Algebra & Number Theory

Volume 19
2025
No. 5

Malle's conjecture for fair counting functions

Peter Koymans and Carlo Pagano

msp

ALGEBRA AND NUMBER THEORY 19:5 (2025)
https://doi.org/10.2140/ant.2025.19.1007

msp

Malle's conjecture for fair counting functions

Peter Koymans and Carlo Pagano

We show that the naive adaptation of Malle's conjecture to fair counting functions is not true in general.

1. Introduction

1.1. ***Malle's conjecture.*** Number field counting has a rich history in number theory, going back to at least Gauss counting quadratic extensions of $\mathbb{Q}$. The leading conjecture in this field is due to Malle.

Conjecture 1.1 [Malle 2004]. *Let G be a nontrivial finite group and let k be a number field. Then there exists an integer $a(G) \geq 1$, an integer $b(G,k) \geq 0$ and a real number $c(G,k) > 0$ with*

$$|\{K/k : \mathrm{Gal}(K/k) \cong G, N_{k/\mathbb{Q}}(\mathrm{Disc}(K/k)) \leq X\}| \sim c(G,k)X^{1/a(G)}(\log X)^{b(G,k)}. \tag{1-1}$$

If we let $\mathrm{Cl}(g)$ be the conjugacy class of an element $g \in G - \{\mathrm{id}\}$ and if we write $g \sim h$ if $\mathrm{Cl}(g)$ and $\mathrm{Cl}(h)$ are equivalent under the cyclotomic action of k, then we have

$$b(G,k) = -1 + n, \tag{1-2}$$

where n is the number of equivalence classes of $G - \{\mathrm{id}\}$ under $\sim$ consisting entirely of elements with minimal order in G.

Although this conjecture has been exceptionally influential, numerous issues have come to light. One problem with Malle's conjecture is that it is not correct with the first counterexample due to Klüners [2005]. However, there are also other undesirable features that are inherently tied with counting by discriminant that we will now discuss.

One desirable feature of a counting function is that the leading constant $c(G,k)$ is an Euler product. This type of leading constants are frequent in rational points counting, and suggest a good compatibility between global and local behavior. In the case of S_n, the leading constant $c(G,k)$ is conjectured to be an Euler product [Bhargava 2007], in which case we say that the *Malle–Bhargava* principle holds. It is however not always the case that the leading constant is an Euler product. This problem already manifests itself when dealing with quartic D_4-extensions, see the work of Cohen, Diaz, y Diaz and Olivier [Cohen et al. 2002] and of Altuğ, Shankar, Varma and Wilson [Altuğ et al. 2021]. In general, it is still unclear when we expect the Malle–Bhargava principle to hold true.

MSC2020: primary 11N45, 11R45; secondary 11R21, 11R29.
Keywords: Malle's conjecture, number fields.

Another related undesirable feature of discriminant counting is the *subfield problem*. When counting by discriminant, it may happen that a positive proportion of the fields counted share a common subfield. This already happens for quartic D_4-extensions, and is the main underlying cause for the failure of the leading constant to be an Euler product.

1.2. ***Fair counting functions.*** The above reasons have led to an increasing interest in *fair counting functions*, first introduced by Wood [2010]. We shall restrict ourselves to the product of ramified primes, which is the most prominent fair counting function. We consider the following naive modification of Malle's conjecture. Write $\mathfrak{f}(K/k)$ for the product of primes of k that ramify in K.

Conjecture 1.2 (folklore adaptation of Malle's conjecture). *Let G be a nontrivial finite group and let k be a number field. Then there exists an integer $b(G,k) \geq 0$ and a real number $c(G,k) > 0$ such that*

$$|\{K/k : \mathrm{Gal}(K/k) \cong G, N_{k/\mathbb{Q}}(\mathfrak{f}(K/k)) \leq X\}| \sim c(G,k) X (\log X)^{b(G,k)}. \tag{1-3}$$

If we let $\mathrm{Cl}(g)$ *be the conjugacy class of an element $g \in G - \{\mathrm{id}\}$ and if we write $g \sim h$ if* $\mathrm{Cl}(g)$ *and* $\mathrm{Cl}(h)$ *are equivalent under the cyclotomic action of k, then we have*

$$b(G,k) = -1 + n, \tag{1-4}$$

where n is the number of equivalence classes of $G - \{\mathrm{id}\}$ under $\sim$.

Maki [1993] proved this conjecture for abelian extensions, and Wood [2010] proved the same for any fair counting function and arbitrary finite sets of local conditions. It is important to emphasize that the leading constant $c(G,k)$ is an Euler product and that the subfield problem also disappears in all known cases. An additional benefit is that this counting function is much more natural from a geometric perspective occurring prominently in function field counting, which is rife with geometric techniques.

Number field counting is intimately related to finding the distribution of class groups. Counting by discriminant also leads to problems in this setting, as first uncovered in [Bartel and Lenstra 2020]. Bartel and Lenstra give a counterexample to the Cohen–Martinet heuristics with the root cause being precisely the subfield problem. These reasons strongly suggests that it may be preferable to count by fair counting functions instead of the discriminant.

1.3. ***Results and conjectures.*** Our main result shows that Conjecture 1.2 is not correct.

Theorem 1.3. *There exists an infinite family of nilpotent groups G of nilpotency class 2 such that Conjecture 1.2 fails for the pair $(G, \mathbb{Q})$. More precisely, the constant $b(G,\mathbb{Q})$ in* (1-4) *is too small.*

Although we have restricted to $\mathbb{Q}$ for simplicity, it is not difficult to adapt our arguments to find many more counterexamples of a similar flavor showing that the above phenomenon persists in a wide number of settings.

Our counterexample is of a genuinely different nature than Klüners' counterexample. Firstly, Klüners takes $G = C_3 \wr C_2$, which is solvable but not nilpotent. Secondly, Klüners' counterexample is no longer a counterexample when counting by product of ramified primes, which was historically another important

motivation to count by ramified primes. In fact, Koymans and Pagano [2023, Section 3.2] have previously given strong heuristic evidence that Malle's original conjecture, see Conjecture 1.1, is correct for nilpotent extensions. Thirdly and perhaps most importantly, although both counterexamples proceed by fixing a cyclotomic subextension, Klüners' counterexample relies on the shrinking of the cyclotomic action, while we fundamentally rely on a certain *entanglement of Frobenius* that shrinks the conjugation action.

A novel feature of our work is the first family of counterexamples when counting G-extensions in their regular representation. This phenomenon has never been observed for discriminant counting. All known modifications of Malle's conjecture (such as [Türkelli 2015]) predict no counterexamples when counting G-extensions by discriminant in their regular representation.

We still expect the veracity of the asymptotic in (1-3), but of course not with the naive choice of $b(G, \mathbb{Q})$ from (1-4). It is at present unclear what the right choice of $b(G, \mathbb{Q})$ is in general. We will however make several predictions. We have opted to restrict ourselves to nilpotent extensions as even merely making predictions for number field counting has proven to be a deceptively difficult task.

To this end, let $\phi : G \twoheadrightarrow H$ be a surjective homomorphism, let $\chi(\mathrm{cyc}) : G_{\mathbb{Q}} \to (\mathbb{Z}/|G|\mathbb{Z})^*$ be the cyclotomic character and let $r : (\mathbb{Z}/|G|\mathbb{Z})^* \twoheadrightarrow H$ be a surjection. We define

$$\mathrm{Epi}_{(H,\phi)}(G_{\mathbb{Q}}, G)$$

be the set of continuous surjective homomorphisms $\psi : G_{\mathbb{Q}} \twoheadrightarrow G$ satisfying the equations

$$\phi \circ \psi = r \circ \chi(\mathrm{cyc}), \quad \mathbb{Q}(\psi) \cap \mathbb{Q}(\zeta_{|G|}) = \mathbb{Q}(\phi \circ \psi).$$

We write $G \times_H (\mathbb{Z}/|G|\mathbb{Z})^* \subseteq G \times (\mathbb{Z}/|G|\mathbb{Z})^*$ for the subgroup consisting of pairs (g, α) such that $\phi(g) = r(\alpha)$. We let $G \times (\mathbb{Z}/|G|\mathbb{Z})^*$ act on $\ker(\phi) - \{\mathrm{id}\}$ by sending n to $gn^{\alpha}g^{-1}$. We restrict this action to the subgroup $G \times_H (\mathbb{Z}/|G|\mathbb{Z})^*$, and we denote by

$$b_{(H,\phi)}(G) := |(\ker(\phi) - \{\mathrm{id}\})/(G \times_H (\mathbb{Z}/|G|\mathbb{Z})^*)|$$

the resulting number of equivalence classes.

Conjecture 1.4 (Conjecture 5.1). *Let G be a nilpotent group. For each H, ϕ as above, there exists a positive constant $c_{(H,\phi)}(G)$ such that*

$$|\{\psi \in \mathrm{Epi}_{(H,\phi)}(G_{\mathbb{Q}}, G) : \mathfrak{f}(\psi) \leq X\}| \sim c_{(H,\phi)}(G) \cdot X \cdot \log(X)^{b_{(H,\phi)}(G)-1}.$$

Conjecture 1.5 (Conjecture 5.5). *Let G be a nilpotent group with $|G|$ odd. Then the leading constant $c_{(H,\phi)}(G)$ satisfies the Malle–Bhargava principle.*

For the precise computation of the leading constant provided by the Malle–Bhargava principle, we refer to Conjecture 5.5. It is tempting to speculate that both conjectures are true in a much wider generality, which we shall leave as an open question. However, Conjecture 5.5 does not hold when $|G|$ is even, in which case a rational correction factor is needed.

We will now explicate Theorem 1.3, in particular the construction of the infinite family G. We take $Q_n = \mathbb{Z}/3\mathbb{Z} \oplus (\mathbb{Z}/9\mathbb{Z})^n$. We let $\pi_0 : Q_n \to \mathbb{Z}/3\mathbb{Z}$ be the projection on the first $\mathbb{Z}/3\mathbb{Z}$ and we let $\pi_i : Q_n \to \mathbb{Z}/3\mathbb{Z}$ be the projection on the i-th $\mathbb{Z}/9\mathbb{Z}$ composed with the quotient map $\mathbb{Z}/9\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$. We introduce the 2-cocycles

$$\theta_i(\sigma, \tau) := \pi_0(\sigma) \cdot \pi_i(\tau) \in H^2(Q_n, \mathbb{Z}/3\mathbb{Z})$$

and $\theta := (\theta_1, \dots, \theta_n) \in H^2(Q_n, (\mathbb{Z}/3\mathbb{Z})^n)$. Given such a θ, we have a corresponding central exact sequence given by

$$1 \to (\mathbb{Z}/3\mathbb{Z})^n \to G_n \to Q_n \to 1.$$

In our proofs, we will choose the family $(G_n)_{n\geq 2}$ for the infinite family of Theorem 1.3. In the process we will also prove a special case of Conjectures 1.4 and 1.5.

Theorem 1.6 (Theorem 3.4). *Let G_n be as above and write $q_n : G_n \to Q_n$ for the natural quotient map. Let $H_n := \mathbb{Z}/3\mathbb{Z}$ and let $\phi := \pi_0 \circ q_n$. Let $\rho : G_{\mathbb{Q}} \to \mathbb{Z}/3\mathbb{Z}$ be any character such that the fixed field of the kernel equals $\mathbb{Q}(\zeta_9 + \zeta_9^{-1})$. Then we have*

$$\sum_{\substack{\psi \in \mathrm{Epi}(G_{\mathbb{Q}}, G_n) \\ \pi_0 \circ q_n \circ \psi = \rho \\ \mathfrak{f}(\psi) \leq X}} 1 \sim 27^n \cdot \frac{X \cdot (\log X)^{\alpha - 1}}{3 \cdot \Gamma(\alpha)} \cdot c_0,$$

where $\alpha := (9^n - 1)/3 + (27^n - 1)/6$ and c_0 equals the conditionally convergent Euler product

$$c_0 := \prod_p \left(1 + \frac{(9^n - 1)\mathbf{1}_{p \equiv 4,7 \bmod 9} + (27^n - 1)\mathbf{1}_{p \equiv 1 \bmod 9}}{p}\right)\left(1 - \frac{1}{p}\right)^{\alpha}.$$

One pleasant feature is that $\ker(\phi) \cong (\mathbb{Z}/9\mathbb{Z})^n \oplus (\mathbb{Z}/3\mathbb{Z})^n$ is abelian despite the fact that G_n is not. It is no coincidence that the logarithmic exponent matches exactly the logarithmic exponent when counting $(\mathbb{Z}/9\mathbb{Z})^n \oplus (\mathbb{Z}/3\mathbb{Z})^n$-extensions. In fact, once one fixes the subextension $\mathbb{Q}(\zeta_9 + \zeta_9^{-1})$, we have the remarkable property that any $G_n/[G_n, G_n]$-extension lifts to a G_n-extension. This is the crux of our counterexample stemming from Lemma 2.1. Once we have proven Theorem 1.6 in Section 3, the computation of $b(G_n, \mathbb{Q})$ in Section 4 immediately gives Theorem 1.3.

In fact, it is plausible that one can use [Alberts and O'Dorney 2021, Theorem 1.1] or [Darda and Yasuda 2023, Theorem 1.3.3] to prove Conjectures 1.4 and 1.5 as soon as $\ker(\phi)$ is abelian, with substantial work required to deduce explicitly from those works the leading constant c_0 and the logarithmic exponent α. We have opted to give a different proof to keep our work completely self-contained.

We remark that if H and ϕ are trivial, then $b_{(H,\phi)}(G)$ equals the right-hand side of (1-4). In particular, we predict that the full Malle–Bhargava principle holds when counting tame, nilpotent G-extensions with $|G|$ odd. We emphasize that, once one accounts for the counterexamples found in Theorem 1.3, all good properties of fair counting functions are restored again: the leading constant is an Euler product and the subfield problem disappears.

1.4. ***Comparison with previous results and conjectures.*** Malle's original conjecture has been proven over $\mathbb{Q}$ for a handful of specific groups namely for:

- Cubic S_3-extensions [Davenport and Heilbronn 1971].
- Quartic S_4-extensions and quintic S_5-extensions [Bhargava 2005; 2010].
- Sextic S_3-extensions [Belabas and Fouvry 2010; Bhargava and Wood 2008].
- Abelian extensions [Wright 1989].
- Direct products $G \times A$ with $G \in \{S_3, S_4, S_5\}$ and A abelian [Masri et al. 2020], building on the earlier work [Wang 2021].
- Quartic D_4-extensions [Cohen et al. 2002].
- Nonic Heisenberg extensions [Fouvry and Koymans 2021].
- Certain wreath products [Klüners 2012].
- Nilpotent groups such that all minimal order elements are central [Koymans and Pagano 2023].

In many situations we have upper and lower bounds for number field counting instead of asymptotics. This comprises a vast literature as well, including work of Alberts [2021], Klüners and Malle [2004], Ellenberg and Venkatesh [2006], Couveignes [2020] and Lemke Oliver and Thorne [2022].

Of particular relevance to our work is the recent spur of other modifications of Malle's conjecture. This was initiated by Türkelli [2015] for discriminant counting, who modified Conjecture 1.1 to account for Klüners' counterexample. Our prediction for $b_{(H,\phi)}(G)$ is a direct parallel of Türkelli's modification.

Gundlach [2022, Conjecture 1.5] proposed a variant of Malle's conjecture where one counts by multiple fair invariants. He avoids our counterexamples by demanding that this invariant lies in the range $(\delta X, X)$ for some $\delta > 0$. Our conjecture however does not impose this condition, which necessitates a more thorough treatment of the logarithmic exponent $b_{(H,\phi)}(G)$.

Darda and Yasuda [2023, Conjecture 1.3.1] propose a far reaching conjecture for counting points on stacks by a wide class of height functions. Their conjecture is similar in spirit than ours but substantially less precise: our conjecture is more precise under what circumstances the logarithmic exponent may increase and also more precise about the leading constant; with no prediction being made in [loc. cit.]. We remark that none of the aforementioned works [Darda and Yasuda 2023; Gundlach 2022; Türkelli 2015] make a prediction about the leading constant $c_{(H,\phi)}(G)$.

1.5. ***Overview of the paper.*** The key result for our counterexample is Lemma 2.1. This lemma shows that the group G_n has the key property that all $G_n/[G_n, G_n]$-extensions lift to a G_n-extension once one fixes a suitable cyclotomic subextension. We will exploit Lemma 2.1 to show in Section 3 that the count of $\psi \in \mathrm{Hom}(G_{\mathbb{Q}}, G_n)$, containing this suitably constructed cyclotomic subextension, equals the number of abelian $(\mathbb{Z}/9\mathbb{Z})^n \oplus (\mathbb{Z}/3\mathbb{Z})^n$-extensions. In Section 4 we will compute the naive Malle constant $b(G_n, \mathbb{Q})$. These results immediately give Theorem 1.3. In our final Section 5 we motivate Conjectures 1.4 and 1.5.

2. The construction

We fix in the rest of the paper an algebraic closure $\mathbb{Q}^{\mathrm{sep}}$ of $\mathbb{Q}$ and for each place v an algebraic closure $\mathbb{Q}_v^{\mathrm{sep}}$ of $\mathbb{Q}_v$. We furthermore fix an embedding

$$i_v : \mathbb{Q}^{\mathrm{sep}} \to \mathbb{Q}_v^{\mathrm{sep}},$$

providing us with an embedding

$$i_v^* : G_{\mathbb{Q}_v} \to G_{\mathbb{Q}}.$$

We denote by $\mathcal{G}(3)$ the pro-3 completion of a profinite group $\mathcal{G}$. We fix a choice of the cyclotomic character

$$\chi_{\mathrm{cyc}}(3) : G_{\mathbb{Q}} \twoheadrightarrow \mathbb{Z}_3.$$

For each prime number p congruent to 1 modulo 3, we fix an element $\sigma_p' \in G_{\mathbb{Q}_p}$ such that its image in $G_{\mathbb{Q}_p}(3)$ is a topological generator of the inertia subgroup. We denote by σ_p the image of σ_p' in $G_{\mathbb{Q}}(3)$ by applying i_p^* followed by the natural projection map $G_{\mathbb{Q}} \to G_{\mathbb{Q}}(3)$. We fix any element σ_3 of $G_{\mathbb{Q}}(3)$ with $\chi_{\mathrm{cyc}}(3)(\sigma_3) = 1$ and coming from the inertia subgroup of $G_{\mathbb{Q}_3}$ in the manner just described above.

We define

$$\mathfrak{G} := \{\sigma_p : p \equiv 1 \bmod 3\} \cup \{\sigma_3\} \subseteq G_{\mathbb{Q}}(3).$$

For each p congruent to 1 modulo 3, we put $\chi_p : G_{\mathbb{Q}} \to \mathbb{Z}/3\mathbb{Z}$ to be the unique character which ramifies only at p and with $\chi_p(\sigma_p) = 1$. We define χ_3 to be the reduction modulo 3 of $\chi_{\mathrm{cyc}}(3)$. Furthermore, for each p congruent to 1 modulo 9, we put $\psi_p : G_{\mathbb{Q}} \to \mathbb{Z}/9\mathbb{Z}$ to be the unique character which ramifies only at p and with $\psi_p(\sigma_p) = 1$. We set ψ_3 to be the reduction modulo 9 of $\chi_{\mathrm{cyc}}(3)$. Then the set

$$\{\chi_p : p \equiv 0, 1 \bmod 3\}$$

is a basis for $\mathrm{Hom}(G_{\mathbb{Q}}(3), \mathbb{Z}/3\mathbb{Z})$, which is dual to $\mathfrak{G}$. It follows that $\mathfrak{G}$ is a minimal set of topological generators for $G_{\mathbb{Q}}(3)$.

For a continuous homomorphism $\psi : G_{\mathbb{Q}} \to \mathcal{G}$, where $\mathcal{G}$ is a profinite group, we define

$$\mathbb{Q}(\psi) := (\mathbb{Q}^{\mathrm{sep}})^{\ker(\psi)}.$$

In the case $\mathcal{G}$ is a finite group, we denote by $\mathfrak{f}(\psi)$ the product of the finite rational primes ramifying in $\mathbb{Q}(\psi)/\mathbb{Q}$. Likewise, for $\psi : G_{\mathbb{Q}_p} \to \mathcal{G}$, we define $\mathfrak{f}(\psi)$ to be p in the case ψ is ramified and 1 in the case ψ is unramified.

Consider $Q_n = \mathbb{Z}/3\mathbb{Z} \oplus (\mathbb{Z}/9\mathbb{Z})^n$. Write $\pi_0 : Q_n \to \mathbb{Z}/3\mathbb{Z}$ for the projection on the first $\mathbb{Z}/3\mathbb{Z}$ and write $\pi_i : Q_n \to \mathbb{Z}/3\mathbb{Z}$ for the projection on the i-th $\mathbb{Z}/9\mathbb{Z}$ followed by the quotient map $\mathbb{Z}/9\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$. We define

$$\theta_i(\sigma, \tau) := \pi_0(\sigma) \cdot \pi_i(\tau) \in H^2(Q_n, \mathbb{Z}/3\mathbb{Z})$$

and $\theta := (\theta_1, \ldots, \theta_n) \in H^2(Q_n, (\mathbb{Z}/3\mathbb{Z})^n)$. Given such a θ, we may attach a central extension

$$1 \to (\mathbb{Z}/3\mathbb{Z})^n \to G_n \to Q_n \to 1.$$

We will show, for sufficiently large n, that G_n is a counterexample.

From now on we will consider all our abelian groups as discrete $G_{\mathbb{Q}}$-modules with trivial action. Given $\phi \in \mathrm{Hom}(G_{\mathbb{Q}}, Q_n)$, we write $\theta_{i,\phi} \in H^2(G_{\mathbb{Q}}, \mathbb{Z}/3\mathbb{Z})$ and $\theta_\phi \in H^2(G_{\mathbb{Q}}, (\mathbb{Z}/3\mathbb{Z})^n)$ for the inflation of θ_i and θ to $G_{\mathbb{Q}}$ using ϕ. The following lemma is the crux of the counterexample. Informally speaking, it shows that any homomorphism $\phi : G_{\mathbb{Q}} \to Q_n$ satisfying $\pi_0 \circ \phi \in \{\chi_3, 2\chi_3\}$, i.e., $\mathbb{Q}(\pi_0 \circ \phi) = \mathbb{Q}(\zeta_9 + \zeta_9^{-1})$, lifts to G_n. This will be the source of the abundance of G_n-extensions.

Lemma 2.1. *Let $\phi \in \mathrm{Hom}(G_{\mathbb{Q}}, Q_n)$ be such that $\mathbb{Q}(\pi_0 \circ \phi) = \mathbb{Q}(\zeta_9 + \zeta_9^{-1})$. Then there exists a homomorphism $\psi : G_{\mathbb{Q}} \to G_n$ lifting ϕ.*

Proof. Note that G_n is isomorphic to $(\mathbb{Z}/3\mathbb{Z})^n \times_\theta Q_n$, where multiplication is given by

$$(c_1, a_1) *_\theta (c_2, a_2) = (c_1 + c_2 + \theta(a_1, a_2), a_1 + a_2).$$

Any lift $\psi : G_{\mathbb{Q}} \to G_n$ of ϕ is of the shape (ψ', ϕ) for some map $\psi' : G_{\mathbb{Q}} \to (\mathbb{Z}/3\mathbb{Z})^n$. Imposing that ψ is a homomorphism means precisely that θ_ϕ is trivial in $H^2(G_{\mathbb{Q}}, (\mathbb{Z}/3\mathbb{Z})^n)$, which is the case if and only if each $\theta_{i,\phi}$ is trivial in $H^2(G_{\mathbb{Q}}, \mathbb{Z}/3\mathbb{Z})$.

Therefore it suffices to show that $\theta_{i,\phi}$ is trivial in $H^2(G_{\mathbb{Q}}, \mathbb{Z}/3\mathbb{Z})$ for each i. By class field theory we have an injection

$$H^2(G_{\mathbb{Q}}, \mathbb{Z}/3\mathbb{Z}) \to \bigoplus_v H^2(G_{\mathbb{Q}_v}, \mathbb{Z}/3\mathbb{Z}).$$

Now let v be a place of $\mathbb{Q}$. We will check that the restriction of $\theta_{i,\phi}$ is trivial at v. If v is real, then $H^2(G_{\mathbb{Q}_v}, \mathbb{Z}/3\mathbb{Z}) = 0$. If $v = (3)$, then we also have $H^2(G_{\mathbb{Q}_v}, \mathbb{Z}/3\mathbb{Z}) = 0$ by a well-known result of Shafarevich. Using local Tate duality as in [Neukirch et al. 2000, Theorem 7.2.6], Shafarevich's result follows immediately from $H^2(G_{\mathbb{Q}_3}, \mathbb{Z}/3\mathbb{Z}) \cong H^0(G_{\mathbb{Q}_3}, \mu_3) = 0$.

We define K_i to be the fixed field of $\pi_{0,i} \circ \phi$, where $\pi_{0,i} : Q_n \to (\mathbb{Z}/3\mathbb{Z})^2$ is the homomorphism given by

$$\pi_{0,i}(a) = (\pi_0(a), \pi_i(a)).$$

If v is unramified in K_i, then the restriction of $\theta_{i,\phi}$ to $G_{\mathbb{Q}_v}$ factors through the maximal unramified extension of $\mathbb{Q}_v$, therefore giving a class in $H^2(\hat{\mathbb{Z}}, \mathbb{Z}/3\mathbb{Z}) = 0$.

It remains to treat finite places v, coprime to 3, that are ramified in K_i. Recall that $\theta_{i,\phi}$ is the class of the 2-cochain $c(\sigma, \tau)$ given by

$$(\sigma, \tau) \mapsto \pi_0(\phi(\sigma)) \cdot \pi_i(\phi(\tau)).$$

We claim that $\pi_0(\phi(\sigma))$ is the zero map when restricted to $G_{\mathbb{Q}_v}$. This implies that $c(\sigma, \tau)$ is also the zero map when restricted to $G_{\mathbb{Q}_v}$. In particular, $\theta_{i,\phi}$ is trivial in $H^2(G_{\mathbb{Q}_v}, \mathbb{Z}/3\mathbb{Z})$, and thus the lemma is a consequence of the claim.

In order to prove the claim, observe that our assumptions imply that v ramifies in $\pi_i \circ \phi$ but not in $\pi_0 \circ \phi = \rho$, which is ramified only at 3. Since $v \neq (3)$ and since $\pi_i \circ \phi$ lifts to a $\mathbb{Z}/9\mathbb{Z}$-extension, class field theory over $\mathbb{Q}$ shows that $v \equiv 1 \bmod 9$. But then v splits completely in $\mathbb{Q}(\zeta_9 + \zeta_9^{-1})$, which gives the claim. □

3. Finding many lifts

Call $q_n : G_n \to Q_n$ the natural quotient map.

Definition 3.1. We define $\mathcal{G}_{n,\mathrm{bad}}$ to be the set of tuples $(v_g)_{g \in G_n - \{\mathrm{id}\}}$ satisfying the following conditions:

- v_g is a positive squarefree integer for every $g \in G_n - \{\mathrm{id}\}$.
- v_g and v_h are coprime for every $g, h \in G_n - \{\mathrm{id}\}$ with $g \neq h$.
- If $p \mid v_g$ for some $g \in G_n - \{\mathrm{id}\}$ satisfying $\pi_0(q_n(g)) = 0$, then $p \equiv 1 \bmod \mathrm{ord}(g)$.
- We have
$$\prod_{\substack{g \in G_n - \{\mathrm{id}\} \\ \pi_0(q_n(g)) \neq 0}} v_g = 3.$$

Lemma 3.2. *Let $g \in G_n$ and suppose that $q_n(g) \neq 0$. Then* $\mathrm{ord}(g) = \mathrm{ord}(q_n(g))$.

Proof. Write $G_n = (\mathbb{Z}/3\mathbb{Z})^n \times_\theta Q_n$, write $g = (c, q_n(g))$ and write $m = \mathrm{ord}(q_n(g))$. Then a calculation using the group law on G_n given by θ shows that

$$g^m = \left(\sum_{j=1}^{m-1} \theta(q_n(g), q_n(g)^j), 0 \right).$$

Now observe that

$$\sum_{j=1}^{m-1} \theta(q_n(g), q_n(g)^j) = \left(\sum_{j=1}^{m-1} \pi_0(q_n(g)) \cdot \pi_1(q_n(g)^j), \ldots, \sum_{j=1}^{m-1} \pi_0(q_n(g)) \cdot \pi_n(q_n(g)^j) \right).$$

Since we have $\sum_{j=1}^{m-1} \pi_i(q_n(g)^j) = \pi_i(q_n(g)) \sum_{j=1}^{m-1} j = 0$, the lemma follows. □

Following the Koymans–Pagano parametrization technique [Koymans and Pagano 2023] yields the following key result. For the convenience of the reader we give a direct proof of this special case from scratch.

Theorem 3.3. *There is a bijection* Par *between $\mathcal{G}_{n,\mathrm{bad}}$ and the subset of $\psi \in \mathrm{Hom}(G_{\mathbb{Q}}, G_n)$ such that $\mathbb{Q}(\pi_0 \circ q_n \circ \psi) = \mathbb{Q}(\zeta_9 + \zeta_9^{-1})$. Writing $\mathfrak{f}(\psi)$ for the product of ramified primes of a homomorphism ψ, we have*

$$\mathfrak{f}(\mathrm{Par}((v_g)_{g \in G_n - \{\mathrm{id}\}})) = \prod_{g \in G_n - \{\mathrm{id}\}} v_g. \tag{3-1}$$

Furthermore, the homomorphism $\mathrm{Par}((v_g)_{g \in G_n - \{\mathrm{id}\}}) : G_{\mathbb{Q}} \to G_n$ *is surjective if and only if*

$$\langle q_n(\{g \in G_n - \{\mathrm{id}\} : v_g \neq 1\}) \rangle = Q_n. \tag{3-2}$$

Proof. Let us define $\mathrm{Hom}_{n,\mathrm{bad}}$ to be the set of continuous homomorphisms $\psi : G_{\mathbb{Q}}(3) \to G_n$ with the property that

$$\mathbb{Q}(\pi_0 \circ q_n \circ \psi) = \mathbb{Q}(\zeta_9 + \zeta_9^{-1}).$$

We begin by constructing a map $\mathrm{Ev} : \mathrm{Hom}_{n,\mathrm{bad}} \to \mathcal{G}_{n,\mathrm{bad}}$ in the following manner. Given $\psi \in \mathrm{Hom}_{n,\mathrm{bad}}$, we consider the vector

$$(v_g)_{g \in G_n - \{\mathrm{id}\}}$$

consisting of positive squarefree numbers divisible only by primes congruent to 0, 1 modulo 3 uniquely defined through the property

$$p \mid v_g \quad \Longleftrightarrow \quad \psi(\sigma_p) = g.$$

Let us check that Ev indeed maps $\mathrm{Hom}_{n,\mathrm{bad}}$ to $\mathcal{G}_{n,\mathrm{bad}}$. Since ψ is a function, it follows that the vector $(v_g)_{g \in G_n - \{\mathrm{id}\}}$ consists of pairwise coprime squarefree integers by construction. In other words, the first two points of Definition 3.1 are taken care of. Let us verify the third point and distinguish for that purpose two cases. Suppose first that $q_n(g) = 0$. Then $\mathrm{ord}(g) = 3$, so that the condition becomes $p \equiv 1 \bmod 3$, which is automatically satisfied as primes $p \equiv 2 \bmod 3$ are unramified in 3-extensions. Suppose now that $q_n(g) \neq 0$. Then by Lemma 3.2 we know that $\mathrm{ord}(g) = \mathrm{ord}(q_n(g))$. Hence we need to show that $p \equiv 1 \bmod \mathrm{ord}(q_n(g))$. The map $q_n \circ \psi \circ i_p^*$ induces a continuous homomorphism

$$G_{\mathbb{Q}_p} \to G_{\mathbb{Q}_p}^{\mathrm{ab}} \to Q_n,$$

sending σ_p' to $q_n(g)$. But the order of the image of σ_p' in an abelian extension of $\mathbb{Q}_p$ is always a divisor of $p-1$ so that $p \equiv 1 \bmod \mathrm{ord}(q_n(g))$ as desired.

Let us now show that the vector $(v_g)_{g \in G_n - \{\mathrm{id}\}}$ satisfies the fourth point of Definition 3.1. Observe that for each prime $p \equiv 1 \bmod 3$ we have $\pi_0 \circ q_n \circ \psi(\sigma_p) \in \{\chi_3(\sigma_p), 2 \cdot \chi_3(\sigma_p)\} = \{0\}$. It follows that the variables v_g, with $\pi_0(q_n(g)) \neq 0$, are all equal to 1 or 3. Since we have shown that they are pairwise coprime, at most one of them equals 3, namely $\psi(\sigma_3)$. This gives the desired fourth point of Definition 3.1.

We will now show that (3-1) holds. Indeed, 3 is certainly both a divisor of $\mathfrak{f}(\psi)$ and $\prod_{g \in G_n - \{\mathrm{id}\}} v_g$, since the extension ramifies at 3 and we have just verified the fourth bullet point of Definition 3.1. For a prime $p \equiv 1 \bmod 3$, we have that the ramification index of $\mathbb{Q}^{\ker(\psi)}/\mathbb{Q}$ at p equals precisely the order of $\psi(\sigma_p)$. Primes congruent to 2 modulo 3 are always unramified in a 3-extension.

We now observe that $\mathrm{Ev}(\psi)$ determines the value of ψ on $\mathfrak{G}$, which is a set of topological generators, and therefore $\mathrm{Ev}(\psi)$ determines ψ. In other words, the map Ev is injective. Furthermore, the fact that $\mathfrak{G}$ is a set of topological generators gives at once that

$$\mathrm{im}(\psi) := \langle \psi(\mathfrak{G}) \rangle = \langle \{g \in G_n - \{\mathrm{id}\} : v_g \neq 1\} \rangle.$$

In particular, ψ is surjective if and only if $G_n = \langle \{g \in G_n - \{\mathrm{id}\} : v_g \neq 1\} \rangle$. Recall that a set generates a nilpotent group if and only if it generates the abelianization. Then the elementary observation that Q_n is the abelianization of G_n yields (3-2).

We are only left with showing that Ev is surjective. We will proceed in 3 steps. Let $(v_g)_{g \in G_n - \{\mathrm{id}\}}$ be in $\mathcal{G}_{n,\mathrm{bad}}$:

Step 1: Define $\psi^{\mathrm{ab}} := (\psi_i^{\mathrm{ab}})_{i=0}^n : G_{\mathbb{Q}} \to Q_n$ using the formula

$$\psi_i^{\mathrm{ab}} := \begin{cases} \pi_0(q_n(g_0)) \cdot \chi_3 & \text{for } i = 0, \\ \sum_{g \in G_n - \{\mathrm{id}\}} \sum_{p \mid v_g} \mu_i(g) \cdot \psi_p & \text{for } 1 \leq i \leq n, \end{cases}$$

where g_0 is the unique element of $G_n - \{\mathrm{id}\}$ with $v_{g_0} = 3$, where $\mu_i : G_n \to Q_n \to \mathbb{Z}/9\mathbb{Z}$ is the projection map, where ψ_p is defined in Section 2 and where $\cdot$ denotes the usual multiplication in $\mathbb{Z}/3\mathbb{Z}$, respectively $\mathbb{Z}/9\mathbb{Z}$.

Step 2: We have $\pi_0 \circ \psi^{\mathrm{ab}} = \pi_0(q_n(g_0)) \cdot \chi_3$ by construction. Therefore we have that ψ^{ab} can be lifted to a homomorphism $\psi : G_{\mathbb{Q}} \to G_n$ thanks to Lemma 2.1. The choice of such a lift consists precisely of the choice of a vector of continuous 1-cochains $(\phi_i)_{i=1}^n$ with each $\phi_i : G_{\mathbb{Q}} \to \mathbb{Z}/3\mathbb{Z}$ fulfilling the property

$$d\phi_i(\sigma, \tau) = \theta_i(\psi^{\mathrm{ab}}(\sigma), \psi^{\mathrm{ab}}(\tau)) = \theta_{i,\psi^{\mathrm{ab}}}(\sigma, \tau),$$

where $d\phi_i(\sigma, \tau) = \phi_i(\sigma\tau) - \phi_i(\sigma) - \phi_i(\tau)$. Indeed, such a vector completes the map ψ^{ab} into a set-theoretic map $((\phi_i)_{i=1}^n, \psi^{\mathrm{ab}}) : G_{\mathbb{Q}} \to G_n$, which is a group homomorphism precisely owing to the cocycle equation. Conversely, given a lift ψ, we have that $\phi_i := \rho_i \circ \psi$ provides the desired 1-cochains, where $\rho_i : G_n \to \mathbb{Z}/3\mathbb{Z}$ is the projection on the i-th $\mathbb{Z}/3\mathbb{Z}$ in $(\mathbb{Z}/3\mathbb{Z})^n \times_\theta Q_n$ (note that ρ_i is not a group homomorphism).

We next define

$$\phi_i(\mathrm{clean}) := \phi_i - \phi_i(\sigma_3) \cdot \chi_3 - \sum_{p \equiv 1 \bmod 3} \phi_i(\sigma_p) \cdot \chi_p,$$

which now vanishes at all the elements of $\mathfrak{G}$ (observe that the sum is finite, since ϕ_i vanishes on all but finitely many σ_p by continuity).

Step 3: We now define

$$\phi_i(\mathrm{twist}) := \phi_i(\mathrm{clean}) + \sum_{g \in G_n - \{\mathrm{id}\}} \rho_i(g) \cdot \sum_{p \mid v_g} \chi_p.$$

This gives us a homomorphism

$$\psi(\mathrm{twist}) := ((\phi_i(\mathrm{twist}))_{i=1}^n, \psi^{\mathrm{ab}}) : G_{\mathbb{Q}} \to G_n$$

satisfying by construction that $\psi(\mathrm{twist})(\sigma_p) = g$ if and only if $p \mid v_g$. Therefore

$$\mathrm{Ev}(\psi(\mathrm{twist})) = (v_g)_{g \in G_n - \{\mathrm{id}\}}.$$

This shows that the map Ev is also surjective. Putting $\mathrm{Par} := \mathrm{Ev}^{-1}$ finishes the proof. □

The properties (3-1) and (3-2) are the core features of the Koymans–Pagano parametrization method [Koymans and Pagano 2023]. Using [Granville and Koukoulopoulos 2019, Theorem 1], we get the following result.

Theorem 3.4. *We have*

$$\sum_{\substack{\psi\in\mathrm{Hom}(G_{\mathbb{Q}},G_n)\\ \pi_0\circ q_n\circ\psi\in\{\chi_3,2\chi_3\}\\ \mathfrak{f}(\psi)\le X}} 1\sim 2\cdot 27^n\cdot\frac{X\cdot(\log X)^{\alpha-1}}{3\cdot\Gamma(\alpha)}\cdot c_0,$$

where

$$\alpha:=\sum_{\substack{g\in G_n-\{\mathrm{id}\}\\ \pi_0(q_n(g))=0}}\frac{1}{\varphi(\mathrm{ord}(g))}=\frac{3^n-1}{2}+3^n\cdot\left(\frac{9^n-3^n}{6}+\frac{3^n-1}{2}\right)=\frac{9^n-1}{3}+\frac{27^n-1}{6}$$

and c_0 equals the conditionally convergent Euler product

$$c_0:=\prod_p\left(1+\frac{(9^n-1)\mathbf{1}_{p\equiv 4,7 \bmod 9}+(27^n-1)\mathbf{1}_{p\equiv 1 \bmod 9}}{p}\right)\left(1-\frac{1}{p}\right)^{\alpha}.$$

The same result is true if $\mathrm{Hom}(G_{\mathbb{Q}},G_n)$ *is replaced by* $\mathrm{Epi}(G_{\mathbb{Q}},G_n)$.

Proof. We will first prove the $\mathrm{Hom}(G_{\mathbb{Q}},G_n)$ case. By Theorem 3.3 we have

$$\sum_{\substack{\psi\in\mathrm{Hom}(G_{\mathbb{Q}},G_n)\\ \pi_0\circ q_n\circ\psi\in\{\chi_3,2\chi_3\}\\ \mathfrak{f}(\psi)\le X}}1=\sum_{\substack{(v_g)_{g\in G_n-\{\mathrm{id}\}}\in\mathcal{G}_{n,\mathrm{bad}}\\ \prod_{g\in G_n-\{\mathrm{id}\}}v_g\le X}}1.$$

Recall that

$$\prod_{\substack{g\in G_n-\{\mathrm{id}\}\\ \pi_0(q_n(g))\neq 0}}v_g=3.$$

Write T_n for the subset of $g\in G_n-\{\mathrm{id}\}$ with $\pi_0(q_n(g))=0$. Since there are $2\cdot 27^n$ elements $g\in G_n-\{\mathrm{id}\}$ with $\pi_0(q_n(g))\neq 0$, we obtain that

$$\sum_{\substack{(v_g)_{g\in G_n-\{\mathrm{id}\}}\in\mathcal{G}_{n,\mathrm{bad}}\\ \prod_{g\in G_n-\{\mathrm{id}\}}v_g\le X}}1=2\cdot 27^n\sum_{\substack{(v_g)_{g\in T_n}\\ \prod_{g\in T_n}v_g\le X/3\\ p\mid v_g\Rightarrow p\equiv 1 \bmod \mathrm{ord}(g)}}\mu^2\left(\prod_{g\in T_n}v_g\right).$$

Writing $m:=\prod_{g\in T_n}v_g$, this transforms the sum into

$$2\cdot 27^n\sum_{\substack{(v_g)_{g\in T_n}\\ \prod_{g\in T_n}v_g\le X/3\\ p\mid v_g\Rightarrow p\equiv 1 \bmod \mathrm{ord}(g)}}\mu^2\left(\prod_{g\in T_n}v_g\right)=2\cdot 27^n\sum_{m\le X/3}f(m),$$

where $f(m)$ is the multiplicative function supported on squarefree integers and given on primes by

$$f(p)=(9^n-1)\mathbf{1}_{p\equiv 4,7 \bmod 9}+(27^n-1)\mathbf{1}_{p\equiv 1 \bmod 9}$$

thanks to Lemma 3.2. The average of f on primes is equal to α, and the theorem now follows from [Granville and Koukoulopoulos 2019, Theorem 1].

To deal with $\mathrm{Epi}(G_{\mathbb{Q}}, G_n)$, let S be a subset of T_n and consider the subsum

$$N_1(X, S) := \sum_{\substack{(v_g)_{g\in T_n} \\ \prod_{g\in G_n-\{\mathrm{id}\}} v_g \leq X/3 \\ p \mid v_g \Rightarrow p\equiv 1 \bmod \mathrm{ord}(g) \\ v_g=1 \Longleftrightarrow g\in S}} \mu^2\Big(\prod_{g\in T_n} v_g\Big). \tag{3-3}$$

This dissects the original sum into $2^{|T_n|}$ subsums. Furthermore, S determines whether the resulting map will be surjective or not thanks to Theorem 3.3. Following the argument for the homomorphism case, one may use [Granville and Koukoulopoulos 2019, Theorem 1] to extract an asymptotic for sums of the shape

$$N_2(X, S) := \sum_{\substack{(v_g)_{g\in T_n} \\ \prod_{g\in G_n-\{\mathrm{id}\}} v_g \leq X/3 \\ p \mid v_g \Rightarrow p\equiv 1 \bmod \mathrm{ord}(g) \\ g\in S \Rightarrow v_g=1}} \mu^2\Big(\prod_{g\in T_n} v_g\Big)$$

for every subset S of T_n. By [loc. cit., Theorem 1], we see that

$$N_2(X, \varnothing) \sim 2 \cdot 27^n \cdot \frac{X \cdot (\log X)^{\alpha-1}}{3 \cdot \Gamma(\alpha)} \cdot c_0$$

and $N_2(X, S) = o(X(\log X)^{\alpha-1})$ for $S \neq \varnothing$. But the sums in (3-3) are linear combinations of such sums. More precisely, there holds

$$N_1(X, S) = \sum_{S\subseteq S'} (-1)^{|S'|-|S|} N_2(X, S').$$

This includes the term $N_2(X, \varnothing)$ if and only if $S = \varnothing$. Therefore we also have

$$N_1(X, \varnothing) \sim 2 \cdot 27^n \cdot \frac{X \cdot (\log X)^{\alpha-1}}{3 \cdot \Gamma(\alpha)} \cdot c_0$$

and $N_1(X, S) = o(X(\log X)^{\alpha-1})$ for $S \neq \varnothing$. Since the number of epimorphisms is exactly equal to

$$\sum_{\substack{S\subseteq T_n \\ T_n - S \text{ generates } \ker(\pi_0\circ q_n)}} N_1(X, S),$$

this proves the theorem. □

4. Counting conjugacy classes

Define for $g \in G$ and $\alpha \in (\mathbb{Z}/\mathrm{ord}(g)\mathbb{Z})^*$ the set

$$S_{g,\alpha} := \{h \in G : hgh^{-1} = g^{\alpha}\}.$$

Informally, one may think of $S_{g,\alpha}$ as the admissible Frobenius elements given that an inertia element is sent to g and $p \equiv \alpha \bmod \operatorname{ord}(g)$. Given $g \in G$ and a number field k, we may canonically identify $\operatorname{Gal}(k(\zeta_{\operatorname{ord}(g)})/k)$ as a subgroup of $(\mathbb{Z}/\operatorname{ord}(g)\mathbb{Z})^*$. We will write this group as $T(g,k)$. The next proposition gives an explicit formula for the naive Malle constant in terms of $S_{g,\alpha}$.

Proposition 4.1. *We have*

$$b(G,k) := -1 + \sum_{g \in G-\{\mathrm{id}\}} \frac{1}{[k(\zeta_{\operatorname{ord}(g)}) : k]} \sum_{\alpha \in T(g,k)} \frac{|S_{g,\alpha}|}{|G|}. \tag{4-1}$$

Proof. Observe that

$$\sum_{g \in G-\{\mathrm{id}\}} \frac{1}{[k(\zeta_{\operatorname{ord}(g)}) : k]} \sum_{\alpha \in T(g,k)} \frac{|S_{g,\alpha}|}{|G|} = \sum_{g \in G-\{\mathrm{id}\}} \frac{|\{\alpha \in T(g,k) : S_{g,\alpha} \neq \varnothing\}|}{[k(\zeta_{\operatorname{ord}(g)}) : k] \cdot |\mathrm{Cl}(g)|}.$$

For elements $g, h \in G$, recall that $g \sim h$ if $\mathrm{Cl}(g)$ is equivalent to $\mathrm{Cl}(h)$ under the cyclotomic action and also recall that $b(G,k)$ is the number of equivalence classes of $\sim$. We claim that

$$\frac{|\{\alpha \in T(g,k) : S_{g,\alpha} \neq \varnothing\}|}{[k(\zeta_{\operatorname{ord}(g)}) : k] \cdot |\mathrm{Cl}(g)|} = \frac{1}{|[g]|}. \tag{4-2}$$

But this follows from the Orbit-stabilizer theorem by letting $T(g,k)$ act on the set $X := \{\mathrm{Cl}(g^\alpha) : \alpha \in T(g,k)\}$. Indeed, first observe that

$$|[g]| = |X| \cdot |\mathrm{Cl}(g)|.$$

Since the action is transitive by construction, we get for every $x \in X$

$$|X| = |\mathrm{Orb}(x)| = \frac{[k(\zeta_{\operatorname{ord}(g)}) : k]}{|\mathrm{Stab}(x)|}.$$

Observing that $|\mathrm{Stab}(x)| = |\mathrm{Stab}(\mathrm{Cl}(g))|$ is precisely $|\{\alpha \in T(g,k) : S_{g,\alpha} \neq \varnothing\}|$, (4-2) follows. Therefore the naive Malle constant is equal to

$$b(G,k) = -1 + \sum_{g \in G-\{\mathrm{id}\}} \frac{|\{\alpha \in T(g,k) : S_{g,\alpha} \neq \varnothing\}|}{[k(\zeta_{\operatorname{ord}(g)}) : k] \cdot |\mathrm{Cl}(g)|} = -1 + |(G - \{\mathrm{id}\})/\sim|,$$

as desired. □

We now calculate (4-1) in the special case of $G = G_n$ and $k = \mathbb{Q}$. Let $g \in G_n$. If $q_n(g) = 0$, then we have $\operatorname{ord}(g) = 3$ and

$$S_{g,\alpha} = \begin{cases} G_n & \text{if } \alpha \equiv 1 \bmod 3, \\ \varnothing & \text{otherwise.} \end{cases} \tag{4-3}$$

Now suppose that $q_n(g) \neq 0$. If $h \in S_{g,\alpha}$, we have by definition

$$hgh^{-1} = g^\alpha.$$

Applying q_n to the above expression and recalling Lemma 3.2, we see that $S_{g,\alpha} = \varnothing$ unless $\alpha \equiv 1 \bmod \mathrm{ord}(g)$. Fixing g, we will now compute $S_{g,1 \bmod \mathrm{ord}(g)}$, which is precisely the set of $h \in G_n$ commuting with g.

Observe that the map $f_g : Q_n \to (\mathbb{Z}/3\mathbb{Z})^n$ given by lifting $a \in Q_n$ to an element $h \in G_n$ and then computing

$$hgh^{-1}g^{-1}$$

is a well-defined homomorphism, i.e., does not depend on the choice of lift. Writing out the multiplication rule for G_n given by θ explicitly, we see that this homomorphism equals

$$a \mapsto \big(\pi_0(a) \cdot \pi_i(q_n(g)) - \pi_0(q_n(g)) \cdot \pi_i(a)\big)_{1 \le i \le n}.$$

We will now distinguish two cases. If $\pi_0(q_n(g)) \neq 0$, then the homomorphism f_g is surjective. If instead $\pi_0(q_n(g)) = 0$, then the image of the homomorphism f_g has dimension 0 if $\pi_i(q_n(g)) = 0$ for all i and dimension 1 otherwise.

Note that the homomorphism f_g depends only on $q_n(g)$. Furthermore, we have the key identity

$$|S_{g,1 \bmod \mathrm{ord}(g)}| = 3^n \cdot |\ker(f_g)| = \begin{cases} 3 \cdot 9^n & \text{if } \pi_0(q_n(g)) \neq 0, \\ 27^n & \text{if } \pi_0(q_n(g)) = 0 \text{ and } \exists i : \pi_i(q_n(g)) \neq 0, \\ 3 \cdot 27^n & \text{if } \pi_0(q_n(g)) = 0 \text{ and } \forall i : \pi_i(q_n(g)) = 0. \end{cases} \tag{4-4}$$

Therefore we split the sum

$$\sum_{g \in G_n - \{\mathrm{id}\}} \frac{1}{\varphi(\mathrm{ord}(g))} \sum_{\alpha \in (\mathbb{Z}/\mathrm{ord}(g)\mathbb{Z})^*} \frac{|S_{g,\alpha}|}{|G_n|} = \sum_{g \in G_n - \{\mathrm{id}\}} \frac{1}{\varphi(\mathrm{ord}(g))} \cdot \frac{|S_{g,1 \bmod \mathrm{ord}(g)}|}{|G_n|}$$

in four pieces, namely the piece where $q_n(g) = 0$, the piece where $\pi_0(q_n(g)) \neq 0$, the piece where $\pi_0(q_n(g)) = 0$ and $\pi_i(q_n(g)) \neq 0$ for some i, and the piece where $\pi_0(q_n(g)) = 0$, $q_n(g) \neq 0$ and $\pi_i(q_n(g)) = 0$ for all i. The contribution from $q_n(g) = 0$ equals

$$\sum_{\substack{g \in G_n - \{\mathrm{id}\} \\ q_n(g) = 0}} \frac{1}{\varphi(\mathrm{ord}(g))} \cdot \frac{|S_{g,1 \bmod \mathrm{ord}(g)}|}{|G_n|} = \frac{3^n - 1}{2} \tag{4-5}$$

by (4-3). Using Lemma 3.2, we see that the number of elements of G_n with $\pi_0(q_n(g)) \neq 0$ with order 3 is $2 \cdot 3^n \cdot 3^n$, while the number of elements of order 9 is $2 \cdot 3^n \cdot (9^n - 3^n)$. The contribution from $\pi_0(q_n(g)) \neq 0$ becomes

$$\sum_{\substack{g \in G_n - \{\mathrm{id}\} \\ \pi_0(q_n(g)) \neq 0}} \frac{1}{\varphi(\mathrm{ord}(g))} \cdot \frac{|S_{g,1 \bmod \mathrm{ord}(g)}|}{|G_n|} = \left(2 \cdot 3^n \cdot \frac{9^n - 3^n}{6} + 2 \cdot 3^n \cdot \frac{3^n}{2}\right) \cdot \frac{1}{3^n} = 2 \cdot \frac{9^n - 3^n}{6} + 3^n \tag{4-6}$$

by (4-4). Finally, we treat the contribution from $\pi_0(q_n(g)) = 0$ but $q_n(g) \neq 0$. Firstly, if $\pi_i(q_n(g)) = 0$ for all i, then $\mathrm{ord}(g) = 3$. There are $3^n \cdot (3^n - 1)$ such elements, and they contribute

$$\sum_{\substack{g \in G_n - \{\mathrm{id}\} \\ q_n(g) \neq 0 \\ \pi_0(q_n(g)) = 0 \\ \forall i : \pi_i(q_n(g)) = 0}} \frac{1}{\varphi(\mathrm{ord}(g))} \cdot \frac{|S_{g,1 \bmod \mathrm{ord}(g)}|}{|G_n|} = 3^n \cdot \frac{3^n - 1}{2} \tag{4-7}$$

to the total thanks to (4-4). Now suppose that $\pi_i(q_n(g)) \neq 0$ for some i. Such g have order 9 and there are $3^n \cdot (9^n - 3^n)$ such g. This yields

$$\sum_{\substack{g \in G_n - \{\mathrm{id}\} \\ q_n(g) \neq 0 \\ \pi_0(q_n(g)) = 0 \\ \exists i : \pi_i(q_n(g)) \neq 0}} \frac{1}{\varphi(\mathrm{ord}(g))} \cdot \frac{|S_{g,1 \bmod \mathrm{ord}(g)}|}{|G_n|} = 3^n \cdot \frac{9^n - 3^n}{6} \cdot \frac{1}{3} \tag{4-8}$$

once more due to (4-4). Adding up the contributions from (4-5), (4-6), (4-7) and (4-8) gives the following theorem.

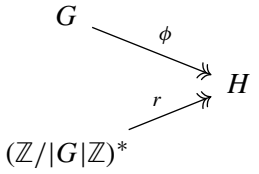
Theorem 4.2. *For all $n \geq 1$ there holds*

$$b(G_n, \mathbb{Q}) + 1 = \frac{3^n - 1}{2} + 2 \cdot \frac{9^n - 3^n}{6} + 3^n + 3^n \cdot \frac{3^n - 1}{2} + 3^n \cdot \frac{9^n - 3^n}{6} \cdot \frac{1}{3}. \tag{4-9}$$

Observe that the logarithmic exponent of Theorem 3.4 is strictly larger than $b(G_n, \mathbb{Q})$ for all $n \geq 2$. This immediately gives Theorem 1.3.

5. A modified Malle conjecture

Let G be a finite nilpotent group and suppose that we have the following diagram:



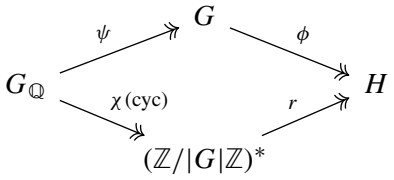
For the rest of this section, $\chi(\mathrm{cyc}) : G_{\mathbb{Q}} \to (\mathbb{Z}/|G|\mathbb{Z})^*$ denotes the cyclotomic character. We now define

$$\mathrm{Epi}_{(H,\phi)}(G_{\mathbb{Q}}, G)$$

to be the set of continuous surjective homomorphisms $\psi : G_{\mathbb{Q}} \twoheadrightarrow G$ satisfying the equations

$$\phi \circ \psi = r \circ \chi(\mathrm{cyc}), \quad \mathbb{Q}(\psi) \cap \mathbb{Q}(\zeta_{|G|}) = \mathbb{Q}(\phi \circ \psi),$$

i.e., we are only considering those ψ with a fixed wildly ramified cyclotomic subextension. In particular, we have the following diagram:



We denote by $G \times_H (\mathbb{Z}/|G|\mathbb{Z})^* \subseteq G \times (\mathbb{Z}/|G|\mathbb{Z})^*$ the subgroup consisting of pairs (g, α) satisfying

$$\phi(g) = r(\alpha).$$

The group $G \times (\mathbb{Z}/|G|\mathbb{Z})^*$ acts on $\ker(\phi) - \{\mathrm{id}\}$ by sending n to $gn^{\alpha^{-1}}g^{-1}$. Restricting this action to $G \times_H (\mathbb{Z}/|G|\mathbb{Z})^*$, we denote by

$$b_{(H,\phi)}(G) := |(\ker(\phi) - \{\mathrm{id}\})/(G \times_H (\mathbb{Z}/|G|\mathbb{Z})^*)|$$

the size of the quotient space. We propose the following conjecture. We thank Jiuya Wang for pointing out that the counting function in Conjecture 5.1 can be zero in some circumstances.

Conjecture 5.1. *Let G be a nilpotent group. For each H, ϕ as above, then either* $\mathrm{Epi}_{(H,\phi)}(G_{\mathbb{Q}}, G)$ *is empty or there exists a positive constant $c_{(H,\phi)}(G)$ such that*

$$|\{\psi \in \mathrm{Epi}_{(H,\phi)}(G_{\mathbb{Q}}, G) : \mathfrak{f}(\psi) \leq X\}| \sim c_{(H,\phi)}(G) \cdot X \cdot \log(X)^{b_{(H,\phi)}(G)-1}.$$

In the following remark we compare this conjecture with the naive adaptation of Malle's conjecture and with Theorem 3.4.

Remark 5.2. (a) We can recover Malle's original exponent as follows. If one takes $H = \{\mathrm{id}\}$, one trivially has that $b_{(H,\phi)}(G) = b(G)$. In particular, Conjecture 5.1 predicts that one can rescue Malle's conjecture in the case one considers the family of extensions that are linearly disjoint from $\mathbb{Q}(\zeta_{|G|})$.

(b) We have restricted ourselves to maps $r : (\mathbb{Z}/|G|\mathbb{Z})^* \twoheadrightarrow H$, but in principle one could consider maps $r : (\mathbb{Z}/|G|^j\mathbb{Z})^* \twoheadrightarrow H$ for every $j \geq 2$ as well. Using that powering with elements $\alpha \equiv 1 \bmod |G|$ is the identity map on G, one can check that this does not lead to higher logarithmic exponents than the ones in our conjecture.

(c) We can recover the exponent in Theorem 3.4 as follows. Let H be the order-3 quotient of $(\mathbb{Z}/9\mathbb{Z})^*$. Fix an identification $i : \mathbb{Z}/3\mathbb{Z} \to H$ and let $\phi := i \circ \pi_0 \circ q_n$. It is easy to verify that α in Theorem 3.4 equals exactly $b_{(H,\phi)}(G_n)$.

(d) It is worthwhile to compare our conjecture with work of Alberts; see Section 3.4, and specifically Conjecture 3.10, of [Alberts 2021]. Both conjectures predict that the correct logarithmic exponent is the maximum of the logarithmic exponents obtained by fixing some collection of subextensions and then applying Türkelli's adaptation to each such subextension. The work of Alberts allows for arbitrary groups G, while our conjecture is more restrictive on G. However, our conjecture is more precise about both the leading constant and the set of subextensions to consider.

We remark that one may reinterpret the exponents $b_{(H,\phi)}(G)$ as an adaptation, to the product of ramified primes, of Türkelli's modification of Malle's conjecture [Türkelli 2015]. Indeed, observe that the fibered product $G \times_H (\mathbb{Z}/|G|\mathbb{Z})^*$ certainly contains $\ker(\phi) \times \{1\}$. Hence the $G \times_H (\mathbb{Z}/|G|\mathbb{Z})^*$-equivalence relation is a further equivalence relation on $\ker(\phi)$-conjugacy classes in $\ker(\phi)$. This further equivalence relation is obtained by acting on a $\ker(\phi)$-conjugacy class via a pair (g, α) with $\phi(g) = r(\alpha)$. A moment's reflection shows that this comes down to the twisted $(\mathbb{Z}/|G|\mathbb{Z})^*$-action on the set of $\ker(\phi)$-conjugacy classes of $\ker(\phi)$ given in [loc. cit., page 198].

Remark 5.3. A nilpotent group G is always the product of its p-Sylow subgroups G_p. So the example in Theorem 3.4 might give the misleading impression that $b_{(H,\phi)}(G) > b(G, \mathbb{Q})$ can only occur by fixing at G_p some character ramified at p. However, choosing the central extension

$$0 \to (\mathbb{Z}/2\mathbb{Z})^n \to G_n \to (\mathbb{Z}/2\mathbb{Z})^{n+1} \times (\mathbb{Z}/3\mathbb{Z})^n \to 0,$$

given by the cocycles

$$\theta_i(\sigma, \tau) := \pi_0(\sigma) \cdot \pi_i(\tau)$$

for $1 \le i \le n$, also leads to examples. Here π_i denotes the projection map on the i-th copy of $\mathbb{Z}/2\mathbb{Z}$. Indeed, one may take $H := \mathbb{Z}/2\mathbb{Z}$, $\phi := \pi_0$ and r such that $\mathbb{Q}(r \circ \chi(\mathrm{cyc})) = \mathbb{Q}(\sqrt{-3})$. Then we have

$$b_{(H,\phi)}(G_n) = \frac{12^n}{2} + O(6^n),$$

while

$$b(G_n, \mathbb{Q}) = \frac{12^n}{4} + O(6^n),$$

hence giving an example for n sufficiently large. We leave the details of this alternative example to the interested reader.

Finally, we adapt the so-called Malle–Bhargava heuristic principle [Bhargava 2007] within the family $\mathrm{Epi}_{(H,\phi)}(G_{\mathbb{Q}}, G)$, in order to specify the leading constant $c_{(H,\phi)}(G)$ in the case $|G|$ is *odd*. To this end, for a prime number p and for G, H, ϕ as above, we denote by

$$\mathrm{Hom}_{(H,\phi)}(G_{\mathbb{Q}_p}, G)$$

the set of homomorphisms $\psi : G_{\mathbb{Q}_p} \to G$ such that $\phi \circ \psi = r \circ \chi(\mathrm{cyc}) \circ i_p^*$. The Malle–Bhargava principle states that if one writes the following Euler product

$$F(s) := \prod_p \left(\frac{1}{|\ker(\phi)|} \cdot \sum_{\psi \in \mathrm{Hom}_{(H,\phi)}(G_{\mathbb{Q}_p}, G)} \mathfrak{f}(\psi)^{-s} \right),$$

as a Dirichlet series

$$F(s) := \sum_{n \ge 1} \frac{f(n)}{n^s},$$

then one expects the asymptotic

$$\sum_{n\leq X} f(n) \sim |\{\psi \in \mathrm{Epi}_{(H,\phi)}(G_{\mathbb{Q}}, G) : \mathfrak{f}(\psi) \leq X\}|.$$

With this principle in mind, let us now compute the left hand side. For $g \in G$ and $\alpha \in (\mathbb{Z}/|G|\mathbb{Z})^*$, we define

$$S_{(H,\phi)}(g,\alpha) := \{h \in G : hgh^{-1} = g^{\alpha} \text{ and } \phi(h) = r(\alpha)\}.$$

For a profinite group $\mathcal{G}$, we denote by $\mathcal{G}(p)$ the pro-p completion of $\mathcal{G}$. Likewise, for a continuous homomorphism $\varphi : \mathcal{G}_1 \to \mathcal{G}_2$ of profinite groups, we denote by $\varphi(p)$ the induced map between pro-p completions. We define $\mathcal{G}(\text{non-}p)$ to be the product of the pro-q completions of $\mathcal{G}$ as q runs over prime divisors of $|G|$ not equal to p. Given a continuous homomorphism $\varphi : \mathcal{G}_1 \to \mathcal{G}_2$, there is a natural induced homomorphism $\varphi(\text{non-}p)$. Write $f : H \to H(p)$ and $g : H \to H(\text{non-}p)$ for the natural surjective maps so that the product map (f, g) is an isomorphism owing to the fact that H is nilpotent.

We fix for each prime number p a generator τ_p of the image of the inertia subgroup of $G_{\mathbb{Q}_p}$ in the quotient $g \circ r \circ \chi(\mathrm{cyc}) \circ i_p^*$: this is a cyclic group because tame inertia is cyclic.

Proposition 5.4. *Notation as immediately above, we have that*

$$\sum_{n\leq X} f(n) \sim c_{(H,\phi)}(G) \cdot X \cdot \log(X)^{b_{(H,\phi)}(G)-1},$$

where $c_{(H,\phi)}(G)$ is the conditionally convergent product

$$c_{(H,\phi)}(G) := \frac{1}{\Gamma(b_{(H,\phi)}(G))} \times \alpha_1 \times \alpha_2 \times \alpha_3,$$

where

$$\alpha_1 := \prod_{p \mid \mathfrak{f}(r\circ\chi(\mathrm{cyc}))} \left(\frac{|\ker(\phi(p))|}{p}\right) \cdot \left(\frac{\sum_{g\in\phi(\text{non-}p)^{-1}(\tau_p)} |S_{(H(\text{non-}p),\phi(\text{non-}p))}(g,\, p)|}{|\ker(\phi(\text{non-}p))|}\right)\left(1-\frac{1}{p}\right)^{b_{(H,\phi)}(G)},$$

$$\alpha_2 := \prod_{\substack{p \mid |G| \\ p\nmid \mathfrak{f}(r\circ\chi(\mathrm{cyc}))}} \left(1 + \frac{|\ker(\phi(p))|\left(\frac{\sum_{g\in\ker(\phi(\text{non-}p))} |S_{(H(\text{non-}p),\phi(\text{non-}p))}(g,p)|}{|\ker(\phi(\text{non-}p))|}\right) - 1}{p}\right)\left(1-\frac{1}{p}\right)^{b_{(H,\phi)}(G)},$$

$$\alpha_3 := \prod_{p\nmid |G|} \left(1 + \frac{\sum_{g\in\ker(\phi)-\{\mathrm{id}\}} |S_{(H,\phi)}(g,\, p)|}{|\ker(\phi)|\cdot p}\right)\left(1-\frac{1}{p}\right)^{b_{(H,\phi)}(G)}.$$

Proof. Note that f is supported on squarefree integers and multiplicative away from primes dividing $|G|$. The proposition will ultimately follow from [Granville and Koukoulopoulos 2019, Theorem 1], with the exponent of $\log(X)$ being the average of f on primes. Let us start by showing that this equals $b_{(H,\phi)}(G)$. We compute

$$\frac{1}{|\ker(\phi)|\cdot\varphi(|G|)} \cdot \sum_{\substack{g\in\ker(\phi)-\{\mathrm{id}\} \\ \alpha\in(\mathbb{Z}/|G|\mathbb{Z})^*}} |S_{(H,\phi)}(g,\alpha)|.$$

Observe that $|\ker(\phi)| \cdot \varphi(|G|) = |G \times_H (\mathbb{Z}/|G|\mathbb{Z})^*|$. We can therefore rewrite the sum as

$$\frac{1}{|G \times_H (\mathbb{Z}/|G|\mathbb{Z})^*|} \cdot \sum_{(h,\alpha)\in G\times_H(\mathbb{Z}/|G|\mathbb{Z})^*} |\{g \in \ker(\phi) - \{\mathrm{id}\} : hgh^{-1} = g^\alpha\}| = b_{(H,\phi)}(G)$$

by Burnside's lemma.

It remains to examine the local factors of the leading constant. In [Granville and Koukoulopoulos 2019], the authors do so by rewriting $F(s)$ as

$$F(s) = \frac{F(s)}{\zeta_{\mathbb{Q}}(s)^{b_{(H,\phi)}(G)}} \cdot \zeta_{\mathbb{Q}}(s)^{b_{(H,\phi)}(G)},$$

in order to obtain the leading coefficient as a conditionally convergent Euler product. This is the reason for the occurrence of the term $(1 - 1/p)^{b_{(H,\phi)}(G)}$ in our formulas. We now wish to explain the remaining contributors:

The constant α_1: Suppose that $p \mid \mathfrak{f}(r \circ \chi(\mathrm{cyc}))$. Then the local contribution is precisely

$$\frac{1}{p \cdot |\ker(\phi)|} \cdot |\mathrm{Hom}_{(H,\phi)}(G_{\mathbb{Q}_p}, G)|.$$

Recalling that these are nilpotent groups, we see that we can split the count in the numerator Sylow by Sylow. Therefore we have that

$$|\mathrm{Hom}_{(H,\phi)}(G_{\mathbb{Q}_p}, G)| = T_p \times T_{\text{non-}p},$$

where T_p equals the number of continuous homomorphisms $\psi : G_{\mathbb{Q}_p} \to G(p)$ such that

$$\phi(p) \circ \psi = f \circ r \circ \chi(\mathrm{cyc}) \circ i_p^*,$$

while $T_{\text{non-}p}$ equals the number of continuous homomorphisms $\psi : G_{\mathbb{Q}_p} \to G(\text{non-}p)$ such that

$$\phi(\text{non-}p) \circ \psi = g \circ r \circ \chi(\mathrm{cyc}) \circ i_p^*.$$

Note that $\psi : G_{\mathbb{Q}_p} \to G(p)$ factors through $G_{\mathbb{Q}_p}(p)$ and recall that $G_{\mathbb{Q}_p}(p)$ is isomorphic to a free pro-p group on 2 generators. It follows that T_p equals the number of pairs of elements in $G(p)$ having prescribed value of $\phi(p)$. Therefore

$$T_p = |\ker(\phi(p))|^2.$$

Note that any map $\psi : G_{\mathbb{Q}_p} \to G(\text{non-}p)$ must factor through $G_{\mathbb{Q}_p}^{\mathrm{tame}}$. Recall that

$$G_{\mathbb{Q}_p}^{\mathrm{tame}} \simeq_{\text{top.gr.}} \left(\prod_{\ell\neq p} \mathbb{Z}_\ell\right) \rtimes \hat{\mathbb{Z}},$$

where the topological generator 1 of the group $\hat{\mathbb{Z}}$ acts by multiplication by p on $\prod_{\ell\neq p} \mathbb{Z}_\ell$. Both groups in this direct product are pro-cyclic. Hence the cardinality

$$T_{\text{non-}p}$$

equals the number of possible choices for two fixed generators. Once we prescribe that a generator of $\prod_{\ell \neq p} \mathbb{Z}_\ell$ goes to an element g of $\phi(\text{non-}p)^{-1}(\tau_p) \in G(\text{non-}p)$, we have that the generator 1 of $\hat{\mathbb{Z}}$ has to be sent in $S_{(H(\text{non-}p),\phi(\text{non-}p))}(g, p) \subseteq G(\text{non-}p)$. And conversely any choice of such a pair gives rise to a valid homomorphism. This proves that

$$T_{\text{non-}p} = \left(\sum_{g \in \phi(\text{non-}p)^{-1}(\tau_p)} |S_{(H(\text{non-}p),\phi(\text{non-}p))}(g, p)| \right),$$

which gives us the desired conclusion on α_1.

The constant α_2: Suppose that $p \mid |G|$ and $p \nmid \mathfrak{f}(r \circ \chi)$. Then splitting the local factor

$$\frac{1}{|\ker(\phi)|} \cdot \sum_{\psi \in \mathrm{Hom}_{(H,\phi)}(G_{\mathbb{Q}_p}, G)} \mathfrak{f}(\psi)^{-1},$$

into unramified and ramified ψ, we get precisely

$$1 + \frac{|\{\psi \text{ ramified and } \psi \in \mathrm{Hom}_{(H,\phi)}(G_{\mathbb{Q}_p}, G)\}|}{p \cdot |\ker(\phi)|}.$$

This is because there are precisely $|\ker(\phi)|$ unramified ones. Indeed, the Galois group of the maximal unramified extension of $\mathbb{Q}_p$ is topologically free on one generator and therefore the unramified elements of $\mathrm{Hom}_{(H,\phi)}(G_{\mathbb{Q}_p}, G)$ correspond to the choices of an element of G with prescribed image under ϕ.

Now we can use again the count of unramified classes in $\mathrm{Hom}_{(H,\phi)}(G_{\mathbb{Q}_p}, G)$ to obtain that

$$|\{\psi \text{ ramified and } \psi \in \mathrm{Hom}_{(H,\phi)}(G_{\mathbb{Q}_p}, G)\}| = |\mathrm{Hom}_{(H,\phi)}(G_{\mathbb{Q}_p}, G)| - |\ker(\phi)|.$$

But we have computed in the evaluation of α_1 that

$$|\mathrm{Hom}_{(H,\phi)}(G_{\mathbb{Q}_p}, G)| = |\ker(\phi(p))|^2 \left(\sum_{g \in \phi(\text{non-}p)^{-1}(\tau_p)} |S_{(H(\text{non-}p),\phi(\text{non-}p))}(g, p)| \right).$$

Since $p \nmid \mathfrak{f}(r \circ \chi(\text{cyc}))$, we have $r \circ \chi(\text{cyc}) \circ i_p^*(I_p) = \{1\}$ and thus $\phi(\text{non-}p)^{-1}(\tau_p) = \ker(\phi(\text{non-}p))$. This gives the desired formula.

The constant α_3: Since p does not divide $|G|$, we now have that all the homomorphisms will be tame. In particular, this implies that the image of a generator of tame inertia has to be in $\ker(\phi)$. The total contribution from unramified homomorphisms is again 1, as already articulated above. The one from ramified ones comes precisely in the same way we have explained in the computation of α_1. □

With the above in mind, we are ready to make the following conjecture.

Conjecture 5.5. *Suppose G is odd and nilpotent. Then Conjecture 5.1 holds with*

$$c_{(H,\phi)}(G) := \frac{1}{\Gamma(b_{(H,\phi)}(G))} \times \alpha_1 \times \alpha_2 \times \alpha_3,$$

where α_i are as in Proposition 5.4.

It is readily verified that Theorem 3.4 is a special case of Conjecture 5.5, with the choice of G, H, ϕ as explained in Remark 5.2. The extra factor 2 in Theorem 3.4 accounts for the fact that one may also choose another identification in Remark 5.2. The factor $\frac{27^n}{3}$ is the local factor at 3 and the constant c_0 therein is the product of the tame factors along with the factor $\left(\frac{2}{3}\right)^{\alpha}$.

The conjecture can be extended also for a finite prescribed set of local conditions by modifying accordingly the local factors defining $F(s)$, namely summing $\mathfrak{f}(\psi)^{-s}$ only among the prescribed local homomorphisms ψ. In particular, if one runs only over tame extensions, one gets the simpler leading constant

$$\prod_{p\,|\,|G|}\left(1-\frac{1}{p}\right)^{b_{(H,\phi)}(G)}\times\prod_{p\nmid|G|}\left(1+\frac{\sum_{g\in\ker(\phi)-\{\mathrm{id}\}}|S_{(H,\phi)}(g,p)|}{|\ker(\phi)|\cdot p}\right)\left(1-\frac{1}{p}\right)^{b_{(H,\phi)}(G)}.$$

We have excluded the groups of even cardinality from Conjecture 5.5, since one can prove that the same conjecture would fail already for the dihedral group on 8 elements, and even among tamely ramified extensions. In this case the leading constant is likely to be an Euler product times a rational correction factor to account for quadratic reciprocity. If also wild extensions are considered, then even further modifications may be needed by Grunwald–Wang-type of obstructions. These problems at 2 correspond to the unspecified constant $C(G)$ in [Bhargava 2007, Equation (8.6), page 17].

Acknowledgements

Koymans gratefully acknowledges the support of Dr. Max Rössler, the Walter Haefner foundation and the ETH Zürich foundation. The authors would like to thank Ratko Darda for fruitful discussions and the anonymous referee for their careful reading of the manuscript.

References

[Alberts 2021] B. Alberts, "Statistics of the first Galois cohomology group: a refinement of Malle's conjecture", *Algebra Number Theory* **15**:10 (2021), 2513–2569. MR Zbl

[Alberts and O'Dorney 2021] B. Alberts and E. O'Dorney, "Harmonic analysis and statistics of the first Galois cohomology group", *Res. Math. Sci.* **8**:3 (2021), art. id. 50. Correction in **10**:3 (2023), art. id. 31. MR Zbl

[Altuğ et al. 2021] S. A. Altuğ, A. Shankar, I. Varma, and K. H. Wilson, "The number of D_4-fields ordered by conductor", *J. Eur. Math. Soc.* **23**:8 (2021), 2733–2785. MR Zbl

[Bartel and Lenstra 2020] A. Bartel and H. W. Lenstra, Jr., "On class groups of random number fields", *Proc. Lond. Math. Soc.* (3) **121**:4 (2020), 927–953. MR Zbl

[Belabas and Fouvry 2010] K. Belabas and É. Fouvry, "Discriminants cubiques et progressions arithmétiques", *Int. J. Number Theory* **6**:7 (2010), 1491–1529. MR Zbl

[Bhargava 2005] M. Bhargava, "The density of discriminants of quartic rings and fields", *Ann. of Math.* (2) **162**:2 (2005), 1031–1063. MR Zbl

[Bhargava 2007] M. Bhargava, "Mass formulae for extensions of local fields, and conjectures on the density of number field discriminants", *Int. Math. Res. Not.* **2007**:17 (2007), art. id. rnm052. MR Zbl

[Bhargava 2010] M. Bhargava, "The density of discriminants of quintic rings and fields", *Ann. of Math.* (2) **172**:3 (2010), 1559–1591. MR Zbl

[Bhargava and Wood 2008] M. Bhargava and M. M. Wood, "The density of discriminants of S_3-sextic number fields", *Proc. Amer. Math. Soc.* **136**:5 (2008), 1581–1587. MR Zbl

[Cohen et al. 2002] H. Cohen, F. Diaz y Diaz, and M. Olivier, "Enumerating quartic dihedral extensions of $\mathbb{Q}$", *Compos. Math.* **133**:1 (2002), 65–93. MR Zbl

[Couveignes 2020] J.-M. Couveignes, "Enumerating number fields", *Ann. of Math.* (2) **192**:2 (2020), 487–497. MR

[Darda and Yasuda 2023] R. Darda and T. Yasuda, "Torsors for finite group schemes of bounded height", *J. Lond. Math. Soc.* (2) **108**:3 (2023), 1275–1331. MR Zbl

[Davenport and Heilbronn 1971] H. Davenport and H. Heilbronn, "On the density of discriminants of cubic fields, II", *Proc. Roy. Soc. Lond. Ser. A* **322**:1551 (1971), 405–420. MR Zbl

[Ellenberg and Venkatesh 2006] J. S. Ellenberg and A. Venkatesh, "The number of extensions of a number field with fixed degree and bounded discriminant", *Ann. of Math.* (2) **163**:2 (2006), 723–741. MR Zbl

[Fouvry and Koymans 2021] É. Fouvry and P. Koymans, "Malle's conjecture for nonic Heisenberg extensions", preprint, 2021. arXiv 2102.09465

[Granville and Koukoulopoulos 2019] A. Granville and D. Koukoulopoulos, "Beyond the LSD method for the partial sums of multiplicative functions", *Ramanujan J.* **49**:2 (2019), 287–319. MR Zbl

[Gundlach 2022] F. Gundlach, "Malle's conjecture with multiple invariants", preprint, 2022. arXiv 2211.16698

[Klüners 2005] J. Klüners, "A counterexample to Malle's conjecture on the asymptotics of discriminants", *C. R. Math. Acad. Sci. Paris* **340**:6 (2005), 411–414. MR

[Klüners 2012] J. Klüners, "The distribution of number fields with wreath products as Galois groups", *Int. J. Number Theory* **8**:3 (2012), 845–858. MR Zbl

[Klüners and Malle 2004] J. Klüners and G. Malle, "Counting nilpotent Galois extensions", *J. Reine Angew. Math.* **572** (2004), 1–26. MR Zbl

[Koymans and Pagano 2023] P. Koymans and C. Pagano, "On Malle's conjecture for nilpotent groups", *Trans. Amer. Math. Soc. Ser. B* **10** (2023), 310–354. MR Zbl

[Lemke Oliver and Thorne 2022] R. J. Lemke Oliver and F. Thorne, "Upper bounds on number fields of given degree and bounded discriminant", *Duke Math. J.* **171**:15 (2022), 3077–3087. MR Zbl

[Mäki 1993] S. Mäki, "The conductor density of abelian number fields", *J. Lond. Math. Soc.* (2) **47**:1 (1993), 18–30. MR Zbl

[Malle 2004] G. Malle, "On the distribution of Galois groups, II", *Exp. Math.* **13**:2 (2004), 129–135. MR Zbl

[Masri et al. 2020] R. Masri, F. Thorne, W.-L. Tsai, and J. Wang, "Malle's conjecture for $G \times A$ with $G = S_3, S_4, S_5$", preprint, 2020. arXiv 2004.04651

[Neukirch et al. 2000] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of number fields*, Grundl. Math. Wissen. **323**, Springer, 2000. MR Zbl

[Türkelli 2015] S. Türkelli, "Connected components of Hurwitz schemes and Malle's conjecture", *J. Number Theory* **155** (2015), 163–201. MR Zbl

[Wang 2021] J. Wang, "Malle's conjecture for $S_n \times A$ for $n = 3, 4, 5$", *Compos. Math.* **157**:1 (2021), 83–121. MR Zbl

[Wood 2010] M. M. Wood, "On the probabilities of local behaviors in abelian field extensions", *Compos. Math.* **146**:1 (2010), 102–128. MR Zbl

[Wright 1989] D. J. Wright, "Distribution of discriminants of abelian extensions", *Proc. Lond. Math. Soc.* (3) **58**:1 (1989), 17–50. MR Zbl

Communicated by Melanie Matchett Wood
Received 2023-09-18 Revised 2024-04-22 Accepted 2024-06-15

peter.koymans@eth-its.ethz.ch *Institute for Theoretical Studies, ETH Zurich, Zurich, Switzerland*

carlo.pagano@concordia.ca *Department of Mathematics and Statistics, Concordia University, Montreal, Quebec, Canada*

Algebra & Number Theory

msp.org/ant

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2025 is US $565/year for the electronic version, and $820/year (+$70, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

Algebra & Number Theory

Volume 19 No. 5 2025