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, a conjecture of Malle giving an upper bound for the number of extensions, and the discriminant multiplicity conjecture. We prove that the latter two conjectures are equivalent in some sense. Altogether, the three conjectures are equivalent for the class of solvable groups. We then prove the ℓ-torsion conjecture for ℓ-groups and the other two conjectures for nilpotent groups.

1. INTRODUCTION

In this paper, we study several conjectures in arithmetic statistics. In all situations E/F will be an extension of degree n of number fields with absolute discriminant $\mathrm{Disc}(E/F)$ which is the absolute norm of the discriminant ideal $\mathfrak{d}(E/F)$.

Conjecture A (ℓ-torsion conjecture, [4, 6, 28])**.** *Let ℓ be a prime number and E/F be an extension with absolute discriminant D and degree $n = [E : F]$. Then the size $h_\ell(E)$ of the ℓ-torsion in the class group of E is*

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

We write $\mathrm{Gal}(E/F) = G \leq S_n$ if the Galois group of the Galois closure $\hat{E}/F$ of E/F viewed as permutation group on the set of embeddings of E into $\hat{E}$ is permutation isomorphic to G. In our second conjecture we consider the function

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

By a famous result of Hermite (e.g. see [19, Theorem 2.24, page 68]) there are only finitely many number fields with the same given discriminant.

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 [16].

Conjecture B (Malle's Conjecture (weak version of the upper bound), [16])**.** *Let F be a number field and $G \leq S_n$ be a transitive group. Then we have*

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

In the same paper Malle conjectures a lower bound which is equivalent to

$$\liminf_{X\to\infty} X^{-1/a(G)} N(F, G; X) > 0.$$

2010 *Mathematics Subject Classification.* Primary 11R29; Secondary 11R37.

We remark that Malle gives a refined version of the conjecture in [17], which we do not need in our context here. There are also counter-examples known due to the first author [12] for this refined conjecture.

In our last conjecture we consider the number

$$a_D := \#\{E/F \mid \mathrm{Gal}(E/F) = G, \mathrm{Disc}(E/F) = D\}$$

of G-extensions of F with discriminant $\mathrm{Disc}(E/F) = D$.

Conjecture C (Discriminant Multiplicity Conjecture, [6, 8])**.** *Let F be a number field and $G \leq S_n$ be a transitive group. Then for all $D \in \mathbb{N}$ we have*

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

The goal of this paper is twofold: on one hand, to show the relations among Conjectures A, B, and C; on the other hand, to show that these conjectures have affirmative answers when we restrict our discussion to certain general families of number fields.

These conjectures share the common feature that they are all about giving upper bounds on the number of arithmetic objects, including number fields and class numbers. We will show that they are almost all equivalent to each other.

Proposition 1.2. *Let F be a number field. Then*

(i) *Assume that Conjecture C is true for all $G \leq S_{n\ell}$, then Conjecture A is true for ℓ and for all extensions E/F of degree n.*
(ii) *Assume that Conjecture A is true for all solvable extensions E/F and all prime numbers ℓ. Then Conjecture B is true for all solvable groups G.*

Proof. Part (i) is shown in [8, p. 164] and [21, Thm 1.7]. The second part is [1, Cor. 1.6]. □

A little bit stronger Alberts proves in [1, Corollary 1.4] that Conjecture B is true for solvable groups, if we assume that the torsion conjecture is true in average.

Noticing that Conjecture B is essentially an average statement of Conjecture C, it is not surprising that in general Conjecture C implies Conjecture B. We manage to prove that they are equivalent.

Theorem 1.3. *Let F be a number field. Then*

(i) *Conjecture B for all finite groups G implies Conjecture C for all finite groups G.*
(ii) *Conjecture C for $G \leq S_n$ implies Conjecture B for G.*

The first part is shown in Theorem 4.1 and the second part in Theorem 4.4.

We remark that Proposition 1.2 (i) and Theorem 1.3 (i) will be also true for the class of solvable extensions, see Corollary 4.7. Therefore we get:

Corollary 1.4. *Conjectures A, B, and C are equivalent when we restrict to solvable extensions E/F.*

We remark that we do not expect that the similar statement for nilpotent extensions E/F is true. The reason is that if you want to consider ℓ–torsion of the class group for p–extensions, then the resulting Galois groups are solvable, but in most cases not nilpotent.

We then focus on proving some special cases of these conjectures. Conjecture A has a clear dichotomy depending on whether $\mathrm{Cl}_E[\ell]$ is randomly distributed.

Classically, it is only known to be true when $F = \mathbb{Q}$ and $\ell = 2$ for $[E : F] = 2$ by Gauss using genus theory. Firstly, we give a compact proof on all cases for Conjecture A where a similar argument with $\ell = 2$ for quadratic extensions applies, i.e., when the distribution of $\mathrm{Cl}_E[\ell]$ is governed by genus theory. We say a field extension E/F is an ℓ-extension when $\mathrm{Gal}(E/F)$ is an ℓ-group.

Theorem 1.5. *Conjecture A holds for the ℓ-torsion of class groups of ℓ-extensions.*

We will prove a more precise version in Theorem 2.7. Results on Conjecture A for ℓ, where E/F is not an ℓ–extension are much more difficult to prove. Heuristically, Conjecture A is shown to be a consequence of the moments version of the Cohen-Lenstra heuristics in [21]. We mention some results in this direction: $\ell = 2$ [3], $\ell = 3$ with $d \leq 4$ [8], and for arbitrary ℓ with $\mathrm{Gal}(E/F) = (\mathbb{Z}/p\mathbb{Z})^r$ $(r > 1)$ [26]. There are also recent works [2, 7, 9, 10, 20, 25, 27] on proving a non-trivial bound on the ℓ-torsion of class groups for almost all number fields in some certain family of number fields.

In Section 3 we prove the following theorem by applying Theorem 1.5.

Theorem 1.6. *Conjecture C holds for nilpotent number field extensions E/F.*

Finally, by applying Theorems 1.6 and 1.3, we recover the following theorem.

Theorem 1.7. *Conjecture B holds for nilpotent number field extensions E/F.*

We mention that Theorem 1.7 is also proved in [13] for Galois nilpotent extensions and in [1] for general nilpotent extensions. We recover this theorem as a direct consequence of Theorem 1.6, and therefore give a short and simplified proof.

We finally remark that, as shown in the proof of Theorem 2.1, the fundamental reason for these conjectures to hold in such a perfect shape in these cases is completely group theoretic, i.e., nilpotent groups have non-trivial center.

All results in this paper are effective.

2. ℓ-TORSION CONJECTURE

In this section we prove Theorem 1.5. We give a more detailed version in Theorem 2.7. We start with the following theorem, which is proved in [5, Theorem 2.2] for odd ℓ and generalized in [23, 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 $\mathrm{Gal}(M/L)$ 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:

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

Remark 2.2. *In case* $\mathrm{rk}_\ell(\mathrm{Cl}_F) = 0$ [23, Theorem 2.2] *and* [5, Theorem 2] *prove a slightly better upper bound for* $\mathrm{rk}_\ell(\mathrm{Cl}_E)$*, i.e.* $\mathrm{rk}_\ell(\mathrm{Cl}_E) \leq (\ell-1)\cdot(e-1)$*. It is known that for* $F = \mathbb{Q}$ *and* $\ell = 2$ *this bound is sharp by genus theory. Furthermore,* [5, Theorem 2.7] *also gives a better bound for the cyclic of order* ℓ^r*-case compared to the inductive approach we present in Theorem 2.4.*

We do not prove this remark since we are only interested in the asymptotic behavior and therefore the change of constants does not matter. In order to prove Theorem 2.4 for non normal extensions we need the following lemma.

Lemma 2.3. *Let* $n = \ell^r$ *and* $G \leq S_n$ *be an* ℓ*-group and* E/F *be an extension of number fields with* $\mathrm{Gal}(E/F) \cong G$*. 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 $G \cong G_0 \supset G_1 \supset \cdots \supset G_r = H$ 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 [5, page 424] describes just before Theorem 3 how to get this result for normal ℓ-extensions.

Theorem 2.4. *Let* $n = \ell^r$*,* $G \leq S_n$ *be a transitive* ℓ*-group, and* E/F *be an extension of number fields with* $\mathrm{Gal}(E/F) \cong G$*, 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 2.3 we find a tower of cyclic extensions of order ℓ. The assertion now follows by applying Theorem 2.1 for each step. $\square$

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 extreme 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 2.5. *Let $G \leq S_n$ be a transitive ℓ-group and E/F be an extension with $\mathrm{Gal}(E/F) \cong G$ 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 [24, Section 5.3, p. 83].

Proposition 2.6. *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 $n > 2$,*

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

Let F be a number field of degree d. Then for an integral ideal $\mathfrak{n} \trianglelefteq O_F$ with absolute norm $n = |\mathfrak{n}| > 2$, the number $\omega(\mathfrak{n})$ of distinct 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 $\log\log n$. Note that we can choose $C = 1.3841$, see [22, Thm. 11].

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 2.6 and Lemma 2.5.

Theorem 2.7. *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:*

$$\mathrm{rk}_\ell(\mathrm{Cl}_E) \leq n\mathrm{rk}_\ell(\mathrm{Cl}_F) + nr \cdot Cd \frac{\log D}{\log\log D} \text{ for } D > 2,$$

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

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

For $D = 1$ we get $\mathrm{rk}_\ell(\mathrm{Cl}_E) \leq n\mathrm{rk}_\ell(\mathrm{Cl}_F)$ and therefore $h_\ell(E) \leq h_\ell(F)^n$.

Note that the case $D = 2$ is not possible by Hilbert's ramification theory. The reader can also find an independent proof of Theorem 2.7 by G. Gras [11, pp. 2 and 9], which he gave after seeing our preprint. We remark that the Galois group of all fields in his family $\mathcal{F}_K^{p^e}$ are also p–groups.

Remark 2.8. *Note that we easily get the following estimate for the ℓ^s-torsion*

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

Theorem 2.4 or Lemma 2.5 are not expected to be sharp, but will be sufficient for our purpose, since we only aim at proving Conjecture A. However, it is also an independent interesting question to study the upper bound at a finer scale. We mention results along this direction [14, 15] for $F = \mathbb{Q}$, where a sharp upper bound is obtained for $\ell = 2$ and certain special family of multi-quadratic number fields.

3. Discriminant Multiplicity Conjecture for Nilpotent Extensions

The goal of this section is to prove Theorem 1.6 which answers Conjecture C positively in the nilpotent case. As usual we can reduce the nilpotent case to the ℓ–group case, but we have to be a little bit careful (see Lemma 3.1) that this reduction is compatible with permutation groups. For the ℓ–group case we use the upper bound proved in Theorems 2.4 and 2.7. 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 3.1. *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 isomorphic to the ℓ-Sylow subgroups of G and n_ℓ is the maximal ℓ-power dividing n.

Proof. Firstly, it is a standard result that a nilpotent group G is equal to the direct product $\prod_{\ell|n} \mathrm{Syl}_\ell(G)$ where $\mathrm{Syl}_\ell(G)$ is the ℓ-Sylow subgroup of G. Let $H \leq G$ be a stabilizer of a point. This means that G can be realized by the action of G on the left cosets of G/H. Now H is nilpotent as well and therefore it is a direct product of its Sylow subgroups. We get:

$$H = \prod_{\ell|n} \mathrm{Syl}_\ell(H) \text{ with } \mathrm{Syl}_\ell(H) \leq \mathrm{Syl}_\ell(G).$$

Now we can define the permutation groups G_ℓ by the action of $\mathrm{Syl}_\ell(G)$ on the left cosets of $\mathrm{Syl}_\ell(G)/\mathrm{Syl}_\ell(H)$ for each prime ℓ dividing n. Since $H = \prod_{\ell|n} \mathrm{Syl}_\ell(H)$ we see that G is permutation isomorphic to the natural direct product $\prod_{\ell|n} G_\ell \leq S_n$ of permutation groups. □

Lemma 3.2. *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:

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

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 $\mathrm{rk}_\ell((\mathcal{O}_F/\mathfrak{p}^{e_\mathfrak{p}})^*) \le 1$ for $\ell \notin \mathfrak{p}$ and $\mathrm{rk}_\ell((\mathcal{O}_F/\mathfrak{p}^{e_\mathfrak{p}})^*) \le [F_\mathfrak{p} : \mathbb{Q}_\ell]+1$, 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:

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

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 2.6. □

Proof of Theorem 1.6. 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 $\binom{d+s-1}{d-1} \le (s+1)^{d-1}$ 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 $G \le S_n$ 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 3.2.

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 $E = E_{r+1} \ge E_r \ge \cdots \ge E_0 = F$ using Lemma 2.3. 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 3.2 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 2.7, 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 $G \le S_n$, by Lemma 3.1, we have

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

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

$\mathfrak{d}$ is bounded by the number of tuples $(E_{\ell_1}, \dots, E_{l_s})$ 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 that the number of such tuples is bounded by $O_{\epsilon,F,n}(D^{\omega(n)\epsilon}) = O_{\epsilon,F,n}(D^\epsilon)$. □

4. Malle's Conjecture for Nilpotent Extensions

The goal of this section is to prove Theorems 1.3 and 1.7. The proof of Theorem 1.3 is split into proving Theorems 4.1 and 4.4. The proof of Theorem 1.7 is the content of Corollary 4.2.

Theorem 4.1. *Let $G \leq S_n$ be a transitive permutation group and F be a number field. Assume that Conjecture C is true for F and G. Then Conjecture B is also true for F and G, i.e. the number of G-extensions E/F with $\mathrm{Disc}(E/F) \leq X$ is bounded above by:*

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

Proof. Let $\mathcal{A} := \{D \in \mathbb{Z} : p \mid D \implies p^{a(G)} \mid D\}$ and $\mathcal{A}(X) := \sharp\{D \in \mathcal{A} : D < X\}$ be the counting function associated to $\mathcal{A}$. 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 [16, Section 7]. Then for any $\epsilon > 0$, there exists a constant $C_{F,\epsilon,n}$ by Conjecture C such that

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

We will show that

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

for some $C' > 0$, therefore $\mathcal{A}(X) = O(X^{1/a(G)})$. 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 [18, p. 121]. Then the result follows since $C_{F,\epsilon,n} \cdot \mathcal{A}(X) \cdot X^\epsilon = O_{F,\epsilon,n}(X^{1/a(G)+\epsilon})$. □

Note in the above proof that $\mathcal{A}(X) = O_\epsilon(X^{1/a(G)+\epsilon})$ for all $\epsilon > 0$ can be easily derived without using a Tauberian theorem. This is certainly sufficient to finish the proof. Using Theorems 1.6 and 4.1 we immediately get the following corollary which is the content of Theorem 1.7.

Corollary 4.2. *Let G be a transitive nilpotent group. Then Conjecture B is true for all $\epsilon > 0$ and all number fields F.*

Now we prove some version of the inverse implication of Theorem 4.1. We cannot expect that Conjecture B for a single G implies Conjecture C for the same G, because it is easy to write down series of numbers a_m which have a given asymptotic behavior, but a single a_m is not bounded by $O(m^\epsilon)$ for all $\epsilon > 0$. E.g. we can take the series

$$a_m = \begin{cases} \sqrt{m} & \text{if } m \text{ is a square,} \\ 0 & \text{otherwise.} \end{cases} \quad \text{and we see } \sum_{m \leq x} a_m \sim x/2,$$

but $a_m = \sqrt{m}$ for infinitely many m. In order to prove Conjecture C we need some control over the higher moments. We can get this control when we assume Conjecture B for so-called allowable permutation groups (see Definition 4.3), which are suitable subgroups of the direct product G^k. Using this assumption we are able to prove in Theorem 4.4 that Conjecture C holds.

Let us consider G-extensions E_i/F for $1 \leq i \leq k$ for a transitive $G \leq S_n$. We are interested in the Galois group of the tensor product $K = \otimes_{i=1}^k E_i$ which is a subgroup of G^k. Note that $K = K_1 \cdots K_m$ is a product of fields and for $m = 1$ it can be interpreted as the compositum of the E_i. We define $\rho : G_F \to G^k \leq S_{n^k}$, where G_F denotes the absolute Galois group of F. The image $\rho(G_F)$ might not be transitive of degree n^k, equivalently, this means that K is not a field. Note that the number of orbits of $\rho(G_F)$ is equal to m and if ordered in the right way we get that $|O_i| = [K_i : F]$. Choosing one orbit $O := O_i$ of size nd and the corresponding field $E := K_i$ we get a permutation representation for $\mathrm{Gal}(E/F) \leq S_{nd}$.

Definition 4.3. Given a transitive $G \leq S_n$ and an integer k. We say $U \leq G^k$ is an *allowable subgroup* of the natural direct product G^k if for every $1 \leq i \leq k$, we have $\pi_i(U) = G$ where $\pi_i : G^k \to G$ is the natural projection to the i-th component. If $O \subseteq \{1, \cdots, n^k\}$ is an orbit of U of size nd, we will say that the transitive action of U on O is an *allowable permutation subgroup* $H \leq S_O$ of G^k.

Theorem 4.4. *Let F be a number field and $G \leq S_n$ be a transitive group. Then the correctness of Conjecture B for F and for all allowable permutation subgroups H of $G^k \leq S_{n^k}$ for all $k > 0$ implies the correctness of Conjecture C for F and G.*

A similar idea was used in [8, Prop. 4.8] for $F = \mathbb{Q}$. Instead of counting by discriminants D they assume a Malle conjecture for counting number fields by the radical of the discriminant. We need two lemmata before we can prove this theorem.

Lemma 4.5. *Given a sequence $\{a_m\}$ of non-negative real numbers, then the following statements are equivalent:*

(i) $\forall \epsilon > 0 : a_m = O_\epsilon(m^\epsilon)$.
(ii) *There exists an $A > 0$ such that for all $k > 0$:* $\sum_{X < m \leq 2X} a_m^k = O_k(X^A)$.
(iii) *There exists an $A > 0$ such that for all $k > 0$:* $\sum_{m \leq X} a_m^k = O_k(X^A)$.

Proof. It is easy to see that (ii) and (iii) are equivalent. To go from (ii) to (iii) it suffices to add up over dyadic ranges. The other direction is immediate.

To go from (i) to (ii) is immediate for any $A > 1$. To go from (ii) to (i), for any fixed $\epsilon > 0$, we apply the following Chebychev type inequality which is easy to see here. We get for all $k > 0$:

$$X^{k\epsilon} \cdot \sum_{X < m \leq 2X, a_m > X^\epsilon} 1 \leq \sum_{X < m \leq 2X, a_m > X^\epsilon} a_m^k \overset{(ii)}{=} O_k(X^A).$$

Choosing $k > A/\epsilon$ we get that

$$\sum_{X<m\leq 2X, a_m>X^\epsilon} 1 = O_k(X^{A-k\epsilon}),$$

which must be 0 when X is large enough. Therefore for any $\epsilon > 0$, there exists a $X > 0$ such that when $m > X$, we have $a_m \leq m^\epsilon$. □

We remind the reader that $\mathrm{ind}(G)$ is defined in Definition 1.1. We denote the degree of the permutation group G by $\deg(G)$.

Lemma 4.6. *Let $G \leq S_n$ be a transitive permutation group, k be an integer and H be an allowable permutation subgroup of G^k. Then we get the following inequality:*

$$\frac{\deg}{\mathrm{ind}}(H) \leq \frac{\deg}{\mathrm{ind}}(G).$$

Proof. Let H be an allowable permutation subgroup of G^k acting on nd points. If $nd < n^k$ it might be that we only see $1 \leq \ell \leq k$ projections to G. Suppose that $g \in H$ is a non-trivial element. This implies that g is a non-trivial element in at least one projection $\kappa : H \to G$ and we define $\bar{g} := \kappa(g)$. By the definition of $\mathrm{ind}(G)$ we have that $\mathrm{ind}(\bar{g}) \geq \mathrm{ind}(G)$. Let us look at all possible preimages of $\bar{g}$ under κ. The index of those elements will be minimal if each cycle of length r of $\bar{g}$ will decompose into d different cycles of length r. Therefore we get for a preimage $\tilde{g}$ of g under κ:

$$\#\{\text{cycles of } \tilde{g}\} \leq d\#\{\text{cycles of } \bar{g}\}.$$

Therefore we get:

$$\begin{aligned}\mathrm{ind}(\tilde{g}) &= nd - \#\{\text{cycles of } \tilde{g}\} \geq nd - d\#\{\text{cycles of } \bar{g}\} \\ &= d(n - \#\{\text{cycles of } \bar{g}\}) = d \cdot \mathrm{ind}(\bar{g}).\end{aligned}$$

This line is equivalent to

$$\frac{1}{\mathrm{ind}(\tilde{g})} \leq \frac{1}{d \cdot \mathrm{ind}(\bar{g})} \Leftrightarrow \frac{nd}{\mathrm{ind}(\tilde{g})} \leq \frac{n}{\mathrm{ind}(\bar{g})} = \frac{\deg(G)}{\mathrm{ind}(\bar{g})} \leq \frac{\deg(G)}{\mathrm{ind}(G)}.$$

Note that $\deg(H) = nd$ and $\mathrm{ind}(\tilde{g}) \leq \mathrm{ind}(H)$ in order to finish the proof. □

Note that in the special case $H = G^k$ the above proof shows

$$\frac{\deg}{\mathrm{ind}}(G^k) = \frac{\deg}{\mathrm{ind}}(G)$$

by using $\mathrm{ind}(g) = \mathrm{ind}(G)$ implies that $\mathrm{ind}((g, 1, \ldots, 1)) = \mathrm{ind}(G^k)$.

Proof of Theorem 4.4. We will prove that there exist constants $C_1 > 0$ and $C_2 > 0$ such that for all $k > 0$

$$\sum_{D\leq X} a_D^k \ll_k \sum_H N(F, H; C_2 X^{C_1 a(H)}) \overset{\text{Conj. B}}{=} O_{F,\epsilon,k}(X^{C_1+\epsilon}), \tag{5}$$

where the (finite) summation goes over all allowable permutation subgroups H of G^k. Then the result follows from condition (iii) in Lemma 4.5 by letting a_D be the number of G-extensions E/F with $\mathrm{Disc}(E/F) = D$.

For proving (5), it suffices to find constants $C_1 > 0$ and $C_2 > 0$ for a given allowable permutation subgroup $H \leq S_{nd}$ we consider composita $E := \prod_{i=1}^k E_i$ such that $\mathrm{Disc}(E/F) \leq C_2 X^{C_1 a(H)}$ when $\mathrm{Disc}(E_i/F) = D \leq X$ for every i and $\mathrm{Gal}(E/F) = H$. Now we study the discriminant $\mathrm{Disc}(E/F)$. Recall by Hilbert's

ramification theory that the valuation $v_{\mathfrak{p}}(\mathfrak{d}(E/F)) < [E:F]$ for an at most tamely ramified prime ideal $\mathfrak{p} \subseteq O_F$. The same estimate is true for all other prime ideals of O_F lying over the same prime number $p = \mathfrak{p} \cap \mathbb{Z}$. Therefore we get $v_p(|\mathfrak{d}(E/F)|) \leq [E:F][F:\mathbb{Q}]$.

This implies that $\mathrm{Disc}(E/F) \leq C_2 D^{[E:\mathbb{Q}]}$, where C_2 is a bounded factor coming from wildly ramified primes. Assuming $D \leq X$ and $\deg(H) = [E:F]$ we get:

$$\mathrm{Disc}(E/F) \leq C_2 X^{[E:\mathbb{Q}]} \leq C_2 X^{[F:\mathbb{Q}]\mathrm{ind}(H)\cdot(\deg/\mathrm{ind})(H)} \leq C_2 X^{[F:\mathbb{Q}]a(H)\cdot(\deg/\mathrm{ind})(G)}$$

by Lemma 4.6. Now we see that we can take $C_1 = [F:\mathbb{Q}](\deg/\mathrm{ind})(G)$. □

Corollary 4.7. *Let F be a number field. Assume that Conjecture B is true for all solvable groups G. Then Conjecture C is true for all solvable groups.*

Proof. Noting that all allowable (permutation) subgroups of G^k are solvable when G is solvable, the results follows directly from Theorem 4.4. □

In a similar way Proposition 1.2 (i) can be proved for the class of solvable extensions. Here we use that subgroups of $C_\ell \wr H$ are solvable when H is solvable.

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] C. An. ℓ-torsion in class groupf of certain D_4-quartic fields. *arXiv:1808.02148v1*, 2018.
[3] M. Bhargava, A. Shankar, T. Taniguchi, F. Thorne, J. Tsimerman, and Y. Zhao. Bounds on 2-torsion in class groups of number fields and integral points on elliptic curves. *arXiv: 1701.02458*, 2017.
[4] Armand Brumer and Joseph H. Silverman. The number of elliptic curves over **Q** with conductor N. *Manuscripta Math.*, 91(1):95–102, 1996.
[5] Gary Cornell. Relative genus theory and the class group of l-extensions. *Trans. Amer. Math. Soc.*, 277(1):421–429, 1983.
[6] 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.
[7] J. Ellenberg, L. B. Pierce, and M. M. Wood. On ℓ-torsion in class groups of number fields. *arXiv: 1606.06103*.
[8] 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.
[9] Christopher Frei and Martin Widmer. Average bounds for the ℓ-torsion in class groups of cyclic extensions. *Res. Number Theory*, 4(3):Art. 34, 25, 2018.
[10] Christopher Frei and Martin Widmer. Averages and higher moments for the ℓ-torsion in class groups. *arXiv:1810.04732*, 2018.

[11] Georges Gras. The p-rank ϵ-conjecture on class groups is true for towers of p-extensions. *arxiv: 2001.07500*, 2020.
[12] Jürgen Klüners. A counterexample to Malle's conjecture on the asymptotics of discriminants. *C. R. Math. Acad. Sci. Paris*, 340(6):411–414, 2005.
[13] Jürgen Klüners and Gunter Malle. Counting nilpotent Galois extensions. *J. Reine Angew. Math.*, 572:1–26, 2004.
[14] Peter Koymans and Carlo Pagano. Higher genus theory, 2019. to appear in IMRN.
[15] Peter Koymans and Carlo Pagano. A sharp upper bound for the 2-torsion of class groups of multiquadratic fields. *arXiv: 1909.13871*, 2020.
[16] Gunter Malle. On the distribution of Galois groups. *J. Number Theory*, 92(2):315–329, 2002.
[17] Gunter Malle. On the distribution of Galois groups. II. *Experiment. Math.*, 13(2):129–135, 2004.
[18] Wladyslaw Narkiewicz. *Number theory*. World Scientific Publishing Co., Singapore; distributed by Heyden & Son, Inc., Philadelphia, PA, 1983.
[19] Wladyslaw Narkiewicz. *Elementary and analytic theory of algebraic numbers*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, third edition, 2004.
[20] L. B. Pierce, C. Turnage-Butterbaugh, and M. M. Wood. An effective Chebotarev density theorem for families of number fields, with an application to ℓ-torsion in class groups. *arXiv: 1709.09637*.
[21] 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.
[22] Guy Robin. Estimation de la fonction de Tchebychef θ sur le k-ième nombre premier et grandes valeurs de la fonction $\omega(n)$ nombre de diviseurs premiers de n. *Acta Arith.*, 42(4):367–389, 1983.
[23] Michael Rosen. Class groups in cyclic ℓ-extensions: comments on a paper by G. Cornell. *Proc. Amer. Math. Soc.*, 142(1):21–28, 2014.
[24] Gérald Tenenbaum. *Introduction to analytic and probabilistic number theory*, volume 163 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, third edition, 2015.
[25] J. Thorner and A. Zaman. A zero density estimate for Dedekind zeta functions. *arXiv:1909.01338v1*, 2019.
[26] Jiuya Wang. Pointwise bound for ℓ-torsion in class groups: Elementary abelian extensions, 2020. to appear in Crelle.
[27] M. Widmer. Bounds for the ℓ-torsion in class groups. *arXiv:1709.10137*, 2017.
[28] 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