Mathematisches
Forschungsinstitut
Oberwolfach

Member of the Leibniz Association

Oberwolfach Preprints

OWP 2020 - 11

JÜRGEN KLÜNERS AND JIUYA WANG

ℓ-Torsion Bounds for the Class Group of Number Fields with an ℓ -Group as Galois Group

Mathematisches Forschungsinstitut Oberwolfach gGmbH
Oberwolfach Preprints (OWP) ISSN 1864-7596

Oberwolfach Preprints (OWP)

The MFO publishes a preprint series **Oberwolfach Preprints (OWP)**, ISSN 1864-7596, which mainly contains research results related to a longer stay in Oberwolfach, as a documentation of the research work done at the MFO. In particular, this concerns the Research in Pairs-Programme (RiP) and the Oberwolfach-Leibniz-Fellows (OWLF), but this can also include an Oberwolfach Lecture, for example.

A preprint can have a size from 1 - 200 pages, and the MFO will publish it on its website as well as by hard copy. Every RiP group or Oberwolfach-Leibniz-Fellow may receive on request 30 free hard copies (DIN A4, black and white copy) by surface mail.

The full copyright is left to the authors. With the submission of a manuscript, the authors warrant that they are the creators of the work, including all graphics. The authors grant the MFO a perpetual, non-exclusive right to publish it on the MFO's institutional repository.

In case of interest, please send a **pdf file** of your preprint by email to *rip@mfo.de* or *owlf@mfo.de*, respectively. The file should be sent to the MFO within 12 months after your stay as RiP or OWLF at the MFO.

There are no requirements for the format of the preprint, except that the introduction should contain a short appreciation and that the paper size (respectively format) should be DIN A4, "letter" or "article".

On the front page of the hard copies, which contains the logo of the MFO, title and authors, we shall add a running number (20XX – XX). Additionally, each preprint will get a Digital Object Identifier (DOI).

We cordially invite the researchers within the RiP or OWLF programme to make use of this offer and would like to thank you in advance for your cooperation.

Imprint:

Mathematisches Forschungsinstitut Oberwolfach gGmbH (MFO)
Schwarzwaldstrasse 9-11
77709 Oberwolfach-Walke
Germany

Tel +49 7834 979 50
Fax +49 7834 979 55
Email admin@mfo.de
URL www.mfo.de

The Oberwolfach Preprints (OWP, ISSN 1864-7596) are published by the MFO.

DOI 10.14760/OWP-2020-11

ℓ-TORSION BOUNDS FOR THE CLASS GROUP OF NUMBER FIELDS WITH AN ℓ-GROUP AS GALOIS GROUP

JÜRGEN KLÜNERS AND JIUYA WANG

ABSTRACT. We describe the relations among the ℓ-torsion conjecture for ℓ-extensions, the discriminant multiplicity conjecture for nilpotent extensions and a conjecture of Malle giving an upper bound for the number of nilpotent extensions. We then prove all of these conjectures in these cases.

1. INTRODUCTION

The goal of this paper is twofold: on one hand, to show the relations between several main conjectures in arithmetic statistics namely, the ℓ-torsion conjecture, the discriminant multiplicity conjecture and Malle's conjecture for the number of number field extensions with given Galois group, with an emphasis on nilpotent extensions; on the other hand, moreover, using genus theory we show that these conjectures have affirmative answers when we restrict our discussion to the ℓ-torsion of class groups of ℓ-extensions, and to nilpotent extensions for the other two conjectures. As shown in the proof, we remark the fundamental reason for conjectures to hold in such a perfect shape for these cases is completely group theoretic, i.e., nilpotent groups have non-trivial center.

Firstly, we consider the class group Cl_E of a number field E of absolute discriminant D. By the proof of finiteness of the class number the size of Cl_E is bounded by $O_{\epsilon,[E:\mathbb{Q}]}(D^{1/2+\epsilon})$ for all $\epsilon > 0$. We denote by $h_\ell(E)$ the size of the ℓ-torsion subgroup $\mathrm{Cl}_E[\ell]$ of Cl_E. The following conjecture is widely expected to hold.

Conjecture A (ℓ-torsion conjecture, [2, 4, 15])**.** *Let E be a number field of absolute discriminant D and degree $n = [E : \mathbb{Q}]$ and ℓ be a prime number. Then*

$$h_\ell(E) = O_{\epsilon,n,\ell}(D^\epsilon) \text{ for all } \epsilon > 0 \text{ and for } D \to \infty.$$

This conjecture is known to be true for $\ell = 2$ and $[E : \mathbb{Q}] = 2$ by genus theory. In general, in [12] Conjecture A is shown to be a consequence of Cohen-Lenstra heuristics. We prove this conjecture for all primes ℓ and all number fields $E/\mathbb{Q}$ such that the normal closure is an ℓ-group extension. In Theorem 2.6 we prove a more general version, where the normal closure of E/F over a number field F is an ℓ-group extension.

The ℓ-torsion conjecture is connected to the question on the number of number fields with the same discriminant, and thus the number of number fields with bounded discriminant.

In order to introduce these problems we define a more general notion for G-extensions. Let F be a number field and $E = F(\alpha)$ be an extension of degree n. Furthermore let $f \in F[x]$ be the minimal polynomial of α. By abuse of notation we

2010 *Mathematics Subject Classification.* Primary 11R37; Secondary 11Y40.

define $\mathrm{Gal}(E/F) := \mathrm{Gal}(f) \leq S_n$ and we call E/F a G-extension for $G = \mathrm{Gal}(f)$. In our notation G is always a transitive subgroup of S_n. For $X \geq 0$ let

$$N(F, G; X) := |\{E/F \mid \mathrm{Gal}(E/F) = G,\ \mathrm{Disc}(E/F) \leq X\}|$$

be the number of field extensions of F (inside a fixed algebraic closure $\bar{\mathbb{Q}}$) of degree n with Galois group $G \leq S_n$ and $\mathrm{Disc}(E/F) = |\mathfrak{d}(E/F)|$ is the (absolute) norm of the discriminant ideal $\mathfrak{d}(E/F)$ bounded above by X. Note that there are only finitely many number fields of given degree and bounded discriminant, hence $N(F, G; X)$ is finite for all G, F, X.

Gunter Malle [9, 10] has given a precise conjecture about the asymptotic behavior of the function $N(F, G; X)$ for $X \to \infty$. In order to state it, we introduce some group theoretic invariants of permutation groups.

Definition 1.1. Let $G \leq S_n$ be a transitive group acting on $\Omega = \{1, \dots, n\}$.

(i) For $g \in G$ we define the index $\mathrm{ind}(g) := n -$ the number of orbits of g on Ω.
(ii) For $n > 1$ let $a(G) := \mathrm{ind}(G) := \min\{\mathrm{ind}(g) : \mathrm{id} \neq g \in G\}$.

Note that $a(G)$ here is the inverse of the $a(G)$ defined in [9].

Conjecture B (Malle's Conjecture (weak version of the upper bound), [9])**.** *For all number fields F and all transitive permutation groups $G \leq S_n$ we have*

$$N(F, G; X) = O_{\epsilon, F}(X^{1/a(G)+\epsilon}) \text{ for all } \epsilon > 0.$$

In the same paper Malle gives also a conjecture for a lower bound which is equivalent to $\liminf_{X\to\infty} X^{a(G)} N(F, G; X) > 0$. We remark that Malle gives a refined version of the conjecture in [10], which we do not need in our context here. There are also counter-examples known due to the first author [7] for this refined conjecture.

Certainly, the upper bound on the number of G-extensions of F is related to the question on an upper bound of the number of extensions with the same absolute discriminant.

Conjecture C (Discriminant Multiplicity Conjecture, [4, 5])**.** *Given a transitive permutation group $G \leq S_n$, a number field F, and $D > 0$, let a_D be the number of G-extensions of F with discriminant* $\mathrm{Disc}(E/F) = D$*. Then*

$$a_D \leq O_{\epsilon, F, n}(D^{\epsilon}) \text{ for all } \epsilon > 0.$$

We organize the paper as following. In Section 2, we prove Theorem 2.6 that Conjecture A holds for the ℓ-torsion of class groups in ℓ-extensions by genus theory. In Section 3, we prove Theorem 3.1 that Conjecture C for nilpotent extensions is a consequence of Theorem 2.6. In Section 4, we reprove that Conjecture B for nilpotent extensions is a consequence of Theorem 3.1. We remark that this result was originally proved in [8, 1]. Using the setting here we get it as an easy application. Therefore these different conjectures have interesting connections. In our eyes this also supports the heuristic of Malle's conjecture. All results in this paper are effective.

2. ℓ-torsion conjecture

In this section, we prove Conjecture A for the ℓ-torsion of class groups of ℓ-extensions in Theorem 2.6. The reader can also find a different perspective on a proof of Theorem 2.6 by G. Gras [6].

We start with the following theorem, which is proved in [3, Theorem 2.2] for odd ℓ and generalized in [13, Theorem 2] to $\ell = 2$. In order to keep this note self-contained we give a proof of this statement here. In the following we use the notion places for finite prime ideals and infinite places.

Theorem 2.1. *Let E/F be a cyclic extension of number fields of degree ℓ ramified in t places. Let $e := \max(t, 1)$. Then*

$$\mathrm{rk}_\ell(\mathrm{Cl}_E) \leq \ell(e - 1 + \mathrm{rk}_\ell(\mathrm{Cl}_F)).$$

Proof. Firstly, the Galois group $\mathrm{Gal}(E/F) = \langle\sigma\rangle$ acts on the $\mathbb{F}_\ell$-vector space $\mathrm{Cl}_E[\ell]$. Since $\sigma^\ell = \mathrm{id}$, the minimal polynomial for σ on $\mathrm{Cl}_E[\ell]$ divides $x^\ell - 1 = (x - 1)^\ell$. Therefore, the only eigenvalue is 1 and each Jordan block has at most size ℓ. It suffices to prove that the number of Jordan blocks is bounded by $e - 1 + \mathrm{rk}_\ell(\mathrm{Cl}_F)$.

The number of Jordan blocks is equal to the dimension of the maximal quotient space on which σ acts trivially. Denote the corresponding class field by M. Notice that since σ acts trivially, the field M/F is Galois and abelian, therefore $\mathrm{Gal}(M/E) \cong C_\ell^s$ for some $s \geq 0$ and $\mathrm{Gal}(M/F) \cong C_\ell^{s+1}$ or $\mathrm{Gal}(M/F) \cong C_{\ell^2} \times C_\ell^{s-1}$. We would like to prove that $s \leq e - 1 + \mathrm{rk}_\ell(\mathrm{Cl}_F)$. We note that the second case can only happen when $t = 0$, i.e. E/F is unramified. In this case we see $s = \mathrm{rk}_\ell(\mathrm{Cl}_F)$ and our claim is proved.

In the first case denote by L/F the maximal unramified (including infinite places) subextension of M/F. We know by construction that $\mathrm{Gal}(L/F) \cong C_\ell^{\mathrm{rk}_\ell(\mathrm{Cl}_F)}$. M/L is abelian and it has no subextension which is everywhere unramified (including infinite places). Therefore M/L is generated by the inertia groups of the ramified prime ideals including the infinite ones. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_F$ which is ramified in M. Since M/E is unramified, we see that the inertia group has size ℓ and is therefore cyclic. The same applies for the prime ideal in L lying above $\mathfrak{p}$. The inertia groups at infinite places are always cyclic and we see that each ramified prime in E/F can increase the rank of $\mathrm{Gal}(M/L)$ by at most 1. We therefore get:

$$\mathrm{rk}_\ell(\mathrm{Gal}(M/F)) \leq \mathrm{rk}_\ell(\mathrm{Cl}_F) + e \text{ and } \mathrm{rk}_\ell(\mathrm{Gal}(M/E)) = \mathrm{rk}_\ell(\mathrm{Gal}(M/F)) - 1. \quad \square$$

We remark that [13, Theorem 2.2] gives a slightly better upper bound if E/F is unramified, Furthermore, it gives a better bound for the cyclic of order ℓ^r-case compared to the inductive approach we present in Theorem 2.3. In order to prove this theorem for non normal extensions we need the following lemma.

Lemma 2.2. *Let $n = \ell^r$ and $G \leq S_n$ be an ℓ-group and E/F be an extension of number fields with $\mathrm{Gal}(E/F) = G$. Then there exists a tower of fields*

$$F = F_0 \leq F_1 \leq \ldots \leq F_{r-1} \leq F_r = E \tag{1}$$

such that $\mathrm{Gal}(F_{i+1}/F_i) = C_\ell$ for all $0 \leq i \leq r - 1$.

Proof. Let $\tilde{E}$ be the normal closure of E over F. Denote H to be the subgroup of G fixing E and choose a maximal subgroup $G_1 \leq G$ that contains H. Note that all maximal subgroups of an ℓ-group have index ℓ and are normal. Define F_1 to be the subfield of $\tilde{E}$ fixed by G_1. Inductively, we can find a sequence of subgroups $G = G_0 \supset G_1 \supset \cdots \supset G_r = H$ with $[G_i : G_{i+1}] = \ell$ for every $0 \leq i \leq r - 1$ and define F_i to be the subfield fixed by G_i. $\square$

Now we prove our main result of this section. We remark that [3, page 424] describes just before Theorem 3 how to get this result for normal ℓ-extensions.

Theorem 2.3. *Let $n = \ell^r$, $G \leq S_n$ be a transitive ℓ-group, and E/F be an extension of number fields with $\mathrm{Gal}(E/F) = G$, and with tower as defined in (1). Let t_i be the number of ramified places in F_{i+1}/F_i and $e_i := \max(t_i, 1)$. Then we get:*

$$\mathrm{rk}_\ell(\mathrm{Cl}_E) \leq \sum_{i=0}^{r-1} \ell^{r-i}(e_i - 1) + n\mathrm{rk}_\ell(\mathrm{Cl}_F). \tag{2}$$

Proof. By Lemma 2.2 we find a tower of cyclic extensions of order ℓ. The assertion now follows by applying Theorem 2.1 for each step. □

The above version is still a little bit complicated since we need to know the number of ramified places in each step. It would be much nicer to have a bound which is only depending on the number of ramified places of F. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_F$ which ramifies for the first time in F_{i+1}. We have the extremal case if $\mathfrak{p}$ splits completely in F_i which means that there are ℓ^i places over $\mathfrak{p}$ lying in F_i.

Therefore, if t is the number of prime ideals in $\mathcal{O}_F$ which are ramified in E/F, then we get that $t_i \leq e_i \leq \max(\ell^i t, 1)$ in (2). Therefore we get:

Lemma 2.4. *Let $G \leq S_n$ be a transitive ℓ-group and E/F be an extension with $\mathrm{Gal}(E/F) = G$ of degree $n = \ell^r$ which is ramified in t places. Then*

$$\mathrm{rk}_\ell(\mathrm{Cl}_E) \leq rnt + n\mathrm{rk}_\ell(\mathrm{Cl}_F). \tag{3}$$

Proof. Note that $e_i - 1 \leq \ell^i t$ and using this in (2) we get $\mathrm{rk}_\ell(\mathrm{Cl}_E) \leq rnt + n\mathrm{rk}_\ell(\mathrm{Cl}_F)$ and the assertion follows easily. □

In the next step we would like to know an upper bound for the number of different prime ideals dividing the discriminant of E/F. We use the following standard result, e.g. see [14, Section 5.3, p. 83].

Proposition 2.5. *For an integer n we denote by $\omega(n)$ the number of distinct prime factors. Then there exists an explicit constant $C > 0$ such that for every n,*

$$\omega(n) \leq C \frac{\log n}{\log \log n}.$$

Let F be a number field of degree d. Then for an integral ideal $\mathfrak{n} \trianglelefteq O_F$ with absolute norm $n = |\mathfrak{n}|$, the number of prime ideal factors is bounded by

$$\omega(\mathfrak{n}) \leq d \cdot \omega(n) \leq Cd \frac{\log n}{\log \log n}.$$

We remark that the average order of $\omega(n)$ is $\log \log n$.

Using that the number of ramified prime ideals in a relative extension E/F is $\omega(\mathfrak{d}(E/F))$, we prove our main result by applying Proposition 2.5 and Lemma 2.4.

Theorem 2.6. *Let E/F be an ℓ-group extension of degree $n = \ell^r$ and absolute discriminant $D := \mathrm{Disc}(E/F)$, and define $d := [F : \mathbb{Q}]$. Then we get:*

$$\mathrm{rk}_\ell(\mathrm{Cl}_E) \leq n\mathrm{rk}_\ell(\mathrm{Cl}_F) + nr \cdot Cd \frac{\log D}{\log \log D},$$

equivalently, we get for the size $h_\ell(E)$ of the ℓ-torsion part $\mathrm{Cl}_E[\ell]$:

$$h_\ell(E) \leq h_\ell(F)^n \cdot D^{\frac{Cdnr \log \ell}{\log \log D}} = O_{\epsilon,F,n}(D^\epsilon) \text{ for all } \epsilon > 0.$$

Remark 2.7. *Note that we easily get the following estimate for the ℓ^s-torsion*

$$h_{\ell^s}(E) \leq h_\ell(E)^s \leq h_\ell(F)^{ns} \cdot D^{\frac{Cdnrs \log \ell}{\log \log D}} = O_{\epsilon,F,n,s}(D^\epsilon).$$

3. Discriminant Multiplicity Conjecture for Nilpotent Extensions

In this section we prove Conjecture C for nilpotent groups.

Theorem 3.1. *Given a transitive nilpotent permutation group $G \leq S_n$ and a number field F, the number a_D of G-extensions E/F with $\mathrm{Disc}(E/F) = D$ is bounded above by*

$$a_D = O_{\epsilon,F,n}(D^\epsilon) \text{ for all } \epsilon > 0.$$

In a first step we prove this theorem for ℓ-groups and then use this for proving the case of arbitrary nilpotent groups. For the latter step we need a group theoretic lemma. This states that any transitive nilpotent permutation group $G \leq S_n$ is isomorphic to a natural direct product of its ℓ-Sylow subgroups. It is a standard fact that all nilpotent groups are isomorphic to the direct product of their ℓ-Sylow subgroups, however we emphasize that we need to prove the isomorphism in the category of *permutation groups*. Equivalently, this means that all nilpotent G-extensions (not necessarily Galois) can be realized as a compositum of ℓ-extensions.

Lemma 3.2. *A transitive nilpotent permutation group $G \leq S_n$ is permutation isomorphic to the natural direct product of transitive permutation groups $G_\ell \leq S_{n_\ell}$,*

$$G \simeq \prod_\ell G_\ell \text{ with } n = \prod_\ell n_\ell,$$

where the G_ℓ are the ℓ-Sylow subgroups of G.

Proof. Firstly, it is a standard result that a nilpotent group G is isomorphic to $\prod_\ell G_\ell$ where G_ℓ are the ℓ-Sylow subgroups of G. For any prime q, let us define the canonical projection $\pi_q : \prod_\ell G_\ell \to G_q$. Next, we show that an arbitrary subgroup $H \leq G$ satisfies $H \simeq \prod_\ell H_\ell$ where we define $H_\ell := \pi_\ell(H) \leq G_\ell$. On the one hand, by definition it is obvious that $H \leq \prod_\ell H_\ell$. On the other hand, by Chinese remainder theorem there exists an integer s such that

$$s \equiv 1 \bmod |H_\ell| \text{ and } s \equiv 0 \bmod |H_q| \text{ for all } q \neq \ell.$$

Therefore if $h = (h_\ell)_\ell \in H$, then $(\mathrm{id}, \ldots, h_p, \ldots, \mathrm{id}) = h^s \in H$, which implies $H_p \times \prod_{q \neq p} \{\mathrm{id}\} \leq H$ and thus $\prod_\ell H_\ell \leq H$.

Now suppose the permutation representation $G \leq S_n$ is realized by the action of G on the left cosets of $g_i H$ for $i = 1, \ldots, n$. It is isomorphic to the componentwise action of $\prod_\ell G_\ell$ on the left cosets of $\prod_\ell g_\ell H_\ell$, i.e., $G \simeq \prod_\ell G_\ell$ as a permutation group of degree $n = [G : H] = \prod_\ell [G_\ell : H_\ell]$. □

Lemma 3.3. *Let F be a number field of degree d, ℓ be a prime number, and $\mathfrak{d}$ be an ideal of $\mathcal{O}_F$. Then the number of C_ℓ-extensions E/F with $\mathfrak{d}(E/F) = \mathfrak{d}$ is bounded above by*

$$O_{d,\ell}(h_\ell(F) \cdot \ell^{\omega(\mathfrak{d})}) = O_{\epsilon,d,\ell}(h_\ell(F) \cdot D^\epsilon) = O_{\epsilon,F,\ell}(D^\epsilon) \text{ for all } \epsilon > 0.$$

Proof. Let E/F be such an extension. Then by class field theory the finite part $\mathfrak{f}_0$ of the conductor has the property that $\mathfrak{d} = \mathfrak{f}_0^{\ell-1}$. Denote by $\mathfrak{f}_\infty$ the set of real places, if $\ell = 2$ and let $\mathfrak{f}_\infty = \emptyset$ otherwise. Then E is contained in the ray class field of $\mathfrak{f} = \mathfrak{f}_0 \mathfrak{f}_\infty$ and we need an upper bound on the size of the ℓ-torsion of this ray class group $\mathrm{Cl}_\mathfrak{f}$. By class field theory we have the following short exact sequence,

where $\mathfrak{f}_0 = \prod_{\mathfrak{p}|\mathfrak{f}_0} \mathfrak{p}^{e_\mathfrak{p}}$:

$$\prod_{\mathfrak{p}|\mathfrak{f}_0} (\mathcal{O}_F/\mathfrak{p}^{e_\mathfrak{p}})^* \times \prod_{\mathfrak{p}|\mathfrak{f}_\infty} C_2 \to \mathrm{Cl}_\mathfrak{f} \to \mathrm{Cl}_F \to 0.$$

Therefore the ℓ-rank of $\mathrm{Cl}_\mathfrak{f}$ is bounded above by $\sum_{\mathfrak{p}|\mathfrak{f}_0} \mathrm{rk}_\ell((\mathcal{O}_F/\mathfrak{p}^{e_\mathfrak{p}})^*)+d+\mathrm{rk}_\ell(\mathrm{Cl}_F)$. Note that $\mathrm{rk}_\ell((\mathcal{O}_F/\mathfrak{p}^{e_\mathfrak{p}})^*) \leq 1$ for $\ell \notin \mathfrak{p}$ and $\mathrm{rk}_\ell((\mathcal{O}_F/\mathfrak{p}^{e_\mathfrak{p}})^*) \leq [F_\mathfrak{p} : \mathbb{Q}_\ell]+1$, if $\ell \in \mathfrak{p}$. Considering the wildly ramified primes, the extreme case happens when all wildly ramified primes are dividing $\mathfrak{f}_0$ and ℓ splits in F. In this situation the wildly ramified primes might increase the ℓ-rank by $2d$. The infinite places might increase the 2-rank by d and therefore we get the following upper bound:

$$\mathrm{rk}_\ell(\mathrm{Cl}_\mathfrak{f}) \leq \omega(\mathfrak{f}_0) + 3d + \mathrm{rk}_\ell(\mathrm{Cl}_F).$$

Therefore the number of C_ℓ-extensions E/F with $\mathfrak{d}(E/F) = \mathfrak{d}$ is bounded by $|\mathrm{Cl}_\mathfrak{f}[\ell]| = O_{d,\ell}(h_\ell(F) \cdot \ell^{\omega(\mathfrak{d})}) = O_{\epsilon,d,\ell}(h_\ell(F) \cdot D^\epsilon) = O_{\epsilon,F,\ell}(D^\epsilon)$ for all $\epsilon > 0$ by Proposition 2.5. □

Proof of Theorem 3.1. Denote by b_D the number of ideals $\mathfrak{d}$ of $\mathcal{O}_F$ such that $|\mathfrak{d}| = D$. We claim that $b_D = O_d(C^{\omega(D)})$ for some C depending on the degree d. This is bounded by $O_{\epsilon,d}(D^\epsilon)$. Therefore it suffices to prove that the number of G-extensions E/F with $\mathfrak{d}(E/F) = \mathfrak{d}$ is bounded by $O_{\epsilon,F,n}(D^\epsilon)$.

In order to prove the claim note that b_D is multiplicative and therefore it suffices to prove it for prime powers $D = p^s$. The worst case happens when p is split in F. Then the number of ideals is equal to $\binom{d+s-1}{d-1} \leq (s+1)^{d-1}$ and $s = O_d(\log D)$ which gives $\binom{d+s-1}{d-1} = O_d((\log D)^{d-1}) = O_{\epsilon,d}(D^\epsilon)$ for all $\epsilon > 0$.

Let us assume that $G \leq S_n$ is a transitive ℓ-group of degree $n = \ell^r$. We proceed by induction on r. When $r = 1$, then $G = C_\ell$ and we apply Lemma 3.3.

Suppose the statement holds for ℓ-extensions of degree $n = \ell^r$. Given an arbitrary ℓ-extension E/F of degree ℓ^{r+1}, there is a chain of subfields $E = E_{r+1} \geq E_r \geq \cdots \geq E_0 = F$ using Lemma 2.2. Denote $\mathfrak{d}(E_r/F) = \mathfrak{m}$, then we have $\mathfrak{m}^\ell \cdot \mathfrak{m}' = \mathfrak{d}$ by the discriminant formula for towers.

By induction for $n = \ell^r$, the number of extensions E_r/F with $\mathfrak{d}(E_r/F) = \mathfrak{m} \mid \mathfrak{d}$ is bounded by $O_{\epsilon,F,n}(|\mathfrak{m}|^\epsilon)$. Using Lemma 3.3 the number of E_{r+1}/E_r with relative discriminant $\mathcal{N}_{E_r/F}(\mathfrak{d}(E_{r+1}/E_r)) = \mathfrak{m}'$ is bounded by $O_{\epsilon,d,\ell}(h_\ell(E_r) \cdot |\mathfrak{m}'|^\epsilon)$. Since $h_\ell(E_r) = O_{\epsilon,F,n}(|\mathfrak{m}|^\epsilon)$ by Theorem 2.6, we get the bound $O_{\epsilon,F,n}(|\mathfrak{m}'|^\epsilon|\mathfrak{m}|^\epsilon)$ for the number of E_{r+1}/E_r with relative discriminant $\mathcal{N}_{E_r/F}(\mathfrak{d}(E_{r+1}/E_r)) = \mathfrak{m}'$.

Therefore for each $\mathfrak{m}^\ell \mid \mathfrak{d}$, the number of extensions E_{r+1}/F with $\mathfrak{d}(E_{r+1}/F) = \mathfrak{d}$ and $\mathfrak{d}(E_r/F) = \mathfrak{m}$ is bounded by $O_{\epsilon,d,n}(D^\epsilon)$. The number of divisors $\mathfrak{m} \mid \mathfrak{d}$ is bounded by $O_\epsilon(D^\epsilon)$. So the number of E_{r+1}/F with $\mathfrak{d}(E_{r+1}/F) = \mathfrak{d}$ in total is bounded by $O_{\epsilon,F,n}(D^\epsilon)$. This finishes the proof of the discriminant multiplicity conjecture for general ℓ-extensions.

Secondly, we deduce the discriminant multiplicity conjecture for nilpotent extensions from the one for ℓ-extensions. Given a transitive nilpotent permutation group $G \leq S_n$, by Lemma 3.2, we have

$$G \simeq \prod_{i=1}^s G_{\ell_i} \leq \prod_{i=1}^s S_{\ell_i^{s_i}} \leq S_n \text{ for } n = \prod_{i=1}^s \ell_i^{s_i}.$$

Therefore each G-extension E/F is the compositum of ℓ_i-extensions E_{ℓ_i}/F with $\mathrm{Gal}(E_{\ell_i}/F) = G_\ell \leq S_{\ell_i^{s_i}}$. Therefore the number of G-extensions E/F with $\mathfrak{d}(E/F) =$

$\mathfrak{d}$ is bounded by the number of tuples $(E_{\ell_1}, \ldots, E_{l_s})$ of ℓ_i-extensions with $\mathfrak{d}(E_{\ell_i}/F) \mid \mathfrak{d}$ and $\mathrm{Gal}(E_{\ell_i}/F) = G_{\ell_i}$ for each i. Combining the result on ℓ-extensions and the fact that the number of divisors of $\mathfrak{d}$ is bounded by $O_{\epsilon,n}(D^\epsilon)$, we deduce that the number of E_ℓ/F for each prime $\ell \mid n$ is bounded by $O_{\epsilon,F,n_\ell}(D^\epsilon)$. Taking the product over all $\ell \mid n$, we get the number of such tuples is bounded by $O_{\epsilon,F,n}(D^{\omega(n)\epsilon}) = O_{\epsilon,F,n}(D^\epsilon)$. □

Remark 3.4. *Since all conjectures are shown to be true in this paper when we restrict to cases of consideration, we do not intend to give a full treatment on the implication from Conjecture C to Conjecture A, which is a inverse direction of the above theorem. In* [5, 12]*, the implication from Conjecture C on degree $\ell \cdot n$-extensions to Conjecture A on ℓ-torsion in class groups of degree n-extensions is given in a general setting.*

4. Malle's Conjecture for Nilpotent Extensions

Corollary 4.1. *Given a transitive nilpotent permutation group $G \leq S_n$ and a number field F, the number of G-extensions E/F with $\mathrm{Disc}(E/F) \leq X$ is bounded above by:*

$$N(F, G; X) = O_{F,\epsilon}(X^{1/a(G)+\epsilon}) \text{ for all } \epsilon > 0.$$

Proof. We define $\mathcal{A} := \{D \in \mathbb{Z} : p \mid D \implies p^{a(G)} \mid D\}$. Let a_D be the number of fields E/F with Galois group G and $D = \mathrm{Disc}(E/F)$. Note that $a_D = 0$, if $D \notin \mathcal{A}$, see [9, Section 7]. Then for any $\epsilon > 0$, there exists a constant C_ϵ by Theorem 3.1 such that

$$N(F, G; X) = \sum_{D \in \mathcal{A}, D < X} a_D \leq \sum_{D \in \mathcal{A}, D < X} C_\epsilon \cdot D^\epsilon \leq C_\epsilon \cdot F(X) \cdot X^\epsilon,$$

where we define $F(X) := \sharp\{D \in \mathcal{A} : D < X\}$ to be the counting function associated to $\mathcal{A}$. We will show that

$$F(X) \sim C' \cdot X^{1/a(G)}, \tag{4}$$

for some $C' > 0$, therefore $F(X) = O(X^{1/a(G)})$. The generating series $f(s)$ of $\mathcal{A}$ is

$$f(s) = \prod_p (1 + \sum_{k \geq a(G)} p^{-ks}) = \zeta(a(G)s) \cdot g(s),$$

where

$$g(s) = \prod_p (1 + \sum_{a(G)+1 \leq k \leq 2a(G)-1} p^{-ks}),$$

is a holomorphic function when $\Re(s) > 1/(a(G)+1)$. The function $f(s)$ thus has an analytic continuation to $\Re(s) \geq 1/a(G)$ except for a simple pole at $s = 1/a(G)$. We get (4) from a Tauberian theorem, e.g. see [11, p. 121]. Then the result follows since $C_\epsilon \cdot F(X) \cdot X^\epsilon = O_\epsilon(X^{1/a(G)+\epsilon})$. Actually, note that an upper bound for $F(X)$ of order $O_\epsilon(X^{1/a(G)+\epsilon})$ is enough for our proof. □

Remark 4.2. *Note that we do not use anything special about nilpotent groups for this proof. The proof for Corollary 4.1 indicates that Conjecture C implies Conjecture B for any finite transitive Galois group G.*

Remark 4.3. *In order to show an inverse direction of the above corollary in the general setting, see* [5] *where Conjecture B on subgroups of G^k for all integers k implies Conjecture C for G-extensions.*

Acknowledgment

Wang is partially supported by Foerster-Bernstein Fellowship at Duke University, and would like to thank Melanie Matchett Wood for helpful conversations. The authors would like to thank for the hospitality of the Mathematisches Forschungsinstitut in Oberwolfach and the organizers of the workshop Explicit Method in Number Theory 2018 where this collaboration begins. The authors would like to thank Manjul Bhargava for many helpful conversations during the time at Oberwolfach. The authors would like to thank Brandon Alberts and Gunter Malle for suggestions on an earlier draft. This project is accomplished during the Research in Pairs (RIP) program at Mathematisches Forschungsinstitut in Oberwolfach in 2019, supported by the Volkswagen-Stiftung.

References

[1] Brandon Alberts. The weak form of Malle's conjecture and solvable groups. *Res. Number Theory*, 6(1):Art. 10, 23, 2020.

[2] Armand Brumer and Joseph H. Silverman. The number of elliptic curves over $\mathbf{Q}$ with conductor N. *Manuscripta Math.*, 91(1):95–102, 1996.

[3] Gary Cornell. Relative genus theory and the class group of l-extensions. *Trans. Amer. Math. Soc.*, 277(1):421–429, 1983.

[4] William Duke. Bounds for arithmetic multiplicities. In *Proceedings of the International Congress of Mathematicians, Vol. II (Berlin, 1998)*, number Extra Vol. II, pages 163–172, 1998.

[5] Jordan S. Ellenberg and Akshay Venkatesh. Counting extensions of function fields with bounded discriminant and specified Galois group. In *Geometric methods in algebra and number theory*, volume 235 of *Progr. Math.*, pages 151–168. Birkhäuser Boston, Boston, MA, 2005.

[6] Georges Gras. The p-rank ϵ-conjecture on class groups is true for towers of p-extensions. *arxiv: 2001.07500*, 2020.

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

[8] Jürgen Klüners and Gunter Malle. Counting nilpotent Galois extensions. *J. Reine Angew. Math.*, 572:1–26, 2004.

[9] Gunter Malle. On the distribution of Galois groups. *J. Number Theory*, 92(2):315–329, 2002.

[10] Gunter Malle. On the distribution of Galois groups. II. *Experiment. Math.*, 13(2):129–135, 2004.

[11] Wladyslaw Narkiewicz. *Number theory*. World Scientific Publishing Co., Singapore; distributed by Heyden & Son, Inc., Philadelphia, PA, 1983.

[12] Lillian B. Pierce, Caroline L. Turnage-Butterbaugh, and Melanie Matchett Wood. On a conjecture for ℓ-torsion in class groups of number fields: from the perspective of moments. *arXiv: 1902.02008*, 2019.

[13] Michael Rosen. Class groups in cyclic ℓ-extensions: comments on a paper by G. Cornell. *Proc. Amer. Math. Soc.*, 142(1):21–28, 2014.

[14] Gérald Tenenbaum. *Introduction to analytic and probabilistic number theory*, volume 163 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, third edition, 2015.

[15] Shou-Wu Zhang. Equidistribution of CM-points on quaternion Shimura varieties. *Int. Math. Res. Not.*, (59):3657–3689, 2005.

Universität Paderborn, Institut für Mathematik, Warburger Str. 100, 33098 Paderborn, Germany

Email address: klueners@math.uni-paderborn.de

Duke University, Department of Mathematics, Durham, NC, 27708, US

Email address: wangjiuy@math.duke.edu