On Induction Theorem of Characters with Positivity

Zizai Cui, Max Fleischer, Pam Gu, Yijia Liu, Jiuya Wang

May 25, 2022

Abstract

We formulate a new character induction problem, motivated by class number problem. We say a group G admits an H-decomposition if $\operatorname{Ind}_H^G 1_H$ is a positive linear combinations of $\operatorname{Ind}_{H_i}^G 1_{H_i}$ up to copies of 1_G. If a transitive group G admits an H-decomposition then $|\operatorname{Cl}_{K^H}[\ell]|$ and $\operatorname{Disc}(K^H)$ can be written as a product of $\operatorname{Disc}(K^{H_i})$ and $\operatorname{Cl}_{K^{H_i}}[\ell]$ when $(\ell, |G|) = 1$. For a transitive permutation group $G \subset S_n$ and any number field k, we prove a non-trivial unconditional pointwise upper bound on $\operatorname{Cl}_K[\ell]$ for G-extension K/k if G admits an Stab(1)-decomposition. For $H = e$, we give if and only if criterias on G with $\{e\}$-decomposition. We also discuss its generalization to non-Galois extensions.

Key words. ℓ-torsion conjecture, partitionable group, decomposable group, induction theorem, positivity

1 Introduction

1.1 A Generalized Induction Problem

In the study of representations, it is often very effective to construct representations of a group G by taking induced representations from representations of subgroups $H \subset G$. In general, the induction problem is to ask whether we can and how to write a character χ_G of G as a linear combination of induced characters $\sum_i c_i \operatorname{Ind}_{H_i}^G \chi_{H_i}$.

Historically, there are several famous induction theorems. Artin firstly proves that every character of G is a linear combination with rational coefficients of characters induced from cyclic subgroups of G, see [Ser92, Theorem 17, Chapter 9.2]. Recall that a group H is called *elementary* if $H = C_n \times P$ where P is a p-group and C_n is cyclic with order n not divided by p. Brauer proves that every character of G is a linear combination with integral coefficients of characters induced from characters of elementary subgroups, [Ser92, Theorem 19, Chapter 10.5]. The theorem of Aramata-Brauer proves that $\operatorname{Reg}_G - 1_G$ is a positive rational linear combination of induced characters from cyclic subgroups, [Ser92, Exercise 9.8]. It also follows from an inclusion-exclusion argument that if G is non-cyclic, then every character of G is a rational linear combination of induced trivial character $\operatorname{Ind}_H^G 1_H$ from cyclic subgroups. We summary all these induction theorems in Table 1 in order to highlight the distinction between these statements.

In this paper, we formulate a new induction problem:

Question 1.1. *Given a finite group G and a subgroup $H \subset G$, can we find a sequence of subgroups $\{H_i \mid i = 1, 2, \cdots, s\}$ such that the equality holds*

$$\operatorname{Ind}_H^G 1_H = \sum_{1 \le i \le s} c_i \operatorname{Ind}_{H_i}^G 1_{H_i} + c_0 1_G, \tag{1.1}$$

Theorem	χ_G	Coefficients	Subgroups	χ_H
Artin	All	$\mathbb{Q}$	Cyclic	Any
Brauer	All	$\mathbb{Z}$	Elementary	Degree 1
Aramata-Brauer	$\mathrm{Reg}_G - 1_G$	$\mathbb{Q}_{\geq 0}$	Cyclic	Any
Non-cyclic G	All	$\mathbb{Q}$	All	1_H
Question 1.1	$\mathrm{Ind}_H^G 1_H$	$\mathbb{Q}_{\geq 0}$	All	1_H

Table 1: Summary of induction theorems

with $c_i > 0$ for all $i \geq 1$?

Comparing to previous induction theorems, we are imposing both strict conditions on induced characters (must be induced from trivial character) and involved coefficients (must be positive) at the same time. This makes this new question different from previous induction problems.

1.2 Motivation

We introduce our motivation in formulating Question 1.1. This induction problem is motivated by a recent number theoretic work of the fifth author [Wan20a] on proving new results towards ℓ-torsion conjecture.

Conjecture 1 (ℓ-torsion Conjecture)**.** *Given an integer $\ell > 1$ and a number field k. For any extension F/k with $\mathrm{Gal}(F/k) = G$, the size of ℓ-torsion in the class group of F is bounded by*

$$|\operatorname{Cl}_F[\ell]| = O_{\epsilon,k,[F:k]}(\operatorname{Disc}(F)^{\epsilon}).$$

This conjecture has been brought forward previously by [BS96, Duk98, Zha05] independently for different purposes. It also has various connections to other questions in arithmetic statistics, including Cohen-Lenstra heuristics [OWW21, PTBW19], Malle's conjecture [BST$^+$17, Alb18, Klü12, KW21], integral points and Selmer groups of curves [BST$^+$17] and so on.

This conjecture is only known when G is a p-group and ℓ being a p-power, see [?]. This includes the famous implication from Gauss's genus theory for quadratic extensions. When $(\ell, |G|) = 1$, there are no results as good as $\operatorname{Disc}(F)^{\epsilon}$. Minkowski's bound on class numbers states that $|\operatorname{Cl}_K| = O_{\epsilon,[K:\mathbb{Q}]}(\operatorname{Disc}(K)^{1/2+\epsilon})$ in general. This gives the so-called *trivial bound* on the ℓ-torsion in class groups $|\operatorname{Cl}_K[\ell]| = O_{\epsilon,[K:\mathbb{Q}]}(\operatorname{Disc}(K)^{1/2+\epsilon})$. The state-of-the-art in this area is to prove any bound that is better than trivial bound. In particular, we will call an upper bound in the form of $O_{\epsilon,[K:\mathbb{Q}]}(\operatorname{Disc}(K)^{1/2-\delta})$ with any $\delta > 0$ a *non-trivial bound*. The first case of proving a non-trivial bound for $\operatorname{Cl}_K[\ell]$ is due to Pierce and Helfgott-Venkatesh independently [Pie05, HV06], for $G = C_2$ and $\ell = 3$. Currently, the best record for $\ell = 3$ is due to Ellenberg-Venkatesh in [EV07] for number fields K with degree $[K : \mathbb{Q}] \leq 4$. For $\ell = 2$, [BST$^+$17] proves a non-trivial bound for all number fields with $\delta = 1/2[K : \mathbb{Q}]$. For every $\ell > 3$, the fifth author proves in sequences of work [Wan20a, Wan20b] a non-trivial bound for Galois nilpotent extensions where each Sylow-p subgroup is non-cyclic and non-quaternion.

Our question is exactly motivated by the approach in [Wan20a]. In particular, when $G = C_p^r$ is an elementary abelian group with $r > 1$, for any G-extension K/k and $p \nmid \ell$, we have a decomposition of class numbers and discriminant into product over subfields

$$|\operatorname{Cl}_{K/k}[\ell]| = \prod_{K_i/k} |\operatorname{Cl}_{K_i/k}[\ell]|, \qquad \operatorname{Disc}(K/k) = \prod_{K_i/k} \operatorname{Disc}(K_i/k), \tag{1.2}$$

where K_i/k varies over all degree p subfields of K/k. These structure theorems on G-modules are exploited at the heart of the argument, in conjunction with Brun-Titchmarsh type theorem on prime counting results, to prove a non-trivial bound on $\mathrm{Cl}_K[\ell]$ for arbitrary $\ell > 0$ that is pointwise and unconditional. Moreover, when $r > 1$, there are multiple ways to factor $\mathrm{Cl}_{K/k}$ using K_i/k with higher degree. Applying these more general decompositions, [Wan20a] also proves that the unconditional bound proved can be made independent from the rank of G, thus becoming better than the general GRH bound $O_{\epsilon,k,[K:k]}(\mathrm{Disc}(K)^{1/2-\Delta(\ell,[K:k])+\epsilon})$ shown by Ellenberg and Venkatesh in [EV07] with $\Delta(\ell,[K:k]) < 1/2\ell([K:k]-1)$. Decompositions for arithmetic interesting objects as in (1.2) can all be explained via a universal character theoretic reason. For example, in this case

$$\mathrm{Reg}_G = \sum_{H_i,[G:H_i]=p} \mathrm{Ind}_{H_i}^G 1_{H_i} + c_0 1_G, \tag{1.3}$$

for some c_0, where Reg_G is the character for regular representation. Such a connection between characters and decomposition of class groups and discriminant are explained in Section 3. It follows from Theorem 3.1 that (1.1) implies that

$$|\mathrm{Cl}_{K^H/k}[\ell]| = \prod_{i\geq 1} |\mathrm{Cl}_{K^{H_i}/k}[\ell]|^{c_i} \tag{1.4}$$

for any $\ell > 0$ with $(\ell, |G|) = 1$ and any G-extension K/k.

The conditions on both induced characters and coefficients are exactly shaped by the motivating number theoretic application. We require the induced character to be induced from trivial character since these are exactly corresponding to arithmetic objects associated to intermediate fields. The condition that $c_i > 0$ is also crucial since we need to use a factorization to derive upper bound on class groups. We do not have any conditions on the coefficient c_0 of 1_G, since we are dealing with relative class groups $\mathrm{Cl}_{K/k}$ and relative discriminant.

In Section 4, we streamline the argument in [Wan20a] and prove the following main application towards number theory.

Theorem 1.2. *Given a number field k, a transitive permutation group $G \subset S_n$ and an integer $\ell > 0$. Let $H = Stab(1)$ be the subgroup. If $\mathrm{Ind}_H^G 1_H$ admits a decomposition as (1.1), then there exists $\delta = \delta(G,\ell,k) > 0$ such that*

$$|\mathrm{Cl}_L[\ell]| = O(\mathrm{Disc}(L)^{1/2-\delta}),$$

for every G-extension L/k.

We also obtain a non-abelian analogue of Theorem 2 in [Wan20a], which states that the unconditional savings on $\mathrm{Cl}_K[\ell]$ away from the trivial bound for elementary abelian extension K can be made uniform from the rank. Consider the fibered product $G = D_p \times_{C_2} D_p = C_p^2 \rtimes C_2$ where C_2 acts on each C_p by -1 independently. Similarly we can construct $C_p^r \rtimes C_2$ which is a fibered product of r copies of D_p. We denote these groups by $(D_p)_{C_2}^r$. Such a group admits a (G,H) decomposition where $H = C_2$ with respect to all index p subgroups $H_i = C_p^{r-1} \rtimes C_2$. Moreover, for any $t < r$, it admits a (G,H) decomposition with respect to all index p^t subgroups H_i. Iterating the decomposition with different t, we can prove the following corollary. Since the proved δ is independent from r, when r is large enough, such a non-trivial bound will be better than the GRH-bound in [EV07].

Corollary 1.3. *Given an arbitrary number field k, an integer $\ell > 0$ and $r > 1$. Let $G = (D_p)^r_{C_2}$ be the transitive permutation subgroup of S_{p^r} with Stab(1) $= C_2$. There exists $\delta = \delta(k, \ell)$ such that*

$$|\operatorname{Cl}_K[\ell]| = O_{\epsilon,k,G}(\operatorname{Disc}(K)^{1/2-\delta}),$$

for any G-extension K/k. When r is large enough, we have $\delta > \Delta(\ell, p^r)$.

To sum up, by Theorem 4.1, we make this approach to this seemingly analytic question completely group theoretic now. It suffices for us to focus on understanding the decomposition Question 1.1.

1.3 Partition of Groups

The study of partionable groups firstly was initiated by Miller by [Mil07]. The full classification was achieved in the year of 1961 by Baer [Bae61], Kegel [Keg61b, Keg61a]and Suzuki[Suz61] in a sequence of works. Later on, the classification for S-paritionable groups was proved by Zappa[Zap66]. A nice exposition on the topic of partitionable groups can be found in [Zap03].

Motivated by a completely modern number theory question, we are naturally led to formulate a character theoretic formulation of certain special property of finite groups, which is then proved to be equivalent to this classic purely group theoretic definition called *partition* of a group. Beyond this, we are also naturally led to formulate a character theoretic generalization called S-decomposition, which is no longer equivalent to S-partition. In fact, we show that S-decomposition comprises a strictly larger family than S-partition. Moreover, an S-partition can exist even when G is not partitionable. This imposes new questions for this old area. The full classification for S-decomposition seems to be much more challenging than the classification of S-partition.

Notations

Core(H): Core of a subgroup H, $\cap_g H^g$
Gal(F/k): Galois group of F/k as a permutation group
Disc(F/k): relative discriminant $|\operatorname{disc}(F/k)|$ of F/k where disc(F/k) is the relative discriminant ideal in k, when $k = \mathbb{Q}$ it is the usual absolute discriminant
$\operatorname{Cl}_{F/k}$: relative class group of F/k, when $k = \mathbb{Q}$ it is the usual class group of F
$\operatorname{Cl}_{F/k}[\ell]$: $\{[\alpha] \in \operatorname{Cl}_{F/k} \mid \ell[\alpha] = 0 \in \operatorname{Cl}_{F/k}\}$
$\pi(Y; L/k, \mathcal{C})$: the number of unramified prime ideals p in k with $|p| < Y$ and $\operatorname{Frob}_p \in \mathcal{C}$ where $\mathcal{C}$ is a conjugacy class of Gal(L/k)
$A \asymp B$: there exist absolute constants C_1 and C_2 such that $C_1 B \leq A \leq C_2 B$
$\Delta(\ell, d)$: a constant number slightly smaller than $\frac{1}{2\ell(d-1)}$
$\operatorname{Ind}_H^G \chi_H$: induced character
Reg_G: character of regular representation

Warning: In order to simplify the notation for the whole paper, unless specifically mentioned otherwise, the implied constants O_ϵ, $O_{\epsilon,k}$, $O_{\epsilon,k,\epsilon_0}$ will always depend on ℓ, and the degree d aside from the dependence indicated in the symbol when we are stating results or conjectures on bounding ℓ-torsion in class groups of degree d extensions.

2 Group Theory

In this section, our main goal is to present a classification result for a group theoretic question, which we give the precise definition as following:

Definition 2.1 (Decomposable)**.** *Given a finite group G and a finite subgroup $H \subset G$ with* $\mathrm{Core}(H) = e$*. If there exists a sequence of non-trivial subgroups $S_H := \{H_i \supset H \mid 1 \leq i \leq n\}$ and a sequence of real number $S_c := \{c_i \mid 0 \leq i \leq n, c_i > 0 \text{ if } i > 0\}$ such that*

$$\mathrm{Ind}_H^G(1_H) = \sum_i c_i \, \mathrm{Ind}_{H_i}^G(1_{H_i}) + c_0 1_G,$$

we say (G, H) is decomposable *or (G, H) is* decomposable with respect to $\{(H_i, c_i)\}$.

Remark 2.2. *We will say a permutation group G is* decomposable *if $(G, \mathrm{Stab}(1))$ is decomposable. In particular, the subgroup* $\mathrm{Stab}(1)$ *is trivial if and only if the embedding $G \subset S_n$ is a regular representation of G, in this case, we will simply say the finite group G is* decomposable.

The motivation for Definition 2.1 is in Corollary 3.2. Our main goal is to understand the following question and give a complete list of decomposable G and decomposable (G, H).

Question 2.3. *What are all decomposable transitive permutation group $G \subset S_n$?*

2.1 Decomposable Groups

In this section, we first treat the case when H is the trivial subgroup. We give a complete answer to this question in the following main theorem:

Theorem 2.4. *A group G is decomposable if and only if one of the following is true.*

1. *G is a p-group with $\langle g \in G | g^p \neq e \rangle \neq G$ and $|G| > p$.*
2. *G is a group of Hughes-Thompson type.*
3. *G is a Frobenius Group.*
4. *G is isomorphic to $PGL(2, p^n)$, where p is an odd prime and $n \in \mathbb{N}$. (Note that $PGL(2, 3)$ is isomorphic to S_4)*
5. *G is isomorphic to $PGL(2, p^n)$, where p is a prime and $n \in \mathbb{N}$.*
6. *G is isomorphic to a Suzuki group $Sz(2^{2n+1})$, where $n \in \mathbb{N}$.*

We prove Theorem 2.4 by relating decomposable G to partitionable G. We first recall the concept of a *partionable group.*

Definition 2.5 (Partionable Group)**.** *A finite group G is called* partionable *if there exists a sequence of non-trivial subgroups $\{H_i \mid 1 \leq i \leq n\}$ such that $H_i \cap H_j = e$ if $i \neq j$, and $\cup_i H_i = G$.*

Partionable group is a classical concept in group theory, see e.g. [Isa08, Chapter 6]. The following theorem builds a very nice connections between partionable groups and decomposable groups. To our knowledge, such a result has not been found in literature before.

Theorem 2.6. *A group G is decomposable if and only if G is partionable.*

Theorem 2.4 now follows from combining Theorem 2.6 and the complete classification on partionable groups by [Bae61], [Keg61b] and [Suz61], which was achieved in 1961.

The rest of the this subsection is devoted to prove Theorem 2.6. We will start with an algorithms constructing a special family of subgroups of G. A similar construction was firstly used by Young [?]. We adapt it to be more convenient for our purpose. For $i \geq 0$, we define for each s in G that

$$\begin{aligned} G_{0,s} &:= \langle s \rangle \\ G_{i+1,s} &:= \langle G_{i,t} \mid G_{i,t} \cap G_{i,s} \neq \{e\} \rangle. \end{aligned} \tag{2.1}$$

Since G is finite and $G_{i,s}$ monotonically increases as i gets large, this construction must terminate for each s after finite steps. We define G_s to be the stabilized subgroup for s. From the construction, we can see the following useful properties of G_s:

1. For any elements $s, t \in G$, we have either $G_s = G_t$ or $G_s \cap G_t = \{e\}$.

2. For any elements $s, x \in G$, we have $G_s^x = G_{x^{-1}sx}$ where $G_s^x = x^{-1}G_s x$.

Here the first property follows from the termination of the construction. We now prove the second property via proving an even stronger intermediate result, i.e., $G_{n,s}^x = G_{n,x^{-1}sx}$ for each n. By definition, $G_{0,x^{-1}sx} = \langle x^{-1}sx \rangle = \langle s \rangle^x = G_{0,s}^x$. Assume $G_{k,s}^x = G_{k,x^{-1}sx}$ for every s and x, we now see that

$$\begin{aligned} G_{k+1,x^{-1}sx} &= \langle G_{k,x^{-1}sx}, G_{k,t} \mid G_{k,t} \cap G_{k,x^{-1}sx} \neq \{e\} \rangle \\ &= \langle x^{-1}G_{k,s}x, x^{-1}G_{k,xtx^{-1}}x \mid G_{k,xtx^{-1}} \cap G_{k,s} \neq \{e\} \rangle \\ &= x^{-1}\langle G_{k,s}, G_{k,t'} \mid G_{k,t'} \cap G_{k,s} \neq \{e\} \rangle x \\ &= G_{k+1,s}^x. \end{aligned} \tag{2.2}$$

Now we are ready to prove our key lemma.

Lemma 2.7. *For any finite group G, the following is equivalent:*

(i) *G is decomposable.*

(ii) *G is partitionable.*

(iii) *$G_s \neq G$ for any $s \neq e$ in G.*

Proof. We firstly show that (ii)is equivalent to (iii). Suppose $G_s \neq G$ for any $s \neq e$ in G, then we obtain a partition of G by $G = \cup_s G_s$ since either $G_s = G_t$ or $G_s \cap G_t = \{e\}$ for any s and t. Conversely, suppose $G = \cup_i H_i$ is a partition of G. For each $s \neq e$, we denote H_s to be the unique subgroup H_i in this partition containing s. Therefore for any non-trivial elements s and t, we have $H_s = H_t$ or $H_s \cap H_t = \{e\}$ from G being partitionable with respect to H_i. We claim that $G_s \subset H_s$ for any non-trivial $s \in G$: by definition $G_{0,s} \subset H_s$; suppose $G_{k,s} \subset H_s$ for any non-trivial s, and $G_{k,t} \cap G_{k,s} \neq \{e\}$, then $G_{k,t} \cap G_{k,s} \subset H_s \cap H_t$ is non-trivial, this indicates that $H_s = H_t$, therefore $G_{k,t} \subset H_t = H_s$ by inductive hypothesis, thus $G_{k+1,s} \subset H_s$. It follows from this claim that $G_s \subset H_s \neq G$.

We next show that (iii) implies (i). Firstly, if $G_s \neq G$ for any $s \neq e$ in G, we can construct a decomposition of G as following. For the set of subgroups $\{G_s \mid s \neq e \in G\}$, we can obtain its conjugacy classes of subgroups, denoted by $\{H_i\}_{i>0}$. Then we claim that there exists $c_i > 0$ such that

$$\mathrm{Reg}_G = \sum_{i>0} c_i \operatorname{Ind}_{H_i}^G 1_{H_i} + c_0 1_G. \tag{2.3}$$

In fact, suppose H_i is conjugate to G_s, then from the property of the subgroup G_s, we can assume $H_i = G_s$ for some s and $H_i^x = G_{x^{-1}sx}$. Thus

$$\operatorname{Ind}_{H_i}^G 1_{H_i} = \sum_{x\in G/H_i} 1_{H_i^x} = \sum_{x\in G/H_i} 1_{G_{x^{-1}sx}}. \tag{2.4}$$

Since either $G_{x^{-1}sx} = G_s$ or $G_{x^{-1}sx} \cap G_s = \{e\}$, we see that $\operatorname{Ind}_{H_i}^G 1_{H_i}(t) = |\{x \in G/G_s \mid G_{x^{-1}sx} = G_s\}|$ takes a constant positive integral value m_i for any nontrivial $t \in G_s = H_i$, thus also for any $t \in H_i^x$ since $\operatorname{Ind}_{H_i}^G$ is a class function. On the other hand, if a non-trivial element t is contained in H_i^x for some x, then $G_t = G_{x^{-1}sx} \cap H_j^y = \{e\}$ for any $j \neq i$, since G_t is only conjugate to H_i via construction of $\{H_i\}$. Therefore we obtain that for $t \in \cup_x H_i^x$ and $j \neq i$ that

$$\operatorname{Ind}_{H_j}^G 1_{H_j}(t) = 0. \tag{2.5}$$

Now it suffices to take

$$c_i = -c_0/m_i, \qquad c_0 = \frac{|G|}{1 - \sum_{i>0} |G|/(|H_i|m_i)}. \tag{2.6}$$

Notice that $m_i|H_i| \leq |G|$ always holds and the equality holds if and only if H_i is normal in G. Therefore the denominator is 0 in the expression of c_0 if and only if H_1 is normal and all $G_s = H_1$, which contradicts with $G_s \neq G$. This finishes the proof of the claim.

Finally we show that (i) implies (iii). Suppose G is decomposable with respect to $\{(H_i, c_i)\}$, we claim that if $s \in H_i^y$ for some i and some y, then $G_s \subset H_i^y$. The implication then follows immediately from this claim. We now focus on proving this claim inductive on $G_{j,s}$ for $j \geq 0$. For $j = 0$, it is trivial that $s \in H_i^y$ implies $G_{0,s} \subset H_i^y$. Suppose the statement holds for general j, that is, $s \in H_i^y$ implies $G_{j,s} \subset H_i^y$. It follows from the inductive hypothesis that $\operatorname{Ind}_{H_i}^G 1_{H_i}(t) \geq \operatorname{Ind}_{H_i}^G 1_{H_i}(s)$ for any $t \in G_{j,s}\backslash\{e\}$ and any $i > 0$. Since G is decomposable, any non-trivial elements x and y in G satisfy

$$\sum_{i>0} c_i \operatorname{Ind}_{H_i}^G 1_{H_i}(x) = \sum_i c_i \operatorname{Ind}_{H_i}^G 1_{H_i}(y) = -c_0, \tag{2.7}$$

with $c_i > 0$ for all $i > 0$. In order for (2.7) to hold, we thus must have $\operatorname{Ind}_{H_i}^G 1_{H_i}(t) = \operatorname{Ind}_{H_i}^G(s)$ for all i and all $t \in G_{j,s}\backslash\{e\}$. This implies that if $G_{n,s} \cap H_i^y \neq \{e\}$ intersects non-trivially, say $t \in H_i^y \cap G_{n,s}$ then $s \in H_i^y$, therefore we must see $G_{n,s}$ as a whole contained in H_i^y. Now suppose $G_{j,s} \in H_i^y$ and $G_{j,t} \cap G_{j,s} \subset G_{j,t} \cap H_i^y \neq \{e\}$. From previous deduction, this implies that the whole set $G_{j,t}$ is contained in H_i^y. Therefore $G_{j+1,s} \subset H_i^y$. This finishes the proof of the claim.

□

2.2 Decomposable (G, H)

In this section, we discuss the family of H-decomposition when H is non-trivial, that is, finding (G, H) such that

$$\operatorname{Ind}_H^G 1_H = \sum_{i>0} c_i \operatorname{Ind}_{H_i}^G 1_{H_i} + c_0 1_G. \tag{2.8}$$

We will give partial results on classification of (G, H) decomposition, including both necessary conditions and sufficient conditions. Before we start to state our results in Theorem 2.13, Theorem and Theorem, we first make several helpful observations.

Firstly, it is straightforward that

Lemma 2.8. *The pair (G, H) is decomposable with respect to $\{H_i, c_i\}$ if and only if the pair $(G/\operatorname{Core}(H), H/\operatorname{Core}(H))$ is decomposable with respect to $\{H_i/\operatorname{Core}(H), c_i\}$.*

This reduces the cases where H is normal to decomposition of G. We will also assume from now on that $\operatorname{Core}(H) = e$.

Lemma 2.9. *Given a finite group G and $H \subset G$ an arbitrary non-trivial subgroup. Then*

$$\cup_g H^g \subsetneq G.$$

Proof. The permutation action of G on left cosets of H is a transitive group action. By Jordan's theorem, for any transitive action there exists $g \in G$ with no fixed point. □

This implies that there exists $x \in G$ such that $\operatorname{Ind}_H^G 1_H(x) = 0$. Since $c_i > 0$ for all i, it is clear that the coefficient c_0 for 1_G is non-positive. Notice that if $H \subset H_i$, then for all $x \in G$ we have

$$\frac{\operatorname{Ind}_{H_i}^G(x)}{\operatorname{Ind}_{H_i}^G(e)} \geq \frac{\operatorname{Ind}_H^G(x)}{\operatorname{Ind}_H^G(e)}. \tag{2.9}$$

When H is non-trivial, by comparing both sides of (2.8) for $x \in H$, we can see that it is necessary $c_0 < 0$. Thus it is necessary that if $g \notin \cup_x H^x$ then there exists i such that $\operatorname{Ind}_{H_i}^G 1_{H_i}(g) > 0$.

Lemma 2.10. *Let (G, H) be decomposable with respect to $\{H_i, c_i\}$. If $g \notin \cup_x H^x$, then there exists some H_i and some x such that $g \in H_i^x$.*

Since $\operatorname{Ind}_{H_i}^G 1_{H_i}(g^k) \geq \operatorname{Ind}_{H_i}^G 1_{H_i}(g)$ for any $g \in G$ and $c_i \geq 0$ for any i, in order to balance both sides of (2.8) for $g \notin \cup_x H^x$, we must have the following lemma.

Lemma 2.11. *Let (G, H) be decomposable with respect to $\{H_i, c_i\}$. If for some $g \in G$ we have $g^k \in H_i \backslash \cup_x H^x$, then $g \in H_i$.*

2.2.1 H-partition

It is a natural thought to compare H-decomposition to H-partition since it works so well when $H = \{e\}$. We now recall the definition for H-partition.

Definition 2.12 (H-partition)**.** *Let H be a subgroup of G. An H-partition is a set of proper subgroups $H_1, \cdots, H_n$, such that each $H_i \supset H$ and every element not in H lies in exactly one H_i.*

We can easily prove the implication from one direction.

Theorem 2.13. *If G has an H-partition, then G is H-decomposable.*

Proof. Let $G = \cup_{1 \leq i \leq n} H_i$ be an H-partition of G. For each $x \in G$, we have the following equality

$$\frac{|H_i|}{|G|} \operatorname{Ind}_{H_i}^G 1_{H_i}(x) = \frac{|\mathcal{C}_x \cap H_i|}{|\mathcal{C}_x|}, \tag{2.10}$$

where $\mathcal{C}_x$ denotes the conjugacy class of x in G. Notice that $\sum_i |\mathcal{C}_x \cap H_i| = |\mathcal{C}_x| - |\mathcal{C}_x \cap H|(n-1)$, we then obtain the H-decomposition by taking $c_i = \frac{|H_i|}{(n-1)|H|}$ and $c_0 = -\frac{|G|}{(n-1)|H|}$. □

The classification for H-partition is proved by Zappa [Zap66].

Theorem 2.14 (Zappa, [Zap66])**.** *Let H be a non-trivial subgroup of G with* $\mathrm{Core}(H) = e$*. A finite group G admits an H-partition with respect to $\{H_i\}$ if and only if $G = K \rtimes H$ is Frobenius with complement H and the kernel K, and K is a p-group with non-trivial partition $\{K_i\}$ and $H_i = HK_i$.*

In particular, we can see that if G admits an H-partition, then G must be partitionable by itself. Interestingly, G can admit an H-decomposition while G is not decomposable.

Example 2.15. *Let $G = C_2 \times (C_7 \rtimes C_6) \simeq \langle a^2 = b^7 = c^6 = 1 \,|\, ab = ba, ac = ca, cbc^{-1} = b^5\rangle$ of order* 84 *and $H = \langle c^2\rangle \simeq C_3$. This group is not decomposable, however it is (G, H)-decomposable with respect to $H_1 = \langle c\rangle, H_2 = \langle ac\rangle, H_3 = \langle a, b, c^2\rangle$. The coefficients are $c_0 = -2, c_1 = 1, c_2 = 1, c_3 = 1$.*

We can see from this example that unlike the case where H is the trivial subgroup, the notion of H-partitionable and H-decomposable is no longer equivalent for general H!

2.2.2 Semi-direct Product

In this section, we are going to give two types of pairs (G, H) that are decomposable. In both cases G is a semi-direct product.

We first give a clean theorem that covers both Frobenius groups and Example 2.15.

Theorem 2.16. *Let $G = K \rtimes_\phi N$ and $H \subset N$, and denote $H_c = \cap_{n\in N} H^n$. If $\phi(n)$ has no non-trivial fixed points for all elements $n \in N \backslash H_c$, then (G, H) is decomposable.*

Proof. We show that it suffices to choose $K \rtimes H$ and N, with coefficients 1 and $|N|/|H|$.

For $h \in H$, let $S(h)$ denote the set of conjugates of h formed by K, and $T(h)$ denote the set of conjugates of h formed by N. We can thus calculate the induced characters as follows:

$$\mathrm{Ind}_N^G 1_N(x) = \begin{cases} \frac{|K|}{|S(h)|} & x \in S(h) \text{ for some } h \in H_c \\ 1 & x \in G\backslash(K \rtimes H_c) \\ 0 & \text{otherwise} \end{cases}$$

$$\mathrm{Ind}_{K\rtimes H}^G 1_{K\rtimes H}(x) = \begin{cases} \frac{|N|\cdot|T(h)\cap H|}{|H|\cdot|T(h)|} & x \in K \rtimes H \\ 0 & \text{otherwise} \end{cases}$$

$$\mathrm{Ind}_H^G 1_H(x) = \begin{cases} \frac{|G|}{|S(h)|\cdot|H|} & x \in S(h) \text{ for some } h \in H_c \\ \frac{|K|\cdot|T(h)\cap H|}{|H|\cdot|T(h)|} & x \in \cup_{g\in T(h)} S(g) \text{ for some } h \in H\backslash H_c \\ 0 & \text{otherwise} \end{cases}$$

Then we verify that

$$\mathrm{Ind}_H^G 1_H = \mathrm{Ind}_{K\rtimes H}^G 1_{K\rtimes H} + \frac{|N|}{|H|} \mathrm{Ind}_N^G 1_N - \frac{|N|}{|H|} 1_G.$$

□

Notice that Theorem 2.16 actually covers all G where G is Frobenius.

Corollary 2.17. *If G is Frobenius and H is any subgroup contained in the Frobenius complement, then (G, H) is decomposable.*

Next we consider the following theorem, which allows us to build a (G, H)-decomposition from smaller ones. In the decompositions considered below, we do not require any of them to be core-free.

Theorem 2.18. *Let $G = K \rtimes N$ and $H = H_K \rtimes H_N$, where $H_K \subset K, H_N \subset N$. Then (G, H) is decomposable if the following are true:*

1. *(N, H_N) is decomposable, where the subgroups are $N_1, ..., N_n$ with coefficients $\alpha_1, ...\alpha_n$. We allow the decomposition where $N_1 = H_N$, $N_2 = N$, and $\alpha_1 = 1, \alpha_2 = |N|/|H_N|$.*
2. *For the subgroups N_i, $i \geq 2$, $(K \rtimes N_i, H)$ is decomposable, where the subgroups in the decomposition are $K \rtimes H_N, M_{i,1}, ...M_{i,n_i}$ with coefficients $1, \beta_{i,1}, ...\beta_{i,n_i}$.*

Proof. By considering the value at e in condition 1 and 2, we get that

$$\sum_{i=2}^{n} \frac{\alpha_i}{|N_i|} = \frac{1}{|H_N|}, \quad \beta_i := \sum_{j=1}^{n_i} \beta_{i,j} = \frac{|N_i|}{|H_N|}.$$

We claim that the decomposition is given precisely by the subgroups $K \rtimes N_1$ and $M_{i,j}$ for $2 \leq i \leq n, 1 \leq j \leq n_i$, with coefficents α_1 and $\frac{\alpha_i \cdot \beta_{i,j}}{\beta_i}$, and the coefficient for 1_G is $\frac{\alpha_1 \cdot |N|}{|N_1|}$.

We write out the formulas that denote condition 1 and 2:

$$\operatorname{Ind}_{H_N}^{N} 1_{H_N} = \sum_{i=1}^{n} \alpha_i \operatorname{Ind}_{N_i}^{N} 1_{N_i} - \frac{\alpha_1 \cdot |N|}{|N_1|} 1_N \tag{2.11}$$

$$\operatorname{Ind}_{H}^{K \rtimes N_i} 1_H = \sum_{j=1}^{n_i} \beta_{i,j} \operatorname{Ind}_{M_{i,j}}^{K \rtimes N_i} 1_{M_{i,j}} + \operatorname{Ind}_{K \rtimes H_N}^{K \rtimes N_i} 1_{K \rtimes H_N} - \frac{|N_i|}{|H_N|} 1_{K \rtimes N_i} \text{ for all } i \geq 2. \tag{2.12}$$

Equation (5) can be further rewritten using the transitive property of an induced character to be

$$\operatorname{Ind}_{H}^{G} 1_H = \sum_{j=1}^{n_i} \beta_{i,j} \operatorname{Ind}_{M_{i,j}}^{G} 1_{M_{i,j}} + \operatorname{Ind}_{K \rtimes H_N}^{G} 1_{K \rtimes H_N} - \frac{|N_i|}{|H_N|} \operatorname{Ind}_{K \rtimes N_i}^{G} 1_{K \rtimes N_i} \text{ for all } i \geq 2. \tag{2.13}$$

Hence using the above equations we have

$$\begin{aligned}
&\sum_{i=2}^{n} \sum_{j=1}^{n_i} \frac{\alpha_i \cdot \beta_{i,j}}{\beta_i} \operatorname{Ind}_{M_{i,j}}^{G} 1_{M_{i,j}} + \alpha_1 \operatorname{Ind}_{K \rtimes N_1}^{G} 1_{K \rtimes N_1} - \frac{\alpha_1 \cdot |N|}{|N_1|} 1_G \\
&= \sum_{i=2}^{n} \frac{\alpha_i}{\beta_i} \left(\operatorname{Ind}_{H}^{G} 1_H - \operatorname{Ind}_{K \rtimes H_N}^{G} 1_{K \rtimes H_N} + \frac{|N_i|}{|H_N|} \operatorname{Ind}_{K \rtimes N_i}^{G} 1_{K \rtimes N_i} \right) + \alpha_1 \operatorname{Ind}_{K \rtimes N_1}^{G} 1_{K \rtimes N_1} - \frac{\alpha_1 \cdot |N|}{|N_1|} 1_G \\
&= \operatorname{Ind}_{H}^{G} 1_H - \operatorname{Ind}_{K \rtimes H_N}^{G} 1_{K \rtimes H_N} + \sum_{i=1}^{n} \alpha_i \operatorname{Ind}_{K \rtimes N_1}^{G} 1_{K \rtimes N_1} - \frac{\alpha_1 \cdot |N|}{|N_1|} 1_G.
\end{aligned}$$

It remains to show that $-\operatorname{Ind}_{K \rtimes H_N}^{G} 1_{K \rtimes H_N} + \sum_{i=1}^{n} \alpha_i \operatorname{Ind}_{K \rtimes N_1}^{G} 1_{K \rtimes N_1} - \frac{\alpha_1 \cdot |N|}{|N_1|} 1_G$ is 0 for any element. We observe that for any element kn, where $k \in K$ and $n \in N$, and $L < N$, $\operatorname{Ind}_{K \rtimes L}^{G} 1_{K \rtimes L}(kn) = \operatorname{Ind}_{L}^{N} 1_L(n)$. The justification for this is that for any $c \in N$, $\operatorname{Stab}_K(kn) = |\{x \in K, x(kn)x^{-1} = kn\}| = |\{x \in K^c, c^{-1}xc(kn)c^{-1}x^{-1}c = kn\}| = |\{x \in K, xc(kn)c^{-1}x^{-1} = c(kn)c^{-1}\}| = \operatorname{Stab}_K(c(kn)c^{-1})$. Hence $\frac{|Cl_L(n) \cap L|}{|L|} = \frac{|Cl_G(kn) \cap K \rtimes L|}{|K \rtimes L|}$, and we have the desired conclusion from equation (4)

□

It is useful to consider several examples illustrating the above theorem.

3 Representation Theory

In this section, our main goal is to prove the following statement.

Theorem 3.1. *If (G, H) is decomposable with respect to $\{(H_i, c_i)\}$ and $\ell \nmid |G|$ is a prime number, then for any finite $\mathbb{Z}_\ell[G]$-module V with $V^G = \{e\}$, then*

$$|V^H| = \prod_i |V^{H_i}|^{c_i}.$$

Proof. Firstly, by Krull-Schmidt theorem for modules, any finite $\mathbb{Z}_\ell[G]$-module V can be written as a direct sum $V = \bigoplus_i V_i$ of indecomposable $\mathbb{Z}_\ell[G]$-modules V_i. Then $V^H = \bigoplus V_i^H$ for any subgroup $H \subset G$. Therefore it suffices to prove the theorem for finite indecomposable $\mathbb{Z}_\ell[G]$-module. We will assume V to be indecomposable and finite from now on.

For each $\mathbb{Z}_\ell[G]$-module V, we can define $V_k := V \otimes_{\mathbb{Z}_\ell} \mathbb{Z}/\ell^k\mathbb{Z}$ for every $k \geq 1$. Since ℓ is relatively prime to $|G|$, V_1 is always projective $\mathbb{F}_\ell[G]$-module, and moreover, each V_1 can be lifted to a unique projective $\mathbb{Z}/\ell^k\mathbb{Z}[G]$-module $\tilde{V}_k$ for any $k > 0$ by, e.g. [Ser92, Chapter 15.5, Proposition 43, Exercise 15.9,]. We denote $\tilde{V}_\infty$ to be the projective $\mathbb{Z}_\ell[G]$-module lift of V_1. For every k, since $\tilde{V}_k$ is projective, there is always a surjective $\mathbb{Z}/\ell^k\mathbb{Z}[G]$-homomorphism from $f_k : \tilde{V}_k \to V_k$ that composes with $g_k : V_k \to V_1 = V_k \otimes \mathbb{F}_\ell$ gives the $\mod \ell$ projection $g_k \circ f_k : \tilde{V}_k \to V_1$.

We claim that a finite and indecomposable $\mathbb{Z}_\ell[G]$ module V with exponent ℓ^k is always a projective $\mathbb{Z}/\ell^k\mathbb{Z}[G]$-module with V_1 being irreducible. If V has exponent ℓ^k, then $V \simeq V_k$. If V is indecomposable, then V_1 is also indecomposable (since otherwise one can lift direct summands of V_1 to be direct summands of $\tilde{V}_k$ and then project to direct summands of $V = V_k$), therefore V_t and $\tilde{V}_t$ are both indecomposable for any $t > 0$ (since otherwise direct summands of V_t and $\tilde{V}_t$ project to direct summands of V_1). As an $\mathbb{F}_\ell[G]$-module, V_1 being indecomposable is equivalent to V_1 being irreducible since $\mathbb{F}_\ell[G]$ is semi-simple. Therefore $\mathbb{F}_\ell[G]\langle m\rangle = V_1$ for any $m \neq 0$ in V_1 and similarly $\mathbb{Z}/\ell^k\mathbb{Z}[G]\langle m\rangle = \tilde{V}_k$ for any m with nontrivial projection in V_1. Suppose $S \subset \tilde{V}_k$ is any sub $\mathbb{Z}/\ell^k\mathbb{Z}[G]$-module with exponent ℓ^r, then there exists $s \in S$ with $\ell^r s = 0$, equivalently, $s = \ell^{k-r}m$ for some $m \in \tilde{V}_k$ with nontrivial projection in V_1. Then $\mathbb{Z}/\ell^k\mathbb{Z}[G]\langle s\rangle = \ell^{k-r}\tilde{V}_k$ and quotient module $\tilde{V}_k/S$ has exponent dividing ℓ^{k-r}. Since V_k has exponent ℓ^k, it follows that the surjective map $f_k : \tilde{V}_k \to V_k = V$ has trivial kernel S, therefore $V = V_k = \tilde{V}_k$.

We now first prove this equality for the size of V_1^H. Notice that V_1 is a $\mathbb{F}_\ell$-vector space. By Frobenius reciprocity, we have for each subgroup $H \subset G$ that

$$V_1^H \simeq \operatorname{Hom}_{\mathbb{F}_\ell[H]}(\mathbb{F}_\ell, \operatorname{Res}_H^G V_1) \simeq \operatorname{Hom}_{\mathbb{F}_\ell[G]}(\mathbb{F}_\ell \otimes_{\mathbb{F}_\ell[H]} \mathbb{F}_\ell[G], V_1). \tag{3.1}$$

Therefore it follows from [Ser92, Chapter 18, (viii)] that

$$\begin{aligned}\dim_{\mathbb{F}_\ell}(V_1^H) &= \dim_{\mathbb{F}_\ell} \operatorname{Hom}_{\mathbb{F}_\ell[G]}(\mathbb{F}_\ell \otimes_{\mathbb{F}_\ell[H]} \mathbb{F}_\ell[G], V_1). = \langle \operatorname{Ind}_H^G 1_H, \Phi_{V_1}\rangle \\ &= \sum_{i\geq 0} c_i \langle \operatorname{Ind}_{H_i}^G 1_{H_i}, \Phi_{V_1}\rangle = \sum_{i \geq 0} c_i \dim_{\mathbb{F}_\ell}(V_1^{H_i}),\end{aligned} \tag{3.2}$$

where $\operatorname{Ind}_H^G 1_H : G \to \mathbb{Z} \subset \mathbb{Z}_\ell$ is interpreted as the modular character for the induced $\mathbb{F}_\ell[G]$-module $\mathbb{F}_\ell \otimes_{\mathbb{F}_\ell[H]} \mathbb{F}_\ell[G]$, and $\Phi_{V_1} : G \to \mathbb{Q}_\ell$ is the character of the $\mathbb{Q}_\ell[G]$-module $\tilde{V}_\infty \otimes \mathbb{Q}_\ell$. The equality for the size follows immediately from the equality on the dimension and $V_1^{H_0} = V_1^G = 0$.

Finally, we consider the equality for general finite and indecomposable $\mathbb{Z}_\ell[G]$-module V. Notice that since $H^1(H, \ell V) = 0$, we obtain a short exact sequence $0 \to (\ell V)^H \to V^H \to (V/\ell V)^H \to 0$. Recall that V is projective as $\mathbb{Z}/\ell^k\mathbb{Z}$-module, it follows from the surjectivity of in this short exact sequence that V^H is also projective as $\mathbb{Z}/\ell^k\mathbb{Z}$ and $\mathrm{rk}_{\mathbb{Z}/\ell^k\mathbb{Z}}(V^H) = \dim_{\mathbb{F}_\ell}(V_1^H)$. Therefore

$$\mathrm{rk}_{\mathbb{Z}/\ell^k\mathbb{Z}}(V^H) = \sum_{i\geq 0} c_i \,\mathrm{rk}_{\mathbb{Z}/\ell^k\mathbb{Z}}(V^{H_i}). \tag{3.3}$$

□

Corollary 3.2. *Let (G, H) be decomposable with respect to $\{(H_i, c_i)\}$. Then for any integer ℓ relatively prime to $|G|$ and any Galois number field extension L/k with $\mathrm{Gal}(L/k) = G$, we have*

$$\mathrm{Disc}(L^H/k) = \prod_i \mathrm{Disc}(L^{H_i}/k)^{c_i},$$

and

$$|\mathrm{Cl}_{L^H/k}[\ell]| = \prod_i |\mathrm{Cl}_{L^{H_i}/k}[\ell]|^{c_i}.$$

Proof. For a Galois extension L/k with $\mathrm{Gal}(L/k) = G$, we denote $V = \mathrm{Cl}_{L/k}[\ell]$ where $(\ell, |G|) = 1$. Then we get

$$|V^H| = |\mathrm{Cl}_{L^H/k}[\ell]| = \prod_i |\mathrm{Cl}_{L^{H_i}/k}[\ell]|^{c_i},$$

where the first equality follows from [**?**] and the second equality follows from Theorem 3.1.

For the discriminant, it suffices to notice that for any subgroup H,

$$\mathrm{disc}(L^H/k) = \mathfrak{f}(L/k, \mathrm{Ind}_H^G(1_H)),$$

and that Artin conductor is multiplicative with respect to characters and is orthogonal to trivial representation 1_G [Neu99]. □

Remark 3.3. *The condition on ℓ being relatively prime to $|G|$ is necessary for the decomposition on $\mathrm{Cl}[\ell^k]$. For example when $\ell = 2$ and $G = C_2 \times C_2$ and $H = \{e\}$, the equality already fails since $\mathrm{Cl}_L^N \neq \mathrm{Cl}_{L^N}$.*

4 Arithmetic Application

In this section, we will give the main arithmetic application that motivates our study about decomposable groups. For each decomposable pair (G, H) where $[G : H] = n$ and $\mathrm{Core}(H) = e$, we can obtain a transitive permutation group $G \subset S_n$ by considering G action on left cosets of H. We will prove a non-trivial pointwise bound on the ℓ-torsion in class groups for every $G \subset S_n$-extension over an arbitrary number field k.

Theorem 4.1. *Given a number field k, a transitive permutation group $G \subset S_n$ and an integer $\ell > 0$. If $(G, \mathrm{Stab}(1))$ is decomposable, then there exists $\delta = \delta(G, \ell, k) > 0$ such that*

$$|\mathrm{Cl}_L[\ell]| = O(\mathrm{Disc}(L)^{1/2-\delta}),$$

for every G-extension L/k.

4.1 Preliminaries

The strategy to prove Theorem 4.1 is based on a widely used lemma of [EV07], which we record as following.

Lemma 4.2 ([EV07])**.** *Given a Galois extension L/K and $0 < \theta < \frac{1}{2\ell(d-1)}$ and an integer $\ell > 1$. Suppose there exists $\mathfrak{p}_1, \cdots, \mathfrak{p}_M$ in K such that: 1.* $\mathrm{Nm}(\mathfrak{p}_i) \leq \mathrm{Disc}(L/K)^\theta$
2. $\mathfrak{p}_i \cap K \neq \mathfrak{p}_j \cap K$ for $i \neq j$
3. $\mathfrak{p}_i \neq qO_F$ for any strict intermediate field $K \subset F \subset L$ and any prime ideal q in F then

$$|\,\mathrm{Cl}_L[\ell]| = O_{\epsilon,[K:\mathbb{Q}],\ell}\Big(\frac{\mathrm{Disc}(L)^{1/2+\epsilon}}{M}\Big). \tag{4.1}$$

We can see that primes in K that are split in L/K with bounded height satisfy the listed conditions. In most cases, the difficulty in applying this lemma is exactly to give good lower bound on prime counting functions $\pi(\mathrm{Disc}(L/K)^\theta; L/K, e)$, where the range for primes $\mathrm{Disc}(L/K)^\theta$ goes arbitrarily small when ℓ becomes large. Actually, if we assume GRH, we can obtain the exact expected lower bound for $\pi(\mathrm{Disc}(L/K)^\theta; L/K, e)$.

Theorem 4.3 ([LO75], Effective Chebotarev Density Theorem on GRH)**.** *Given a Galois extension L/K with Galois group G. Assuming GRH, then for every $x \geq 2$, we have*

$$\big|\pi(x; L/K, e) - \frac{1}{|G|}\mathrm{Li}(x)\big| = O_{[L:\mathbb{Q}]}(x^{1/2}\ln(\mathrm{Disc}(L)x)).$$

On the contrary, the current technology on prime counting theorem and Chebotarev density theorem without assuming GRH can only be applied when the range is much larger.

Lemma 4.4 ([May13, Zam17])**.** *Given L/k a Galois extension of number fields with* $[L:\mathbb{Q}] = d$*. There exists absolute, effective constants $\gamma = \gamma(k, G) > 2$, $\beta = \beta(k, G) > 2$, $D_0 = D_0(k) > 0$ and $C = C(k) > 0$ such that if* $\mathrm{Disc}(L/k) \geq D_0$*, then for $x \geq \mathrm{Disc}(L/k)^\beta$, we have*

$$\pi(x; L/k, \mathcal{C}) \geq C_k \frac{1}{\mathrm{Disc}(L/k)^\gamma} \cdot \frac{|\mathcal{C}|}{|G|} \cdot \frac{x}{\ln x}.$$

The actual values for β and γ can be explicitly determined in [May13] when $k = \mathbb{Q}$ and L/k is abelian and [Zam17] for general G and k. We expect these number can be further improved. For simplicity, we can use $\gamma(k, G) = 19$ and $\beta(k, G) = 35$ for all k and G, as proved in [Zam17]. We mentioned that we haven't listed results on unconditional upper bounds for $\pi(\mathrm{Disc}(L/K)^\theta; L/K, \mathcal{C})$, when $\theta \gg_{G,k} 1$, e.g. in [MV73, May13, TZ18]. For some groups, such upper bound results alone are also sufficient to prove Theorem 4.1. We are only interested in giving a unified argument for all G, k, and ℓ, that's why we are not including them for this paper.

4.2 Proof of Theorem 4.1

Proof of Theorem 4.1. Suppose (G, H) is decomposable with respect to $\{H_i, c_i\}$ with $i = 1, \cdots, s$. For each Galois extension L with $\mathrm{Gal}(L/k) = G$, we denote the number field $K_i := L^{H_i}$ and $K := L^H$. We also denote $[K_i : k] = n_i$. Up to a reordering of H_i, we can assume that $\mathrm{Disc}(K_i) \leq \mathrm{Disc}(K_{i+1})$. By conductor-discriminant formula, for each i, we can find a $m_i > 0$ such that $\mathrm{Disc}(K_i/k)^{m_i} \geq C_G \,\mathrm{Disc}(\tilde{K_i}/k)$ for every L and K_i where $C_G > 0$ is some constant only depending on G. For each i, by Lemma 2.9, we can find a conjugacy class in $\mathrm{Gal}(\tilde{K_i}/k)$, that is $\mathcal{C}_i \subset G/\operatorname{Core}(H_i)$, such that $\mathcal{C}_i \cap (\cup_x H_i^x/\operatorname{Core}(H_i)) = \emptyset$. We denote f_i to be the minimal inertia degree for an unramified p in K_i/k with $\mathrm{Frob}_p = \mathcal{C}_i$.

Now we follow the strategy of [Wan20a].

We define

$$\eta := \frac{\ln \operatorname{Disc}(K_1/k)}{\ln \operatorname{Disc}(K/k)}, \qquad \eta_0 := \min_i \frac{\Delta(\ell, n/n_i)}{\Delta(\ell, n/n_i) \cdot n/n_i + m_i f_i \cdot \max\{\beta, \gamma\}},$$

and then separate the discussion depending on the size of η. We remark that the definition of η_0 does not depend on the ordering of H_i. If $\eta \geq \eta_0$, then we apply the pigeon hole principle to find small degree one primes in K_1/k or K/K_1 ; if $\eta < \eta_0$, then we apply Lemma 4.4 to $\tilde{K_1}/k$ to find enough small degree one primes among in K/K_1 by choosing suitable x and $\mathcal{C}$.

Firstly, if $\eta \geq \eta_0$, then we have $\operatorname{Disc}(K_1/k) \geq \operatorname{Disc}(K/k)^{\eta_0}$. Now we consider prime ideals in the range of $Y := \min\{\operatorname{Disc}(K_1/k)^{\Delta(\ell, n_1)}, \operatorname{Disc}(K/K_1)^{\Delta(\ell, n/n_1)/f_1}$. Aside from $O_\epsilon(\operatorname{Disc}(K)^\epsilon)$ many ramified primes in K, among primes p in k that are unramified in K/k, if $\mathrm{Frob}_p \in \cup_x H_1^x$, then p will split into a product of prime ideals $\prod_j \mathfrak{p}_j$ in K_1 with at least one $\mathfrak{p}_j$ having inertia degree one (since Frob_p has at least one fixed point under coset action of G with respect to H_i); if $\mathrm{Frob}_p \notin \cup_x H_1^x$, and suppose w is an integer such that $\langle \mathrm{Frob}_p^w \rangle = \langle \mathrm{Frob}_p \rangle \cap H_1$ is the decomposition group for certain prime $\mathfrak{p}$ above p in K_1, then by Lemma 2.11, we see that $\mathrm{Frob}_p^w \subset \cup_x H^x$. This implies that there exists at least one prime ideal with relative inertia degree 1 in K above $\mathfrak{p}$ in K_1. By a pigeon hole principle, there exists at least one conjugacy class of elements $\mathcal{C} \subset G$ such that

$$\pi(Y; \tilde{L}/k, \mathcal{C}) \geq \frac{|\mathcal{C}|}{2|G|} \frac{Y}{\ln Y}.$$

If this class of $\mathcal{C}$ is contained in $\cup_x H_1^x/\operatorname{Core}(H_1)$, then by applying Lemma 4.2 on K_1/k we obtain

$$|\operatorname{Cl}_{K_1}[\ell]| = O_\epsilon\Big(\frac{\operatorname{Disc}(K_1)^{1/2+\epsilon}}{Y/\ln Y}\Big),$$

which results in a saving in the order of $Y^{1-\epsilon}$ for Cl_K ; otherwise, by applying Lemma 4.2 on K/K_1 we obtain

$$|\operatorname{Cl}_K[\ell]| = O_\epsilon\Big(\frac{\operatorname{Disc}(K)^{1/2+\epsilon}}{Y}\Big).$$

If $\eta < \eta_0$, then we will apply effective Chebotarev density theorem to $\tilde{K_1}/k$ with $x = \operatorname{Disc}(K/K_1)^{\Delta(\ell, n/n_1)/f_1}$ to the conjugacy class $\mathcal{C}_1$ outside $(\cup_x H_1^x/\operatorname{Core}(H_1))$. By Lemma 4.4, we have

$$\pi(x; \tilde{K_1}/k, \mathcal{C}_1) \gg \frac{1}{\operatorname{Disc}(\tilde{K_1}/k)^\gamma} \cdot \frac{x}{\ln x},$$

where $x = \operatorname{Disc}(K/K_1)^{\Delta(\ell, n/n_1)/f_1} \geq \operatorname{Disc}(\tilde{K_1}/k)^{\max\{\beta, \gamma\}}$ is guaranteed since $\eta < \eta_0$. In this case, we can bound

$$|\operatorname{Cl}_K[\ell]| = O_\epsilon\Big(\frac{\operatorname{Disc}(K)^{1/2+\epsilon}\operatorname{Disc}(\tilde{K_1}/k)^\gamma}{x^{1-\epsilon}}\Big).$$

Combining both cases, we can always bound

$$|\operatorname{Cl}_K[\ell]| = O_\epsilon(\operatorname{Disc}(K)^{1/2-\delta}),$$

with $\delta = \delta(\ell, G, k) < \min_i \min\{\big(\Delta(\ell, n/n_i)/f_i - \eta_0(\Delta(\ell, n/n_i) \cdot n/n_i f_i + \gamma m_i), \eta_0 \Delta(\ell, n_i)\}$. □

Remark 4.5. *We can see that the dependence on k for $\delta(\ell, G, k)$ in Theorem 4.1 is only due to the potential dependence on $\beta(k, G)$ and $\gamma(k, G)$. By choosing $\beta = 35$ and $\gamma = 19$ for example, then this dependence is no longer needed.*

5 Acknowledge

The authors would like to thank DoMath program at Duke University for their support and for providing such a nice opportunity, and thank Samit Dasgupta for his guidance and organization in this DoMath project. We would like to thank Robert Boltjie for helpful communications. The fifth author is partially supported by a Foerster-Bernstein Fellowship at Duke University.

References

[Alb18] B. Alberts. The weak form of Malle's conjecture and solvable groups. *arXiv: 1804.11318v2*, July 2018.

[Bae61] Reinhold Baer. Einfache partitionen endlicher gruppen mit nicht-trivialer Fittingscher untergruppe. *Archiv der Mathematik*, 12(1):81–89, 1961.

[BS96] A. Brumer and J. Silverman. The number of elliptic curves over $\mathbb{Q}$ with conductor n. *Manuscripta Mathematica*, 1996.

[BST$^+$17] M. Bhargava, A. Shankar, T. Taniguchi, F. Thorne, and J. Tsimerman. Bounds on 2-torsion in class groups of number fields and integral points on elliptic curves. *arXiv: 1701. 02458*, 2017.

[Duk98] W. Duke. Bounds for arithmetic multiplicities. *Proc. Intern. Congr. Math.*, II:163–172, 1998.

[EV07] J. S. Ellenberg and A. Venkatesh. Reflection principles and bounds for class group torsion. *Internat. Math. Res. Notices*, 2007.

[HV06] H. A. Helfgott and A. Venkatesh. Integral points on elliptic curves and 3-torsion in class groups. *J. Amer. Math. Soc.*, 19(3):527 – 550, 2006.

[Isa08] I. Martin Isaacs. *Finite Group Theory.* American Mathematical Soc., 2008.

[Keg61a] Otto H Kegel. Die nilpotenz der H_p-gruppen. *Mathematische Zeitschrift*, 75(1):373–376, 1961.

[Keg61b] Otto H Kegel. Nicht-einfache partitionen endlicher gruppen. *Archiv der Mathematik*, 12(1):170–175, 1961.

[Klü12] J. Klüners. The distribution of number fields with wreath products as Galois groups. *Int. J. Number Theory*, (8):845–858, 2012.

[KW21] J. Klüners and J. Wang. ℓ-torsion bounds for the class group of number fields with an ℓ-group as Galois group. *Proc. Amer. Math. Soc.*, 2021.

[LO75] J. Lagarias and A. Odlyzki. Effective versions of the Chebotarev density theorem. *Proc. Sympos.*, 1975.

[May13] J. Maynard. On the brun-titchmarsh theorem. *Acta Arithmetica*, 157, 2013.

[Mil07] G. A. Miller. Groups in which all the operators are contained in a series of subgroups such that any two have only identity in commun. *Bull. Amer. Math. Soc*, 17:446–449, 1906/1907.

[MV73] H.L. Montgomery and R.C. Vaughan. The large sieve. *Mathematika*, 20:119–134, 1973.

[Neu99] J. Neukirch. *Algebraic number theory*, volume 322. Springer-Verlag, 1999.

[OWW21] R.J. Lemke Oliver, J. Wang, and M. M. Wood. 3-torsion in class groups of 2-extensions. *preprint, https://wangjiuya.github.io/research/3tor2ext.pdf*, 2021.

[Pie05] L. B. Pierce. The 3-part of class numbers of quadratic fields. *J. London Math. Soc.*, 71:579–598, 2005.

[PTBW19] L. B. Pierce, C. Turnage-Butterbaugh, and M. M. Wood. On a conjecture for ℓ-torsion in class groups of number fields: from the perspective of moments. *arXiv: 1902.02008*, 2019.

[Ser92] J. P. Serre. *Topics in Galois Theory.* Jones and Bartlett Publ., 1992.

[Suz61] Michio Suzuki. On a finite group with a partition. *Archiv der Mathematik*, 12(1):241–254, 1961.

[TZ18] J. Thorner and A. Zaman. A Chebotarev variant of the Brun-Titchmarsh theorem and bounds for the Lang-Trotter conjectures. *Int. Math. Res. Not.*, 11(4991-5027), 2018.

[Wan20a] J. Wang. Pointwise bound for ℓ-torsion in class groups: Elementary abelian extensions. *J. Reine Angew. Math*, 2020.

[Wan20b] J. Wang. Pointwise bound for ℓ-torsion in class groups II: Nilpotent extensions. *arXiv: 2006.10295*, 2020.

[Zam17] A. Zaman. Analytic estimates for the Chebotarev density theorem and their applications. *Ph.D. thesis, University of Toronto*, 2017.

[Zap66] Guido Zappa. Sulle S-partizioni di un gruppo finito. *Annali di Matematica Pura ed Applicata*, 74(1):1–14, 1966.

[Zap03] Guido Zappa. Partitions and other coverings of finite groups. *Illinois Journal of Mathematics*, 47(1-2):571–580, 2003.

[Zha05] S.-W. Zhang. Equidistribution of CM-points on quaternion Shimura varieties. *Int. Math. Res. Not.*, 59:3657–3689, 2005.

Jiuya Wang, Department of Mathematics, Duke University, 120 Science Drive 117 Physics Building Durham, NC 27708, USA

E-mail address: wangjiuy@math.duke.edu