Pointwise Bound for ℓ-torsion in Class Groups II: Nilpotent Extensions

Jiuya Wang

September 9, 2020

Abstract

For every finite p-group G_p that is non-cyclic and non-quaternion and every positive integer $\ell \neq p$ that is greater than 2, we prove the first non-trivial bound on ℓ-torsion in class group of every G_p-extension. More generally, for every nilpotent group G where every Sylow-p subgroup $G_p \subset G$ is non-cyclic and non-quaternion, we prove a non-trivial bound on ℓ-torsion in class group of every G-extension for every integer $\ell > 1$.

Key words. ℓ-torsion conjecture, nilpotent group, descendant tree of p-groups

1 Introduction

This is a sequel paper of the author [Wan20] on the following conjecture.

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

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

This conjecture has been brought forward previously by [BS96, Duk98, Zha05]. We refer the audience to the first paper [Wan20] for an introduction of its relations to many other questions in arithmetic statistics (including Malle's conjecture, Cohen-Lenstra heuristics, integral points and Selmer groups of curves).

By a theorem of Brauer-Siegel, see for example [Lan94], the class number of F with $[F:\mathbb{Q}] = d$ is bounded by $O_{\epsilon,d}(\operatorname{Disc}(F)^{1/2+\epsilon})$. This gives the so-called *trivial bound* for ℓ-torsion in class groups:

$$|\operatorname{Cl}_F[\ell]| = O_{\epsilon}(\operatorname{Disc}(F)^{1/2+\epsilon}). \tag{1.1}$$

Although Conjecture 1 proposes a bound as small as $O_{\epsilon,k}(\operatorname{Disc}(F)^{\epsilon})$, in terms of what can be really proved, it is still wildly open to break $1/2$ into $1/2-\delta$ where $\delta > 0$ is an arbitrarily small positive number. We will call such a bound a *non-trivial bound* for ℓ-torsion in class groups.

We now give a brief summary on progress towards Conjecture 1. Firstly, we mention all cases where Conjecture 1 is currently known, that is, ℓ-torsion in class groups of all ℓ-extensions over an arbitrary number field k, see e.g. [KW, section 2] for a compact treatment. This includes, for example, Gauss's classical results on 2-torsion for quadratic extensions, which is usually considered the only case where Conjecture 1 is achieved. These results all essentially come from a direct use of genus theory, and was mentioned in previous literatures on isolated small degree cases.

Other than special cases from genus theory, results on this question are basically categorized into two directions: conditional result assuming GRH and unconditional result. The most broad conclusion is due to Ellenberg-Venkatesh [EV07] where a non-trivial bound in the order of $O_{\epsilon,k}(\mathrm{Disc}(F)^{1/2-1/2\ell(d-1)+\epsilon})$ is proved upon assuming GRH for Artin L-functions. On the other hand, for the unconditional result, we know much less. When $\ell = 2$, [BST$^+$17] gives a non-trivial bound for 2-torsion in class groups for all extensions by using geometry of numbers. In the same work of Ellenberg-Venkatesh [EV07], using reflection principle, an unconditional result for $\ell = 3$ for all small degree extensions with $d \leq 4$ is given. Earlier results on $\ell = 3$ for quadratic extensions can also be found in [Pie05, HV06]. For every $\ell > 3$, in the author's previous paper [Wan20], we show a non-trivial bound for ℓ-torsion in class groups of number fields where Galois group is $G = (\mathbb{Z}/p\mathbb{Z})^r$ with $r > 1$.

We mention that there are also recent results, see e.g. [EPW, PTBW, Wid17, FW18a, An18, FW18b, TZ19] on removing the GRH condition in [EV07] and get a non-trivial bound on ℓ-torsion in class groups *on average*. In contrast to results on average, this paper, together with the first paper [Wan20] in this sequence, focuses on proving results for *every* extension while removing the GRH assumption. Notice that for most cases treated in this paper (aside from $\ell = 2$ and the special cases $\ell = p$), even an average result hasn't been worked out before.

Comparing to the previous paper [Wan20] where we focus on very restricted Galois groups, in this paper we enlarge the set of Galois groups where a non-trivial point-wise bound holds unconditionally for arbitrary $\ell > 1$ to a much more general family of groups. For an arbitrary integer $\ell > 1$, we denote $\mathcal{G}_k(\ell)$ to be the set of permutation Galois groups G where there exists $\delta_k(G,\ell) > 0$ such that $|\mathrm{Cl}_F[\ell]| = O_{\epsilon,G,k}(\mathrm{Disc}(F)^{1/2-\delta(G,\ell)+\epsilon})$ for every G-extension F/k. We write $\mathcal{G}(\ell)$ and $\delta(G,\ell)$ in short when $k = \mathbb{Q}$. In this language, aside from special cases that can be handled by genus theory, we know that: by [BST$^+$17], the group $G \in \mathcal{G}(2)$ for every transitive permutation group $G \subset S_n$; by [EV07], the group $G \in \mathcal{G}(3)$ if $G \subset S_n$ is a transitive permutation group with degree $n \leq 4$; by [Wan20], for general ℓ, the group $A \in \mathcal{G}(\ell)$ for all elementary abelian groups $A = (\mathbb{Z}/p\mathbb{Z})^r$ with $r > 1$. Our main theorem is to greatly enlarge the set $\mathcal{G}_k(\ell)$ for every ℓ.

Our main theorem is as follows. A group G is *non-quaternion* if G is not a generalized quaternion group, see 4.3.1 for more details on generalized quaternion groups.

Theorem 1.1. *The regular representation of every non-cyclic and non-quaternion p-group G_p is in $\mathcal{G}(\ell)$ for every integer $\ell > 1$. More generally, the regular representation for every nilpotent group G is in $\mathcal{G}(\ell)$ for every integer $\ell > 1$ if its Sylow-p subgroup G_p is in $\mathcal{G}(\ell)$ for every $p||G|$.*

Remark 1.2. *An analogue of Theorem 1.1 also holds over arbitrary base field k. All results are effective.*

For example, Theorem 1.1 proves that every non-cyclic abelian p-group A_p is in $\mathcal{G}(\ell)$. This largely generalizes the previous result of the author, which we can rephrase as follows:

Theorem 1.3 ([Wan20], Theorem 1.1)**.** *Every non-cyclic elementary abelian group A is in $\mathcal{G}(\ell)$.*

The proof of Theorem 1.3 heavily relies on a result from representation theory, i.e., for every non-cyclic elementary abelian group A, we have for every A-extension L/k,

$$|\mathrm{Cl}_{L/k}[\ell]| = \prod_{K_i/k} |\mathrm{Cl}_{K_i/k}[\ell]|, \qquad \mathrm{Disc}(L/k) = \prod_{K_i/k} \mathrm{Disc}(K_i/k),$$

where K_i/k ranges over all degree p subfields of L, see [Wan20, section 3] for more details. However such a nice structure does not hold for general finite groups G. In particular, one can show that among all abelian groups, elementary abelian groups are the only groups carrying such a nice structure. Although such a rigid group structure is the key reason in obtaining good upper bounds on ℓ-torsion in [Wan20] (better than GRH-bound [EV07] in most cases), it largely limits the Galois groups where the method applies. As a contrast, in this paper, we will develop a much softer way, so that we can prove results for a much broader set of Galois groups.

The main strategy of this work is two-sided.

- (Arithmetic) Firstly, we introduce a new type of group extension, we call it *forcing extension*, see Definition 3.5. We develop an Extension Lemma 3.7, which is an induction on Lemma 3.1 in [EV07], specially for forcing extensions. This enables us to deduce the ℓ-torsion bound for a large degree number field from the ℓ-torsion bound for a small degree number field. More precisely, if $G \in \mathcal{G}_k(\ell)$, then for a forcing extension π,

$$\begin{tikzcd} 0 \arrow[r] & H \arrow[r] & \tilde{G} \arrow[r, "\pi"] & G \arrow[r] & 0, \end{tikzcd}$$

  we prove that $\tilde{G}$ is also in $\mathcal{G}_k(\ell)$.

- (Group Theory) Secondly, we show that most p-groups can be constructed via forcing extensions. In particular we prove that every non-cyclic and non-quaternion p-group can be constructed via iterated forcing extensions from its Frattini quotient. This enables us to apply the Extension Lemma proved before to all such p-groups, with the initial cases $G_p = (\mathbb{Z}/p\mathbb{Z})^r$ $(r > 1)$ in Theorem 1.3 proved in [Wan20]. This requires a careful analysis on the composition series of finite p-groups, see Section 4.

The arithmetic part can be thought of as a *vertical* version of the idea in [Wan20] where the local behavior of prime ideals are forced to split *horizontally.* More precisely, in [Wan20] we use splitting behaviors of a certain prime ideal in other neighboring subfields to force it to split in a single subfield. Here in this paper, we use splitting behavior of a certain prime ideal in bottom fields to force it to split in top fields. The group theory is sharp in the sense that among p-groups, we fully characterize groups that the current method applies, and for the cyclic and quaternion groups we explain in Section 4.3.1 and Section 5 why the method does not apply.

The organization of the paper is following. In section 3, we prove two induction lemmas: in section 3.1, we give the Extension Lemma for an inductive use of [EV07] on forcing group extensions; in section 3.2, we give the Compositum Lemma for an inductive use of [EV07] on compositum of extensions. In section 4, we focuses on studying p-groups, and we prove that every non-cyclic and non-quaternion p-group can be constructed via iterated forcing group extensions. Finally in section 5, we give the proof for the main theorem and provide a lower bound on the non-trivial saving for typical cases.

2 Notations

k: a number field considered as the base field
$\tilde{F}/k$: Galois closure of F over k
$\mathrm{Gal}(F/k)$: Galois group of F/k as a permutation group
$Z(G)$: center of a finite group G
G^{ab}: abelianization of a finite group G
$\mathrm{Disc}(F/k)$: absolute norm of relative discriminant $\mathrm{Nm}_{k/\mathbb{Q}}(\mathrm{disc}(F/k))$ of F/k where $\mathrm{disc}(F/k)$ is the relative discriminant ideal in k, when $k = \mathbb{Q}$ it is the usual absolute discriminant

$\mathrm{Cl}_{F/k}$: relative class group of F/k, when $k = \mathbb{Q}$ it is the usual class group of F
$\mathrm{Cl}_{F/k}[\ell]$: $\{[\alpha] \in \mathrm{Cl}_{F/k} \mid \ell[\alpha] = 0 \in \mathrm{Cl}_{F/k}\}$
$|\mathrm{Cl}_{F/k}[\ell]|$, $|\mathrm{Cl}_F[\ell]|$: the size of $\mathrm{Cl}_{F/k}[\ell]$, $\mathrm{Cl}_F[\ell]$
$\pi(Y; L/k, \mathcal{C})$: for a Galois extension L/k, the number of unramified prime ideals p in k with $|p| < Y$ and $\mathrm{Frob}_p \in \mathcal{C}$ where $\mathcal{C}$ is a conjugacy class of $\mathrm{Gal}(L/k)$
$\Delta(\ell, d)$: a constant slightly smaller than $\frac{1}{2\ell(d-1)}$, for details see Lemma 3.1

3 Induction over Ellenberg-Venkatesh

In this section, we are going to prove two versions of inductive methods to apply the following critical lemmas by Ellenberg-Venkatesh [EV07].

Lemma 3.1 ([EV07]). *Given a Galois extension L/K and $0 < \theta < \frac{1}{2\ell(d-1)}$ and an integer $\ell > 1$, denote*

$$M := \pi(\mathrm{Disc}(L/K)^\theta; L/K, e),$$

then

$$|\mathrm{Cl}_L[\ell]| = O_{\epsilon, [K:\mathbb{Q}], \ell}\Big(\frac{\mathrm{Disc}(L)^{1/2+\epsilon}}{M}\Big). \tag{3.1}$$

As one can observe, a critical input in applying Lemma 3.1 is a good estimate for M. It would be fantastic if we have a good lower bound on the value of M in terms of $\mathrm{Disc}(L)$. However, the exact challenge comes from the condition we impose on θ, that is, θ need to be really small. In particular, the bound $\mathrm{Disc}(L/K)^\theta$ by which we count prime ideals is so small that no current versions of effective Chebotarev density theorem can guarantee a single prime that is split in L/K without assuming GRH. If we are allowed to use GRH, then the effective Chebotarev density theorem proven by [LO75] immediately give a good lower bound on M.

Theorem 3.2 ([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*

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

As a corollary, assuming GRH, we can take $\theta = \Delta(\ell, d)$ in Lemma 3.1, i.e., arbitrarily close to $\frac{1}{2\ell(d-1)}$, and then get $M = \mathrm{Disc}(L/K)^{\Delta(\ell,d)}$.

In fact, if we do not assume GRH, [LO75] also proves an unconditional result which requires the bound x to be at least $\exp(10[L:\mathbb{Q}](\ln \mathrm{Disc}(L))^2)$ sub-exponential in $\mathrm{Disc}(L)$ if there is no Siegel zero. A complete unconditional threshold is even worse and can be found in [LO75, TZ18b]. It is of course too far away from the allowable range in Lemma 3.1.

In this paper we will show how to apply Lemma 3.1 to get a pointwise saving by unconditional knowledge on distribution of prime ideals. Actually it suffices if we can count prime ideals where the range x is a polynomial in $\mathrm{Disc}(L)$. We will apply the following statement in our proof since the format of the statement is convenient for us to give a uniform treatment for a large family of groups all at once.

Lemma 3.3 ([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*

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

Remark 3.4. *The actual values for β and γ are determined in [May13] when $k = \mathbb{Q}$ and L/k is abelian. The actual values for general cases are also determined in [Zam17]. We leave them as a symbol since these numbers could potentially be improved in the future. In all cases, the value for β is much larger than γ. So we will always assume $\beta > \gamma + 1/2$ in this paper. The reason we make this assumption is to simplify the numerical analysis in the proof of Extension Lemma 3.7.*

We mention that results in this direction have also appeared previously in [Wei83, Deb17, TZ17, TZ18a, MV73]. We expect that other versions of statements in this type (including both upper and lower bounds) can also be applied to some groups in our argument, and will result in different amount of power savings in the final answer. For example, in the author's previous paper [Wan20], an upper bound result in [MV73] seems to give optimal savings among all results in this direction. However, since we do not aim to optimize the savings in this work, we will simply apply Lemma 3.3 by which we can get a uniform proof.

3.1 Induction by Group Extension

In this section, our main goal is to prove Extension Lemma 3.7. We first define a new type of group extension *forcing extensions.*

Definition 3.5 (Forcing Extension)**.** *We say that a group extension $(\tilde{G}, \pi)$ of G*

$$\begin{tikzcd} 0 \arrow[r] & H \arrow[r] & \tilde{G} \arrow[r, "\pi"] & G \arrow[r] & 0, \end{tikzcd}$$

is forcing *if there exists a conjugacy class $\mathcal{C} \subset G$ such that for every element $c \in \mathcal{C}$, all elements in $\pi^{-1}(c) \subset \tilde{G}$ has the same order with $c \in G$. We will also say that $(\tilde{G}, \pi)$ is* forcing with respect to *$\mathcal{C}$.*

Remark 3.6. *This notion of forcing extension does not fit with other common seen concepts of group extensions. Split extensions are not necessarily forcing, and central extensions are not necessarily forcing. For example, the cyclic group C_6, as a group extension of C_3 by C_2, is both split and central, but it is not forcing. However, we will see that this notion of forcing extension is particularly amenable to discussions on p-groups.*

Lemma 3.7 (Extension Lemma)**.** *Given two finite groups G and H with $|G| = n$ and $|H| = m$ and an arbitrary integer $\ell > 1$. Suppose the regular representation of G is in $\mathcal{G}_k(\ell)$ with respect to $\delta = \delta_k(G, \ell)$. If the extension $(\tilde{G}, \pi)$ of G*

$$\begin{tikzcd} 0 \arrow[r] & H \arrow[r] & \tilde{G} \arrow[r, "\pi"] & G \arrow[r] & 0. \end{tikzcd}$$

is a forcing extension with respect to $\mathcal{C}$, then the regular representation $\tilde{G}$ is in $\mathcal{G}_k(\ell)$ with respect to

$$\delta_k(\tilde{G}, \ell) = \delta_k(G, \ell) \cdot \eta_0$$

where $\eta_0 = \frac{\Delta(\ell,m)}{m\cdot\Delta(\ell,m)+r\cdot\max\{\beta,\gamma\}}$ and $r = \mathrm{ord}(g)$ for $g \in \mathcal{C}$.

We first give a lemma on the size of ℓ-torsion in relative class groups for a general $\ell > 1$.

Lemma 3.8. *Given a relative extension $L/F/k$ and an arbitrary integer $\ell > 1$, we have*

$$\frac{|\operatorname{Cl}_{L/k}[\ell]|}{|\operatorname{Cl}_{F/k}[\ell]|} \leq |\operatorname{Cl}_{L/F}[\ell]| \leq |\operatorname{Cl}_{L/F}| \leq [L:F] \cdot \frac{|\operatorname{Cl}_L|}{|\operatorname{Cl}_F|} \leq [L:F] \cdot \frac{\operatorname{Disc}(L)^{1/2}}{\operatorname{Disc}(F)^{1/2}}.$$

Proof. By the definition of relative class group, there exists a subgroup $N = \mathrm{Nm}_{L/F}(\mathrm{Cl}_L) \subset \mathrm{Cl}_F$ such that

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Cl}_{L/F} \arrow[r] \arrow[d] & \mathrm{Cl}_L \arrow[r, "\mathrm{Nm}_{L/F}"] \arrow[d, "\mathrm{Nm}_{L/k}"] & N \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & 0 \arrow[r] & \mathrm{Cl}_k \arrow[r] & \mathrm{Cl}_k \arrow[r] & 0
\end{tikzcd}$$

Taking the kernel of the two short exact sequences, we get

$$0 \longrightarrow \mathrm{Cl}_{L/F} \longrightarrow \mathrm{Cl}_{L/k} \longrightarrow \mathrm{Cl}_{F/k} \cap \mathrm{Nm}_{L/F}(\mathrm{Cl}_L) \longrightarrow 0.$$

Since $\mathrm{Hom}(\mathbb{Z}/\ell\mathbb{Z}, -)$ is left exact, we have for arbitrary integer ℓ that

$$0 \longrightarrow \mathrm{Cl}_{L/F}[\ell] \longrightarrow \mathrm{Cl}_{L/k}[\ell] \xrightarrow{\mathrm{Nm}} (\mathrm{Cl}_{F/k} \cap N)[\ell]$$

This proves the first inequality. The second inequality is trivial. The third inequality comes from the fact that $\mathrm{Coker}(\mathrm{Nm}) = \mathrm{Cl}_F / N = \mathrm{Gal}(M/F)$ where $M = h_F \cap L$ is the maximal abelian unramified extension of F inside L. The last inequality comes from a combination of an absolute lower bound $\frac{\mathrm{Rg}_L}{\mathrm{Rg}_k} \geq O_{[L:\mathbb{Q}]}(1)$ by [FS99] and the theorem of Brauer-Siegel, see for example in [Lou00]. □

We are now ready to give the proof of the Extension Lemma 3.7.

Proof of Lemma 3.7. Every $\tilde{G}$-extension L/k is realized as an H-extension L/K over a G-extension F/k. Given $\mathcal{C} \subset G$, we denote $r = r(\mathcal{C})$ to be the order of elements $c \in \mathcal{C}$. Firstly, we show that if a prime p in k is unramified in L/k and $\mathrm{Frob}_p(F/k) \in \mathcal{C} \subset G$, then every prime $\mathfrak{p}\,|p$ above p in F will split in L/F. We fix a prime $\mathfrak{P}|p$ in L/k and $\mathfrak{p} = \mathfrak{P} \cap O_F$. Suppose the decomposition group is $D_{\mathfrak{P}/p} = \langle g \rangle \subset \tilde{G}$, then $D_{\mathfrak{p}\,/p} = \langle g \rangle H/H = \langle \pi(g) \rangle \subset G$ and $D_{\mathfrak{P}/\,\mathfrak{p}} = \langle g \rangle \cap H \subset H$. Notice that

$$D_{\mathfrak{P}/\,\mathfrak{p}} = e \iff \langle g \rangle \cap H = e \iff g^r = e. \tag{3.2}$$

It follows from the assumption on $\mathcal{C}$ that $D_{\mathfrak{P}/\,\mathfrak{p}} = e$. Therefore every $\mathfrak{p}$ above p will split in L/F.

Next, we separate the discussion into two cases based on how large

$$\eta(L/k) := \frac{\ln \mathrm{Disc}(F/k)}{\ln \mathrm{Disc}(L/k)},$$

is, i.e., whether $\eta(L/k) \leq \eta_0$ or $\eta(L/k) \geq \eta_0$ where

$$\eta_0 := \frac{\Delta(\ell, m)}{m \cdot \Delta(\ell, m) + r \cdot \max\{\beta, \gamma\}},$$

is the cut-off, and $\beta = \beta(G, k)$, $\gamma = \gamma(G, k)$ and $D_0 = D_0(k)$ are parameters in Lemma 3.3. For the rest of the proof, we will write η for $\eta(L/k)$ in short.

Case 1 **(Big** η**):** If $\eta(L/k) \geq \eta_0$, then we always have

$$\begin{aligned}
|\,\mathrm{Cl}_{L/k}[\ell]| \leq &|\,\mathrm{Cl}_{F/k}[\ell]| \cdot |\,\mathrm{Cl}_{L/F}[\ell]| = O_{\epsilon,k}(\mathrm{Disc}(F/k)^{1/2-\delta+\epsilon}) \cdot \frac{\mathrm{Disc}(L)^{1/2+\epsilon}}{\mathrm{Disc}(F)^{1/2+\epsilon}}. \\
=&O_{\epsilon,k}\Big(\frac{\mathrm{Disc}(L/k)^{1/2+\epsilon}}{\mathrm{Disc}(F/k)^{\delta}}\Big) = O_{\epsilon,k}(\mathrm{Disc}(L/k)^{1/2-\delta_b(\eta,\ell)+\epsilon}),
\end{aligned} \tag{3.3}$$

where $\delta_b(\eta,\ell)=\delta\cdot\eta$. Here the first inequality follows from Lemma 3.8, the first equality follows from Lemma 3.8 and the assumption on that G is in $\mathcal{G}(\ell)$ with respect to $\delta=\delta_k(G,\ell)$. The second equality comes from conductor-discriminant formula for relative extensions (notice that we have suppressed the dependence on k). The last equality follows from definition of η. We remark here that we actually do not use the assumption $\eta\geq\eta_0$ here. This bound holds universally true no matter how large η is, but it will behave better when η is relative large, and when $\eta\geq\eta_0$, we get a uniform saving $\delta_b(\eta,\ell)\geq\delta\cdot\eta_0$ that is independent of L/k. So we will need treat the case when η is small in another way.

Case 2 **(Small** η**):** If $\eta(L/k)\leq\eta_0$, then we separate the discussion when $\operatorname{Disc}(F/k)\leq D_0$ and $\operatorname{Disc}(F/k)\geq D_0$ where $D_0=D_0(k)$ in Lemma 3.3.

If $\operatorname{Disc}(F/k)\leq D_0$, we denote $x=\operatorname{Disc}(L/F)^{\Delta(\ell,m)/r}$. Notice that there are only finitely many extensions F/k with $\operatorname{Disc}(F/k)\leq D_0$, by the standard effective Chebotarev density theorem [LO75], there exists $C_0(k,n)$ such that when $x\geq C_0(k,n)$ and $\operatorname{Disc}(F/k)\leq D_0$, we have

$$\pi(x;F/k,\mathcal{C})\geq\frac{1}{2}\frac{|\mathcal{C}|}{|G|}\cdot\frac{x}{\ln x}. \tag{3.4}$$

Therefore when $\operatorname{Disc}(L/k)\geq C_0(k,n)D_0^m$ is sufficiently large comparing to k, we have $\operatorname{Disc}(L/F)=\operatorname{Disc}(L/k)\operatorname{Disc}(F/k)^{-m}\geq\operatorname{Disc}(L/k)D_0^{-m}\geq C_0(k,n)$, thus (3.4) holds.

If $\operatorname{Disc}(F/k)\geq D_0$, then we apply Lemma 3.3 to F/k with $x=\operatorname{Disc}(L/F)^{\Delta(\ell,m)/r}$, and we obtain

$$\pi(x;F/k,\mathcal{C})\geq C_k\frac{1}{\operatorname{Disc}(F/k)^{\gamma}}\cdot\frac{|\mathcal{C}|}{|G|}\cdot\frac{x}{\ln x}, \tag{3.5}$$

when $x\geq\operatorname{Disc}(F/k)^{\beta}$. By the definition of η, we have

$$\operatorname{Disc}(L/F)^{\Delta(\ell,m)/r}\geq\operatorname{Disc}(F/k)^{\beta}\iff\eta\leq\eta_0,$$

so (3.5) always holds as long as $\operatorname{Disc}(F/k)\geq D_0$ and $\eta\leq\eta_0$. Denote $C_k'=\min\{1/2,C_k\}$, then for every L/k with $\eta\leq\eta_0$ and $\operatorname{Disc}(L/k)$ sufficiently large, we have

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

which is a lower bound on the number of prime ideals p in k such that p become unramified with $\operatorname{Frob}_p(F/k)\in\mathcal{C}\subset G$. By the argument at the beginning of this proof, all primes $\mathfrak{p}\,|p$ above p in F will split in L/F. Since the inertia degree at p for F/k is r, we have $\operatorname{Nm}_{F/\mathbb{Q}}(\mathfrak{p})=\operatorname{Nm}_{k/\mathbb{Q}}(p)^r$. Therefore

$$\pi(\operatorname{Disc}(L/F)^{\Delta(\ell,m)};L/F,e)\geq\pi(x;F/k,\mathcal{C})\geq C_k'\frac{|\mathcal{C}|}{|G|}\cdot\frac{1}{\operatorname{Disc}(F/k)^{\gamma}}\cdot\frac{\operatorname{Disc}(L/F)^{\Delta(\ell,m)/r}}{\ln\operatorname{Disc}(L/F)^{\Delta(\ell,m)/r}}.$$

Therefore by Lemma 3.1 we have

$$|\operatorname{Cl}_{L/k}[\ell]|=O_{\epsilon,k,[F:\mathbb{Q}]}\Big(\frac{\operatorname{Disc}(L)^{1/2+\epsilon}}{\operatorname{Disc}(L/F)^{\Delta(\ell,m)/r}\cdot\operatorname{Disc}(F/k)^{-\gamma}}\Big)=O_{\epsilon,k}(\operatorname{Disc}(L/k)^{1/2-\delta_s(\eta,\ell)+\epsilon}), \tag{3.6}$$

where

$$\delta_s(\eta,\ell)=(1-m\eta)\cdot\Delta(\ell,m)/r-\eta\cdot\gamma.$$

The last equality in (3.6) comes from the definition of η and that $\operatorname{Disc}(L/F)=\operatorname{Disc}(L/k)^{1-m\eta}$.

Finally, after the discussion for two ranges of η, we notice that $\delta_s(\eta,\ell)$ decreases as η increases, and $\delta_b(\eta,\ell)$ increases as η increases. It suffices to compare their value at $\eta=\eta_0$:

$$\begin{aligned}\delta_s(\eta,\ell)=(1-m\eta_0)\cdot\frac{\Delta(\ell,m)}{r}-\eta\cdot\gamma\geq\delta\cdot\eta_0=\delta_b(\eta,\ell)\iff\\ \max\{\beta,\gamma\}-\gamma\geq\delta.\end{aligned}\tag{3.7}$$

Assuming $\beta>\gamma+1/2$, we will always have $\max\{\beta,\gamma\}-\gamma\geq\delta$. Therefore we can take

$$\delta_k(\tilde{G},\ell)=\delta_b(\eta_0,\ell)=\delta\cdot\eta_0.$$

□

3.2 Induction by Compositum

In this section, we will prove a lemma on applying the method of Ellenberg-Venkatesh to compositum of number fields.

Lemma 3.9 (Compositum Lemma). *Given two permutation groups $G_1\subset S_n$ and $G_2\subset S_m$ and any integer $\ell>1$. Suppose G_1 and G_2 are both in $\mathcal{G}(\ell)$ with respect to $\delta_i=\delta_k(G_i,\ell)$. Denote $G=G_1\times G_2\subset S_{mn}$ to be a direct product of G_1 and G_2 as permutation groups, we have $G\in\mathcal{G}(\ell)$ with respect to*

$$\delta_k(G,\ell)=\frac{\delta_1\delta_2}{m\delta_2+n\delta_1}.$$

Proof. Every G-extension L/k is the compositum L_1L_2/k of L_i/k where $\mathrm{Gal}(L_i/k)=G_i$ for $i=1,2$ and $\tilde{L}_1/k\cap\tilde{L}_2/k=k$.

We separate the discussion by

$$\eta_i(L/k):=\frac{\ln\mathrm{Disc}(L_i/k)}{\ln\mathrm{Disc}(L/k)},\quad i=1,2.$$

It follows from the definition that $\mathrm{Disc}(L_i/k)=\mathrm{Disc}(L/k)^{\eta_i}$.

For any G-extension L/k, we have

$$\begin{aligned}|\operatorname{Cl}_{L/k}[\ell]|\leq&|\operatorname{Cl}_{L_1/k}[\ell]|\cdot|\operatorname{Cl}_{L/L_1}[\ell]|=O_{\epsilon,k}(\mathrm{Disc}(L_1/k)^{1/2-\delta_1+\epsilon})\cdot\frac{\mathrm{Disc}(L)^{1/2+\epsilon}}{\mathrm{Disc}(L_1)^{1/2+\epsilon}}.\\ =&O_{\epsilon,k}\Big(\frac{\mathrm{Disc}(L/k)^{1/2+\epsilon}}{\mathrm{Disc}(L_1/k)^{\delta_1}}\Big)=O_{\epsilon,k}(\mathrm{Disc}(L/k)^{1/2-\delta_1\cdot\eta_1+\epsilon}).\end{aligned}\tag{3.8}$$

Here the first inequality comes from Lemma 3.8. The first equality comes from the assumption $G_1\in\mathcal{G}(\ell)$. The second equality comes from the conductor-discriminant formula. Similarly,

$$|\operatorname{Cl}_{L/k}[\ell]|=O_{\epsilon,k}(\mathrm{Disc}(L/k)^{1/2-\delta_2\cdot\eta_2+\epsilon}).\tag{3.9}$$

It follows from conductor-discriminant formula that $\mathrm{Disc}(L_1/k)^m\,\mathrm{Disc}(L_2/k)^n\geq\mathrm{Disc}(L/k)$ when $[L_1L_2:k]=[L_1:k][L_2:k]$. So we get

$$\mathrm{Disc}(L/k)^{m\eta_1}\,\mathrm{Disc}(L/k)^{n\eta_2}\geq\mathrm{Disc}(L/k),\tag{3.10}$$

which gives an inequality between η_i that

$$m\eta_1+n\eta_2\geq1.\tag{3.11}$$

If $\eta_1 \geq M$, then by (3.8) we have

$$|\operatorname{Cl}_{L/k}[\ell]| = O_{\epsilon,k}(\operatorname{Disc}(L/k)^{1/2-\delta_1\cdot M+\epsilon}).$$

If $\eta_1 \leq M$, then $\eta_2 \geq \frac{1-M\eta_1}{n}$ from (3.11). Therefore by (3.9) we have

$$|\operatorname{Cl}_{L/k}[\ell]| = O_{\epsilon,k}(\operatorname{Disc}(L/k)^{1/2-\delta_2\frac{1-Mm}{n}+\epsilon}).$$

To get the optimal bound for $|\operatorname{Cl}_{L/k}[\ell]|$, we choose M such that

$$\delta_1 \cdot M = \delta_2 \cdot \frac{1-Mm}{n}.$$

We solve that

$$M_0 = \frac{\delta_2}{n\delta_1 + m\delta_2},$$

with the corresponding optimal saving $\delta_k(G, \ell)$ is

$$\delta_k(G,\ell) = \delta_1 M_0 = \frac{\delta_1\delta_2}{m\delta_2 + n\delta_1}. \tag{3.12}$$

□

Remark 3.10. *Notice that both (3.8), (3.9) and (3.10) still hold when L_1/k and L_2/k are linearly disjoint, i.e., $[L_1L_2 : k] = [L_1 : k][L_2 : k]$. So the exact same argument of Lemma 3.9 applies with no change to all permutation groups arising from linearly disjoint compositum of a G_1 extension with a G_2 extension. Equivalently, these are the permutation groups $G \subset G_1 \times G_2 \subset S_{mn}$ that is transitive and $S_1 := \{g_1 \in G_1 \mid \exists g_2 \in G_2, (g_1, g_2) \in G\} = G_1$ and similarly $S_2 = G_2$.*

4 Forcing Sequence for p-Groups

In [Wan20], the author has proved Theorem 1.1 for $G = (\mathbb{Z}/p\mathbb{Z})^r$ with $r > 1$. Notice that the Frattini quotient of a r-generated p-group is always isomorphic to $(\mathbb{Z}/p\mathbb{Z})^r$. This leads to our strategy to prove Theorem 1.1 for r-generated p-groups, i.e., to do an induction via Extension Lemma 3.7 with the base case $G = (\mathbb{Z}/p\mathbb{Z})^r$.

The key group theoretic lemma we will prove is the following. It is a crucial input for applying Extension Lemma 3.7.

Theorem 4.1. *Every non-cyclic and non-quaternion p-group G has a decreasing sequence of normal subgroups N_i*

$$G \supset \Phi(G) = N_0 \supset N_1 \supset N_2 \supset \cdots \supset N_m = e,$$

where for every $0 \leq i < m$:
1) $[N_i : N_{i+1}] = p$;
2) $(G/N_{i+1}, \pi)$ is a forcing extension of G/N_i where $\pi : G/N_{i+1} \to G/N_i$.

See the proof in section 4.2 and section 4.3.2. In general we will say a sequence $G = N_0 \supset N_1 \supset \cdots \supset N_m = e$ of normal subgroups of G is a *forcing sequence of G* if $(G/N_{i+1}, \pi)$ is a forcing extensions of G/N_i where $\pi : G/N_{i+1} \to G/N_i$ for every $0 \leq i < m$.

4.1 Basics for p-Group

We first introduce some basic concepts for p-groups. Given a finite p-group G, the *Frattini subgroup* $\Phi(G) \subset G$ is defined to the intersection of all maximal subgroups of G. We call $G/\Phi(G)$ the *Frattini quotient* of G. It follows from Burnside's basis theorem that $G/\Phi(G)$ is the largest elementary abelian quotient of G. Therefore $\Phi(G) = G^p \cdot [G, G]$ is the subgroup generated by the set of all the p-th power G^p and the commutator $[G, G]$. It is clearly normal since it is a characteristic subgroup. Now suppose $G/\Phi(G) \simeq (\mathbb{Z}/p\mathbb{Z})^r$, then we say the *generator rank* of G is r. Equivalently, the generator rank is $r = \dim(H^1(G, \mathbb{Z}/p\mathbb{Z}))$ where $\mathbb{Z}/p\mathbb{Z}$ is considered as a trivial G-module.

We define $G_0 = G$ to be the group itself and $G_1 = \Phi(G)$ to be the Frattini subgroup. Inductively we define $G_j := G_{j-1}^p \cdot [G_{j-1}, G]$ for $j > 0$, equivalently G_j is defined to be the minimal subgroup such that G_{j-1}/G_j is central in G/G_j with exponent p. These subgroups form a strictly decreasing sequence of subgroups

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_c = \{e\}.$$

This sequence is called *lower exponent p central series* of G. We define the minimal integer c such that $G_c = \{e\}$ to be *p-class* of the finite p-group G. We will denote the p-class of G by $c(G)$. We will write $\bar{G}_k := G/G_k$ in short.

We can parametrize all finite p-groups with generator rank r by the *p-group generating algorithm* [O'B90] by putting all p-groups into a *descendant tree*. The root of the tree is the elementary abelian p-group $A = (\mathbb{Z}/p\mathbb{Z})^r$. The *immediate descendants* of a finite p-group G are all finite p-groups D such that $D/D_{c-1} \simeq G$ where $c = c(D)$. Since these characteristic groups G_j are defined inductively by an explicit formula, one can show that the operation of taking j-th subgroup in the sequence commutes with group homomorphism, i.e., if $f : M \to N$ are two p-groups, then $f(M_j) = N_j$ for all $j > 0$. Therefore if $D/D_k \simeq G$ for some $1 < k < c(D)$, then $c(G) = k$, and $D/D_j \simeq G/G_j$ for all $0 < j < c(G)$. This guarantees that ancestors of a p-group G are the quotients G/G_j with $0 < j < c(G)$, the descendants of a finite p-group G are all finite p-groups D such that $D/D_k \simeq G$ where $0 < k < c$ and c is the p-class of D. Since G/G_1 is always isomorphic to one elementary abelian group, G belongs to the unique tree with the root $(\mathbb{Z}/p\mathbb{Z})^r$ where $r = r(G)$. In particular, a p-group G is one descendant in $c(G)$-th generation if we count elementary abelian group as the 1-st generation. This tree encodes many properties of p-groups. If a p-group G does not have any descendants, equivalently there are no p-group D with $D/D_j \simeq G$ where D_j defined in the sequence, then we call such a group a *leaf.*

4.2 Odd p-Group

In this section, we will prove Theorem 4.1 for odd p-groups. Notice that for odd p, there is no quaternion group, so we will prove Theorem 4.1 for every non-cyclic odd p-groups.

Lemma 4.2. *Given a p-group G, there exists a series of normal subgroups*

$$G \supset \Phi(G) = N_0 \supset N_1 \supset \cdots \supset N_m = e,$$

where for every $0 \leq i < m$:
1) $[N_i : N_{i+1}] = p$;
2) N_i/N_{i+1} is in the center of G/N_{i+1};
3) the sequence is a refinement of the lower exponent p central series of G, or equivalently, for all $j < c(G)$ the subgroup G_j is equal to N_i for some i.

Proof. For every p-group G with $c(G) = c$, let's say $G = G_0 \supset G_1 \supset \cdots \supset G_c = \{e\}$ is the lower exponent p central series of G. By construction, for every $j < c$, the subgroup G_j is normal in G since it is characteristic, G_j/G_{j+1} is in the center of G/G_{j+1}, and G_j/G_{j+1} has exponent p.

Fix j. Let $G_j = S_0 \supset S_1 \supset \cdots \supset S_K = G_{j+1}$ be an arbitrary refinement of $G_j \supset G_{j+1}$ with $[S_k : S_{k+1}] = p$. Since G_j/G_{j+1} is in the center of G/G_{j+1}, for all k, we have S_k/S_{k+1} is in the center of G/S_{k+1}. We will show that S_k is also normal in G for all k. In fact, since $S_k/G_{j+1} \subset G/G_{j+1}$ is in the center of G/G_{j+1}, clearly S_k/G_{j+1} is normal in G/G_{j+1}. Then denote $\phi : G \to G/G_{j+1}$ to be the canonical projection, the preimage $S_k = \phi^{-1}(S_k/G_{i+1})$ is also normal in G.

Therefore we could refine the lower exponent p central series by inserting normal subgroups $S_{k,j}$ as above between G_j and G_{j+1} for every $j > 0$. We will get a descending sequence of subgroups $G \supset \Phi(G) = N_0 \supset N_1 \supset \cdots \supset N_m = 1$ that satisfies all three conditions. □

Proof of Theorem 4.1 for odd p. Let G be a non-cyclic odd p-group. By Lemma 4.2, we have a sequence

$$G \supset \Phi(G) = N_0 \supset N_1 \supset \cdots \supset N_m = e,$$

of descending subgroups, where $N_i/N_{i+1} \simeq \mathbb{Z}/p\mathbb{Z}$ in the center of G/N_{i+1}. It suffices to prove that the following extension $(G/N_{i+1}, \pi)$ is forcing for each i.

$$0 \longrightarrow N_i/N_{i+1} \longrightarrow G/N_{i+1} \xrightarrow{\pi_i} G/N_i \longrightarrow 0.$$

Since N_i/N_{i+1} is in the center of G/N_{i+1}, the extension π is a central extension. Suppose $g_0 \in G/N_i$ is not identity. Denote the conjugacy class containing g_0 by $\mathcal{C} \subset G/N_i$. We will show that for any $c \in \mathcal{C}$, all elements in $\pi^{-1}(c)$ have the same order. If $\pi(\tilde{c}) = c$, then all preimages of c is $a\tilde{c}$ for $a \in N_i/N_{i+1}$. Since $\operatorname{ord}(a) = p$ and a is central we get $\operatorname{ord}(\tilde{c}) = \operatorname{ord}(a\tilde{c})$. On the other hand, if $c' = x^{-1}cx \in G/N_i$, then $\tilde{x}^{-1}\tilde{c}\tilde{x} \in \pi^{-1}(c')$ when $\tilde{x} \in \pi^{-1}(x)$. It follows that $\operatorname{ord}(\tilde{x}^{-1}\tilde{c}\tilde{x}) = \operatorname{ord}(\tilde{c})$.

Therefore it suffices to find an element $y \in G/N_{i+1}$ such that $\operatorname{ord}(y) = \operatorname{ord}(\pi(y))$. If G is not cyclic, then G/N_{i+1} is not cyclic since $G/\Phi(G) = G/N_{i+1}/\Phi(G/N_{i+1}) = (\mathbb{Z}/p\mathbb{Z})^r$ with $r > 1$, then when p is odd there exists at least two cyclic subgroups of order p, see e.g. Theorem 12.5.2 in [Hal99]. Therefore there must be a subgroup T of order p and $T \neq N_i/N_{i+1}$. Denote the generator of T by y. By construction, $\operatorname{ord}(y) = p = \pi(y)$ since $y \notin N_i/N_{i+1}$. Then π is forcing with respect to the conjugacy class $\mathcal{C} \subset G/N_i$ of $\pi(y)$. □

4.3 Even p-Group

In this section, we will prove Theorem 4.1 for 2-groups. Such a good picture for odd p-groups where all non-cyclic p-groups satisfy Theorem 4.1 no longer holds for 2-group. We will first introduce these exceptional groups, *generalized quaternion groups*, and list their properties in section 4.3.1. Then we will give the proof for all non-cyclic and non-quaternion 2-groups in section 4.3.2.

4.3.1 Generalized Quaternion Groups

We define the *generalized quaternion group* by

$$Q(n) := \langle x, y \mid x^{2^{n+1}} = y^4 = 1, x^{2^n} = y^2, y^{-1}xy = x^{-1} \rangle.$$

When $n = 1$, we get the smallest such group, which is usually called quaternion group and denoted by Q_8. The generalized quaternion groups have the special property that all abelian subgroups are cyclic, see Figure 1 for the subgroup lattice of $Q(1)$ as an example.

We will prove that this family of 2-groups is the only exceptional groups aside from cyclic 2-groups for Theorem 4.1 in section 4.3.2. In preparation for the proof, we will first list several useful properties of $Q(n)$ in Lemma 4.3.

Before we state the properties, we briefly recall the concept of *Schur multiplier*. Given a finite group G, we say E is a *stem extension* of G

$$0 \longrightarrow Z \longrightarrow E \longrightarrow G \longrightarrow 0,$$

if $Z \subset [E,E] \cap Z(E)$ where $Z(E)$ is the center of E. We then define *Schur multiplier* $M(G)$ of G to be the kernel of the unique largest stem extension of G. Equivalently, if $G = F/R$ where F is a free group, then there is a formula $M(G) = R \cap [F,F]/[R,F]$ for Schur multiplier.

Lemma 4.3. *The generalized quaternion group $Q(n)$ has the following property:*

1. *The order of $Q(n)$ is 2^{n+2}.*

2. *The 2-class of $Q(n)$ is $n+1$.*

3. *The center of $Q(n)$ is $\mathbb{Z}/2\mathbb{Z}$.*

4. *It has trivial Schur multiplier.*

5. *It is a leaf on the descendant tree.*

Proof. 1. Consider the cyclic subgroup $N = \langle x \rangle$ generated by x. Then $Q(n)/N = C_2$ since $y^2 \in N$. Therefore $|Q(n)| = 2^{n+2}$.

2. We can write down the exponent p lower central series for $Q(n)$. Recall that $G_1 = \Phi(G) = G^2[G,G]$. By definition, it is clear that $x^2 \in G_1$, and $G_1/\langle x^2 \rangle = C_2 \times C_2 = \langle \bar{x}, \bar{y} \rangle$. So $G_1 = \langle x^2 \rangle$ is a cyclic group with order 2^n. For $k = 2$, notice that the only subgroup G_2 of G_1 with G_1/G_2 exponent 2 is $G_2 = \langle x^4 \rangle$. Similarly $G_k = \langle x^{2^k} \rangle$. Therefore we have the 2-class of $Q(n)$ is $n+1$.

3. Suppose x^s is in the center, then $y \cdot x^s = x^s \cdot y = y \cdot x^{-s}$ implies that $s = 2^n$. One can show that it is the only element that commute both with x and y. Therefore $Z(Q(n)) = \{e, x^{2^n}\}$.

4. See Exercise $5A.7$ in [Isa08].

5. Given $G = Q(n)$, we have shown that $G_k = \langle x^{2^k} \rangle$, and $(G/G_k)^{ab} = G^{ab} = C_2 \times C_2$ for every $k > 0$. The abelianization $G^{ab} \simeq (G/G_{c-1})^{ab}$ where $c = c(G)$, then all immediate descendants D of G must have $D^{ab} = G^{ab}$ by Theorem 4.4 [Nov09]. Therefore if G has any immediate descendant D, then D is a central extension of G with $D^{ab} = G^{ab}$. By definition, a central extension is a stem extension if and only if $E^{ab} = G^{ab}$. So the existence of immediate descendants contradicts with G having trivial Schur multiplier.

□

We can see that Theorem 4.1 cannot hold for generalized quaternion group. As an example, the smallest quaternion group Q_8 is a central extension of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$,

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow Q_8 \xrightarrow{\pi} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \longrightarrow 0.$$

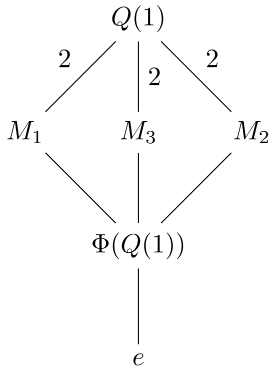

Figure 1: Quaternion Group of Order 8

Such an extension (Q_8, π) is not forcing since for every element $c \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, elements in $\pi^{-1}(c)$ all have order 4 whereas c has order 2. One can similarly show that for general n, the extension $(Q(n), \pi)$ where $\pi : Q(n) \to Q(n)/Z(Q(n))$ is not forcing. This failure has a lot to do with the fact that $Z(Q(n))$ is the only $\mathbb{Z}/2\mathbb{Z}$ subgroup of $Q(n)$. This turns out to be a characterizing property of $Q(n)$ by the following lemma.

Lemma 4.4 (Theorem 12.5.2, [Hal99]). *A p-group which contains only one subgroup of order p is cyclic or generalized quaternion group.*

4.3.2 Proof of Theorem 4.1 for $p = 2$

In last section, we have shown that Theorem 4.1 does not hold for quaternion group and cyclic group. Therefore the best we can hope for is that Theorem 4.1 is true for all 2-groups that are non-quaternion and non-cyclic. We will show that is really the case!

Unlike the case for odd p where an arbitrary refinement of the lower exponent p central series satisfies the property stated in Theorem 4.1, when $p = 2$, it can happen that some refinement of the lower exponent p central series will not be forcing when the refinement $G/N_i \simeq Q(n)$ for some i. Therefore our main focus in the following proof is to show that we can always find a detour in the refinement to avoid such quaternion quotients.

Proof of Theorem 4.1 for $p = 2$. We will separate the discussion for 2-group G with generator rank $r = 2$ and $r > 2$.

Firstly, we consider the case when G is a 2-group with $r > 2$. Then G is non-cyclic and non-quaternion since cyclic 2-group has $r = 1$ and quaternion group has $r = 2$. By Lemma 4.2, we have a sequence

$$G \supset \Phi(G) = N_0 \supset N_1 \supset \cdots \supset N_m = e,$$

of descending groups, where $N_i/N_{i+1} \simeq \mathbb{Z}/p\mathbb{Z}$ in the center of G/N_{i+1}. We will to show that the following extension is forcing for every i,

$$0 \longrightarrow N_i/N_{i+1} \longrightarrow G/N_{i+1} \xrightarrow{\pi_i} G/N_i \longrightarrow 0.$$

Since $G/\Phi(G) = (\mathbb{Z}/p\mathbb{Z})^r$ and $Q(n)$ has $r = 2$, the quotient G/N_{i+1} is not quaternion for every i. Then by Lemma 4.4, there must exist a subgroup $T = \langle y \rangle$ of order 2 and $T \neq N_i/N_{i+1}$. Then the same proof for odd p-group shows that π is forcing with respect to the conjugacy class $\mathcal{C} \subset G/N_i$ of $\pi(y)$.

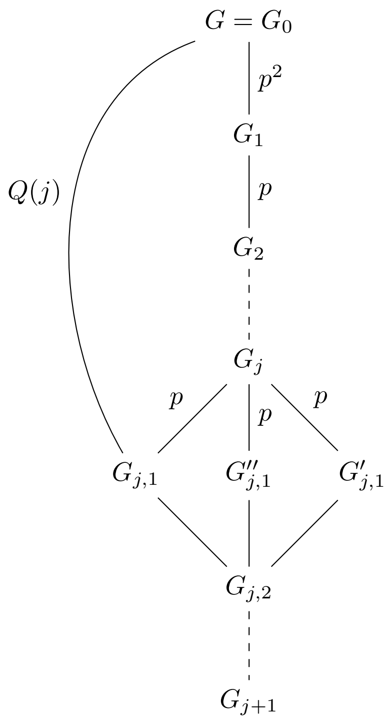

Figure 2: Subgroup lattice of G

Secondly, we consider the case when G has $r = 2$ and is non-quaternion. It suffices to construct a sequence

$$G \supset \Phi(G) = N_0 \supset N_1 \supset \cdots \supset N_m = e,$$

where for every i, $[N_i : N_{i+1}] = 2$, N_i/N_{i+1} is in the center of G/N_{i+1}, and finally G/N_i is non-quaternion. Indeed if we find such a sequence then the proof for $r > 2$ carries over.

We firstly take the lower exponent p central series $G = G_0 \supset \cdots \supset G_j \supset \cdots \supset G_c = 1$ where c is the 2-class of G. By the construction of G_j, the quotient G/G_j has 2-class $c(G/G_j) = j$. By Lemma 4.3, the group $Q(n)$ has no descendants, so G/G_j is non-quaternion for every $j < c$. For $j = c$, $G/G_c = G$ is non-quaternion by assumption. Then we start to refine the exponent p lower central series of G. We denote the dimension of $[G_j : G_{j+1}]$ to be r_j, i.e., $[G_j : G_{j+1}] = 2^{r_j}$. If $r_j > 1$ for certain j, then we have multiple options to choose intermediate subgroups $G_j = G_{j,0} \supset G_{j,1} \supset \cdots G_{j,i} \cdots \supset G_{j,r_j} = G_{j+1}$ for $0 \le i \le r_j$ with $[G_{j,i} : G_{j,i+1}] = 2$. By the proof of Lemma 4.2, an arbitrary choice of refinement $G = N_0 \supset N_1 \supset \cdots \supset N_m = e$ we choose will satisfy that $[N_i : N_{i+1}] = p$ and $N_i/N_{i+1} \subset G/N_{i+1}$.

We will prove that we can refine the lower exponent p central series in a careful way so that none of the quotient is quaternion. Fix j. Firstly, by the standard property of p-class and lower exponent p central series, we have that $c(G/G_{j,i}) = j + 1$ for all $0 < i \le r_j$. If $G/G_{j,i} \simeq Q(s)$ for some s, then $Q(s)$ has 2-class $j+1$. By Lemma 4.3, we must have $s = j$. Again by Lemma 4.3, we get $|Q(j)| = [G : G_{j,i}] = 2^{j+2}$. However since G has generator rank 2 and $[G : G_1] = 2^2$, we must have $[G_m : G_{m+1}] = 2$ for every $1 \le m < j$ and $i = 1$. Since $r_j > 1$, there are at least 3 options in choosing $G_{j,1}$, see Figure 2. Suppose $G/G_{j,1} \simeq Q(j)$, then since $G_j/G_{j,1}$ is central in $G/G_{j,1}$ and by Lemma 4.3 the center of $Q(j)$ is cyclic of order 2, then we can see that $G_j = Q(j)/Z(Q(j))$.

Suppose for two of the choices, we get both quotients $G/G_{j,1} \simeq G/G'_{j,1} \simeq Q(j)$ isomorphic to $Q(j)$. Then by the universal property of fibered product, we get

$$G/G_{j,2} = Q(j) \times_{G_j} Q(j) \simeq Q(j) \times C_2.$$

However $Q(j) \times C_2$ has generator rank 3, and $G/G_{j,2}$ is a quotient of G/G_{j+1}, therefore must have generator rank at most 2. Contradiction. So we prove that at most one of the 3 choices of $G_{j,1}$ satisfies $G/G_{j,1} = Q(j)$, and therefore we can always find a normal subgroup $G_{j,1}$ such that $G/G_{j,1}$ is non-quaternion. □

5 ℓ-torsion in Class Group of Nilpotent Extensions

5.1 Proof of the Main Theorem

In this section, we will prove the following theorems building on results in section 3 and 4.

Theorem 5.1. *Given an arbitrary integer $\ell > 1$ and any number field k, the regular representation of a p-group G is in $\mathcal{G}(\ell)$ if G is non-cyclic and non-quaternion.*

Proof. By Theorem 4.1, for every non-cyclic and non-quaterion p-group G, we can find a decreasing sequence of normal subgroups N_i such that the following is a forcing extension

$$0 \longrightarrow N_i/N_{i+1} \longrightarrow G/N_{i+1} \xrightarrow{\pi_i} G/N_i \longrightarrow 0.$$

for each i, and $G/N_0 = G/\Phi(G) = (\mathbb{Z}/p\mathbb{Z})^r$ is an elementary abelian group with generator rank r.

We will apply induction on i. For $i = 0$, we have $G/N_0 \in \mathcal{G}(\ell)$ by [Wan20]. Suppose that $G/N_i \in \mathcal{G}(\ell)$, then by Extension Lemma 3.7, we have $G/N_{i+1} \in \mathcal{G}(\ell)$ since $(G/N_{i+1}, \pi_i)$ is a forcing extension. □

Remark 5.2. *For cyclic extension and generalized quaternion groups, the method does not apply since we cannot use the group structure to force primes to split. When G is cyclic, we cannot rule out the possibility of small prime ideals being all totally inert. When G is generalized quaternion, say Q_8, we cannot rule out the possibility of small primes ideals being all inert even if they are all non-split in the bi-quadratic quotients. See Section 4.3.1 for corresponding explanation on group theory.*

Theorem 5.3. *Given any integer $\ell > 1$ and any number field k, the regular representation of a nilpotent group G is in $\mathcal{G}(\ell)$ if for every $p||G|$, the Sylow-p subgroup G_p of G is non-cyclic and non-quaternion.*

Proof. It is a standard fact that a nilpotent group G is the direct product of its Sylow-p subgroups G_p, i.e., $G = \prod_{p||G|} G_p$. If for every $p||G|$, the subgroup G_p is non-cyclic and non-quaternion, then by Theorem 5.1, all $G_p \in \mathcal{G}(\ell)$. Using Lemma 3.9 inductively, we get $G \in \mathcal{G}(\ell)$. □

Remark 5.4. *We mention that Theorem 5.1 and 5.3 will also result in corresponding improvements in upper bounds for Malle's conjecture, discriminant multiplicity conjecture and generalized version for these conjectures in [EV06], for implications of these conjectures see [EV06, PTBW19, KW].*

5.2 Discussion on D_4

In [EPW], all number fields with degree less or equal to 5 are shown to have non-trivially bounded ℓ-torsion in class groups on average, with D_4 being the only exceptional case. In [PTBW], the method of using L-functions also does not seem to apply to D_4 quartic extensions since a positive density of D_4 extensions can contain a common subextension. In order to address this issue for D_4 extensions, it is suggested in [PTBW] and proved in [An18], that when one considers the family of D_4-extensions containing a common $C_2 \times C_2$ quotient M, denoted by $\mathcal{F}_M$, the obstacle from the common subfield is avoided. Precisely, the ℓ-torsion in class groups $|\operatorname{Cl}_F[\ell]|$ is non-trivially bounded on average when F is among the family of all D_4-quartic extensions over $\mathbb{Q}$ with a fixed $C_2 \times C_2$ quotient (with a pointed C_2 quotient).

We remark that our result cannot prove that the permutation group $D_4 \subset S_4$ is in $\mathcal{G}(\ell)$ yet, however, the regular representation of D_4, as shown by our proof, is in $\mathcal{G}_k(\ell)$ for every number field k and every integer ℓ.

This gives an improvement on [An18]. Let's denote F to be a D_4 quartic extension. When we impose the condition on $\tilde{F}$ having a fixed $C_2 \times C_2$ quotient M_0 along with a pointed C_2 quotient K_0, there is a fixed quadratic subfield K_0 for all F. Notice that $|\operatorname{Cl}_F[\ell]| = |\operatorname{Cl}_{K_0}[\ell]| \cdot |\operatorname{Cl}_{F/K_0}[\ell]|$ when ℓ is odd and $|\operatorname{Cl}_{F/K_0}[\ell]|^2 = |\operatorname{Cl}_{\tilde{F}/M_0}[\ell]|$. Therefore a non-trivial bound on $\operatorname{Cl}_F[\ell]$ on average within $\mathcal{F}_{M_0}$ is equivalent to a non-trivial bound on $|\operatorname{Cl}_{\tilde{F}}[\ell]| = |\operatorname{Cl}_{M_0}[\ell]| \cdot |\operatorname{Cl}_{\tilde{F}/M_0}[\ell]|$ on average within the family of all D_4 octic extensions $\tilde{F}$ with a fixed $C_2 \times C_2$ quotient M_0. Theorem 5.1 proves that we can actually prove a point-wise non-trivial bound for $\operatorname{Cl}_{\tilde{F}}[\ell]$ for every D_4-octic extensions $\tilde{F}$. This means that we not only drop the "on average" condition, moreover, we drop the condition on containing a fixed $C_2 \times C_2$ quotient.

5.3 On $\delta_k(G, \ell)$

In this section, we give a brief discussion on the amount of power saving $\delta_k(G, \ell)$.

We remark that there are potentially several sources of optimizing the pointwise saving $\delta_k(G, \ell)$. For example in Theorem 5.1, notice that for a p-group G_p, when $p|\ell$, we can always write $\ell = \ell_p \cdot \ell_{(p)}$ where ℓ_p is the maximal p-power divisor of ℓ and $\ell_{(p)}$ is the maximal divisor relatively prime to p. Writing $|\operatorname{Cl}_F[\ell]| = |\operatorname{Cl}_F[\ell_p]| \cdot |\operatorname{Cl}_F[\ell_{(p)}]|$, we can thus use the perfect bound for $\operatorname{Cl}_F[\ell_p]$ and use the method of Theorem 5.1 for the part $\operatorname{Cl}_F[\ell_{(p)}]$. Another source of improving the saving is to construct different forcing sequences for a single p-group.

Although we do not intend to give optimal savings for this work, we will give a quantification on how much saving one can derive away from the trivial bound from this work. Since the expression of $\delta_k(G, \ell)$ in general will be very complicated after applying the induction, we will only give an estimation (actually a lower bound on $\delta_k(G, \ell)$) in the main example: $k = \mathbb{Q}$, G is a p-group with p odd and $\ell \neq p$ is another odd prime.

Example 5.5 ($k = \mathbb{Q}$, $p \neq \ell$ both odd and prime)**.** *Let G be a p-group with order p^n and generator rank r, and $\ell \neq p$ be an odd prime. By [Zam17], we can take $\gamma = 19$ and $\beta = 35$ universally for any k and G in Lemma 3.3. For $G/\Phi(G) = (\mathbb{Z}/p\mathbb{Z})^r$ with $r > 1$, by [Wan20], we know that*

$$\delta_0 = \delta_{\mathbb{Q}}(G/\Phi(G), \ell) = \frac{\Delta(\ell, p)}{p(1+t_0)},$$

where $t_0 = 1/(p-1)\Delta(\ell, p)(1-2/p)$. For each step of induction, by Lemma 3.7, the saving $\delta_{\mathbb{Q}}(G, \ell)$ gets an extra factor η_0. Notice that by taking the forcing sequence for G constructed by

Theorem 4.1, we always have $r = p$ and $m = p$. Therefore we know that

$$\delta_{\mathbb{Q}}(G,\ell) = \delta_0 \cdot \eta_0^{n-r},$$

where $\eta_0 = \frac{1}{p}\frac{\Delta(\ell,p)}{\cdot\Delta(\ell,p)+35} \geq \frac{1}{72p^2\ell}$. *So we have*

$$\delta_{\mathbb{Q}}(G,\ell) \geq \frac{\Delta(\ell,p)}{p} \cdot \frac{1}{9\ell} \cdot \big(\frac{1}{72p^2\ell}\big)^{n-r} \geq \frac{1}{18 \cdot 72^{n-r}} \cdot \frac{1}{p^{2n+2-r}} \cdot \frac{1}{\ell^{n+2-r}}.$$

6 Acknowledgement

The author is partially supported by Foerster-Bernstein Fellowship at Duke University. I would like to dedicate this paper to Prof. Nigel Boston, from whom I learnt a lot on both p-group theory and number theory in my graduate school. I would like to thank Dimitris Koukoulopoulos, Robert J. Lemke Oliver, Jesse Thorner, Melanie Matchett Wood and Asif Zaman for helpful conversations. I would like to thank Jesse Thorner and Asif Zaman for providing helpful references. I would like to thank Frank Thorne, Jesse Thorner and Melanie Matchett Wood for suggestions on an earlier draft.

References

[An18] C. An. ℓ-torsion in class groupf of certain D_4-quartic fields. *arXiv:1808.02148v1*, 2018.

[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, 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.

[Deb17] K. Debaene. Explicit counting of ideals and a Brun-Titchmarsh inequality for the Chebotarev Density Theorem. *arXiv: 1611.10103*, 2017.

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

[EPW] J. Ellenberg, L. B. Pierce, and M. M. Wood. On ℓ-torsion in class groups of number fields. *arXiv: 1606.06103.*

[EV06] J. S. Ellenberg and A. Venkatesh. The number of extensions of a number field with fixed degree and bounded discriminant. *Ann. of Math.*, pages 723–741, 2006.

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

[FS99] E. Friedman and N-P. Skoruppa. Relative regulators of number fields. *Invent. Math.*, 1999.

[FW18a] 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.

[FW18b] Christopher Frei and Martin Widmer. Averages and higher moments for the ℓ-torsion in class groups. *arXiv:1810.04732*, 2018.

[Hal99] M. Hall. *The Theory of Groups.* American Mathematical Soc., 1999.

[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.

[KW] J. Klüners and J. Wang. ℓ-torsion bounds for the class group of number fields with an ℓ-group as Galois group. *arXiv:2003.12161.*

[Lan94] S. Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics.* Springer-Verlag New York, 1994.

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

[Lou00] S. Louboutin. Explicit bounds for residue of Dedekind zeta functions, values of L-Functions at $s = 1$, and relative class numbers. *J. Number Theory*, 85:263–282, 2000.

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

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

[Nov09] H. Nover. Computation of Galois groups of 2-class towers. *University of Wisconsin-Madision thesis*, 2009.

[O'B90] E. A. O'Brien. The p-group generation algorithm. *J. Symbolic Computation*, 9:677–698, 1990.

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

[PTBW] 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.*

[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.

[TZ17] J. Thorner and A. Zaman. An explicit bound for the least prime ideal in the Chebotarev density theorem. *Algebra & Number Theory*, 11(5):1135–1197, 2017.

[TZ18a] 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.

[TZ18b] J. Thorner and A. Zaman. A unified and improved Chebotarev density theorem. *arXiv: 1803.002823*, 2018.

[TZ19] J. Thorner and A. Zaman. A zero density estimate for Dedekind zeta functions. *arXiv:1909.01338v1*, 2019.

[Wan20] J. Wang. Pointwise bound for ℓ-torsion in class groups: Elementary abelian groups. *arXiv:2001.03077*, 2020.

[Wei83] A. Weiss. The least prime ideal. *J. Reine Angew. Math*, 1983.

[Wid17] M. Widmer. Bounds for the ℓ-torsion in class groups. *arXiv:1709.10137*, 2017.

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

[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