theorem 1, this means that all the x_{ij} with at most one exception act trivially. However, a cyclic group of order p_i cannot act transitively on a set of cardinality other than 1 or p_i. □

As a first application of Proposition 5 we obtain the following statement.[3]

Corollary 2. *Let* p *and* q *be primes. Then every normal subgroup of finite index in* $\Gamma = C_p * C_q$ *is free, unless it is of index* 1*,* p*, or* q*.*

Proof. If $\Delta \trianglelefteq \Gamma$ is not free, then $\sum_i (e_i - \frac{\lambda_i}{n}) < 2$, hence $(\Gamma : \Delta)$ is 1, p, or q by the previous proposition. □

Furthermore, we have

Corollary 3. *Let* Γ *be as in* (1)*, and let* Δ *be a finite index subgroup of* Γ *of type* $\tau(\Delta) = (\lambda_1, \ldots, \lambda_t; \mu)$*. Then* $(N_\Gamma(\Delta) : \Delta) \mid \gcd(\lambda_1, \ldots, \lambda_t)$*; in particular,* Δ *is self-normalizing, provided that* $\gcd(\lambda_1, \ldots, \lambda_t) = 1$*.*

[3] For the special case of Corollary 2 where Γ is the modular group cf. for instance [6, Theorem 3.4.1].

Proof. Replace Γ with $N_\Gamma(\Delta)$, and apply Proposition 5. □

In the remainder of this section we take a look at the existence problem for normal subgroups. Denote by $f_n^\triangleleft(\Gamma)$ the number of free normal subgroups of index n in Γ, and let $s_n^\triangleleft(\Gamma)$ be the number of all normal subgroups of index n. Moreover, the difference $s_n^\triangleleft(\Gamma) - f_n^\triangleleft(\Gamma)$, that is, the number of non–free normal subgroups of index n in Γ, will be denoted by $\overline{f}_n^\triangleleft(\Gamma)$. By Theorem 1, the number $\overline{f}_n^\triangleleft(\Gamma)$ of non–free normal index n subgroups, after multiplication with $(n-1)!$, equals the number of regular Γ–actions on $[n]$, with at least one of the generators x_{ij} of Γ acting as the identity. Furthermore, the number of regular Γ–actions on $[n]$ mapping the generator x_{ij} onto the identity equals the number of all regular representations of degree n of the group

$$C_{p_1}^{*e_1} * \cdots * C_{p_{i-1}}^{*e_{i-1}} * C_{p_i}^{*e_i-1} * C_{p_{i+1}}^{*e_{i+1}} * \cdots * C_{p_t}^{*e_t} * F_r.$$

Classifying regular Γ–actions of degree n by specifying the set of those generators x_{ij} acting as fixed–point–free permutations, we find that

$$s_n^\triangleleft(\Gamma) = \sum \prod_i \binom{e_i}{e_i'} f_n^\triangleleft(C_{p_1}^{*e_1'} * \cdots * C_{p_t}^{*e_t'} * F_r), \tag{24}$$

where the summation extends over all t–tuples $(e_1', \dots, e_t')$ of non–negative integers such that $e_i' \leq e_i$ for all i. In order to invert equation (24), consider the poset

$$\mathcal{P} = \Big\{\delta \in \{0,1\}^{\Pi\times\mathbb{N}} : \sum_{p,n} \delta(p,n) < \infty\Big\},$$

where Π denotes the set of all primes, with componentwise definition of the partial order. We interpret $s_n^\triangleleft$ and $f_n^\triangleleft$ as functions on $\mathcal{P}$ by setting

$$s_n^\triangleleft(\delta) := s_n^\triangleleft\big(\mathop{*}_{p,n} C_p^{*\delta(p,n)} * F_r\big),$$

with a similar convention for $f_n^\triangleleft$. Note that $f_n^\triangleleft(\Gamma) = f_n^\triangleleft(\delta)$, where

$$\delta(p,m) := \begin{cases} 1, & p = p_i \text{ for some } 1 \leq i \leq t \text{ and } m \leq e_i \\ 0, & \text{otherwise.} \end{cases}$$

With these conventions, equation (24) becomes

$$s_n^\triangleleft(\delta) = \sum_{\gamma\leq\delta} f_n^\triangleleft(\gamma), \quad \delta \in \mathcal{P}.$$

Möbius inversion now gives

$$f_n^\triangleleft(\delta) = \sum_{\gamma\leq\delta} (-1)^{||\delta||-||\gamma||}\, s_n^\triangleleft(\gamma), \quad \delta \in \mathcal{P},$$

where $||\delta|| := \sum_{(p,m)} \delta(p,m)$. Returning to our original setting, the last equation yields

$$f_n^\triangleleft(\Gamma) = \sum_{(e_1',\dots,e_t')\leq(e_1,\dots,e_t)} (-1)^{\sum_i (e_i - e_i')} \prod_i \binom{e_i}{e_i'} s_n^\triangleleft\big(C_{p_1}^{*e_1'} * \cdots * C_{p_t}^{*e_t'} * F_r\big).$$

Summarizing our discussion, we have obtained the following.

Proposition 6. *We have*

$$\overline{f}_n^{\triangleleft}(\Gamma) = \sum_{(e_1',\ldots,e_t')<(e_1,\ldots,e_t)} (-1)^{1+\sum_i(e_i-e_i')} \prod_i \binom{e_i}{e_i'} s_n^{\triangleleft}\big(C_{p_1}^{*e_1'} * \cdots * C_{p_t}^{*e_t'} * F_r\big). \tag{25}$$

There are two cases where the right-hand side of Equation (25) becomes particularly simple.

Corollary 4. (i) *Let $\Gamma = C_2^{*3}$. Then Γ has exactly 3 non–free normal subgroups of any even index, and none of odd index greater than* 1.

(ii) *Let $\Gamma = C_p * C_\infty$, where p is a prime. Then Γ has precisely one non–free normal subgroup of index n for each n.*

Proof. By Proposition 6, we have

$$\overline{f}_n^{\triangleleft}(C_2^{*3}) = s_n^{\triangleleft}(1) \;-\; 3\,s_n^{\triangleleft}(C_2) \;+\; 3\,s_n^{\triangleleft}(C_2^{*2}).$$

The infinite dihedral group $C_2 * C_2$ contains 2 subgroups of index 2, as well as one normal subgroup of every other even index, and none of odd index greater than 1, whence (i). Similarly, Equation (25) gives

$$\overline{f}_n^{\triangleleft}(C_p * C_\infty) = s_n^{\triangleleft}(C_\infty) = 1.$$

□

5. ASYMPTOTIC ENUMERATION OF SUBGROUPS WITH GIVEN TYPE

For a $(t+1)$–tuple $\tau = (\lambda_1, \ldots, \lambda_t; \mu) \in \mathbb{N}_0^{t+1}$ define $s_\tau(\Gamma)$ to be the number of finite index subgroups in Γ with isomorphism type τ, and let $s_n(m_{11}, \ldots, m_{te_t})$ be the number of index n subgroups Δ in Γ such that, for $1 \le i \le t$ and $1 \le j \le e_i$, the group $\langle x_{ij}\rangle$ acts as a product of precisely m_{ij} cycles of length p_i on $\Delta\backslash\Gamma$. Similarly, denote by $h_n(m_{11}, \ldots, m_{te_t})$ the number of homomorphisms $\varphi : \Gamma \to S_n$ such that $\varphi(x_{ij})$ consists of m_{ij} cycles of length p_i and $n - p_i m_{ij}$ fixed points, and let $t_n(m_{11}, \ldots, m_{te_t})$ be the corresponding number of transitive representations. Among these quantities we have the following relations.

Proposition 7. *Let Γ be as in* (1).

(i) $s_n(m_{11}, \ldots, m_{te_t}) = t_n(m_{11}, \ldots, m_{te_t})/(n-1)!$;

(ii) *for* $\tau = (\lambda_1, \ldots, \lambda_t; \mu) \in \mathbb{N}_0^{t+1}$,

$$s_\tau(\Gamma) = \sum_{\substack{m_{11},\ldots,m_{te_t}\ge 0\\ m_{i1}+\cdots+m_{ie_i} = \frac{e_i n - \lambda_i}{p_i}\ (1\le i\le t)}} s_n(m_{11}, \ldots, m_{te_t}),$$

where

$$n = \frac{\sum_i \lambda_i(1-\frac{1}{p_i}) \;+\; \mu \;-\; 1}{\sum_i e_i(1-\frac{1}{p_i}) \;+\; r \;-\; 1},$$

provided this fraction is integral, and $s_\tau(\Gamma) = 0$ otherwise;

(iii)

$$h_n(m_{11},\dots,m_{te_t}) = \sum_{\nu=1}^{n}\binom{n-1}{\nu-1}\sum_{\mu_{11},\dots,\mu_{te_t}\geq 0} t_\nu(\mu_{11},\dots,\mu_{te_t})$$
$$h_{n-\nu}(m_{11}-\mu_{11},\dots,m_{te_t}-\mu_{te_t});$$

(iv) $h_n(m_{11},\dots,m_{te_t}) = (n!)^r \prod_{i=1}^{t}\prod_{j=1}^{e_i} \frac{n!}{m_{ij}!\,(n-p_im_{ij})!\,p_i^{m_{ij}}}.$

Proof. (i) This reflects the fact that a finite index subgroup Δ of Γ gives rise to a permutation representation of Γ on the cosets of Δ, and that every numbering of these cosets as $1,\dots n$ such that $\Delta\cdot 1\mapsto 1$ yields a representation $\Gamma\to S_n$ with $\mathrm{stab}(1)=\Delta$.

(ii) This is a reformulation of Theorem 1.

(iii) A permutation representation $\Gamma\to S_n$ taking x_{ij} to a product of precisely m_{ij} p_i–cycles is completely determined by specifying its domain of transitivity containing 1, the transitive action of Γ with certain parameters μ_{ij} on this domain, and the action of Γ on the complement of this domain with parameters $m_{ij}-\mu_{ij}$.

(iv) This follows from the mapping property of Γ and enumeration of the corresponding set of permutations. □

In principle, Proposition 7 contains complete information concerning the function $s_\tau(\Gamma)$. However, since the relation between h and t involves multiple summation over independent variables, Proposition 7 does not immediately lead to an asymptotic evaluation of $s_\tau(\Gamma)$; in particular, a generating function approach as in [24] seems difficult. In order to investigate the asymptotics of $s_\tau(\Gamma)$, we will need the following purely analytical result.

Lemma 2. *Let $p\geq 2$ be an integer, $\ell\in(1/p,1)$, and let $\epsilon>0$. Then there exists a constant C depending on p,ℓ and ϵ, such that for all n,ν and m, subject to the restriction $0\leq n-pm<n^\ell$, the inequality*

$$\sum_{\mu=0}^{m}\binom{m}{\mu}\binom{n-pm}{\nu-p\mu} < C\binom{n}{\nu}^{\ell+\epsilon} \tag{26}$$

holds true.

Proof. Without further mention we shall assume that n is sufficiently large. Also, by symmetry, we can suppose that $\nu \leq n/2$. Assume first that $\nu < \log n$. Then we have

$$\begin{aligned}\sum_{\mu=0}^{m} \binom{m}{\mu}\binom{n-pm}{\nu-p\mu} &\leq \sum_{\mu=0}^{m} m^{\mu}(n-pm)^{\nu-p\mu}\\ &\leq \sum_{\mu=0}^{m} m^{\mu}\, n^{\ell(\nu-p\mu)}\\ &= n^{\ell\nu}\sum_{\mu=0}^{m}\Big(\frac{m}{n^{\ell p}}\Big)^{\mu} \leq 2n^{\nu\ell}.\end{aligned}$$

On the other hand, we have

$$\binom{n}{\nu} \geq \big(\frac{n}{2\nu}\big)^{\nu} > n^{\nu(1-2\log\log n/\log n)}.$$

Comparing these two bounds, we find that

$$\sum_{\mu=0}^{m} \binom{m}{\mu}\binom{n-pm}{\nu-p\mu} \leq 2\binom{n}{\nu}^{\frac{\ell}{1-2\log\log n/\log n}} < \binom{n}{\nu}^{\ell+\epsilon}.$$

Hence, we may assume from now on that ν is large. First, we consider the contribution to the left-hand side of (26) of large values of μ, that is, $\nu - p\mu < 4\nu^{\ell}$. We have

$$\begin{aligned}\sum_{\nu/p-4\nu^{\ell}/p\leq\mu\leq\nu/p} \binom{m}{\mu}\binom{n-pm}{\nu-p\mu} &\leq \nu\binom{n/p}{\nu/p}\binom{n-pm}{\lfloor 4\nu^{\ell}\rfloor}\\ &\leq \nu\binom{n}{\nu}^{1/p} n^{4\nu^{\ell}}\\ &\leq \binom{n}{\nu}^{\ell+\epsilon}.\end{aligned}$$

For n and m fixed, let $C(\nu)$ be the constant defined by the equation

$$\sum_{\mu=0}^{m} \binom{m}{\mu}\binom{n-pm}{\nu-p\mu} = C(\nu)\binom{n}{\nu}^{\ell+\epsilon}.$$

We already know that $C(\nu) \leq 1$ for $\nu < \log n$. We have to show that $C(\nu)$ is bounded independently of ν. For this we use induction on ν. We have

$$\begin{aligned}\sum_{\mu=0}^{m} \binom{m}{\mu}\binom{n-pm}{\nu+1-p\mu} &\leq \sum_{\mu=0}^{\frac{\nu-4(\nu+1)^{\ell}+1}{p}} \binom{m}{\mu}\binom{n-pm}{\nu+1-p\mu} + \binom{n}{\nu+1}^{\ell+\epsilon}\\ &\leq \sum_{\mu=0}^{\frac{\nu-4(\nu+1)^{\ell}+1}{p}} \binom{m}{\mu}\binom{n-pm}{\nu-p\mu}\frac{n-pm}{\nu+1-p\mu} + \binom{n}{\nu+1}^{\ell+\epsilon}\\ &\leq \frac{n-pm}{4(\nu+1)^{\ell}} \sum_{\mu=0}^{\frac{\nu-4(\nu+1)^{\ell}+1}{p}} \binom{m}{\mu}\binom{n-pm}{\nu-p\mu} + \binom{n}{\nu+1}^{\ell+\epsilon}\\ &\leq \frac{n^{\ell}}{4(\nu+1)^{\ell}} C(\nu)\binom{n}{\nu}^{\ell+\epsilon} + \binom{n}{\nu+1}^{\ell+\epsilon}.\end{aligned}$$

On the other hand

$$\binom{n}{\nu+1}^{\ell+\epsilon} = \Big(\frac{n-\nu}{\nu+1}\Big)^{\ell+\epsilon}\binom{n}{\nu}^{\ell+\epsilon} > \Big(\frac{n}{2(\nu+1)}\Big)^{\ell}\binom{n}{\nu}^{\ell+\epsilon}.$$

Comparing these bounds, we see that

$$C(\nu+1) \leq \frac{C(\nu)}{2} + 1,$$

implying $C(\nu) \leq 2$ for all ν. □

With Lemma 2 in hand, we can now establish the following.

Theorem 3. *Let Γ be as in (1), and let t_n and h_n be as in Proposition 7. For $1 \leq i \leq t$ and $1 \leq j \leq e_i$, let ℓ_{ij} be real parameters subject to the relation $\sum_{i,j}(\ell_{ij}-1) < r-1$, and the boundary conditions $1/p_i < \ell_{ij} < 1$. Then, for every $\epsilon > 0$, n sufficiently large, and with quantities m_{ij} satisfying $n - p_i m_{ij} < n^{\ell_{ij}}$, we have*

$$\left|\frac{t_n(m_{11},\dots,m_{te_t})}{h_n(m_{11},\dots,m_{te_t})} - 1\right| < n^{1+\sum_{i,j}(\ell_{ij}-1)-r+\epsilon}.$$

Proof. Consider the terms on the right–hand side of Proposition 7 (iii) with $\nu = n$. These terms involve a factor $h_0(m_{11}-\mu_{11},\dots,m_{te_t}-\mu_{te_t})$, which is zero unless $m_{ij} = \mu_{ij}$ for all i and j, in which case it is 1. Hence, the only term with $\nu = n$ is $t_n(m_{11},\dots,m_{te_t})$. Thus, we have

$$h_n(m_{11},\dots,m_{te_t}) - t_n(m_{11},\dots,m_{te_t}) =$$
$$\sum_{\nu=1}^{n-1}\binom{n-1}{\nu-1}\sum_{\mu_{11},\dots,\mu_{te_t}\geq 0} t_\nu(\mu_{11},\dots,\mu_{te_t})h_{n-\nu}(m_{11}-\mu_{11},\dots,m_{te_t}-\mu_{te_t}).$$

Replacing t by h on the right–hand side of the latter equation, and substituting the explicit expression for h_n given by Proposition 7 (iv) gives

$$|h_n(m_{11},\dots,m_{te_t}) - t_n(m_{11},\dots,m_{te_t})| \leq$$
$$\sum_{\nu=1}^{n-1}\binom{n-1}{\nu-1}\sum_{\mu_{11},\dots,\mu_{te_t}\geq 0}(\nu!)^r\prod_i\prod_j\frac{\nu!}{\mu_{ij}!\,(\nu-p_i\mu_{ij})!\,p_i^{\mu_{ij}}}$$
$$\times\big((n-\nu)!\big)^r\prod_i\prod_j\frac{(n-\nu)!}{(m_{ij}-\mu_{ij})!\,(n-\nu-p_i(m_{ij}-\mu_{ij})!\,p_i^{m_{ij}-\mu_{ij}}}.$$

Dividing this inequality by

$$h_n(m_{11},\dots,m_{te_t}) = (n!)^r\prod_i\prod_j\frac{n!}{m_{ij}!\,(n-p_im_{ij})!\,p_i^{m_{ij}}}$$

and collecting terms we find that

$$\left|\frac{t_n(m_{11},\dots,m_{te_t})}{h_n(m_{11},\dots,m_{te_t})} - 1\right| \leq$$
$$\sum_{\nu=1}^{n-1}\binom{n-1}{\nu-1}\binom{n}{\nu}^{-r}\prod_{i=1}^{t}\prod_{j=1}^{e_i}\binom{n}{\nu}^{-1}\sum_{\mu_{ij}=0}^{m_{ij}}\binom{m_{ij}}{\mu_{ij}}\binom{n-p_im_{ij}}{\nu-p_i\mu_{ij}}. \tag{27}$$

Applying Lemma 2 to each of the factors on the right-hand side of (27), we get

$$\left|\frac{t_n(m_{11},\dots,m_{te_t})}{h_n(m_{11},\dots,m_{te_t})} - 1\right| \leq \sum_{\nu=1}^{n-1}\binom{n-1}{\nu-1}\binom{n}{\nu}^{-r}$$
$$\times\prod_i\prod_j C(p_i,\ell_{ij},\epsilon)\binom{n}{\nu}^{-1+\ell_{ij}+\epsilon}$$
$$\leq \tilde{C}\sum_{\nu=1}^{n-1}\binom{n}{\nu}^{\sum_{i,j}(\ell_{ij}+\epsilon-1)-r+1}.$$

By assumption, $\sum_{i,j}(\ell_{ij}-1)-r+1 = -\delta$ for some $\delta > 0$, hence the exponent is negative, provided that, say, $\epsilon \leq \frac{\delta}{2\sum e_i}$, in which case the whole sum can be estimated by its largest term $n^{\sum_{ij}(\ell_{ij}+\epsilon-1)-r+1}$, and the assertion of Theorem 3 follows upon renaming ϵ. Since the right–hand side of (26) increases with ϵ, the result follows in general. □

For future reference we note that in the proof of Theorem 3 we did not expand the summation over ν; in fact, for each ν, the proportion of homomorphisms counted by $h_n(m_{11},\dots,m_{te_t})$ such that the domain of transitivity of 1 consists of precisely ν points, is $\mathcal{O}\big(\binom{n}{\nu}^{\sum_{i,j}(\ell_{ij}+\varepsilon-1)-r+1}\big)$.

Corollary 5. *Let Γ be as in* (1), *and let $\mu = n(\sum_{i=1}^t e_i(1-\frac{1}{p_i}) + r - 1)$. Then we have for $s_{(0,\ldots,0;\mu)}(\Gamma)$, the number of free subgroups of index n, the estimate*[4]

$$s_{(0,\ldots,0;\mu)}(\Gamma) = \Big(1 + \mathcal{O}\Big(n^{1+\sum_i(1/p_i-1)-r+\epsilon}\Big) + \mathcal{O}((n^{-1})\Big)$$

$$\times (n!)^{\chi(\Gamma)} n^{1-\sum_{i=1}^t e_i/2} \prod_{i=1}^t p_i^{e_i/2} n^{e_i/2p_i},$$

provided that $p_i|n$ for all i, and $s_{(0,\ldots,0;\mu)}(\Gamma) = 0$ otherwise.

Proof. From Theorem 1 it follows that the condition $p_i|n$ is necessary. Hence, assume that this condition is satisfied. By Proposition 7, we can compute $h_n(n/p_1, \ldots, n/p_t)$, and by Theorem 3 we can approximate t_n by h_n, where we choose $\ell_{ij} = 1/p_i + c\epsilon$ with some sufficiently small c. From this we obtain

$$s_{(0,\ldots,0;\mu)}(\Gamma) = \left(1 + \mathcal{O}\left(n^{1+\sum_i(1/p_i-1)-r+\epsilon}\right)\right) \frac{(n!)^r}{(n-1)!} \prod_{i=1}^t \prod_{j=1}^{e_i} \frac{n!}{(n/p_i)! p_i^{n/p_i}}.$$

Approximating the factorials by means of Stirling's formula, we obtain

$$\begin{aligned} s_{(0,\ldots,0;\mu)}(\Gamma) &= \left(1 + \mathcal{O}\left(n^{1+\sum_i(1/p_i-1)-r+\epsilon}\right)\right) \cdot n \cdot (n!)^{r-1} \\ &\qquad \times \prod_{i=1}^t \prod_{j=1}^{e_i} n!^{1-1/p_i} \sqrt{p_i} n^{-1/2+1/2p_i} \left(1 + \mathcal{O}\left(\frac{1}{n}\right)\right) \\ &= \left(1 + \mathcal{O}\left(n^{1+\sum_i(1/p_i-1)-r+\epsilon}\right) + \mathcal{O}\left(\frac{1}{n}\right)\right) \\ &\qquad \times n!^{\chi(\Gamma)} n^{1-\sum_{i=1}^t e_i/2} \prod_{i=1}^t p_i^{e_i/2} n^{e_i/2p_i}. \end{aligned}$$

□

Remark 5. *Theorem* 3 *becomes vacuous in the case when $\chi(\Gamma) \geq 0$, since in this case the assumptions on the parameters ℓ_{ij} cannot be simultaneously satisfied. On the other hand, if $\chi(\Gamma) < 0$, then such ℓ_{ij} always exist.*

6. Further asymptotic results

6.1. **Enumerating subgroups by rank.** Among the subgroups of a free product, free groups naturally play a prominent role. In connection with the construction of automorphic functions, Poincaré asked whether 'almost all' finite index subgroups of the modular group are free. If subgroups are enumerated by index, a negative answer was given in [22, Proposition 3] for all groups Γ of the form (3) with $\chi(\Gamma) < 0$; however, in the case of the modular group for instance, the probability of index n subgroups to be free decays like $e^{-cn^{1/2}}$, which is rather slow compared to the size of the sample

[4] A more precise result for the free subgroup growth of an arbitrary virtually free group can be found in [21].

space, which tends to infinity like $n!^{1/6}$. Moreover, as we shall see in Section 7, almost all subgroups Δ have a free factor accounting for all but $\mathcal{O}(n^{1/2})$ of the generator of Δ; thus, in two different senses, Poincaré's question 'almost' has a positive answer.

If $\mathrm{PSL}_2(\mathbb{Z})$ acts in the usual way on the upper half plane, the rank of a finite index subgroup Δ determines the genus of a fundamental domain for Δ; hence, from an analytical point of view, it appears more natural to enumerate finite index subgroups by rank rather than by index. Our next result shows that, in this sense, a positive proportion of all finite index subgroups is free. For Γ as in (1) and an integer n, let $r_n(\Gamma)$ be the number of finite index subgroups Δ of Γ of rank n. Note that for such a group Δ, we have $1-n \leq \chi(\Delta) \leq 1-n/2$, thus, by (2), $(\Gamma : \Delta)$ is bounded, and $r_n(\Gamma)$ is finite for all n. Let $r_n^f(\Gamma)$ be the number of free subgroups of Γ of finite index and rank n. Trivially, $r_n(\Gamma)=0$, unless $n-1$ is divisible by the numerator of $\chi(\Gamma)$, in which case we call n *admissible*. With these definitions, we have the following.

Proposition 8. *Let Γ be as in* (1)*. Then, as n tends to infinity through admissible numbers, we have*

$$\frac{r_n^f(\Gamma)}{r_n(\Gamma)} \to C(\Gamma),$$

where

$$C(\Gamma) = \left(\sum_{\substack{\kappa_{11},\ldots,\kappa_{te_t} \\ \sum \kappa_{ij} \equiv 0 \ (\mathrm{rk}(\Gamma)-1)}} \prod_{i=1}^{t} \prod_{j=1}^{e_t} \frac{1}{(p_i\kappa_{ij} - \frac{|\vec{\kappa}|}{\mathrm{rk}(\Gamma)-1})!} \right)^{-1}$$

satisfies $0 < C(\Gamma) < 1$. In particular, for Hecke-groups $H_q = C_2 * C_q$ with $q \geq 3$ a prime, we have

$$C(H_q) = \left(\frac{1}{q-2} \sum_{\nu=1}^{q-2} e^{2+2\pi i\nu/(q-2)} \right)^{-1}.$$

Here and in the sequel, we adopt the conventions that factorials of negative integers are evaluated as ∞, and that $\frac{1}{\infty}=0$.

Proof. Let Δ be a finite index subgroup of representation type (m_{ij}, ν). By Theorem 1, the rank of Δ can be computed to be

$$\mathrm{rk}(\Delta) = \sum_{k=1}^{t} \lambda_k + \mu = n(\mathrm{rk}(\Gamma)-1) - \sum_{k=1}^{t} M_k(\Delta).$$

Summing over all possible indices of rank n subgroups, we obtain

$$\begin{aligned} r_n(\Gamma) &= \sum_\nu \big|\{\Delta : (\Gamma:\Delta)=\nu, \mathrm{rk}(\Delta)=n\}\big| \\ &= \sum_\nu \frac{1}{(\nu-1)!}\big|\{\varphi:\Gamma\to S_\nu, \varphi(\gamma) \text{ transitive}, (\mathrm{rk}(\Gamma)-1)\nu - \sum_k M_k(\varphi)=n\}\big| \\ &= \sum_{\substack{\mu_{11},\dots,\mu_{te_t}\\ \sum\mu_{ij}\equiv n-1\ (\mathrm{rk}(\Gamma)-1)}} \frac{1}{(\nu(\vec{\mu})-1)!}\cdot\prod_{i=1}^t\prod_{j=1}^{e_t}\frac{\nu(\vec{\mu})!}{p_i^{\mu_{ij}}\mu_{ij}!(\nu(\vec{\mu})-p_i\mu_{ij})!} \qquad (28) \\ &\qquad\times\underbrace{\frac{\big|\{\varphi:\Gamma\to S_{\nu(\vec{\mu})}, \varphi(\Gamma) \text{ transitive and of representation type } (\mu_{ij},\nu(\vec{\mu}))\}\big|}{\big|\{\varphi:\Gamma\to S_{\nu(\vec{\mu})} \text{ of representation type } (\mu_{ij},\nu(\vec{\mu}))\}\big|}}_{=:\delta(\vec{\mu})}, \end{aligned}$$

where $\nu(\vec{\mu}) = \frac{n-1+\sum\mu_{ij}}{\mathrm{rk}(\Gamma)-1}$. As Δ ranges over all finite index subgroups of rank n, the parameters μ_{ij}, ν become maximal for Δ free. Denoting by $\mu_{ij}^{(0)}, \nu^{(0)}$ these maximal values, we have

$$\nu^{(0)} = -\frac{n-1}{\chi(\Gamma)}, \qquad \mu_{ij}^{(0)} = -\frac{n-1}{p_i\chi(\Gamma)}.$$

Since $\delta(\vec{\mu})\leq 1$, the sum above is dominated by

$$\begin{aligned} &\sum_{\substack{\mu_{11},\dots,\mu_{te_t}\\ \sum\mu_{ij}\equiv n-1\ (\mathrm{rk}(\Gamma)-1)}} \frac{1}{(\nu(\vec{\mu})-1)!}\prod_{i=1}^t\prod_{j=1}^{e_t}\frac{\nu(\vec{\mu})!}{p_i^{\mu_{ij}}\mu_{ij}!(\nu(\vec{\mu})-p_i\mu_{ij})!} \\ &\quad= \nu^{(0)}(\nu^{(0)}!)^{\mathrm{rk}(\Gamma)-1}\prod_{i=1}^t\prod_{j=1}^{e_t}\frac{1}{p_1^{\mu_{ij}^{(0)}}\mu_{ij}^{(0)}!} \sum_{\substack{\kappa_{11},\dots,\kappa_{te_t}\\ \sum\kappa_{ij}\equiv 0\ (\mathrm{rk}(\Gamma)-1)}} \frac{(\nu^{(0)}-1)!}{(\nu^{(0)}-\frac{|\vec{\kappa}|}{\mathrm{rk}(\Gamma)-1}-1)!} \qquad (29) \\ &\qquad\times\prod_{i=1}^t\prod_{j=1}^{e_t}\frac{p_i^{\kappa_{ij}}\mu_{ij}^{(0)}!}{(\mu_{ij}^{(0)}-\kappa_{ij})!(p_i\kappa_{ij}-\frac{|\vec{\kappa}|}{\mathrm{rk}(\Gamma)-1})!}\left(\frac{(\nu^{(0)}-\frac{|\vec{\kappa}|}{\mathrm{rk}(\Gamma)-1})!}{\nu^{(0)}!}\right)^{\mathrm{rk}(\Gamma)}, \end{aligned}$$

where we put $|\vec{\kappa}| = \sum\kappa_{ij}$. For a tuple $\vec{\kappa}$, define $S(\vec{\kappa})$ by

$$\begin{aligned} S(\vec{\kappa}) := &\frac{(\nu^{(0)}-1)!}{\Gamma(\nu^{(0)}-\frac{|\vec{\kappa}|}{\mathrm{rk}(\Gamma)-1})} \\ &\times\prod_{i=1}^t\prod_{j=1}^{e_t}\frac{p_i^{\kappa_{ij}}\mu_{ij}^{(0)}!}{(\mu_{ij}^{(0)}-\kappa_{ij})!\Gamma(p_i\kappa_{ij}-\frac{|\vec{\kappa}|}{\mathrm{rk}(\Gamma)-1}+1)}\left(\frac{\Gamma(\nu^{(0)}-\frac{|\vec{\kappa}|}{\mathrm{rk}(\Gamma)-1}+1)}{\nu^{(0)}!}\right)^{\mathrm{rk}(\Gamma)}; \end{aligned}$$

in particular, $S(\vec{0})=1$. Fix a pair of indices $i_0\leq t, j_0\leq e_{i_0}$. For a tuple $\vec{\kappa}$, let $\vec{\kappa}'$ be the vector obtained by increasing $\kappa_{i_0j_0}$ by 1. Then we have

$$\begin{aligned}
S(\vec{\kappa}') &= S(\vec{\kappa})\cdot\frac{\Gamma(\nu^{(0)}-\frac{|\vec{\kappa}|}{\mathrm{rk}(\Gamma)-1})}{\Gamma(\nu^{(0)}-\frac{|\vec{\kappa}|+1}{\mathrm{rk}(\Gamma)-1})}\left(\frac{\Gamma(\nu^{(0)}-\frac{|\vec{\kappa}|}{\mathrm{rk}(\Gamma)-1}+1)}{\Gamma(\nu^{(0)}-\frac{|\vec{\kappa}|+1}{\mathrm{rk}(\Gamma)-1}+1)}\right)^{\mathrm{rk}(\Gamma)}(\mu_{i_0j_0}^{(0)}-\kappa_{i_0j_0})\\
&\quad\times p_{i_0j_0}\cdot\frac{\Gamma(p_{i_0}\kappa_{i_0j_0}-\frac{|\vec{\kappa}|}{\mathrm{rk}(\Gamma)-1}+1)}{\Gamma(p_{i_0}\kappa_{i_0j_0}-\frac{|\vec{\kappa}|+1}{\mathrm{rk}(\Gamma)-1}+1+p_{i_0})}\prod_{\substack{i=1\\(i,j)\neq(i_0,j_0)}}^{t}\prod_{j=1}^{e_t}\frac{\Gamma(p_i\kappa_{ij}-\frac{|\vec{\kappa}|}{\mathrm{rk}(\Gamma)-1}+1)}{\Gamma(p_i\kappa_{ij}-\frac{|\vec{\kappa}|+1}{\mathrm{rk}(\Gamma)-1}+1)}\\
&= S(\vec{\kappa})\cdot A\cdot p_{i_0j_0}\cdot B,
\end{aligned}$$

say. Using the log-convexity of the Γ-function together with its functional equation, we obtain

$$A\leq\left(\nu^{(0)}-\frac{|\vec{\kappa}|}{\mathrm{rk}(\Gamma)-1}\right)^{-1}\cdot(\mu_{i_0j_0}^{(0)}-\kappa_{i_0j_0})=\frac{1}{p_{i_0j_0}}\cdot\frac{\nu^{(0)}-p_{i_0j_0}\kappa_{i_0j_0}}{\nu^{(0)}-\frac{|\vec{\kappa}|}{\mathrm{rk}(\Gamma)-1}}$$

and

$$B\leq\left(p_{i_0}\kappa_{i_0j_0}-\frac{|\vec{\kappa}|}{\mathrm{rk}(\Gamma)-1}\right)^{-p_{i_0}+\frac{1}{\mathrm{rk}\Gamma}}\prod_{\substack{i=1\\(i,j)\neq(i_0,j_0)}}^{t}\prod_{j=1}^{e_t}\left(p_i\kappa_{ij}-\frac{|\vec{\kappa}|}{\mathrm{rk}(\Gamma)-1}+1\right)^{1/(\mathrm{rk}(\Gamma)-1}.$$

If we assume that (i_0,j_0) is chosen in such a way that $p_{i_0}\kappa_{i_0j_0}\geq p_i(\kappa_{ij}-1)$ for all i,j, these estimates can be simplified to

$$\begin{aligned}
A &\leq \frac{1}{p_{i_0j_0}}\cdot\frac{\nu^{(0)}}{\nu^{(0)}-2},\\
B &\leq \left(p_{i_0}\kappa_{i_0j_0}-\frac{|\vec{\kappa}|}{\mathrm{rk}(\Gamma)-1}\right)^{-p_{i_0}}\left(p_{i_0}\kappa_{i_0j_0}-\frac{|\vec{\kappa}|}{\mathrm{rk}(\Gamma)-1}+1+\max_i p_i\right);
\end{aligned}$$

in particular, for n sufficiently large, $S(\vec{\kappa})$ is bounded independent of n, and if $\kappa_{i_0j_0}$ is sufficiently large, and $p_{i_0}\kappa_{i_0j_0}\geq p_i(\kappa_{ij}-1)$ for all i,j, then $S(\vec{\kappa}')\leq\frac{1}{2}S(\vec{\kappa})$. Hence, the sum on the right-hand side of (29) is dominated by an absolute converging sum, which is independent of n. By Theorem 3, for $\vec{\kappa}$ fixed and $n\to\infty$, we have $\delta(\vec{\mu})\to 1$, where $\vec{\mu}$ denotes the transformed parameters corresponding to κ_{ij} and n. Hence, the right-hand side of (28) and the left-hand side of (29) are asymptotically equal, and we may interchange the limit $n\to\infty$ with the summation on the right hand side of (29). To prove our claim, it suffices now to compute the limit as $n\to\infty$ of a single summand. We have, as $\nu^{(0)}\to\infty$,

$$\begin{aligned}
&\frac{(\nu^{(0)}-1)!}{(\nu^{(0)}-\frac{|\vec{\kappa}|}{\mathrm{rk}(\Gamma)-1}-1)!}\prod_{i=1}^{t}\prod_{j=1}^{e_t}\frac{p_i^{\kappa_{ij}}\mu_{ij}^{(0)}!}{(\mu_{ij}^{(0)}-\kappa_{ij})!(p_i\kappa_{ij}-\frac{|\vec{\kappa}|}{\mathrm{rk}(\Gamma)-1})!}\left(\frac{(\nu^{(0)}-\frac{|\vec{\kappa}|}{\mathrm{rk}(\Gamma)-1})!}{\nu^{(0)}!}\right)^{\mathrm{rk}(\Gamma)}\\
&\sim(\nu^{(0)})^{|\vec{\kappa}|}\prod_{i=1}^{t}\prod_{j=1}^{e_t}\frac{p_i^{\kappa_{ij}}(\nu^{(0)}/p_i)^{\kappa_{ij}}}{(p_i\kappa_{ij}-\frac{|\vec{\kappa}|}{\mathrm{rk}(\Gamma)-1})!}\\
&\sim\prod_{i=1}^{t}\prod_{j=1}^{e_t}\frac{1}{(p_i\kappa_{ij}-\frac{|\vec{\kappa}|}{\mathrm{rk}(\Gamma)-1})!}.
\end{aligned}$$

It follows that

$$r_n(\Gamma) \sim r_n^f(\Gamma) \cdot \sum_{\substack{\kappa_{11},\ldots,\kappa_{te_t} \\ \sum \kappa_{ij} \equiv 0 \ (\mathrm{rk}(\Gamma)-1)}} \prod_{i=1}^{t} \prod_{j=1}^{e_t} \frac{1}{(p_i\kappa_{ij} - \frac{|\vec{\kappa}|}{\mathrm{rk}(\Gamma)-1})!}.$$

From this our first claim as well as the estimate $0 < C(\Gamma) < 1$ follow. Moreover, for Γ a Hecke-group $H_q = C_2 * C_q$, $q \geq 3$ prime, we obtain

$$\begin{aligned} r_n(H_q) &\sim r_n^f(H_q) \sum_{i,j \geq 0} \frac{1}{(i-j)!((q-1)j-i)!} \\ &= r_n^f(H_q) \sum_{j=0}^{\infty} \sum_{k=0}^{j} \binom{(q-2)j}{k} \frac{1}{((q-2)j)!} \\ &= r_n^f(H_q) \sum_{j=0}^{\infty} \frac{2^{(q-2)j}}{((q-2)j)!} \\ &= r_n^f(H_q) \cdot \left(\frac{1}{q-2} \sum_{\nu=1}^{q-2} e^{2+2\pi i\nu/(q-2)} \right). \end{aligned}$$

□

6.2. **Maximal subgroups of free products.** Our next result establishes the fact, already mentioned in Section 4.1, that, with probability tending to 1, a subgroup of finite index in Γ is maximal.

Proposition 9. *Let Γ be as in* (1), *and suppose that $\chi(\Gamma) < 0$. Denote by $s_n^{\neg max}(\Gamma)$ the number of non–maximal subgroups of index n in Γ. Then we have*

$$\frac{s_n^{\neg max}(\Gamma)}{s_n(\Gamma)} = o(1) \quad (n \to \infty);$$

that is, almost all finite index subgroups of Γ are maximal.

Proof. Define $t_n^{\neg max}(\Gamma)$ to be the number of homomorphisms $\varphi : \Gamma \to S_n$ such that $\varphi(\Gamma)$ acts transitively and imprimitively on $[n]$. As $s_n^{\neg max}(\Gamma) = t_n^{\neg max}(\Gamma)/(n-1)!$, it suffices to show that $t_n^{\neg max}(\Gamma)/t_n(\Gamma)$ tends to 0. Since $t_n \sim h_n$ (cf. [22, Prop. 2]), the latter assertion is equivalent to the statement that $t_n^{\neg max}(\Gamma)/h_n(\Gamma) \to 0$. Let φ be a homomorphism counted by $t_n^{\neg max}(\Gamma)$, $\Omega \subseteq [n]$ a domain of imprimitivity for φ, and put $|\Omega| = d$. Then there exists a partition of $[n]$ into n/d sets which is invariant under $\varphi(\Gamma)$, in particular d divides n. The image $\varphi(\Gamma)$ is contained in a subgroup of S_n isomorphic to $S_d \wr S_{n/d}$, which is determined by Ω and its translates. From this observation, we obtain the inequality

$$\begin{aligned} t_n^{\neg max}(\Gamma) &\leq \sum_{\substack{d\mid n\\ 1<d<n}} \big((n/d)!\big)^{-1} \binom{n}{d,\dots,d} \big|\mathrm{Hom}(\Gamma, S_d \wr S_{n/d})\big| \\ &= \sum_{\substack{d\mid n\\ 1<d<n}} \big((n/d)!\big)^{-1} \binom{n}{d,\dots,d} |S_d \wr S_{n/d}|^r \prod_{i=1}^{t} \big|\mathrm{Hom}(C_{p_i}, S_d \wr S_{n/d})\big|^{e_i}. \end{aligned} \tag{30}$$

For $i = 1, \dots, t$ define functions

$$f_{p_i}(n) := \left(\frac{|\mathrm{Hom}(C_{p_i}, S_n)|}{(n!)^{1-1/p_i}}\right)^{1/n}.$$

Then we find from the asymptotic formula[5]

$$|\mathrm{Hom}(C_{p_i}, S_n)| \sim K_{p_i}\, (n!)^{1-1/p_i}\, \mathrm{e}^{n^{1/p_i}}\, n^{-1/2} \quad (n \to \infty) \tag{31}$$

that $f_{p_i}(n) \to 1$ as $n \to \infty$; in particular, $f_{p_i}(n)$ is bounded for every i. Putting $f(n) := \max_{1\leq i\leq t} f_{p_i}(n)$, it follows that f is bounded, too. We can compute $|\mathrm{Hom}(C_{p_i}, S_d \wr S_{n/d})|$ by first fixing the cycle structure of the canonical image in $S_{n/d}$, and then defining homomorphisms $\varphi : C_{p_i} \to S_d \wr C_{p_i}$ respectively $C_{p_i} \to S_d$ in the same way as we did in the proof of Theorem 1. This gives

$$\begin{aligned} |\mathrm{Hom}(C_{p_i}, S_d \wr S_{n/d})| &= \sum_{j\leq \frac{n}{dp_i}} \binom{n/d}{\underbrace{p_i,\dots,p_i}_{j}, \underbrace{1,\dots,1}_{n/d-jp_i}} \frac{(d!)^{j(p_i-1)}}{j!\,(n/d-jp_i)!} |\mathrm{Hom}(C_{p_i}, S_d)|^{n/d-jp_i} \\ &\leq \sum_{j\leq \frac{n}{dp_i}} \binom{n/d}{p_i,\dots,p_i,1,\dots,1} \frac{(d!)^{\frac{n}{d}(1-\frac{1}{p_i})}}{j!\,(n/d-jp_i)!} \big(f(d)\big)^{n-jdp_i} \\ &\leq (d!)^{\frac{n}{d}(1-\frac{1}{p_i})} \big(f(d)\big)^n \sum_{j\leq \frac{n}{dp_i}} \binom{n/d}{p_i,\dots,p_i,1,\dots,1} \big(j!\,(n/d-jp_i)!\big)^{-1} \\ &= (d!)^{\frac{n}{d}(1-\frac{1}{p_i})} \big(f(d)\big)^n |\mathrm{Hom}(C_{p_i}, S_{n/d})| \\ &\leq (d!)^{\frac{n}{d}(1-\frac{1}{p_i})} \big(f(d)\big)^n \big((n/d)!\big)^{1-1/p_i} \big(f(n/d)\big)^{n/d}. \end{aligned}$$

[5] Cf. [18] and [19]. More precise results concerning the asymptotic enumeration of finite G–actions for an arbitrary finite group G can be found in [24].

Using the last bound in (30), we find that

$$\begin{aligned}
t_n^{\neg max}(\Gamma) &\leq \sum_{\substack{d|n\\ 1<d<n}} \big((n/d)!\big)^{-1}\binom{n}{d,\dots,d}\prod_{i=1}^{t}\Big[(d!)^{\frac{n}{d}(1-\frac{1}{p_i})}\big((n/d)!\big)^{1-1/p_i}\Big]^{e_i}\\
&\qquad\qquad\times \big((d!)^{n/d}(n/d)!\big)^{r}\big(f(d)\big)^{n\sum_i e_i}\big(f(n/d)\big)^{\frac{n}{d}\sum_i e_i}\\
&= \sum_{\substack{d|n\\ 1<d<n}} \big((n/d)!\big)^{-1}\binom{n}{d,\dots,d}\big((d!)^{n/d}(n/d)!\big)^{1-\chi(\Gamma)}\big(f(d)\big)^{n\sum_i e_i}\big(f(n/d)\big)^{\frac{n}{d}\sum_i e_i}.
\end{aligned}$$

Applying (31) again, we see that $h_n(\Gamma) \geq (n!)^{1-\chi(\Gamma)}$ for n sufficiently large. Dividing by this inequality, we obtain for large n that

$$\frac{t_n^{\neg max}(\Gamma)}{h_n(\Gamma)} \leq \sum_{\substack{d|n\\ 1<d<n}} \Big(\frac{n!}{(d!)^{n/d}(n/d)!}\Big)^{\chi(\Gamma)}\big(f(d)\big)^{n\sum_i e_i}\big(f(n/d)\big)^{\frac{n}{d}\sum_i e_i}. \tag{32}$$

First, consider terms on the right-hand side of (32) with $d \geq n^{1/3}$. For such pairs (n, d), the terms involving f are uniformly of magnitude $\mathrm{e}^{o(n)}$, since $f(d) \to 1$ and $n/d = o(n)$. Since the same estimate also holds for $\big((n/d)!\big)^{-\chi(\Gamma)}$, we have

$$\sum_{\substack{d|n\\ n^{1/3}\leq d<n}} \Big(\frac{n!}{(d!)^{n/d}(n/d)!}\Big)^{\chi(\Gamma)}\big(f(d)\big)^{n\sum_i e_i}\big(f(n/d)\big)^{\frac{n}{d}\sum_i e_i} = \mathrm{e}^{o(n)}\sum_{\substack{d|n\\ n^{1/3}\leq d<n}}\Big(\frac{n!}{(d!)^{n/d}}\Big)^{\chi(\Gamma)}.$$

As $(d!)^{1/d}$ is increasing with d, the largest term of the last sum will occur for the maximal value of d, which in turn is at most $n/2$. Consequently, since $\frac{n!}{((n/2)!)^2} > 2^n/n$, the whole sum is bounded above by $2^{\chi(\Gamma)n+o(n)}$, and hence, in view of our assumption that $\chi(\Gamma) < 0$, tends to 0 as n tends to infinity.

Now consider terms with $d \leq n^{1/3}$. Here, the terms involving f may grow exponentially fast. We have

$$\sum_{\substack{d|n\\ 1<d\leq n^{1/3}}} \Big(\frac{n!}{(d!)^{n/d}(n/d)!}\Big)^{\chi(\Gamma)}\big(f(d)\big)^{n\sum_i e_i}\big(f(n/d)\big)^{\frac{n}{d}\sum_i e_i} =$$

$$\mathrm{e}^{\mathcal{O}(n)}\sum_{\substack{d|n\\ 1<d\leq n^{1/3}}}\Big(\frac{n!}{(d!)^{n/d}(n/d)!}\Big)^{\chi(\Gamma)}.$$

Using Stirling's formula in the form $n! \geq (n/\mathrm{e})^n$ together with the trivial bounds $d! \leq d^d$ and $(n/d)! \leq (n/d)^{n/d}$, the right–hand side becomes

$$\begin{aligned}\mathrm{e}^{\mathcal{O}(n)} \sum_{\substack{d|n\\1<d\leq n^{1/3}}} \Big(\frac{n!}{(d!)^{n/d}(n/d)!}\Big)^{\chi(\Gamma)} &\leq \mathrm{e}^{\mathcal{O}(n)} \sum_{\substack{d|n\\1<d\leq n^{1/3}}} \Big(\frac{n^n}{d^n(n/d)^{n/d}}\Big)^{\chi(\Gamma)}\\ &\leq \mathrm{e}^{\mathcal{O}(n)} \sum_{\substack{d|n\\1<d\leq n^{1/3}}} \Big(\frac{n^n}{n^{n/3}n^{n/2}}\Big)^{\chi(\Gamma)}\\ &\leq \mathrm{e}^{\mathcal{O}(n)}\, n^{\chi(\Gamma)n/6},\end{aligned}$$

which also tends to 0 as $n \to \infty$. □

7. DISTRIBUTION OF ISOMORPHISM TYPES

In this section, we establish limit laws for the distribution of isomorphism types of finite index subgroups in a free product $\Gamma = C_{p_1}^{*e_1} * \cdots * C_{p_t}^{*e_t} * F_r$. For $i \in [t]$ and $n \in \mathbb{N}$ define random variables ξ_{in} by choosing a subgroup Δ of index n in Γ at random with respect to uniform weights, and putting $\xi_{in} = \lambda_i$, where $\tau(\Delta) = (\lambda_1, \dots, \lambda_t; \mu)$. Then we have the following.

Theorem 4. *Let Γ and ξ_{in} be as above, and suppose that $\chi(\Gamma) < 0$. Then, as $n \to \infty$, the variables $\xi_{1n}, \dots, \xi_{tn}$ are asymptotically independent. Moreover, for each $i \in [t]$, the distribution of ξ_{in} converges weakly to a normal distribution with mean $e_i n^{1/p_i}$ and standard deviation $\sqrt{e_i}n^{1/(2p_i)}$. More precisely, we have, for real x,*

$$P\Big(\xi_{in} \leq e_i n^{1/p_i} + x\sqrt{e_i}n^{1/(2p_i)}\Big) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-s^2/2}\, ds \,+\, \mathcal{O}(n^{-\delta(\Gamma)}), \tag{33}$$

where $\delta(\Gamma) := \frac{1}{5}\min\big(\frac{1}{p_1}, \dots, \frac{1}{p_t}\big)$.

Each statement on distributions depends on a weight function. While uniform weights are certainly the most straightforward choice, they are by no means the only interesting one; for instance, one could define the weight of a subgroup to be the reciprocal value of its class number. In the context of wreath product representations, it appears natural to assign to a subgroup Δ the weight $|\mathrm{Hom}(\Delta, H)|$ with some fixed finite group H. For a prime q, define random variables $\xi_{in}^{(q)}$ by choosing a transitive representation $\psi : \Gamma \to C_q \wr S_n$ (with respect to uniform weights), putting $\Delta = \mathrm{stab}_{\epsilon\psi}(1)$, and setting $\xi_{in}^{(q)} = \lambda_i$, where $\tau(\Delta) = (\lambda_1, \dots, \lambda_t; \mu)$. Then the analogue of Theorem 4 reads as follows.

Theorem 5. *Let Γ be as in* (1)*, and let q be a prime. Then, as $n \to \infty$, the variables $\xi_{1n}^{(q)}, \dots, \xi_{tn}^{(q)}$ are asymptotically independent. Moreover,*

(i) *if $q \neq p_i$, then the distribution of $\xi_{in}^{(q)}$ converges weakly to a normal distribution with mean $\frac{e_i}{q^{1-1/p_i}} n^{1/p_i}$ and standard deviation $\frac{\sqrt{e_i}}{q^{1/2-1/(2p_i)}} n^{1/(2p_i)}$,*

(ii) *the distribution of* $\xi_{in}^{(p_i)}$ *converges weakly to a normal distribution with mean* $e_i(p_i n)^{1/p_i}$ *and standard deviation* $\sqrt{e_i}(p_i n)^{1/(2p_i)}$.

In both cases, the error term is as in Theorem 4.

For the proof of Theorem 4 we need the following lemma.

Lemma 3. *For* $1 \leq i \leq t$ *and* $1 \leq j \leq e_i$, *define a random variable* $\hat{\xi}_{ij}$ *by choosing* $\varphi \in \mathrm{Hom}(\Gamma, S_n)$ *at random, and setting*

$$\hat{\xi}_{ij} := \text{number of } p_i\text{–cycles of } \varphi(x_{ij}).$$

Then these variables $\hat{\xi}_{ij}$ *are independent, and satisfy*

$$P\Big(\hat{\xi}_{ij} \leq m_0 + x\frac{n^{1/(2p_i)}}{p_i}\Big) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x} \mathrm{e}^{-s^2/2}\,ds \;+\; \mathcal{O}\big(n^{-1/(5p_i)}\big), \tag{34}$$

where $m_0 := \Big\lfloor \dfrac{n - n^{1/p_i}}{p_i} \Big\rfloor$.

Proof. Independence of the $\hat{\xi}_{ij}$ follows from the universal property of Γ. For fixed i and j, consider the number

$$X(m) = \frac{n!}{m!(n-p_i m)!p_i^m} = |\mathrm{Hom}(C_{p_i}, S_n)| \cdot P\big(\hat{\xi}_{ij} = m\big)$$

of permutations in S_n consisting of m cycles of length p_i and $n - p_i m$ fixed points. Put $h := m - m_0$ with m_0 as defined in the lemma. Then, for $h > 0$,

$$\begin{aligned}
\frac{X(m)}{X(m_0)} &= \frac{m_0!(n-p_i m_0)!p_i^{m_0}}{(m_0+h)!(n-p_i m_0 - p_i h)!p_i^{m_0+h}} \\
&= \prod_{\nu=1}^{h} \frac{(n-p_i m_0 - p_i\nu + p_i)(n - p_i m_0 - p_i \nu + p_i - 1)\cdots(n-p_i m_0 - p_i\nu + 1)}{p_i(m_0+\nu)} \\
&= \prod_{\nu=1}^{h} \frac{\big(n^{1/p_i} - p_i\nu + \mathcal{O}(1)\big)^{p_i}}{n - n^{1/p_i} + p_i\nu + \mathcal{O}(1)} \\
&= \prod_{\nu=1}^{h} \frac{n - p_i^2 \nu n^{1-1/p_i} + \mathcal{O}(n^{1-1/p_i} + \nu^2 n^{1-2/p_i} + \nu^{p_i})}{n + \mathcal{O}(n^{1/p_i} + \nu)} \\
&= \prod_{\nu=1}^{h} \bigg[1 - \frac{p_i^2\nu}{n^{1/p_i}} + \mathcal{O}\Big(\frac{1}{n^{1/p_i}} + \frac{\nu^2}{n^{2/p_i}} + \frac{\nu^{p_i}}{n}\Big)\bigg] \\
&= \exp\bigg(-\sum_{\nu=1}^{h}\bigg(\frac{p_i^2 h^2}{n^{1/p_i}} + \mathcal{O}\Big(\frac{1}{n^{1/p_i}} + \frac{\nu^2}{n^{2/p_i}} + \frac{\nu^{p_i}}{n}\Big)\bigg)\bigg) \\
&= \exp\bigg(-\frac{p_i^2 h^2}{2n^{1/p_i}} + \mathcal{O}\Big(\frac{h}{n^{1/p_i}} + \frac{h^3}{n^{2/p_i}} + \frac{h^{p_i+1}}{n}\Big)\bigg),
\end{aligned}$$

which is non–trivial for $h = o(n^{2/(3p_i)})$. A similar computation for $h < 0$ gives

$$\frac{X(m)}{X(m_0)} = \exp\Big(- \frac{p_i^2 h^2}{2n^{1/p_i}} + \mathcal{O}\Big(\frac{|h|}{n^{1/p_i}} + \frac{|h|^3}{n^{2/p_i}} + \frac{|h|^{p_i+1}}{n}\Big)\Big),$$

i.e., we obtain the same main term and the same restriction on h. Since $X(m+1)/X(m)$ is decreasing, $X(m)$ is unimodal; hence, the contributions coming from the tails of the distribution are negligible. Let $x \in [-n^{1/(10p_i)}, n^{1/(10p_i)}]$. By what we have shown so far,

$$\begin{aligned}\frac{P\big(\hat{\xi}_{ij} \leq m_0 + x\frac{n^{1/(2p_i)}}{p_i}\big)}{P\big(\hat{\xi}_{ij} = m_0\big)} &= \sum_{-n^{3/(5p_i)} \leq h \leq x\frac{n^{1/(2p_i)}}{p_i}} \exp\Big(- \frac{p_i^2 h^2}{2n^{1/p_i}} + \mathcal{O}\big(n^{-1/(5p_i)}\big)\Big)\\ &\qquad + \mathcal{O}\Big(n \exp\Big(- \frac{p_i^2 n^{1/(5p_i)}}{2}\Big)\Big)\\ &= \Big(1 + \mathcal{O}\big(n^{-1/(5p_i)}\big)\Big) \int_{-n^{3/(5p_i)}}^{x\frac{n^{1/(2p_i)}}{p_i}} \exp\Big(- \frac{p_i^2 h^2}{2n^{1/p_i}}\Big)\, dh\\ &\qquad + \mathcal{O}\big(n^{-1/p_i}\big)\\ &= \Big(1 + \mathcal{O}\big(n^{-1/(5p_i)}\big)\Big)\frac{n^{1/(2p_i)}}{p_i} \int_{-\infty}^{x} \mathrm{e}^{-s^2/2}\, ds\\ &\qquad + \mathcal{O}\big(n^{-1/p_i}\big).\end{aligned}$$

Evaluating this equation at $x = n^{1/(10p_i)}$, and using the fact that

$$P\big(\hat{\xi}_{ij} \leq m_0 + \frac{n^{3/(5p_i)}}{p_i}\big) = 1 \, + \, \mathcal{O}\Big(n \exp\Big(- \frac{n^{1/(5p_i)}}{2}\Big)\Big),$$

gives

$$P\big(\hat{\xi}_{ij} = m_0\big) = \frac{\sqrt{2\pi}\, p_i}{n^{1/(2p_i)}}\Big(1 + \mathcal{O}\big(n^{-1/(5p_i)}\big)\Big).$$

Using this equation in the previous computation now yields (34). □

Proof of Theorem 4. By Lemma 3,

$$P\Big(\forall i \forall j : \hat{\xi}_{ij} \leq m_0 + x_{ij}\frac{n^{1/(2p_i)}}{p_i}\Big) =$$

$$(2\pi)^{-\sum_i e_i/2} \int_{-\infty}^{x_{11}} \mathrm{e}^{-s^2/2}\, ds \cdots \int_{-\infty}^{x_{te_t}} \mathrm{e}^{-s^2/2}\, ds \, + \, \mathcal{O}\big(n^{-\delta(\Gamma)}\big). \quad (35)$$

For $i \in [t]$ and $j \in [e_i]$, define a random variable ζ_{ij} by choosing a transitive permutation representation φ of Γ of degree n, and setting

$$\zeta_{ij} = \text{number of } p_i\text{–cycles of } \varphi(x_{ij}).$$

Since $\chi(\Gamma) < 0$, [22, Prop. 2] ensures that

$$t_n(\Gamma) = h_n(\Gamma)\big(1 + \mathcal{O}(n^{\chi(\Gamma)})\big) \quad (n \to \infty),$$

hence, using the fact that $\delta(\Gamma) < -\chi(\Gamma)$, we see that (35) remains valid, if we replace each of the $\hat{\xi}_{ij}$ with the corresponding random variable ζ_{ij}. The latter observation implies: (i) that the variables ζ_{ij} are asymptotically independent, and (ii) that the estimate

$$P\Big(\zeta_{ij} \leq m_0 + x\frac{n^{1/(2p_i)}}{p_i}\Big) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} \mathrm{e}^{-s^2/2}\, ds \,+\, \mathcal{O}\big(n^{-\delta(\Gamma)}\big) \tag{36}$$

holds for each choice of i and j. Transforming the variables ζ_{ij} into the random variables ξ_{in} by means of the equations

$$\xi_{in} = e_i n \,-\, p_i \sum_{j=1}^{e_i} \zeta_{ij}, \tag{37}$$

which follow from Theorem 1, we find that the ξ_{in} are indeed asymptotically independent. We now use the well–known fact that the convolution product of finitely many normal distributions is again a normal distribution with mean and variance behaving additively. Theorem 4 follows from the latter assertion, together with Equations (36) and (37). □

Proof of Theorem 5. For $i \in [t]$, $j \in [e_i]$, and a prime q, define a random variable $\hat{\xi}_{ij}^{(q)}$ by choosing $\varphi \in \mathrm{Hom}(\Gamma, C_q \wr S_n)$ at random, and setting

$$\hat{\xi}_{ij}^{(q)} = \text{number of } p_i\text{–cycles of } (\epsilon\varphi)(x_{ij}).$$

By an argument already encountered in the proof of Theorem 1, we have

$$|\mathrm{Hom}(C_{p_i}, C_q \wr S_n)| \cdot P\big(\hat{\xi}_{ij}^{(q)} = m\big) = \begin{cases} \dfrac{n!\, q^{m(p_i-1)}}{m!\,(n-p_i m)!\, p_i^m}, & q \neq p_i \\[2ex] \dfrac{n!\, p_i^n}{m!\,(n-p_i m)!\, p_i^{2m}}, & q = p_i. \end{cases}$$

The proof of Theorem 5 proceeds now in a fashion analogous to that of Theorem 4, replacing Lemma 3 by the following.

Lemma 4. *For fixed q, the variables $\hat{\xi}_{ij}^{(q)}$ are independent, and satisfy*

(i) $P\Big(\hat{\xi}_{ij}^{(q)} \leq \dfrac{n}{p_i} - \dfrac{n^{1/p_i}}{p_i\, q^{1-1/p_i}} + x\dfrac{n^{1/(2p_i)}}{p_i\, q^{1/2-1/p_i}}\Big) = \dfrac{1}{\sqrt{2\pi}} \displaystyle\int_{-\infty}^{x} \mathrm{e}^{-s^2/2}\, ds \,+\, \mathcal{O}\big(n^{-1/(5p_i)}\big)$ *if $q \neq p_i$,*

(ii) $P\Big(\hat{\xi}_{ij}^{(p_i)} \leq \dfrac{n}{p_i} - \dfrac{n^{1/p_i}}{p_i^{1-1/p_i}} + x\dfrac{n^{1/(2p_i)}}{p_i^{1-1/(2p_i)}}\Big) = \dfrac{1}{\sqrt{2\pi}} \displaystyle\int_{-\infty}^{x} \mathrm{e}^{-s^2/2}\, ds \,+\, \mathcal{O}\big(n^{-1/(5p_i)}\big).$

□

8. The modular group

The purpose of this final section is to summarize the impact of the theory developed so far towards the solution of the Poincaré–Klein problem (problems I–III) for the modular group $\Gamma = \mathrm{PSL}_2(\mathbb{Z})$. While some of the results in this section follow immediately from corresponding results of previous sections, the simple structure of $\mathrm{PSL}_2(\mathbb{Z})$ in some cases also allows us to obtain improved versions. Furthermore, we demonstrate that some of the seemingly technical hypotheses in Sections 4 and 5 are indeed necessary, and we establish an asymptotic expansion for $s_\tau(\mathrm{PSL}_2(\mathbb{Z}))$ considerably refining Theorem 3 for the modular group under similar hypotheses. For the remainder of this section, Γ will denote the modular group. The isomorphism type of a subgroup $\Delta \leq \Gamma$, $\Delta \cong C_2^{*\alpha} * C_3^{*\beta} * F_\gamma$, will be denoted by $\tau(\Delta) = (\alpha, \beta; \gamma)$. Moreover, we shall suppress the second index in the representation type of Δ; that is, m_1 denotes the number of 2–cycles, m_2 the number of 3–cycles.

8.1. **The realization problem.** Our first result is a restatement of Theorem 1.

Corollary 6. *Let Δ be a subgroup of finite index in Γ. Then the representation type and the isomorphism type of Δ determine each other via the equations*

$$\begin{aligned} \alpha &= n - 2m_1 & m_1 &= \alpha + 2\beta + 3(\gamma - 1)\\ \beta &= n - 3m_2 & m_2 &= \alpha + \beta + 2(\gamma - 1)\\ \gamma &= m_1 + 2m_2 - n + 1 & n &= 3\alpha + 4\beta + 6(\gamma - 1). \end{aligned}$$

□

Corollary 7. *A tuple $(\alpha, \beta; \gamma) \in \mathbb{N}_0^3$ is realized in Γ if and only if $3\alpha + 4\beta + 6\gamma \geq 7$; that is, Γ has a finite index subgroup isomorphic to $\Delta = C_2^{*\alpha} * C_3^{*\beta} * F_\gamma$ if and only if $\chi(\Delta) < 0$.*

Proof. Necessity is clear. We have to check conditions (i) and (ii) of Theorem 2. The equation defining n can be rewritten as $n = 3\alpha + 4\beta + 6(\gamma - 1)$, which is always integral, and positive by assumption. Assume that (ii) fails, say $\alpha > n$. Then $n \geq 3(n + 1) - 6$, that is, $n \leq 1$, and $(\alpha, \beta; \gamma)$ would be a non-negative solution of $3\alpha + 4\beta + 6\gamma = 7$ with $\alpha \geq 2$, which does not exist. A similar argument shows that $\beta > n$ is impossible. □

Corollary 8. (i) *Let $\tau = (\alpha, \beta; \gamma)$ be an isomorphism type such that $n = 3\alpha + 4\beta + 6(\gamma - 1)$ is neither 1 nor prime, and with $\gamma > 2\min_{p|n} p$. Then there exists a non–maximal subgroup of finite index in Γ realizing τ.*

(ii) *Let $q \equiv 1$ (12) be a prime number, $1 \leq a \leq q - 1$ an integer, and define $\tau := \big(q + 2a, \frac{q^2 - 9q + 12}{4}, q - a - 1\big)$. Then there exists a subgroup of index q^2 realizing τ, and every such subgroup is maximal.*

Proof. (i) restates Proposition 4.

(ii) We have

$$3(q + 2a) \;+\; 4 \cdot \frac{q^2 - 9q + 12}{4} \;+\; 6(q - a - 2) = q^2.$$

Hence, any finite index subgroup realizing τ has index q^2, and such subgroups exist by Corollary 7. Let Δ be a subgroup realizing τ, and suppose that there exists Δ' such that $\Delta < \Delta' < \Gamma$. Then Δ' is of index q and of type $(\alpha', \beta'; \gamma')$, say. From Theorem 2, when applied to the groups Δ and Δ' (that is, $e_1 = \alpha'$, $e_2 = \beta'$, $n = q$, and $(\lambda_1, \lambda_2; \mu) = \tau$), we deduce that $\alpha' > 1$, and that $\beta' > \frac{q-9}{4}$. Theorem 1, when applied to Γ and Δ', shows that $\alpha' \equiv q \equiv 1$ (2) and $\beta' \equiv q \equiv 1$ (3). This gives $\alpha' \geq 3$, $\beta' \geq \frac{q+3}{4}$, and we obtain the contradiction

$$q = 3\alpha' + 4\beta' + 6(\gamma' - 1) \geq 9 + (q+3) - 6 = q + 6.$$

□

Comparing the two parts of Corollary 8, we see that the lower bound on γ is sharp up to a constant factor; in particular, Proposition 4 is close to being best possible.

8.2. **Asymptotics of $s_\tau(\Gamma)$.** An immediate consequence of Theorem 3 is the following.

Corollary 9. *Let $\tau_i = (\alpha_i, \beta_i; \gamma_i)$ be a sequence of types in $\mathbb{N}_0^3$ such that $n_i := 3\alpha_i + 4\beta_i + 6(\gamma_i - 1)$ tends to infinity with i. Assume that for all i we have $\alpha_i < n_i^{\frac{2}{3}-\varepsilon}$, $\beta_i < n_i^{\frac{1}{2}-\varepsilon}$, and $\alpha_i\beta_i < n_i^{1-\varepsilon}$ with some fixed $\varepsilon > 0$. Then*

$$s_{\tau_i}(\Gamma) \sim \frac{n_i \cdot n_i!}{\alpha_i!\, \beta_i!\, (\frac{n_i - \alpha_i}{2})!\, (\frac{n_i - \beta_i}{3})!\, 2^{\frac{n_i - \alpha_i}{2}}\, 3^{\frac{n_i - \beta_i}{3}}} \quad (i \to \infty).$$

Exploiting the simple structure of the modular group, we shall obtain a more precise estimate. In order to state this result, we need a few preliminaries. Given two functions $F, G : \mathbb{N}_0^2 \times \mathbb{N} \to \mathbb{R}$, we say that F *dominates* G ($F \succ G$), if there exists a formal power series $Q(x,y,z) = \sum_{i,j,k \geq 0} q_{ijk}\, x^i y^j z^{-k/6} \in \mathbb{R}[[x, y, z^{-1/6}]]$ such that

(a) $q_{ijk} = 0$, unless $4i \leq k$ and $3(i+j) \leq k$,

(b) for each $\varepsilon > 0$ and every integer $N \geq 1$, we have

$$G(x,y,z) = F(x,y,z)$$
$$\times \left\{ \sum_{0 \leq i,j,k < N} q_{ijk}\, x^i y^j z^{-k/6} + \mathcal{O}\Big(\big(\frac{x}{z^{2/3}}\big)^N + \big(\frac{y}{z^{1/2}}\big)^N + \big(\frac{xy}{z}\big)^N + z^{-N/6} \Big) \right\},$$

where the estimate for the error term holds uniformly in the domain

$$\Omega_\varepsilon = \Big\{ (x,y,z) \in \mathbb{N}_0^2 \times \mathbb{N} : \ 0 \leq x < z^{2/3-\varepsilon},\ 0 \leq y < z^{1/2-\varepsilon}, \text{ and } xy < z^{1-\varepsilon} \Big\}.$$

Moreover, F and G are called *equivalent* ($F \approx G$), if $F \succ G$ and $G \succ F$.

Lemma 5. *Let $F, F_1, F_2, G, G_1, G_2 \in \mathbb{R}^{\mathbb{N}_0^2 \times \mathbb{N}}$.*

(i) *If $F \succ G$ with $q_{000} \neq 0$, and if F and G have the same zero set, then $F \approx G$. Conversely, for F and G not of compact support, $F \approx G$ implies $q_{000} \neq 0$.*

(ii) *If $F_1 \succ G_1$ and $F_2 \succ G_2$, then $F_1 F_2 \succ G_1 G_2$.*

(iii) *If $F \succ G_1$ and $F \succ G_2$, then $F \succ G_1 + G_2$.*

(iv) *The relation $\succ$ is transitive, and $\approx$ is an equivalence relation on $\mathbb{R}^{\mathbb{N}_0^2 \times \mathbb{N}}$.*

The proof of Lemma 5 will be given in the next subsection. For $(\alpha, \beta; n) \in \mathbb{N}_0^2 \times \mathbb{N}$ define $s(\alpha, \beta; n)$ to be the number of subgroups of index n and type $(\alpha, \beta; \frac{n-3\alpha-4\beta+6}{6})$. Similarly, define

$$h(\alpha,\beta;n) := \begin{cases} \dfrac{n\cdot n!}{\alpha!\,\beta!\,(\dfrac{n-\alpha}{2})!\,(\dfrac{n-\beta}{3})!\,2^{\frac{n-\alpha}{2}}\,3^{\frac{n-\beta}{3}}}; & n\equiv\alpha\,(2), n\equiv\beta\,(3)\\ 0; & \text{otherwise.}\end{cases}$$

With this notation, we can now state the following refinement of Corollary 9.

Proposition 10. *We have $s(\alpha, \beta; n) \approx h(\alpha, \beta; n)$ with $Q(x, y, z) \in \mathbb{Q}[[x, y, z^{-1/6}]]$ and $q_{000} = 1$.*

Proof. We may assume that $n \equiv \alpha\,(2)$, and that $n \equiv \beta\,(3)$, since otherwise $s(\alpha, \beta; n) = h(\alpha, \beta; n) = 0$. Let $\Omega = \Omega(m_1, m_2, n)$ be the measure space consisting of all pairs $(\sigma, \pi) \in S_n \times S_n$ such that the corresponding permutation representation has type $(m_1, m_2; n)$, equipped with the uniform measure. For $\ell \in \mathbb{N}_0$ and $k_1, \dots, k_\ell \in \mathbb{N}$, define

$$P_{k_1,\dots,k_\ell}(\nu) := P\begin{pmatrix} |1^{\langle\sigma,\pi\rangle}| = \nu,\ \exists\, A_1,\dots,A_\ell \subseteq [n] : A_i \cap A_j = \emptyset\ (i \neq j),\\ \forall i\,\big(|A_i| = k_i,\ A_i^\sigma = A_i^\pi = A_i,\ 1 \notin A_i\big)\end{pmatrix}.$$

Then, by the proof of Proposition 7, we have

$$s_\tau(\Gamma) = \frac{h_n(m_1,m_2)}{(n-1)!}\left\{1 - \sum_{\nu=1}^{n-1} P(\nu)\right\},$$

where $\tau = (\alpha, \beta; \gamma)$ is the isomorphism type of the modular group Γ corresponding to $(m_1, m_2; n)$. Our task is thus to estimate $P(\nu)$. Fix an integer $N \geq 1$ and a real number $\varepsilon > 0$, and suppose that $(\alpha, \beta, n) \in \Omega_\varepsilon$. We show first that $P(\nu)$ is negligible if $\nu \in [N + 1, n - N - 1]$. By the observation following the proof of Theorem 3, there exists a constant $\tilde{C} = \tilde{C}(\delta)$ for each $\delta > 0$ such that

$$P(\nu) \leq \tilde{C}\binom{n}{\nu}^{\ell_1+\ell_2+\delta-1}, \quad 1 \leq \nu \leq n,$$

where $\ell_1 := \max\left(\frac{1}{2}, \frac{\log\alpha}{\log n}\right)$ and $\ell_2 := \max\left(\frac{1}{3}, \frac{\log\beta}{\log n}\right)$. It follows that

$$\begin{aligned}\sum_{\nu=N+1}^{n-N-1} P(\nu) &= \mathcal{O}\Big(n^{(\ell_1+\ell_2+\delta-1)(N+1)}\Big)\\ &= \mathcal{O}\Big(\big((n^{1/2}+\alpha)(n^{1/3}+\beta)n^{\delta-1}\big)^{N+1}\Big)\\ &= \mathcal{O}\Big(\big(\frac{\alpha}{n^{2/3}}\big)^N + \big(\frac{\beta}{n^{1/2}}\big)^N + \big(\frac{\alpha\beta}{n}\big)^N + n^{-N/6}\Big),\end{aligned}$$

provided that

$$\ell_1 + \ell_2 + \delta < 1 \ \text{ and } \ n^{\delta(N+1)}\Big(\frac{\alpha}{n^{2/3}} + \frac{\beta}{n^{1/2}} + \frac{\alpha\beta}{n} + n^{-1/6}\Big) < 1.$$

Both these conditions are satisfied for $\delta = \frac{\varepsilon}{N+1}$. Next, we show that, for each $\nu \in [1, N] \cup [n-N, n-1]$, the probability $P(\nu)$ is dominated by the function $\mathbf{1}$ with $q_{000} = 0$

and $q_{ijk} \in \mathbb{Q}$. Having completed this step, our claim will follow from Lemma 5 (iii). By the inclusion-exclusion-principle, we have, for $\nu \geq n - N$,

$$P(\nu) = \sum_{0 \leq \rho \leq n} (-1)^\rho \sum_{\kappa_1, \dots, \kappa_\rho \geq 1} \sum_{n-N \leq \eta \leq n} P_{n-\nu, \kappa_1, \dots, \kappa_\rho}(\eta). \tag{38}$$

If $(n-\nu) + \kappa_1 + \cdots + \kappa_\rho > N$ and $\eta \in [n-N, n)$, then $P_{n-\nu, \kappa_1, \dots, \kappa_\rho}(\eta) = 0$. Hence, the number of non–vanishing summands occurring in (38) is bounded in terms of N alone; more precisely, we have $\rho < N$ and $\kappa_i \leq N$ for all i. In order to get rid of the transitivity condition, rewrite (38) as

$$P(\nu) = \sum_{0 \leq \rho \leq N} (-1)^\rho \sum_{1 \leq \kappa_1, \dots, \kappa_\rho \leq N} \Bigg[\sum_{\eta=1}^{n} P_{n-\nu, \kappa_1, \dots, \kappa_\rho}(\eta) - \sum_{\eta=1}^{N} P_{n-\nu, \kappa_1, \dots, \kappa_\rho}(\eta) \\ + \mathcal{O}\Big(\big(\frac{\alpha}{n^{2/3}}\big)^N + \big(\frac{\beta}{n^{1/2}}\big)^N + \big(\frac{\alpha\beta}{n}\big)^N + n^{-N/6} \Big) \Bigg].$$

By Lemma 5, it suffices to prove that

$$\mathbf{1} \succ \sum_{\eta=1}^{n} P_{d_1, \dots, d_r}(\eta), \tag{39}$$

and that

$$\mathbf{1} \succ P_{d_1, \dots, d_r}(\eta) \tag{40}$$

in the range $r \geq 1$, $\eta \leq N$, $d_i \geq 1 (1 \leq i \leq r)$, $\sum_{i=1}^{r} d_i \leq N$, and with $q_{000} = 0$ and $q_{ijk} \in \mathbb{Q}$ in each case. In order to prove (39), we first choose the sets $A_1, \dots, A_r \subseteq [n]$, then prescribe the action of σ and π on each of these sets, and finally weight the resulting expression by the probability that a random element $(\sigma, \pi) \in \Omega$ acts as prescribed. Proceeding in this way, we find that

$$\sum_{\eta=1}^{n} P_{d_1, \dots, d_r}(\eta) = \\ \binom{n-1}{d_1, \dots, d_r, n - \sum_i d_i - 1} \sum_{\substack{a_1, \dots, a_r \geq 0 \\ b_1, \dots, b_r \geq 0 \\ a_i \leq d_i/2 \\ b_i \leq d_i/3}} \left(\prod_i \frac{(d_i!)^2}{a_i! b_i! (d_i - 2a_i)! (d_i - 3b_i)! 2^{a_i} 3^{b_i}} \right) \\ \times P\begin{pmatrix} \sigma \text{ fixes } \sum_i (d_i - 2a_i) \text{ prescribed points and contains } \sum_i a_i \text{ prescribed 2–cycles,} \\ \pi \text{ fixes } \sum_i (d_i - 3b_i) \text{ prescribed points and contains } \sum_i b_i \text{ prescribed 3–cycles} \end{pmatrix}. \tag{41}$$

Since the events for σ and π are now independent, we can consider them separately. Putting $d := \sum_i d_i$, $a := \sum_i a_i$, and $b := \sum_i b_i$, we have

$$P\begin{pmatrix}\sigma \text{ fixes } 1,\dots,d-2a \text{ and contains the}\\ 2\text{–cycles } (d-2a+1, d-2a+2),\dots,(d-1,d)\end{pmatrix}$$

$$= \frac{\dfrac{(n-d)!}{(m_1-a)!\,(n-2m_1-(d-2a))!\,2^{m_1-a}}}{\dfrac{n!}{m_1!\,(n-2m_1)!\,2^{m_1}}} = \frac{(m_1)_a\,(n-2m_1)_{d-2a}\,2^a}{(n)_d}$$

$$= \frac{(\alpha)_{d-2a}\,(\frac{n-\alpha}{2})_a\,2^a}{(n)_d} \prec \frac{\alpha^{d-2a}}{n^{d-a}}.$$

Similarly,

$$P\begin{pmatrix}\pi \text{ fixes } 1,\dots,d-3b \text{ and contains the 3–cycles}\\ (d-3b+1, d-3b+2, d-3b+3),\dots,(d-2,d-1,d)\end{pmatrix} = \frac{(\beta)_{d-3b}\,\big(\frac{n-\beta}{3}\big)_b 3^b}{(n)_d}$$

$$\prec \frac{\beta^{d-3b}}{n^{d-b}}.$$

Combining these estimates with (41), and using Lemma 5 we find that

$$\sum_{\eta=1}^{n} P_{d_1,\dots,d_r}(\eta) \prec \sum_{0\le a\le d/2}\ \sum_{0\le b\le d/3} \alpha^{d-2a}\beta^{d-3b}n^{-(d-a-b)}.$$

In order to see that the latter sum is dominated by $\mathbf{1}$, it suffices to check the inequalities $4(d-2a) \le 6(d-a-b)$ and $3(2d-2a-3b) \le 6(d-a-b)$ coming from condition (a); these however are immediate consequences of the summation conditions. Also, we have $6(d-a-b) \ge d$, thus every monomial occurring in the power series associated with the latter dominance contains a positive power of $n^{-1/6}$, whence $q_{000} = 0$. Moreover, at each step where dominance was used to simplify expressions, the power series introduced had rational coefficients, and this property is inherited under forming products and rational linear combinations. In order to deal with $P_{d_1,\dots,d_r}(\eta)$ for $\eta \le N$, we choose a domain of transitivity of 1 in $\binom{n-1}{\eta-1}$ possible ways, and then choose a transitive action on this set, which can be done in a number of ways bounded in terms of N alone. In this way, $P_{d_1,\dots,d_r}(\eta)$ is transformed into a sum analogous to (41), which can be dealt with in a fashion similar to the argument above, proving (40). □

A similar but considerably simpler argument allows us to prove the following.

Proposition 11. *Let $\varepsilon > 0$ be given.*

(i) *In S_n choose an involution σ with α fixed points, and an element π of order 3 having β fixed points at random. If $\alpha\beta > n^{1+\varepsilon}$, then, with probability tending to 1 as $n \to \infty$, $\langle\sigma,\pi\rangle$ fixes a point of $[n]$. Moreover, if $\alpha > n^{\frac{2}{3}+\varepsilon}$ and $\beta < \frac{n}{2}$, then almost certainly $\langle\sigma,\pi\rangle$ has a domain of transitivity consisting of exactly 3 points. Finally, if $\beta > n^{\frac{1}{2}+\varepsilon}$ and $\alpha < \frac{n}{2}$, then $\langle\sigma,\pi\rangle$ almost certainly has a domain of transitivity consisting of precisely 2 points.*

(ii) *Let $\tau_i = (\alpha_i, \beta_i; \gamma_i)$ be a sequence of isomorphism types in the modular group Γ such that $n_i := 3\alpha_i + 4\beta_i + 6(\gamma_i - 1)$ tends to infinity with i. Then, if for every i at least one of the inequalities $\alpha_i > n_i^{\frac{2}{3}+\varepsilon}$, $\beta_i > n_i^{\frac{1}{2}+\varepsilon}$, or $\alpha_i\beta_i > n_i^{1+\varepsilon}$ holds, we have*

$$s_{\tau_i}(\Gamma) = o\biggl(\frac{n_i \cdot n_i!}{\alpha_i!\,\beta_i!\,(\frac{n_i-\alpha_i}{2})!\,(\frac{n_i-\beta_i}{3})!\,2^{\frac{n_i-\alpha_i}{2}}\,3^{\frac{n_i-\beta_i}{3}}}\biggr) \quad (i \to \infty).$$

Proposition 11 shows in particular that the hypotheses of Theorem 3 are sharp, and that the definition of the domain Ω_ε is natural.

8.3. **Proof of Lemma 5.** For a power series $Q(x, y, z) \in \mathbb{R}[[x, y, z^{-1/6}]]$ and an integer $N \geq 1$ write

$$Q^{(N)}(x, y, z) := \sum_{0 \leq i,j,k < N} q_{ijk}\, x^i y^j z^{-k/6},$$

and put

$$R_N := \bigl(\frac{x}{z^{2/3}}\bigr)^N + \bigl(\frac{y}{z^{1/2}}\bigr)^N + \bigl(\frac{xy}{z}\bigr)^N + z^{-N/6}.$$

(i) Let $\hat{Q}(x, y, z) = \sum_{i,j,k \geq 0} \hat{q}_{ijk}\, x^i y^j z^{-k/6}$ be the formal inverse of the series Q occurring in the definition of the relation $F \succ G$. Rewriting $\hat{Q}$ as a von Neumann series, we find that for $\varepsilon > 0$, $N \geq 1$, and $(x, y, z) \in \Omega_\varepsilon$

$$\hat{Q}^{(N)}(x, y, z) = q_{000}^{-1} \sum_{0 \leq \nu \leq 3N-3} (-1)^\nu \Bigl(Q^{(N)}(x, y, z) - 1\Bigr)^\nu + \mathcal{O}(R_N). \tag{42}$$

Indeed, if $4i \leq k$, $3(i + j) \leq k$, and $\max(i, j, k) \geq N$, then $(x, y, z) \in \Omega_\varepsilon$ satisfies $x^i y^j z^{-k/6} = \mathcal{O}(R_N)$, and the two sides of (42) differ by a linear combination of finitely many such monomials. If $\hat{q}_{ijk} \neq 0$, then, by (42), there exist ν and vectors $(i_1, j_1, k_1), \ldots, (i_\nu, j_\nu, k_\nu) \in \mathbb{N}_0^3$ summing to (i, j, k), such that $q_{i_\mu j_\mu k_\mu} \neq 0$ for $\mu = 1, \ldots, \nu$. Hence, the series $\hat{Q}$ inherits property (a) in the definition of dominance from Q. Moreover, multiplying the equation

$$\begin{aligned} F(x, y, z) - G(x, y, z)\,\hat{Q}^{(N)}(x, y, z) &= F(x, y, z) - G(x, y, z) \\ &\quad \times \biggl[q_{000}^{-1} \sum_{0 \leq \nu \leq 3N-3} (-1)^\nu \Bigl(Q^{(N)}(x, y, z) - 1\Bigr)^\nu + \mathcal{O}(R_N)\biggr] \end{aligned}$$

by

$$Q^{(N)}(x, y, z) = q_{000} + \mathcal{O}(R_1),$$

which is at least $q_{000}/2$ for z sufficiently large, we obtain

$$\begin{aligned} \Bigl(F(x, y, z) - G(x, y, z)\,\hat{Q}^{(N)}(x, y, z)\Bigr)\Bigl(q_{000} + \mathcal{O}(R_1)\Bigr) &= -G(x, y, z) \\ \times \biggl[1 + \sum_{0 \leq i,j,k \leq 3N^2} \tilde{q}_{ijk}\, x^i y^j z^{-k/6}\biggr] &+ \mathcal{O}(R_N)\bigl(F(x, y, z) + G(x, y, z)\bigr), \end{aligned}$$

where $\tilde{q}_{ijk} = 0$ unless $\max(i,j,k) \geq N$, $4i \leq k$, and $3(i+j) \leq k$. As above, we see that

$$\sum_{0 \leq i,j,k \leq 3N^2} \tilde{q}_{ijk}\, x^i y^j z^{-k/6} = \mathcal{O}(R_N).$$

Since $q_{000} \neq 0$, there exists a compact set $C \subseteq \mathbb{R}^3$ such that $F(x,y,z) = \mathcal{O}\big(G(x,y,z)\big)$ for $(x,y,z) \in \Omega_\varepsilon - C$, that is, property (b) in the definition of $G \succ F$ holds for all but finitely many points. By increasing the implied constant, we can take care of those exceptional points (x,y,z) such that $G(x,y,z) \neq 0$. Finally, if $G(x,y,z) = 0$, then the claimed estimate holds trivially, since in this case by assumption also $F(x,y,z) = 0$.

(ii) For $\ell = 1,2$, let $Q_\ell(x,y,z) = \sum_{i,j,k\geq 0} q_{ijk}^{(\ell)} x^i y^j z^{-k/6}$ be the formal power series associated with the dominance relation $F_\ell \succ G_\ell$. Given $\varepsilon > 0$ and a positive integer N, we have for $(x,y,z) \in \Omega_\varepsilon$ that $Q_\ell^{(N)} = \mathcal{O}(1)$, $R_N = \mathcal{O}(1)$, and that $Q_1^{(N)} Q_2^{(N)} = (Q_1Q_2)^{(N)} + \mathcal{O}(R_N)$, where Q_1Q_2 is the Cauchy product. Hence, under these assumptions,

$$G_1G_2 = F_1F_2\Big[Q_1^{(N)} + \mathcal{O}(R_N)\Big]\Big[Q_2^{(N)} + \mathcal{O}(R_N)\Big] = F_1F_2\Big[(Q_1Q_2)^{(N)} + \mathcal{O}(R_N)\Big],$$

that is, condition (b) holds. Since, by an argument already given in the proof of (i), condition (a) is inherited, our claim follows.

(iii) This is shown by a similar argument, using the fact that $Q_1^{(N)} + Q_2^{(N)} = (Q_1+Q_2)^{(N)}$.

(iv) Reflexivity and symmetry of $\approx$ are clear, transitivity of $\succ$ follows by an argument analogous to the one given in (ii), while transitivity of $\approx$ is implied by that of $\succ$.

8.4. **Further asymptotic results.** The results of Sections 6, when specialized to the modular group, immediately give the following.

Corollary 10. *As n tends to infinity, we have $r_n^f(\Gamma) \sim e^{-2} r_n(\Gamma)$.*

Corollary 11. *Almost all subgroups of Γ are maximal.*

8.5. **The distribution of isomorphism types.** Define random variables ξ_{1n}, ξ_{2n}, $\xi_{1n}^{(q)}$, $\xi_{2n}^{(q)}$ as in section 7.

Corollary 12. *As $n \to \infty$, the variables ξ_{1n} and ξ_{2n} are asymptotically independent. Similarly, for each fixed prime q, the variables $\xi_{1n}^{(q)}$ and $\xi_{2n}^{(q)}$ are asymptotically independent. Furthermore, the distributions of these variables converge weakly to normal distributions with parameters as given by the following table:*

	ξ_{1n}	ξ_{2n}	$\xi_{1n}^{(q)}, q \neq 2$	$\xi_{1n}^{(2)}$	$\xi_{2n}^{(q)}, q \neq 3$	$\xi_{2n}^{(3)}$
Mean	$n^{1/2}$	$n^{1/3}$	$q^{-1/2}n^{1/2}$	$2^{1/2}n^{1/2}$	$q^{-2/3}n^{1/3}$	$3^{1/3}n^{1/3}$
Variance	$n^{1/2}$	$n^{1/3}$	$q^{-1/2}n^{1/2}$	$2^{1/2}n^{1/2}$	$q^{-2/3}n^{1/3}$	$3^{1/3}n^{1/3}$

In each case, the error introduced by approximating the distribution function of one of these variables by the corresponding normal distribution is bounded above by $\mathcal{O}(n^{-1/15})$.

References

[1] A. O. L. Atkin and H. P. F. Swinnerton–Dyer, Modular forms on non–congruence subgroups, *Amer. Math. Soc. Symposium on Combinatorics*, Los Angeles, 1971.

[2] W. Dicks and M. Dunwoody, *Groups acting on graphs*, Cambridge University Press, 1989.

[3] A. Dress and T. Müller, Decomposable functors and the exponential principle, *Adv. in Math.* **129** (1997), 188 – 221.

[4] M. du Sautoy, Finitely generated groups, p-adic analytic groups and Poincaré series, *Ann. of Math.* **137** (1993), 639 – 670.

[5] M. du Sautoy and F. Grunewald, Analytic properties of zeta functions and subgroup growth, *Annals of Math.*, **152** (2000), 793–833.

[6] B. Fine, *Algebraic theory of the Bianchi groups*, Marcel Dekker, New York, 1989.

[7] R. C. Gunning, *Lectures on modular forms*, Ann. of Math. Studies 48, Princeton University Press, Princeton, New Jersey, 1962.

[8] F. Klein and R. Fricke, *Vorlesungen über die Theorie der elliptischen Modulfunctionen*, Teubner, Leipzig, 1890 (Vol. 1) and 1892 (Vol. 2).

[9] F. Klein and R. Fricke, *Vorlesungen über die Theorie der automorphen Funktionen*, Teubner, Leipzig, 1897 (Vol. 1) and 1901 (Vol. 2).

[10] A. Lubotzky, *Subgroup growth*, lecture notes prepared for the conference Groups '93 Galway/St Andrews, University College Galway.

[11] A. Lubotzky, Counting finite index subgroups. In: Groups '93 Galway/St Andrews, LMS Lecture Notes Series No. 212, Cambridge University Press, 1995, 368 – 404.

[12] A. Lubotzky, Subgroup growth and congruence subgroups, *Invent. Math.* **119** (1995), 267 – 295.

[13] A. Lubotzky, A. Mann, and D. Segal, Finitely generated groups of polynomial subgroup growth, *Israel J. Math.* **82** (1993), 363 – 371.

[14] A. Lubotzky and D. Segal, *Subgroup Growth*, Progress in Mathematics, Birkhäuser, Basel, to appear.

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

[16] M. H. Millington, On cycloidal subgroups of the modular group, *Proc. London Math. Soc.* **19** (1969), 164 – 176.

[17] M. H. Millington, Subgroups of the classical modular group, *J. London Math. Soc.* **1** (1969), 351 – 357.

[18] L. Moser and M. Wyman, On solutions of $x^d = 1$ in symmetric groups, *Can. J. Math.* **7** (1955), 159 – 168.

[19] L. Moser and M. Wyman, Asymptotic expansions, *Can. J. Math.* **8** (1956), 225 – 233.

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

[21] T. Müller, Counting free subgroups of finite index, *Archiv d. Math.* **59** (1992), 525 – 533.

[22] T. Müller, Subgroup growth of free products, *Invent. Math.* **126** (1996), 111 – 131.

[23] T. Müller, Combinatorial classification of finitely generated virtually free groups, *J. Algebra* **195** (1997), 285 –294.

[24] T. Müller, Finite group actions and asymptotic expansion of $\mathrm{e}^{P(z)}$, *Combinatorica* **17** (1997), 523 – 554.

[25] T. Müller, Enumerating representations in finite wreath products, *Adv. in Math.* **153** (2000), 118 – 154.

[26] T. Müller, Representations in finite wreath products. Enumerative theory and applications. *Proceedings of the conference Groups Korea '98* (Y. G. Baik, D. L. Johnson, and A. C. Kim editors), pp. 243 – 290, Walter de Gruyter, Berlin, 2000.

[27] T. Müller, Five lectures on generalized permutation representations, *Matemática Contemporânea* **20** (2001), 227 – 272.

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

[29] T. Müller, Counting wreath product representations of finite groups, submitted.

[30] T. Müller, Modular subgroup arithmetic. To appear in: Proc. 2001 Durham Symposium on Groups, Geometries, and Combinatorics.

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

[32] T. Müller, Representations in finite wreath products and subgroup growth, in preparation.

[33] T. Müller, Poincaré's problem for free products, in preparation.

[34] T. Müller and J. Shareshian, Enumerating representations in finite wreath products II: Explicit formulae, *Adv. in Math.* **171** (2002), 276–331.

[35] J. Neukirch, *Algebraische Zahlentheorie*, Springer, Berlin, 1992.

[36] M. Newman, *Integral matrices*, Academic Press, 1972.

[37] M. Newman, Asymptotic formulas related to free products of cyclic groups, *Math. Comp.* **30** (1976), 838 – 846.

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

[39] H. Petersson, Über einen einfachen Typus von Untergruppen der Modulgruppe, *Archiv d. Math.* **4** (1953), 308 – 315.

[40] H. Petersson, Über die Konstruktion zykloider Kongruenzgruppen in der rationalen Modulgruppe, *J. Reine u. Angew. Math.* **250** (1971), 182 – 212.

[41] H. Petersson, Konstruktionsprinzipien für Untergruppen der Modulgruppe mit einer oder zwei Spitzenklassen, *J. Reine u. Angew. Math.* **268/69** (1974), 94 – 109.

[42] J.-P. Serre, *Trees*, Springer–Verlag, Berlin, 1980.

[43] C. L. Siegel, *Topics in Complex Function Theory, Vol. II*, John Wiley & Sons, New York, 1971.

[44] W. W. Stothers, The number of subgroups of given index in the modular group, *Proc. Royal Soc. Edinburgh* **78A** (1977), 105 – 112.

Thomas W. Müller, School of Mathematical Sciences, Queen Mary, University of London, Mile End Road, London E1 4NS, UK (T.W.Muller@qmul.ac.uk)

Jan-Christoph Schlage-Puchta, Mathematisches Institut, Universität Freiburg, Eckerstr. 1, 79104 Freiburg, Germany (jcp@math.uni-freiburg.de)