Ann. Sci. Math. Québec **32** (2008), no 2, 125–138

RANDOM p-GROUPS AND GALOIS GROUPS

NIGEL BOSTON

Dedicated to John Labute on the occasion of his retirement.

RÉSUMÉ. Nous comparons des pro-p -groupes sélectionnés au hasard et des groupes de Galois de p-extensions non ramifiées en dehors d'un ensemble aléatoire de nombres premiers. Dans chaque cas, nous calculons la probabilité qu'un tel groupe soit sélectionné au hasard. Par exemple, nous montrons qu'un pro-p -groupe avec 2 générateurs et 2 relations choisis au hasard est fini avec une probabilité de plus de 99%, mais moins de 100%. De plus, nous montrons que la probabilité de sélectionner un pro-p -groupe infini est non nulle et que la probabilité qu'un pro-p -groupe ayant autant de relations que de générateurs satisfasse une conjecture dite modérée de Fontaine-Mazur est de 100%.

ABSTRACT. We compare random pro-p-groups and Galois groups of p-extensions unramified outside a random set of primes. In each case, we compute probabilities that a given group arises. We show, for instance, that a random 2-generator, 2-relator pro-p-group is more than 99% but less than 100% likely to be finite. We also show that there exist infinite pro-p-groups that arise with non zero probability, and that pro-p-groups with as many relators as generators satisfy a tame Fontaine-Mazur conjecture with 100% probability.

1. Introduction

In this paper, we describe what, for a given g, r, and p, a typical g-generator, r-relator pro-p-group looks like. The motivation for this comes from our lack of knowledge of the structure of the Galois group of the maximal pro-p extension unramified outside a finite set S of places of a number field K. This is particularly true in the tame case, which means that S does not contain any place above p. In the tame case $g \leq r$, we show that, with probability 100%, a g-generator, r-relator pro-p-group has no infinite analytic quotients. Thus, the Fontaine-Mazur conjecture [16], which says that this should hold for the tame Galois groups above, may be viewed as simply saying that these Galois groups are typical.

This approach is inspired by that of Dunfield and Thurston [12]. There is a well-developed analogy between number fields and 3-manifolds. Ideas from each have enriched the other, such as in Labute's recent breakthrough [21] giving some information

Reçu le 30 avril 2008 et, sous forme définitive, le 3 septembre 2008.

about the mysterious tame Galois groups above. Like their number theoretical counterparts, the fundamental groups of 3-manifolds are conjectured to satisfy important conjectures but are poorly understood. To improve our understanding, Dunfield and Thurston addressed the question of whether the finite quotients of a random 3-manifold group resemble those of a random discrete group with the same number of generators as relators.

In our scenario, we begin by computing the probability that a pro-p-group is isomorphic to a given group. One consequence of our formula is, for instance, that for a given prime p, a 2-generator, 2-relator pro-p presentation gives a finite group with probability more than 99% but less than 100%. We also introduce the notion of a positive probability pro-p-group (meaning that a non zero proportion of presentations yields it) and find several families of such groups which are infinite. We then study related questions for Galois groups of p-extensions with restricted ramification as the set of ramified primes varies.

Gromov [17] introduced one notion of random group and Gowers [18] recently considered quasi-random groups. We take a different approach, picking r relators from the free pro-p-group on g generators uniformly, according to the Haar measure on its Frattini subgroup. Then, we investigate which pro-p-group these present.

2. The main formula

Given a prime p and positive integer g, let F be the free pro-p-group on g generators. Its Frattini subgroup will be denoted $\Phi(F)$. Since $\Phi(F)$ is a profinite group, it is compact and Hausdorff and so has a Haar measure, which we normalize so that $\Phi(F)$ has measure 1. For a given non negative integer r, we shall pick r elements of $\Phi(F)$ uniformly with respect to this measure. If Γ is a g-generator, r-relator pro-p-group, we consider the set of r-tuples from $\Phi(F)$ that yields a presentation of Γ. This set is measurable as explained in Theorem 2.1 when Γ is finite and in Theorem 4.1 for the general case. We let $pr(\Gamma)$ denote its measure; in other words, the probability that r randomly selected relators will present Γ.

Define $\phi_p(n) = (p^n - 1)(p^{n-1} - 1)\cdots(p - 1)$ if n is a positive integer and $\phi_p(0) = 1$, otherwise. Let

$$c_{p,g,r} = \phi_p(g)\phi_p(r)p^{gr-g(g+1)/2-r(r+1)/2}.$$

For example, one has $c_{2,2,2} = 9/4$. Let $d(\Gamma), r(\Gamma)$ denote the generator and relator ranks of Γ, respectively.

Theorem 2.1. *Let Γ be a finite p-group with $d(\Gamma) = g$ and $r(\Gamma) = r$. Then,*

$$pr(\Gamma) = c_{p,g,r}\frac{|\Gamma|^{g-r}}{|\mathrm{Aut}(\Gamma)|}.$$

Remarks 2.2. (i) Since Γ has g generators, the map $F/\Phi(F) \to \Gamma/\Phi(\Gamma)$ is an isomorphism. If $\Gamma = F/N$, then it follows that $N \leq \Phi(F)$, which is why any relators for Γ have to be in $\Phi(F)$.

(ii) It is noteworthy that $c_{p,g,r}$ is symmetric in g and r. This comes out of the proof, but one wonders if there is some deeper reason underlying this observation.

We can also give a relative version, which will be necessary in understanding these probabilities for infinite groups. In preparation, we need to define the property of being of p-class c.

Definition 2.3. If G is a pro-p-group, its *lower p-central series* is given by

$$P_0(G) = G, P_{i+1}(G) = [G, P_i(G)]P_i(G)^p, \quad i \in \mathbb{N},$$

where, for pro-p-groups, we mean the closed subgroup so generated. Thus, $P_1(G) = \Phi(G)$. The quotient $G/P_c(G)$ is called the *p-class c quotient* of G. If $G/P_c(G) \cong H$, then G is called a *descendant* of H and if, furthermore, $P_{c+1}(G) = \{1\}$ and $G \neq H$, then G is called an *immediate descendant* of H.

Let $\mathcal{V}$ be some subclass of pro-p-groups given by a verbal condition V, such as "all abelian groups" or "all metabelian groups" or "all groups with a given bound on their p-class". Then there is a g-generator free pro-p-group $\overline{F} = F/V(F)$ in this class, and we can talk of pro-p-groups being g-generator, r-relator *qua* this class. For example, all finite g-generator abelian p-groups Γ are g-relator *qua* abelian. Indeed, since Γ is a product $\langle x_1\rangle \times \cdots \times \langle x_g\rangle$ of cyclic groups of orders $r_1, \ldots, r_g$, respectively, the relators $x_i^{r_i}$, for $i = 1, \ldots, g$, present Γ *qua* abelian, the commutation relations coming for free. In this case, $\overline{F} = F/[F, F]$ is the free abelian pro-p-group on g generators. Once again, we can pick r relators from its Frattini subgroup and ask if they present a given group Γ in the class.

Now, let $pr_V(\Gamma)$ denote the measure of the set of r-tuples of $\Phi(\overline{F})$ that present Γ *qua* V. Let $d_V(\Gamma), r_V(\Gamma)$ denote the generator and relator ranks of Γ *qua* V, respectively.

Theorem 2.4. *Let Γ be a finite p-group in the class V with $d_V(\Gamma) = g$ and $r_V(\Gamma) = r$. Then,*

$$pr_V(\Gamma) = c_{p,g,r}\frac{|\Gamma|^{g-r}}{|\mathrm{Aut}(\Gamma)|}.$$

The proofs of the two theorems are similar, with $\overline{F}$ playing the role of F in the second. However, before going into the proof of the above theorem, we need some preliminary material.

Definition 2.5. Let Γ be a finite group and G be a finitely generated (profinite) group.

(i) $\mathrm{Hom}(G, \Gamma)$ $(\mathrm{Epi}(G, \Gamma))$ denotes the set of continuous homomorphisms (surjective continuous homomorphisms, respectively) from G to Γ.

(ii) The *Moebius function* of the lattice of subgroups of Γ is defined inductively by $\mu(\Gamma) = 1$ and by $\sum_{K \leq H \leq \Gamma} \mu(H) = 0$ for every $K < \Gamma$.

(iii) *Hall's invariant* $\delta_\Gamma(G)$ [24] is defined to be the number of closed normal subgroups N of G such that G/N is isomorphic to Γ.

(iv) *The probabilistic zeta function* [3, 23] is defined to be the proportion of s-tuples of elements of Γ that generate Γ and is denoted $P(\Gamma, s)$.

Lemma 2.6. *The following statements hold true:*

(i) $|\mathrm{Hom}(G,\Gamma)| = \sum_{H\leq\Gamma} |\mathrm{Epi}(G,H)|$.

(ii) $|\mathrm{Epi}(G,\Gamma)| = \sum_{H\leq\Gamma} \mu(H)|\mathrm{Hom}(G,H)|$.

(iii) $\delta_\Gamma(G) = \dfrac{|\mathrm{Epi}(G,\Gamma)|}{|\mathrm{Aut}(\Gamma)|} = \left(\sum_{H\leq\Gamma} \mu(H)|\mathrm{Hom}(G,H)|\right) \Big/ |\mathrm{Aut}(\Gamma)|$.

(iv) $P(\Gamma,s) = \sum_{H\leq\Gamma} \dfrac{\mu(H)}{[\Gamma:H]^s}$.

Proof. Part (ii) follows from Part (i) by Mobius inversion. Part (iv) is in [3, 23]. □

Proof of Theorem 2.1. Suppose that $x_1,\ldots,x_r$ is an ordered r-tuple of elements of F. Denote by N the closed normal subgroup they generate.

We shall calculate the probability that they present Γ by computing how many N satisfy $F/N \cong \Gamma$ and, for each such N, the measure of the set X_N of r-tuples that topologically generate N as a normal subgroup. We begin with the latter.

Given such an N, an r-tuple $x_1,\ldots,x_r$ generates N if and only if their images in the elementary abelian p-group $N/[N,F]N^p$ $\big($which has order p^r - it is dual to $H^2(\Gamma,\mathbf{Z}/p)\big)$ generate $N/[N,F]N^p$. This occurs with probability $\phi_p(r)/p^{r(r+1)/2}$. Thus, X_N is measurable and has measure $\phi_p(r)/p^{r(r+1)/2}$ times the measure of N raised to the power r. Since $\Phi(F)$ has measure 1, N has measure

$$\frac{1}{[\Phi(F):N]} = \frac{[F:\Phi(F)]}{[F:N]} = \frac{p^g}{[F:N]}.$$

Thus, X_N has measure

$$\frac{\phi_p(r)}{p^{r(r+1)/2}} \cdot \left(\frac{p^g}{|F/N|}\right)^r.$$

Let X denote the set of r-tuples that present Γ. The measure of X is the number of N such that $F/N \cong \Gamma$ times the measure of X_N just computed. The number of such N is

$$\delta_\Gamma(F) = \left(\sum_{H\leq\Gamma} \mu(H)|H|^g\right) \Big/ |\mathrm{Aut}(\Gamma)|,$$

since $|\mathrm{Hom}(F,H)| = |H|^g$. Combining, we obtain that the measure of S is

$$\begin{aligned}
\frac{\phi_p(r)}{p^{r(r+1)/2}}\left(\frac{p^g}{|\Gamma|}\right)^r\left(\frac{\sum_{H\leq\Gamma}\mu(H)|H|^g}{|\mathrm{Aut}(\Gamma)|}\right) &= \left(\frac{\phi_p(r)}{p^{r(r+1)/2}}\right)p^{gr}|\Gamma|^{g-r}\left(\frac{P(\Gamma,g)}{|\mathrm{Aut}(\Gamma)|}\right)\\
&= \left(\frac{\phi_p(r)}{p^{r(r+1)/2}}\right)p^{gr}\left(\frac{|\Gamma|^{g-r}}{|\mathrm{Aut}(\Gamma)|}\right)\prod_{i=1}^{g}\left(1-\frac{1}{p^i}\right)\\
&= \phi_p(g)\phi_p(r)p^{gr-(g(g+1)-r(r+1))/2}\frac{|\Gamma|^{g-r}}{|\mathrm{Aut}(\Gamma)|}\\
&= c_{p,g,r}\frac{|\Gamma|^{g-r}}{|\mathrm{Aut}(\Gamma)|},
\end{aligned}$$

since $P(\Gamma,s) = P\left(\dfrac{\Gamma}{\Phi(\Gamma)},s\right) = \displaystyle\prod_{i=1}^{g}\left(1-\frac{1}{p^{s-i+1}}\right)$. □

Remarks 2.7. (i) If $g = r$ (as in the case of finite abelian p-groups *qua* abelian), then this simplifies to

$$\frac{\phi_p(g)^2}{p^g|\mathrm{Aut}(\Gamma)|}.$$

(ii) If $r = 0$, in which case with certainty we present the g-generator free pro-p-group, then the formula simplifies to

$$\frac{\phi_p(g)|\Gamma|^g}{p^{g(g+1)/2}|\mathrm{Aut}(\Gamma)|} = 1,$$

where $\Gamma = F/V(F)$. In fact, this is a convenient way to compute $|\mathrm{Aut}(F/P_c(F))|$.

(iii) Since a probability is at most 1, an immediate corollary is that

$$\frac{|\Gamma|^{g-r}}{|\mathrm{Aut}(\Gamma)|} \leq \frac{1}{c_{p,g,r}}.$$

Equality can occur when Γ is one of the p-class quotients of a free pro-p-group, as noted in the last remark.

3. Finite examples and mass formulae

Using the computer algebra system MAGMA [2], the formulae in Theorems 1 and 2 can be tested experimentally. For example, we let MAGMA pick many pairs of words of length at most 50 from the free group on 2 generators and compute the maximal quotient of 2-power order (if finite) of the group so presented, only saving those with generator rank 2. In fact, 9.5% of these yielded the quaternion group of order 8, whereas $15.0\%, 13.9\%$ and 6.1% yielded the three groups of order 16 which have both generator and relator ranks 2. According to Theorem 2.1, these proportions should approximate $9/(4|\mathrm{Aut}(\Gamma)|)$ which is $9.4\%, 14.1\%, 14.1\%$ and 7.0%, respectively. Note that MAGMA uses the product replacement algorithm [8] to produce random words. However, the distribution so produced does tend in the limit to the Haar measure we use.

These 4 groups already account for almost 50% of all pairs of relators. We next investigate what proportion of pairs of relators yield a finite 2-group. This naturally leads to some mass formulae.

A mass formula is usually the sum of the reciprocals of the orders of certain automorphism groups. They arise all over mathematics and appear here because, for fixed V, p, g, r, the sum of the probabilities $pr_V(\Gamma)$ over all g-generator, r-relator finite p-groups cannot exceed 1. Since the r relators could conceivably present an infinite pro-p-group, the sum may be strictly less than 1.

Theorem 3.1 (Partial Mass formula). *Summing over all finite p-groups Γ of class V with $d_V(\Gamma) = g$ and $r_V(\Gamma) = r$, we have*

$$\sum \frac{|\Gamma|^{g-r}}{|\mathrm{Aut}(\Gamma)|} \leq \frac{1}{c_{p,g,r}}.$$

A natural question is to ask when there is equality in this mass formula. It is easy to see that there is equality if $g = r = 1$. More generally, if the class consists of all abelian p-groups (see below - this was noted by Cohen and Lenstra [9]), there is equality. This result implies that a pro-p-group with $g = r$ (and so with any $g \leq r$) has finite abelianization with probability 1.

Theorem 3.2 (Mass formula). *Summing over all finite abelian p-groups Γ with $d(\Gamma) = g$, we have*

$$\sum \frac{1}{|\mathrm{Aut}(\Gamma)|} = \frac{1}{c_{p,g,g}}.$$

Proof. The automorphism groups of finite abelian p-groups are explicitly known [19]. The formula then comes from summing two nested geometric series. □

In general, summing over all finite g-generator, g-relator p-groups, one can show that the sum is always strictly less than $1/c_{p,g,g}$ if $g \geq 2$. For $g \geq 4$, this follows from the fact that there are actually no such groups by the Golod-Shafarevich inequality and so the sum is zero. For $g = 2$ or $g = 3$, refinements of this inequality [20] show that if the relations are at a certain depth inside the Zassenhaus filtration, then the group presented is infinite. In fact, we can prove the following.

Theorem 3.3. *Let p be a fixed prime. If $g \geq 4$, then there are no finite g-generator, g-relator p-groups. If $g \geq 2$, then the sum of $1/|\mathrm{Aut}(\Gamma)|$ over all finite g-generator, g-relator p-groups is strictly less than $1/c_{p,g,g}$. This assertion is equivalent to saying that the probability that the g relators present a finite p-group is strictly less than 100%.*

Moreover, we have the following theorem which makes explicit the case $g = 2$ of the above theorem.

Theorem 3.4. *Consider the sum $S(p)$ of $1/|\mathrm{Aut}(\Gamma)|$ over all 2-generator, 2-relator finite p-groups. Then, for $p = 2$, we have*

$$0.44189 < S(2) < 4/9 = 0.4444\ldots.$$

If $p > 3$, then

$$\frac{\left(1+\frac{2}{p}+\frac{4}{p^2}+\frac{6}{p^3}+\frac{5}{p^4}-\frac{1}{p^6}\right)}{(p^4-p^2)} \;\leq\; S(p) \;<\; \frac{1}{c_{p,2,2}} \;=\; \frac{p^2}{(p^2-1)^2(p-1)^2}.$$

This in turn implies that the sum of $pr(\Gamma)$ over all 2-generator, 2-relator finite p-groups is at least

$$1-\frac{4}{p^4}-\frac{4}{p^5}+\frac{7}{p^6}+\frac{6}{p^7}-\frac{5}{p^8}-\frac{2}{p^9}-\frac{1}{p^{10}},$$

which is greater than 99% for every such p.

Before going into the proof of the above theorems, one needs the following lemma which classify the 2-generator, 2-relator p-groups of order at most p^7 (see [28]).

Lemma 3.5. *Let $p > 3$ be a prime. The following is a complete list of 2-generator, 2-relator p-groups of order at most p^7.*

(i) *There is only one such group of order p^3. Its automorphism group has order $(p-1)p^3$.*

(ii) *There is only one such group of order p^4. Its automorphism group has order $(p-1)p^4$.*

(iii) *There are $p+3$ such groups of order p^5. Of their automorphism groups, 2 have order $(p-1)p^5$, $(p-3)/2$ have order $(p-1)p^6$, $(p-1)/2$ have order $(p+1)p^6$, 2 have order $2p^7$, and 1 has order $(p^2-1)p^7$.*

(iv) *There are $p+2$ such groups of order p^6. Of their automorphism groups, 1 has order $(p-1)p^6$, 1 has order p^7, and p have order $(p-1)p^7$.*

(v) *There are p^2+3p+2 such groups of order p^7. Of their automorphism groups, 2 have order $(p-1)p^7$, 2 have order p^8, $2p-2$ have order $2p^8$, p have order $(p-1)p^8$, and p^2 have order p^9.*

Proof of Theorems 3.3 and 3.4. The comments before the theorem establish all but the case $g = 2$. So assume $g = 2$. We treat the three cases, $p = 2, p = 3, p > 3$, separately.

For $p = 2$, O'Brien [27] calculated a lower bound for the sum by finding many 2-generator, 2-relator 2-groups, some as large as 2^{25}. He does this by employing his p-group generation algorithm [26], which produces very many 2-generator, 2-groups by iteratively computing descendants. By lemma 3.5 above, the 2-relator ones are detected as those with multiplicator rank equal to 2. This lower bound was

$$62191043501935/140737488355328 \approx 0.44189394189640296417564968 5785,$$

more than 99% of $1/c_{2,2,2} = 0.4444\ldots$. The question remains as to what is the true value of the sum, a quantitative form of the Golod-Shafarevich inequality. The case $p = 3$ is handled similarly.

Consider now 2-generator, 2-relator p-groups with $p > 3$. The proof is completed by summing the reciprocals of the orders of the above automorphism groups in the lemma. □

One wonders whether a similar classification to that in the above lemma holds for p-groups of order p^n for n greater than 7. Namely perhaps, analogously to the PORC conjecture [13], the groups can be partitioned into sets of size a polynomial in p, where each group in the set has the same automorphism group size, again polynomial in p. If so, the sum of the $pr(\Gamma)$ will be an infinite series in $1/p$.

4. Infinite positive probability pro-p-groups

Next, we turn to infinite pro-p-groups. Using the relative version, Theorem 2.4, we obtain a formula for the probability that r relators present a given, possibly infinite, pro-p-group Γ.

Theorem 4.1. *Let Γ be a g-generator, r-relator pro-p-group. Then the probability $pr(\Gamma)$ that r relators picked from the Frattini subgroup of the free pro-p-group on g generators present Γ is given by*

$$pr(\Gamma) = \lim_{c\to\infty} \phi_p(g)\phi_p(r)p^{gr-g(g+1)/2-r(r+1)/2}\frac{|\Gamma/P_c(\Gamma)|^{g-r}}{|\mathrm{Aut}(\Gamma/P_c(\Gamma))|}.$$

Proof. An r-tuple presents Γ if and only if, for every $c \geq 1$, their images in $F/P_c(F)$ present $\Gamma/P_c(\Gamma)$ *qua* a p-class $\leq c$ group. Call the set of such r-tuples X_c. By Theorem 2.4, since for large enough c the group $\Gamma/P_c(\Gamma)$ is r-relator, X_c is a closed set and has measure

$$\frac{\phi_p(g)\phi_p(r)p^{gr-g(g+1)/2-r(r+1)/2}|\Gamma/P_c(\Gamma)|^{g-r}}{|\mathrm{Aut}(\Gamma/P_c(\Gamma))|}.$$

The set of r-tuples that present Γ equals the intersection of the X_c's which, as an intersection of closed sets, is closed. Hence, it is measurable with measure the limit of the measures of the X_c as $c \to \infty$, since

$$\cdots \subseteq X_c \subseteq \cdots \subseteq X_2 \subseteq X_1.$$

□

If $r = 0$, then, with probability 1, the free pro-p-group F is presented, that is $pr(F) = 1$. In this section, we observe that there are many other infinite pro-p-groups occurring with probability greater than 0.

Definition 4.2. A *positive probability* pro-p-group Γ is one that satisfies $pr(\Gamma) > 0$. We call this a *PPP group* for short.

All finite p-groups are PPP. There are also many infinite PPP groups.

Theorem 4.3. (i) *Consider, for $k \geq 2$, the sequences of pro-2-groups*

$$G_k = \left\langle x, y \mid x^y = x^{2^k-1} \right\rangle \text{ and } H_k = \left\langle x, y \mid x^y = x^{2^k+1} \right\rangle.$$

Then G_k is PPP with $pr(G_k) = 3/2^{k+2}$ and H_k is PPP with $pr(H_k) = 3/2^{2k+1}$.

(ii) *Suppose p is an odd prime. Consider, for $k \geq 1$, the sequence of pro-p-groups*

$$G_k = \left\langle x, y \mid x^y = x^{p^k+1} \right\rangle.$$

Then G_k is PPP with $pr(G_k) = (p^2-1)(p-1)/p^{2k+1}$.

(iii) *For any p, these are prometacyclic groups and the sum of the $pr(\Gamma)$ over the above groups Γ is $(1-1/p)$.*

Proof. The finite quotients $\Gamma/P_c(\Gamma)$ of these pro-p-groups are metacyclic of order p^{2c}, and the automorphism groups of metacyclic p-groups are all known [1, 10, 11]. Plugging $c_{p,2,1} = (p^2-1)(p-1)^2/p^2$ and the orders of $\Gamma/P_c(\Gamma)$ and its automorphism group into the above formula yields the claimed values for $pr(\Gamma)$. For a given p, summing the geometric series gives that the sum of these $pr(\Gamma)$ is $(p-1)/p$. □

What happens if the relator is picked from the remaining $1/p$ of the Frattini subgroup $\Phi(F)$? In fact, it appears that the groups so obtained all have $pr(\Gamma) = 0$. The best way to look at this is in terms of the p-group generation algorithm. MAGMA implements an algorithm of O'Brien [26] that finds all immediate descendants of a given finite p-group H and computes associated non negative integers called *the nuclear rank* and *multiplicator rank* of H. The following lemma allows us to tell which of those descendants could come from a 1-relator group.

Lemma 4.4. *Let Γ be a g-generator, r-relator pro-p-group. Then the multiplicator rank minus the nuclear rank of $\Gamma/P_c(\Gamma)$ is non negative and at most r.*

Proof. See the lemma in section 3 of [6]. □

For instance, let p be odd. If G is a 2-generator, 1-relator pro-p-group, then $G/P_1(G) \cong C_p \times C_p$. This group has 4 immediate descendants whose multiplicator rank minus nuclear rank is at most 1 (call such a descendant *viable*). Two of these are metacyclic. Of them, one has just one viable descendant, which has just one viable descendant, and so on. Call such a group *stable*. The inverse limit of the viable descendants of a stable group is PPP (in this case it is G_1).

The other metacyclic group has two viable descendants, one of which is stable (leading to G_2), the other of which has two viable descendants. Similarly, one of these descendants is stable (leading to G_3), and so on. The periodic structure of the viable descendants is reminiscent but different to Conjecture P of Newman and O'Brien [13, 14, 15, 25].

As for $p = 2$, $C_2 \times C_2$ has two metacyclic viable descendants. In this case, both of these have two viable descendants, one of which is stable, the other of which has two viable descendants. Again, one of these two descendants is stable, and so on. Thus, we get two sequences of PPP pro-2-groups.

The two non metacyclic descendants of $C_p \times C_p$ have many viable descendants, all of which have many viable descendants, and so on. We therefore believe that they have no stable descendants and that the above list of 2-generator, 1-relator PPP groups is complete. This problem will be addressed in a forthcoming paper of the author with Charles Leedham-Green.

In that paper, it will also be proven that, if a group has just one viable descendant, then it is stable. This allows us to prove that several other pro-p-groups are PPP. For example, if Γ is the pro-2-group $< x, y, z \mid x^y = x^3z^2 >$, then $pr(\Gamma) = 21/64$. It

is surprising that this most common 3-generator, 1-relator pro-2-group has apparently never previously arisen in research.

5. Random Galois groups

For a fixed prime p, we shall denote by $\mathcal{P}$ the set of primes that are congruent to 1 modulo p and by $\mathcal{P}(x)$ the subset of those primes less or equal to x . Given a subset Y of $\mathcal{P}^g$, its *relative Dirichlet density* is defined to be the limit (if it exists) as $x \to \infty$ of $|(Y \cap \mathcal{P}(x)^g)|/|\mathcal{P}(x)^g|$.

For any set S of g elements of $\mathcal{P}$, we consider the Galois group G_S of the maximal p-extension of $\mathbb{Q}$ unramified outside S (allowing ramification at infinity if $p = 2$). This is a pro-p-group with $d(G_S) = r(G_S) = g$, where $g = |S|$ [20].

Given a pro-p-group Γ, let Y consists of all g-tuples of primes in $\mathcal{P}$ which form a set S such that $G_S \cong \Gamma$. We give Y its Dirichlet density relative to $\mathcal{P}^g$ (and conjecture that it always exists). For example, if $g = 1$, then $\Gamma \cong C_{p^r}$ for some r. If $S = \{q\}$ and p is odd, then $G_S \cong C_{p^s}$ where p^s exactly divides $q - 1$. Thus, Y consists of all primes q that are congruent to 1 modulo p^s and not congruent to 1 modulo p^{s+1}. Therefore, Y has measure $(p - 1)/p^s$.

We set $pr'(\Gamma)$ to the the above Dirichlet density. Thus, the above argument gives the following theorem.

Theorem 5.1. *Suppose $\Gamma \cong C_{p^s}$. Then, $pr'(\Gamma) = (p - 1)/p^s$.*

Next, consider the case $g = 2$ and Γ a finite 2-group.

Theorem 5.2. *Suppose Γ is a finite 2-group with abelianization $C_2 \times C_2$ (so Γ is dihedral, generalized quaternion, or semidihedral). If Γ is dihedral or generalized quaternion, then $pr'(\Gamma) = 0$. If Γ is the semidihedral group S_{2^s} of order 2^s with $s \geq 4$, then $pr'(\Gamma) = 1/2^{s-1}$.*

Proof. G_S has abelianization $C_2 \times C_2$ precisely when the two primes are both congruent to 3 modulo 4, which comprises $1/4$ of all cases for $p = g = 2$. Without loss of generality, if we order the primes so that the first is a square modulo the second (call that one q), then by [7], G_S is semidihedral of order 2^{k+1} where 2^{k-1} exactly divides $q+1$. For example, in half of cases, q is congruent to 3 modulo 8 and G_S is semidihedral S_{16} of order 16. It follows that $pr'(S_{16}) = 1/8$, and likewise $pr'(S_{2^s}) = 1/2^{s-1}$. □

Remark 5.3. In comparison, note that the automorphism group of S_{2^s}, with $s \geq 4$, has order 2^{2s-4} and hence, $pr(S_{2^s}) = 9/2^{2s-2}$.

Theorem 5.4. *Suppose that Γ is the modular group M_{2^s} of order 2^s, $s \geq 4$. Then $pr'(\Gamma) = 1/2^s$.*

Proof. Since the abelianization of Γ is $C_2 \times C_{2^{s-2}}$, one prime is congruent to 3 modulo 4 and the other, say q, is congruent to $(2^{s-2} + 1)$ modulo 2^{s-1}. Now, Γ has a cyclic subgroup of index 2. Calculating ray class groups of quadratic fields shows that the only time one is cyclic is in the situation of Theorem 2.2 in [7], *i.e.* when the Legendre symbol is -1. Putting this with the congruence conditions above yields $pr'(\Gamma) = (1/2)(1/2)(1/2^{s-2}) = 1/2^s$. □

Remark 5.5. In comparison, note that the automorphism group of M_{2^s}, with $s \geq 4$, has order 2^s and hence, $pr(M_{2^s}) = 9/2^{s+2}$.

Likewise, we can show that the groups in the third family of [7] and the first family of [6] only arise in those circumstances and no others. So we can state the following result.

Theorem 5.6. *Let $n \geq 2$ and let $\Gamma = P_n$ with*

$$P_n := \left\langle a, b \mid a^2 = b^{-1}ababab^{2^n-1} = 1 \right\rangle,$$

of order 2^{3n+1}. Then $pr'(\Gamma) = 1/2^{n+3}$.

Proof. This arises when one of the primes is congruent to 3 modulo 4, the other is congruent to $(2^n + 1)$ modulo 2^{n+1}, and the first lies in a particular quarter of the congruence classes modulo the second. So $pr'(\Gamma) = (1/2)(1/2^n)(1/4) = 1/2^{n+3}$. □

Remark 5.7. However, note that the automorphism group of P_n, with $n \geq 3$, has order 2^{4n} and hence, $pr(P_n) = 9/2^{4n+2}$. The automorphism group of P_2 has order 2^9 and thus, $pr(P_2) = 9/2^{11}$.

Theorem 5.8. *Let Γ_1, Γ_2 be the groups of order 2^{5n+9}, with $n \geq 2$, arising in* [6]. *Then $pr'(\Gamma_1) + pr'(\Gamma_2) = 1/2^{n+4}$.*

Proof. In the given situation, we know that G_S is one of Γ_1 or Γ_2, but we do not know which. One prime is congruent to $(2^n - 1)$ modulo 2^{n+1}, the other is congruent to 5 modulo 8, and the first is a square but not a 4-th power modulo the second. Then, $pr'(\Gamma_1) + pr'(\Gamma_2) = (1/2^n)(1/4)(1/4) = 1/2^{n+4}$. □

Remark 5.9. In comparison, note that the automorphism groups of the smallest groups (of order 2^{19}) have order 2^{25} and therefore, $pr(\Gamma_i) = 9/2^{27}$ in each case.

It is a mystery as to how often Γ_1 versus Γ_2 arises as G_S. It appears that this phenomenon persists into the case where Γ is infinite. Consider, for example, [5] where S consists of two primes, both congruent to 5 modulo 8, one a 4-th power modulo the other but not vice versa. The probability of this occurring is

$$(1/4)(1/4)(1/4)(1/2) = 1/128$$

Indeed, note that quadratic reciprocity ensures that both is a square modulo the other, leading to a last factor of $1/2$ instead of $1/4$. Let $\mathcal{F}$ be the family of infinite pro-2-groups arising in that paper, where G_S is known to belong to. Then,

$$\sum_{\mathcal{F}} pr'(\Gamma) = 1/128,$$

but we do not know the relative frequencies with which the different groups in $\mathcal{F}$ occur as G_S or, indeed, if any are PPP.

Remarks 5.10. (i) A closer analogue to the approach of Dunfield and Thurston is to consider, given g and a p-group Γ with $d(\Gamma) \leq g$, how often it arises as a quotient, on one hand, of a random g-generator, g-relator pro-p-group and, on the other hand, of G_S for a random S of size g. For instance, for $g = 2$ and Γ the quaternion group of order 8, there is a Γ-extension of $\mathbb{Q}$ unramified outside two odd primes if and only if

both primes are congruent to 1 modulo 4 and their Legendre symbol is 1. Such a pair of primes has density $1/8$ among all pairs of odd primes.

A random 2-generator, 2-relator pro-2-group G has this Γ as a quotient if and only if $G/P_2(G)$ does. Of the 7 possibilities for $G/P_2(G)$, 3 have a Γ-quotient. Summing their probabilities of arising (computed by Theorem 2.1) shows that the probability that a random 2-generator, 2-relator pro-2-group has a quotient isomorphic to the quaternion group of order 8 is $87/512$. As this example illustrates, the formulae obtained are not as clean as with the less direct analogue to Dunfield-Thurston pursued in this paper.

(ii) A separate joint work consists of studying the frequency with which certain p-groups arise as Galois groups of p-class towers of imaginary quadratic fields. This leads to a non abelian analogue of the Cohen-Lenstra heuristics [9].

(iii) We can also look at pro-p Galois groups that are not tame. For instance, consider the Galois group of the maximal pro-p extension of $\mathbb{Q}$ unramified outside p and q, where p is odd and q is congruent to 1 modulo p and ± 3 modulo 8. It has presentation $\langle x, y \mid x^y = x^q \rangle$ [20], and so is one of the PPP groups in Theorem 4.3(ii). One idea that may help in understanding the mysterious tame Galois pro-p-groups is that the most popular random groups should arise as Galois groups.

In a forthcoming paper with Ellenberg and Venkatesh, the author will give a conjectural formula for $pr'(\Gamma)$.

6. Tame Fontaine-Mazur conjecture

If S is a finite set of primes of the number field K, none lying above the prime p, then the tame Fontaine-Mazur conjecture [16] says that the Galois group of the maximal pro-p extension of K unramified outside S should have no infinite, analytic quotients. Recall that an analytic pro-p-group is one that embeds in $GL_n(\mathbb{Z}_p)$ for some n. The conjecture was published 7 years after it was first made in a seminar at IHES, one concern being that the tame case of the conjecture was making a strong claim. In fact, this Galois group has g generators and r relators where $g \leq r$ and in this section we show that, with probability 1, such a group has no infinite, analytic quotients. In other words, the Fontaine-Mazur conjecture can be viewed as simply saying that these Galois groups are just typical.

Lemma 6.1. *Let H be an infinite finitely generated pro-p-group and suppose that $g \leq r$. The probability that a random g-generator, r-relator pro-p-group has H as a quotient is* 0.

Proof. Let F be the free pro-p-group on g generators. Let Γ be a finite p-group. For each open normal subgroup N of F such that $F/N \cong \Gamma$, we compute the probability that r relators chosen independently at random from $\Phi(F)$ lie in N to be

$$\frac{1}{([\Phi(F) : \Phi(F) \cap N])^r} = \left(\frac{1}{[\Phi(F)N : N]}\right)^r = \left(\frac{[F : \Phi(F)N]}{[F : N]}\right)^r \leq \frac{p^{gr}}{|\Gamma|^r}.$$

The number of open subgroups N such that $F/N \cong \Gamma$ is

$$\delta_\Gamma(F) \leq |\Gamma|^g / |\mathrm{Aut}(\Gamma)|.$$

It follows that the probability that a g-generator, r-relator pro-p-group has Γ as a quotient is less than

$$\frac{p^{gr}|\Gamma|^{g-r}}{|\mathrm{Aut}(\Gamma)|} \leq \frac{p^{gr}}{|\mathrm{Aut}(\Gamma)|}.$$

Only finitely many finite groups have automorphism group of any given order. Thus, as Γ runs through a sequence of quotients of H of order tending to infinity, $|\mathrm{Aut}(\Gamma)|$ tends to infinity and so the probability tends to 0. □

Taking $H = \mathbb{Z}_p$ shows (again) that a g-generator, r-relator pro-p-group with $g \leq r$ has finite abelianization with probability 1. Taking H to be virtually finitely generated abelian (of which there are countably many isomorphism classes) and using that Haar measure is countably additive shows that with probability 1, a g-generator, r-relator pro-p-group with $g \leq r$ is FAb, meaning that every finite index subgroup has finite abelianization. A similar approach proves the main result of this section.

Theorem 6.2. *The probability that a random g-generator, r-relator pro-p-group, with $g \leq r$, has an infinite analytic quotient is 0.*

Proof. The group has an infinite analytic quotient if and only if it has a just-infinite analytic quotient [4]. Moreover, there are only countably many just-infinite analytic pro-p-groups [22]. By the above lemma and countable additivity of Haar measure, the probability of the group having such a quotient is 0. □

Acknowledgements. The author thanks Yiftach Barnea, Jordan Ellenberg, Charles Leedham-Green, and Eamonn O'Brien for stimulating discussions and feedback.

REFERENCES

[1] J.N.S. Bidwell and M.J. Curran, *The automorphism group of a split metacyclic p-group*, Arch. Math. (Basel) **87** (2006), no. 6, 488–497.

[2] W. Bosma, J.J. Cannon, *Handbook of Magma functions*, School of Mathematics and Statistics, University of Sydney, 1996.

[3] N. Boston, *A probabilistic generalization of the Riemann zeta function*, Analytic Number Theory, Vol. 1, Progr. Math. **138** (Birkhauser, 1996), 155–162.

[4] N. Boston, *Some Cases of the Fontaine-Mazur conjecture II*, J. Number Theory **75** (1999), no. 2, 161–169.

[5] N. Boston, *Reducing the Fontaine-Mazur conjecture to group theory*, Progress in Galois theory, Dev. Math., 12, Springer, New York, 2005, 39–50.

[6] N. Boston and C.R. Leedham-Green, *Explicit computation of Galois p-groups unramified at p*, J. Algebra **256** (2002), no. 2, 402–413.

[7] N. Boston and D. Perry, *Maximal 2-extensions with restricted ramification*, J. Algebra **232** (2000), no. 2, 664–672.

[8] F. Celler, C.R. Leedham-Green, S.H. Murray, A.C. Niemeyer, and E.A. O'Brien, *Generating random elements of a finite group*, Comm. Algebra **23** (1995), no. 13, 4931–4948.

[9] H. Cohen, H.W. Lenstra, Jr., *Heuristics on class groups of number fields*, pp. 33–62 in *Number Theory : Noordwijkerhout 1983*, edited by H. Jager, Lecture Notes in Math. **1086**, Springer-Verlag, Berlin, 1984.

[10] M.J. Curran, *The automorphism group of a split metacyclic 2-group*, Arch. Math. (Basel) **89** (2007), no. 1, 10–23.

[11] R.M. Davitt, *The automorphism group of a finite metacyclic p-group*, Proc. Amer. Math. Soc. **25** (1970), 876–879.

[12] N.M. Dunfield and W.P. Thurston, *Finite covers of random 3-manifolds*, Invent. Math. **166** (2006), no. 3, 457–521.

[13] M. du Sautoy, *Zeta functions and counting finite p-groups*, Electron. Res. Announc. Amer. Math. Soc. **5** (1999), 112–122.

[14] M. du Sautoy, *Counting p-groups and nilpotent groups*, Inst. Hautes Études Sci. Publ. Math. **92** (2000),63–112.

[15] B. Eick and C.R. Leedham-Green, *On the classification of prime-power groups by coclass*, Bull. Lond. Math. Soc. **40** (2008), no. 2, 274–288.

[16] J.-M. Fontaine and B. Mazur, *Geometric Galois representations*, Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993), 41–78, Ser. Number Theory, I, Int. Press, Cambridge, MA, 1995.

[17] E. Ghys, *Groupes aléatoires (d'après Misha Gromov, ...)*, Astérisque **294** (2004), viii, 173–204.

[18] W.T. Gowers, *Quasirandom groups*, Combin. Probab. Comput. **17** (2008), no. 3, 363–387.

[19] C.J. Hillar and D.L. Rhea, *Automorphisms of finite abelian groups*, Amer. Math. Monthly, **114** (2007), no. 10, 917–923.

[20] H. Koch, *Galois theory of p-extensions*, with a foreword by I.R. Shafarevich, translated from the 1970 German original by Franz Lemmermeyer with a postscript by the author and Lemmermeyer, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002, xiv+190 pp.

[21] J. Labute, *Mild pro-p-groups and Galois groups of p-extensions of $\mathbb{Q}$*, J. reine Angew. Math. **596** (2006), 155–182.

[22] C.R. Leedham-Green and S. McKay, *The structure of groups of prime power order*, London Mathematical Society Monographs, New Series, 27, Oxford Science Publications, Oxford University Press, Oxford, 2002, xii+334 pp.

[23] A. Mann, *Positively finitely generated groups*, Forum Math. **8** (1996), no. 4, 429–459.

[24] D. Matei and A.I. Suciu, *Hall invariants, homology of subgroups, and characteristic varieties*, Int. Math. Res. Not. **9** (2002), 465–503.

[25] M.F. Newman and E.A. O'Brien, *Classifying 2-groups by coclass*, Trans. Amer. Math. Soc. **351** (1999), no. 1, 131–169.

[26] E.A. O'Brien, *The p-group generation algorithm*, J. Symbolic Comput. **9** (1990), no. 5-6, 677–698.

[27] E.A. O'Brien, private communication (2008).

[28] E.A. O'Brien and M.R. Vaughan-Lee, *The groups with order p^7 for odd prime p*, J. Algebra **292** (2005), no. 1, 243–258.

N. BOSTON, SCHOOL OF MATHEMATICAL SCIENCES, U. COLLEGE DUBLIN, DUBLIN 4, IRELAND.
boston@math.wisc.edu