A generalized character induction theorem with positivity

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

June 9, 2021

Abstract

Brauer's induction theorem states that any character of a finite group G can be written as a linear combination of induced 1-dim characters from its subgroups. We fully classify all finite groups G where its regular representation character admits such a positive decomposition. As an application, we prove a non-trivial bound on the ℓ-torsion in class groups for any G-extension when Reg_G admits such a positive decomposition. We also discuss its generalization to non-Galois extensions.

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

1 Introduction

Motivation.... my paper on class number/ equality from class numbers and discriminant/

Question... give the exact formulation of in terms of characters/Frobenius reciprocity/mention the definition

History... give different decomposition of character statement

Main theorem... give the list of groups and decomposable groups

Application... gives non-trivial class number bound

2 Notation

3 Notations

Core(G):

========= k: a number field considered as the base field

$|\cdot|$: the absolute norm $\mathrm{Nm}_{k/\mathbb{Q}}$

$\mathrm{Gal}(F/k)$: Galois group of F/k

$\mathrm{Disc}(F/k)$: relative discriminant $|\operatorname{disc}(F/k)|$ of F/k where $\operatorname{disc}(F/k)$ 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 $\mathrm{Cl}_{F/k}[\ell]$, $\mathrm{Cl}_F[\ell]$

M^G: the maximal submodule of the G-module M that is invariant under G

M_G: the maximal quotient module $M/I_G(M)$ of the G-module M that is invariant under G

I_G: the augmentation ideal $\langle \sigma-1 \mid \sigma\in G\rangle \subset R[G]$ in the group ring with coefficient ring R

$\pi(Y;q,a)$: the number of prime numbers p such that $p<Y$ and $p\equiv a \mod q$

$\pi(Y; L/k, \mathcal{C})$: 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 $\mathrm{Gal}(L/k)$
$\pi(Y; L/k, \hat{C})$: the number of unramified prime ideals p in L with $|p| < Y$ and $\mathrm{Frob}_p \notin \mathcal{C}$ where $\mathcal{C}$ is a conjugacy class of $\mathrm{Gal}(L/k)$
$A \asymp B$: 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 $\frac{1}{2\ell(d-1)}$, see Remark 13.4
$\ell_{(p)}$: the maximal factor of ℓ that is relatively prime to a prime number p for an integer $\ell > 1$
$\eta(L/k)$: see (14.1) when $\mathrm{Gal}(L/k) = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ with p odd and see (15.1) when $\mathrm{Gal}(L/k) = (\mathbb{Z}/2\mathbb{Z})^3$
$\eta_0(\ell, p)_k$: a cut-off for $\eta(L/k)$ that is determined in Theorem 14.3 and 14.4 when $\mathrm{Gal}(L/k)$ has rank 2; we will drop k when $k = \mathbb{Q}$
δ: through out the paper we always use δ to denote a power saving from the trivial power $1/2$ in the bound; we use δ_c to denote the power saving when $\eta(L/k)$ is small and δ_{ic} to denote the power saving when $\eta(L/k)$ is big. *Small* and *big* are quantified by comparing to $\eta_0(\ell, p)_k$.

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, 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.

4 Preliminary and Notation

5 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 5.1 (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 5.2. *For any transitive permutation group $G \subset S_n$, the subgroup $H :=$* Stab(1) *has* $\mathrm{Core}(H) = e$. *We will say a permutation group G is* decomposable *if $(G, \mathrm{Stab}(1))$ is decomposable. In particular, the subgroup* 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 5.1 is in Corollary 6.2. Our main goal is to understand the following question and give a complete list of decomposable G and decomposable (G, H).

Question 5.3. *What are all decomposable transitive permutation group $G \subset S_n$?*

5.1 Decomposable Groups

In this section, we first treat the case when H is the trivial subgroup. We first recall the the concept of a partionable group.

Definition 5.4 (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. [**?**]. 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.

Definition 5.5. *For a finite group G and an element $s \neq e \in G$, we define the* root closure of s *to be the smallest subgroup G_s of G containing s such that if $g^k \in G_s$ for some $g \in G$ and some non-zero integer k, then $g \in G_s$.*

One can see that such a group G_s is uniquely determined by s via constructing this subgroup in a canonical way. Indeed, we can start with $H_{0,s} := \langle s \rangle$ and inductively define that

$$H_{i+1,s} := \langle H_{i,s}, H_{i,y} \mid y \in H_{i,s} \rangle.$$

Since G is finite, this construction will always terminates. From the construction it is clearly to be the subgroup G_s.

On the other hand, since G_s is uniquely determined by s, we know if $s \neq t \in G$, then either $G_s = G_t$ or $G_s \cap G_t = e$.

Lemma 5.6. *$H_s = H_t$ or $H_s \cap H_t = e$.*

Theorem 5.7. *A group G is decomposable if and only if G is partionable.*

Proof. Both are equivalent to the statement that $H_s \neq G$. It is clear that H_s forms a partition of G.

□

5.2 Decomposable Pairs

In this section, we will first

5.3 Integral Decomposition

6 Representation Theory

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

Theorem 6.1. *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 $V^G = e$, we have*

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

Proof. For any $\mathbb{Z}_\ell[G]$ module V, we denote $V_k := V \otimes \mathbb{Z}/\ell^k\mathbb{Z}$. By Krull-Schmidt, it suffices to consider indecomposable module V.

Firstly, if $V = V_1$, then for any subgroup $H \subset G$, we denote $d_H := \dim_{\mathbb{F}_\ell}(V^H)$, then we have

$$d_H = \langle \mathrm{Res}^G_H V, 1_H \rangle_H = \langle V, \mathrm{Ind}^G_H 1_H \rangle_G. \tag{6.1}$$

Therefore for the given subgroup H_i and H, we have

$$d_H = \langle V, \mathrm{Ind}^G_H 1_H \rangle_G = \sum_i c_i \langle V, \mathrm{Ind}^G_{H_i} 1_{H_i} \rangle_G = \sum_i c_i d_{H_i}. \tag{6.2}$$

Here we need to use Brauer characters.

Here the second equality follows from the (G, H) being decomposable and $V^G = e$. Therefore we obtain

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

Secondly, if V is a projective $\mathbb{Z}/\ell^k\mathbb{Z}[G]$-module, then equivalently V is projective as a $\mathbb{Z}/\ell^k\mathbb{Z}$-module. We first show that there exists a bijection between $\mathbb{F}_\ell[G]$-module and projective $\mathbb{Z}/\ell^k\mathbb{Z}[G]$-module (using Serre's lifting theorem inductively and vanishing of cohomology for such a lifting.) Then we need to show that V^H is also projective with $\mathrm{rk}(V^H) = \dim(V_1^H)$. Notice that the embedding question restricted to H also has a unique solution, therefore mush coincides with the restriction of the lift of G. Consider V_1^H as an H-module, then there exists a unique projective module V as the extension, which is the module with trivial action. □

Corollary 6.2. *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

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

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

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

where the first equality follows from **[?]** and the second equality follows from Theorem 6.1.

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 **[?]**. □

7 Arithmetic Application

In this section, we will prove, for a decomposable pair (G, H), a non-trivial pointwise bound for the ℓ-torsion in class groups of $G \subset S_n$-extension, where the permutation representation is given by G left multiplication on left cosets of H.

7.1 Preliminaries

Lemma 7.1 (Ellenberg-Venkatesh,[EV07])**.**

Lemma 7.2. *Given a finite group G and $H \subset G$ an arbitrary 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. The lemma follows from the fact that the stabilizer of gH under this action is $H^g = gHg^{-1}$. □

Lemma 7.3 (Maynard-Zaman, [May13, Zam17])**.**

7.2 Main Theorem

Theorem 7.4. *Given a number field k, and a transitive permutation group $G \subset S_n$. If $(G, \mathrm{Stab}(1))$ is decomposable with respect to $\{(H_i, c_i)\}$, then there exists $\delta > 0$ such that for every G-extension L/k,*

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

Proof. Let's denote the number field K_i to be L^{H_i}, and without loss of generality we can assume $\mathrm{Disc}(K_i) \leq \mathrm{Disc}(K_{i+1})$ up to a reordering of H_i. We separate the discussion depending on $\eta := \frac{\ln \mathrm{Disc}(K_1/k)}{\ln \mathrm{Disc}(L/k)}$.

If $\eta > \eta_0$, then we have $\mathrm{Disc}(K_1/k) \geq \mathrm{Disc}(L/k)^{\eta_0}$. Now we consider prime ideals in the range of $Y := \mathrm{Disc}(L/k)^{\eta_0}$. There are $O_\epsilon(\mathrm{Disc}(L)^\epsilon)$ many ramified primes for L. For unramified primes p, if $\mathrm{Frob}_p \in H_i$ (or some conjugates of H_i), then there p will split into a product of prime ideals $\prod_i \mathfrak{p}_i$ in K_i with at least one $\mathfrak{p}_i$ having inertia degree one. Notice that since G is decomposable, then there exists at least one subgroup H_i such that $\mathrm{Frob}_p \in H_i$ (or conjugates of H_i). By a pigeon hole principle, there exists at least one conjugacy class of elements $\mathcal{C} \subset G$ such that

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

therefore at least one subfield K_i such that

$$|\operatorname{Cl}_{K_i}[\ell]| = O_\epsilon(\frac{\mathrm{Disc}(K_i)^{1/2+\epsilon}}{\mathrm{Disc}(L/k)^{\eta_0}}).$$

If $\eta < \eta_0$, then we will apply effective Chebotarev density theorem to $\tilde{K_1}/k$. This subfield has $\mathrm{Gal}(\tilde{K_1}/k) = G/\operatorname{Core}(H_1)$. By Lemma 7.2, there exists $\bar{g} \in G/\operatorname{Core}(H_1)$ such that $\bar{g} \notin H_1^x/\operatorname{Core}(H_1)$ for any $x \in G/\operatorname{Core}(H_1)$. By Chebotarev density theorem, we have

$$\pi(Y; \tilde{K_1}/k, \mathcal{C}(\bar{g})) \gg \frac{Y}{\ln Y} \ldots$$

Then since $\bar{g}$ is not contained in any conjugates of $H_1/\operatorname{Core}(H_1)$, in $\tilde{L}/k$ the Frobenius Frob_p is not contained in any conjugates of H_1, therefore must be contained in H_i for some $i > 1$. □

Example 7.5. *Check the Frobenius group $C_3^r \rtimes C_2$, break the GRH bound pointwisely.*

8 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.

==========

9 Introduction

10 Notations

k: a number field considered as the base field
$|\cdot|$: the absolute norm $\mathrm{Nm}_{k/\mathbb{Q}}$
$\mathrm{Gal}(F/k)$: Galois group of F/k
$\mathrm{Disc}(F/k)$: relative discriminant $|\mathrm{disc}(F/k)|$ 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 $\mathrm{Cl}_{F/k}[\ell]$, $\mathrm{Cl}_F[\ell]$
M^G: the maximal submodule of the G-module M that is invariant under G
M_G: the maximal quotient module $M/I_G(M)$ of the G-module M that is invariant under G
I_G: the augmentation ideal $\langle \sigma-1 \mid \sigma\in G\rangle \subset R[G]$ in the group ring with coefficient ring R
$\pi(Y;q,a)$: the number of prime numbers p such that $p<Y$ and $p\equiv a \mod q$
$\pi(Y;L/k,\mathcal{C})$: 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 $\mathrm{Gal}(L/k)$
$\pi(Y;L/k,\hat{C})$: the number of unramified prime ideals p in L with $|p|<Y$ and $\mathrm{Frob}_p\notin\mathcal{C}$ where $\mathcal{C}$ is a conjugacy class of $\mathrm{Gal}(L/k)$
$A\asymp B$: there exist absolute constants C_1 and C_2 such that $C_1B\le A\le C_2B$
$\Delta(\ell,d)$: a constant number slightly smaller than $\frac{1}{2\ell(d-1)}$, see Remark 13.4
$\ell_{(p)}$: the maximal factor of ℓ that is relatively prime to a prime number p for an integer $\ell>1$
$\eta(L/k)$: see (14.1) when $\mathrm{Gal}(L/k)=\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$ with p odd and see (15.1) when $\mathrm{Gal}(L/k)=(\mathbb{Z}/2\mathbb{Z})^3$
$\eta_0(\ell,p)_k$: a cut-off for $\eta(L/k)$ that is determined in Theorem 14.3 and 14.4 when $\mathrm{Gal}(L/k)$ has rank 2; we will drop k when $k=\mathbb{Q}$
δ: through out the paper we always use δ to denote a power saving from the trivial power $1/2$ in the bound; we use δ_c to denote the power saving when $\eta(L/k)$ is small and δ_{ic} to denote the power saving when $\eta(L/k)$ is big. *Small* and *big* are quantified by comparing to $\eta_0(\ell,p)_k$.

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,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.

11 Algebraic Theory

In this section, firstly we are going to state several standard equalities of class group and discriminants, Lemma 11.1 and 11.3 from algebraic number theory that will be of crucial use for later proof. These results and equalities are known previously, for example see [CM87]. Close results on Brauer-Kuroda relations can also be found in [Smi01]. Here we only include a proof for the convenience of the readers. Secondly, we will give a ramification analysis on A-extensions and prove critical Lemma 11.4 and 11.5 throughout the proof.

11.1 Relative Class Group

In this section, we define the notion of relative class group. The relative class group $\mathrm{Cl}_{F/k} \subset \mathrm{Cl}_F$ is defined to be $\mathrm{Ker}(\mathrm{Nm})$ where $\mathrm{Nm} : \mathrm{Cl}_F \to \mathrm{Cl}_k$ is induced from the usual norm on fractional ideals of F.

Fix an integer $\ell > 1$ that is relatively prime to the degree $[F : k]$, we will show that the following forms a short exact sequence

$$0 \to \mathrm{Cl}_{F/k}[\ell] \to \mathrm{Cl}_F[\ell] \to \mathrm{Cl}_k[\ell] \to 0.$$

Indeed, denote the map $\iota : \mathrm{Cl}_k \to \mathrm{Cl}_F$ which is induced from the usual embedding of fractional ideals. We know that $\mathrm{Nm} \circ \iota : \mathrm{Cl}_k \to \mathrm{Cl}_k$ is equivalent to multiplication by $[F : k]$, which is an isomorphism on the ℓ-torsion part $\mathrm{Cl}_k[\ell]$. Therefore $\mathrm{Nm} : \mathrm{Cl}_F[\ell] \to \mathrm{Cl}_k[\ell]$ is surjective and $\iota : \mathrm{Cl}_k[\ell] \to \mathrm{Cl}_F[\ell]$ is injective and gives a section of the short exact sequence above.

If F/k is Galois with $\mathrm{Gal}(F/k) = G$, then the ℓ-torsion of class group $\mathrm{Cl}_F[\ell]$ can be considered as a Galois module with Galois group G. Since $(|G|, \ell) = 1$, the Tate cohomology $\hat{H}^i(G, \mathrm{Cl}_F[\ell])$ vanishes for every i. It follows from $\hat{H}^0(G, \mathrm{Cl}_F[\ell]) = (\mathrm{Cl}_F[\ell])^G/\iota \circ \mathrm{Nm}(\mathrm{Cl}_F[\ell]) = 0$ that $(\mathrm{Cl}_F[\ell])^G = \iota \circ \mathrm{Nm}(\mathrm{Cl}_F[\ell]) = \iota(\mathrm{Cl}_k[\ell]) \simeq \mathrm{Cl}_k[\ell]$. The last two equalities come from Nm being surjective and ι being injective. Similarly, it follows from $\hat{H}^{-1}(G, \mathrm{Cl}_F[\ell]) = \mathrm{Cl}_{F/k}[\ell]/I_G(\mathrm{Cl}_F[\ell]) = 0$ that $(\mathrm{Cl}_F[\ell])_G = \mathrm{Cl}_F[\ell]/I_G(\mathrm{Cl}_F[\ell]) = \mathrm{Cl}_F[\ell]/\mathrm{Cl}_{F/k}[\ell] \simeq \mathrm{Cl}_k[\ell]$.

11.2 Class Group Decomposition

The main goal of the following lemma is to reduce the questions about elementary abelian extensions to those of their sub-extensions.

Lemma 11.1. *Given an elementary abelian group $A = (\mathbb{Z}/p\mathbb{Z})^r$ with $r > 1$ and an integer $\ell > 1$ with $(\ell, p) = 1$. For any A-extension L/k,*

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

where K_i/k ranges over all subfields of L with $[K_i : k] = p$.

Proof. The class group $\mathrm{Cl}_{L/k}[\ell]$ is naturally an $\mathbb{Z}/\ell\mathbb{Z}[A]$-module since $\mathrm{Gal}(L/k)$ acts on it. For an elementary abelian group A and an integer ℓ with $(|A|, \ell) = 1$, we have that $\mathbb{Z}/\ell\mathbb{Z}[A]$ is semi-simple by Maschke's theorem. We can decompose the augmentation ideal

$$I_A = \oplus_i \epsilon_i I_A,$$

where $\epsilon_i = \frac{1}{|A_i|} \sum_{a \in A_i} a$ and A_i ranges over all index-p subgroup of A. It can be easily shown that $\epsilon_i^2 = \epsilon_i$ and $\epsilon_i \circ \epsilon_j I_A = 0$. Therefore any faithful $\mathbb{Z}/\ell\mathbb{Z}[A]$-module M (meaning M_A is trivial), M can be written as a direct sum

$$M = M \otimes (\mathbb{Z}/\ell\mathbb{Z})[A] = M \otimes I_A \oplus M \otimes (\mathbb{Z}/\ell\mathbb{Z})[A]/I_A = \oplus_i \epsilon_i M \oplus M_A = \oplus_i \epsilon_i M,$$

where the summation is over all index-p subgroups $A_i \subset A$.

By the discussion in section 11.1, the module $M = \mathrm{Cl}_{L/k}[\ell]$ as a submodule of $\mathrm{Cl}_L[\ell]$ is faithful: it can be easily seen by applying $(\cdot)_G$ to the short exact sequence in section 11.1 and noticing $\mathrm{Cl}_F[\ell]_G \simeq \mathrm{Cl}_k[\ell]$. Given ϵ_i corresponding to $A_i \subset A$ and K_i the field fixed by A_i, the sub-module $\epsilon_i M = \mathrm{Nm}_{A_i}(M) = \mathrm{Cl}_{L/k}[\ell]/\mathrm{Cl}_{L/K_i}[\ell]$: it can be seen by the following diagram. Therefore $|\epsilon_i M| = |\mathrm{Cl}_{K_i/k}[\ell]|$.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Cl}_{L/K_i}[\ell] \cap \mathrm{Cl}_{L/k}[\ell] = \mathrm{Cl}_{L/K_i}[\ell] & \longrightarrow & \mathrm{Cl}_{L/k}[\ell] & \longrightarrow & \mathrm{Nm}_{A_i}(\mathrm{Cl}_{L/k}[\ell]) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Cl}_{L/K_i}[\ell] & \longrightarrow & \mathrm{Cl}_{L}[\ell] & \xrightarrow{\mathrm{Nm}_{A_i}} & \mathrm{Cl}_{K_i}[\ell] & \longrightarrow & 0
\end{array}$$

□

Next we apply Lemma 11.1 to degree p^2 subfields of $A = (\mathbb{Z}/p\mathbb{Z})^r$ with $r > 2$. Notice that every K_i are contained in exactly $(p^{r-1}-1)/(p-1)$ subfields M_j with $[M_j : k] = p^2$, so we have the following equality.

Corollary 11.2. *Given an elementary abelian group $A = (\mathbb{Z}/p\mathbb{Z})^r$ with $r > 2$ and an integer $\ell > 1$ with $(\ell, p) = 1$. For any A-extension L/k,*

$$|\operatorname{Cl}_{L/k}[\ell]| = \prod_{M_j/k} |\operatorname{Cl}_{M_j/k}[\ell]|^{(p-1)/(p^{r-1}-1)} = \prod_{F_s/k} |\operatorname{Cl}_{F_s/k}[\ell]|^{(p-1)/(p^{r+1-t}-1)},$$

where M_j/k ranges over all subfields of L with $[M_j : k] = p^2$, and F_s/k ranges over all subfields of L with $[F_s : k] = p^t$.

11.3 Ramification Analysis

The main goal of this section is to give an analysis on the discriminants of all sub-extensions of L/k when $\mathrm{Gal}(L/k) = A$ and A is an elementary abelian group.

Lemma 11.3. *Given an elementary group $A = (\mathbb{Z}/p\mathbb{Z})^r$ with $r > 1$. For any A-extension L/k, we have*

$$\operatorname{Disc}(L/k) = \prod_{K_i/k} \operatorname{Disc}(K_i/k),$$

where K_i/k ranges over all subfield of L with $[K_i : k] = p$.

Proof. Recall that $\operatorname{Disc}(L/k)$ is the Artin-conductor of L/k with the representationρ of A where ρ is the regular representation of A over $\mathbb{C}$. Then $\rho - 1 = \oplus_i \rho_i$ where $\rho_i = (\rho-1)^{A_i} = \rho^{A_i} - 1$ where 1 is denoted to be the trivial representation of A. Therefore notice that the Artin-conductor with trivial character is trivial, we get the Artin conductor $\mathfrak{f}$ associated to ρ is decomposed as:

$$\operatorname{Disc}(L/k) = \mathfrak{f}_{L/k}(\rho) = \prod_{[A:A_i=p]} \mathfrak{f}_{L/k}(\rho^{A_i}) = \prod_{[K_i:k]=p} \mathfrak{f}_{K_i/k}(\rho_i) = \prod_{[K_i:k]=p} \operatorname{Disc}(K_i/k).$$

□

Similarly with Corollary 11.2, we also have

$$\operatorname{Disc}(L/k) = \prod_{M_j/k} \operatorname{Disc}(M_j/k)^{(p-1)/(p^{r-1}-1)} = \prod_{F_s/k} |\operatorname{Disc}(F_s/k)|^{(p-1)/(p^{r+1-t}-1)}, \tag{11.1}$$

where M_j/k ranges over all subfields of L with $[M_j : k] = p^2$ and F_s/k ranges over all subfields of L with $[F_s : k] = p^t$.

Lemma 11.4. *Given an elementary group $A = (\mathbb{Z}/p\mathbb{Z})^2$. For any A-extension L/k, denote K_1 and K_2 to be two arbitrary subfields of L/k with degree p. Given $\eta = \frac{\ln \operatorname{Disc}(K_2/k)}{\ln \operatorname{Disc}(K_1/k)}$. Then we have a lower bound for $\operatorname{Disc}(K_1/k)$ and $\operatorname{Disc}(K_2/k)$ as following*

$$\operatorname{Disc}(K_1/k) \geq \operatorname{Disc}(L/k)^{1/p(\eta+1)}, \qquad \operatorname{Disc}(K_2/k) \geq \operatorname{Disc}(L/k)^{\eta/p(\eta+1)}.$$

Proof. By the conductor discriminant formula, we have that the discriminant of the compositum satisfies the following inequality, see for example [Wan17, Theorem 2.1]

$$\mathrm{Disc}(K_1/k)^p \cdot \mathrm{Disc}(K_2/k)^p \geq \mathrm{Disc}(L/k).$$

By assumption, we have

$$\mathrm{Disc}(K_1/k)^{p(\eta+1)} \geq \mathrm{Disc}(L/k),$$

therefore

$$\mathrm{Disc}(K_1/k) \geq \mathrm{Disc}(L/k)^{1/p(\eta+1)}, \qquad \mathrm{Disc}(K_2/k) \geq \mathrm{Disc}(L/k)^{\eta/p(\eta+1)}.$$

□

A similar proof yields the following lower bound for $A = (\mathbb{Z}/2\mathbb{Z})^3$. We will need to use the following lemma when we discuss the abelian group $A = (\mathbb{Z}/2\mathbb{Z})^3$ in section 15.2 and 15.3.

Lemma 11.5. *Given the elementary abelian group $A = (\mathbb{Z}/2\mathbb{Z})^3$. For any A-extension L/k, denote M/k to be a quartic subfield of L/k and K/k to be a quadratic subfield of L/k that is not a quadratic subfield of M/k. Given $\eta = \frac{\ln \mathrm{Disc}(K/k)}{\ln \mathrm{Disc}(M/k)}$, we have*

$$\mathrm{Disc}(M/k) \geq \mathrm{Disc}(L/k)^{1/(4\eta+2)}, \qquad \mathrm{Disc}(K/k) \geq \mathrm{Disc}(L/k)^{\eta/(4\eta+2)}.$$

12 Analytic Theory

As a preparation for the main proof, we are going to state Brun-Titchmarsh theorem [MV73] and a lower bound theorem in [May13], and generalizations of [May13] to general number fields [Zam17] that we can conveniently use. Results in this direction have also appeared previously in [Wei83, Deb17, TZ17, TZ18]. We apply the following statements in our proofs since the format of the statements is convenient to use in our application.

The main reason that these bounds are good for us is that they hold for $x > f(q)$ where x is the range of consideration, q is the modulus and $f(q)$ is some polynomial in q.

Lemma 12.1 (Brun-Titchmarsh, [MV73])**.** *For $x > q$, we have*

$$\pi(x; q, a) \leq \frac{2}{1 - \ln q/\ln x} \cdot \frac{x}{\phi(q)\ln x}.$$

Lemma 12.2 ([May13],Theorem 3.2)**.** *For $x \geq q^8$, there exists an absolute constant $C > 0$ and an effectively computable constant q_2 such that for $q \geq q_2$, we have*

$$\pi(x; q, a) \geq C\frac{\ln q}{q^{1/2}} \cdot \frac{x}{\phi(q)\ln x}.$$

Lemma 12.3 ([Zam17], Theorem 1.3.1 [TZ18], Theorem 1.2)**.** *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*

$$C_k \frac{1}{\mathrm{Disc}(L/k)^\gamma} \cdot \frac{|\mathcal{C}|}{|G|} \cdot \frac{x}{\ln x} \leq \pi(x; L/k, \mathcal{C}) \leq (2 + O(dx^{-\frac{1}{166d+327}})) \cdot \frac{|\mathcal{C}|}{|G|} \cdot \frac{x}{\ln x}.$$

We will navigate where these theorems are used in this paper. For results over $\mathbb{Q}$, we use Lemma 12.1 in section 14 for all odd degree extensions, in section 15 for all even degree extensions with rank $r > 2$; we use Lemma 12.2 in section 15.3 for $(\mathbb{Z}/2\mathbb{Z})^2$ extensions. For results over general number field k, we did not seek after an optimal bound in this work. For simplicity, we always use the lower bound in Lemma 12.3, see both section 14 and 15. The main reason for doing this is that by using the lower bound, we can write down the power saving away from the trivial bound explicitly in terms of $\beta(k, G)$ and $\gamma(k, G)$. And these numbers are determined explicitly in previous work: for example, in Theorem 1.3.1 in [Zam17], if we only consider the lower bound side, then $\gamma(k, G)$ can be taken to be 19 and $\beta(k, G)$ can be taken to be 35. The upper bound in Lemma 12.3 can also be used to obtain a non-trivial bound for $(\mathbb{Z}/p\mathbb{Z})^r$-extensions over k with $r > 1$, following a similar proof over $\mathbb{Q}$ in Theorem 14.3. However we did not use them in this paper since the saving will depend on the implied constant in the error term $O(dx^{-1/(166d+327)})$.

13 Ellenberg-Venkatesh Revisited

In this section, we will revisit [EV07] and rephrase their critical lemma that we base on. By defining the notion of Δ-good/bad in Definition 13.1, we rephrase this lemma in Lemma 13.5 in the form that we can conveniently use.

Given an element $a \in A$ in an abelian group A (or a conjugacy class $\mathcal{C} \subset G$ for a general finite group G), for a Galois extension L/k, we denote $\pi(Y; L/k, a)$ (or $\pi(Y; L/k, \mathcal{C})$) to be the number of unramified primes ideals p in k with $\mathrm{Frob}_p = a \in A$ (or $\mathrm{Frob}_p \in \mathcal{C} \subset G$). We will always denote $e \in A$ (or $e \in G$) to mean the identity element, and $\mathrm{Frob}_p = e \in A$ (or $\mathrm{Frob}_p = e \in G$) corresponds to p splitting in L/k. We will denote $\pi(Y; L/k, \hat{a})$ to be the number of primes ideals p in k with $\mathrm{Frob}_p \in A \backslash \{a\}$.

We define

$$\mathcal{B}(G, \theta, c) := \Big\{ L/k \mid \mathrm{Gal}(L/k) = G, \pi(\mathrm{Disc}(L/k)^\theta; L/k, e) \leq c \frac{\mathrm{Disc}(L/k)^\theta}{\ln \mathrm{Disc}(L/k)^\theta} \Big\}, \tag{13.1}$$

where $c > 0$ is an absolute small number. In reality, the choice of c will be determined from the proof.

Definition 13.1. *Given $\Delta > 0$, we call an extension L/k* Δ-bad with respect to c *if $L/k \in \mathcal{B}(A, \Delta, c)$ where $A = \mathrm{Gal}(L/k)$. If L/k is not Δ-bad with respect to c, we will say L/k is* Δ-good with respect to c. *When c is clear in the set up, we will simply say* Δ-bad *or* Δ-good.

The following is the critical lemma from [EV07].

Lemma 13.2 ([EV07])**.** *Given a Galois extension L/k and $0 < \theta < \frac{1}{2\ell(d-1)}$, denote*

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

then

$$|\mathrm{Cl}_L[\ell]| = O_{\epsilon,k}\Big(\frac{\mathrm{Disc}(L)^{1/2+\epsilon}}{M}\Big). \tag{13.2}$$

Remark 13.3 (Transition between Absolute/Relative setting)**.** *When $(\ell, [L : k]) = 1$, we have $|\mathrm{Cl}_L[\ell]| = |\mathrm{Cl}_{L/k}[\ell]| \cdot |\mathrm{Cl}_k[\ell]|$. Notice that we always have $\mathrm{Disc}(L) = \mathrm{Disc}(L/k) \cdot \mathrm{Disc}(k)^{[L:k]}$, we can easily adapt the original statement (13.2) to the statement about $\mathrm{Cl}_{L/k}$ and $\mathrm{Disc}(L/k)$:*

$$|\mathrm{Cl}_{L/k}[\ell]| = O_{\epsilon,k}\Big(\frac{\mathrm{Disc}(L/k)^{1/2+\epsilon}}{M}\Big). \tag{13.3}$$

More specifically, fix a number field k, an elementary abelian group A and an integer $\ell > 1$ with $(\ell, |A|) = 1$. Denote $\mathcal{F}$ to be the set of all L/k with $\mathrm{Gal}(L/k) = A$, then

$$\begin{aligned} &\exists \delta > 0, \forall L/k \in \mathcal{F}, \quad |\mathrm{Cl}_{L/k}[\ell]| = O_{k,\epsilon}(\mathrm{Disc}(L/k)^{1/2-\delta+\epsilon}) \iff \\ &\exists \delta > 0, \forall L/k \in \mathcal{F}, \qquad |\mathrm{Cl}_{L}[\ell]| = O_{k,\epsilon}(\mathrm{Disc}(L)^{1/2-\delta+\epsilon}). \end{aligned} \tag{13.4}$$

Since the two statements are equivalent, we will focus on bounding $\mathrm{Cl}_{L/k}[\ell]$ by $\mathrm{Disc}(L/k)$ for the whole paper.

Remark 13.4. *In most situations in this paper, the parameter Δ in Definition 13.1 will be taken to be $\Delta < \frac{1}{2\ell(d-1)}$ where $d = [L : k]$. We will denote $\Delta(\ell, d)$ for such a number that is very close to $\frac{1}{2\ell(d-1)}$ for simplicity.*

Then in our language, we will use the following format of this critical lemma throughout the proof of the theorems in section 14 and 15:

Lemma 13.5 ([EV07])**.** *Given a Galois extension L/k, an integer $\ell > 1$ with $(\ell, [L : k]) = 1$, $0 < \theta < \frac{1}{2\ell(d-1)}$. If L/k is θ-good with respect to c, then*

$$|\mathrm{Cl}_{L/k}[\ell]| = O_{\epsilon,k,c}(\mathrm{Disc}(L/k)^{1/2-\theta+\epsilon}).$$

14 Odd p

In this section, we work with the elementary abelian groups $A = (\mathbb{Z}/p\mathbb{Z})^r$ with p odd and $r > 1$. Firstly, in section 14.1, section 14.2 and section 14.3, we will focus on the case $r = 2$. In section 14.4, we will apply the result we obtained for $r = 2$ to obtain results for every $r > 2$.

We introduce the notation for section 14. For $A = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, there are $p + 1$ non-trivial subgroups $A_i \simeq \mathbb{Z}/p\mathbb{Z}$ with $A/A_i \simeq \mathbb{Z}/p\mathbb{Z}$ for $i = 1, \cdots, p + 1$. Therefore given an arbitrary A-extension L/k, there are $p + 1$ non-trivial sub-extensions K_i/k. For simplicity of our discussion, we will order K_i by $\mathrm{Disc}(K_i/k)$, i.e., we order them so that

$$\mathrm{Disc}(K_i/k) \leq \mathrm{Disc}(K_j/k) \text{ iff } i \leq j.$$

We will separate the discussion depending on the size of

$$\eta = \eta(L/k) := \frac{\ln \mathrm{Disc}(K_2/k)}{\ln \mathrm{Disc}(K_1/k)} \geq 1. \tag{14.1}$$

We will say L/k is *comparable* if η is small, and *incomparable* if η is big. We give the proof for the two cases in section 14.1 and 14.2 respectively with two different strategies. The cut-off for the two cases is denoted $\eta_0 = \eta_0(\ell, p)_k$, which is determined in section 14.2 (see Theorem 14.3, 14.4 and Remark 14.7):

$$\eta_0(\ell, p)_k = \begin{cases} ((p-1) \cdot \Delta(\ell, p) \cdot (1 - 2/p))^{-1} & \text{if } k = \mathbb{Q}; \\ \max\{\beta(k, \mathbb{Z}/p\mathbb{Z}), \gamma(k, \mathbb{Z}/p\mathbb{Z}) + \Delta(\ell, p)\}/\Delta(\ell, p) & \text{if } k \neq \mathbb{Q}. \end{cases} \tag{14.2}$$

The power saving δ_c in section 14.1 stands for **c**omparable case and δ_{ic} in section 14.2 stands for **in**comparable case.

In cases where all parameters ℓ, k and p are clear, we will write η_0 instead of $\eta_0(\ell, p)_k$ for simplicity. In cases where $k = \mathbb{Q}$, we will drop k in the notation for simplicity, i.e., we will write $\eta_0(\ell, p)$ instead of $\eta_0(\ell, p)_{\mathbb{Q}}$.

14.1 Comparable Size

In this section, we will consider L/k with small η. The approach used in this section will be universally true for any bounded range of η. For example, we will state the theorem with $\eta \le \eta_0 \cdot (1+\epsilon_0) = \eta_0(\ell,p)_k \cdot (1+\epsilon_0)$ where $\epsilon_0 > 0$ is a small number, and $\eta_0(\ell,p)_k$ is listed in (14.2). We will use this strategy especially when η is small. When η is big, we refer to section 14.2. Here the introduction of ϵ_0 is only a technical treatment in order to simplify the dependence on c, the constant defined in Definition 13.1.

Theorem 14.1. *Given $A = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, an integer $\ell > 1$ with $(\ell,p) = 1$ and a number field k. For any A-extension L/k with $\eta = \eta(L/k) \le \eta_0 \cdot (1+\epsilon_0) = \eta_0(\ell,p)_k \cdot (1+\epsilon_0)$, we have the pointwise bound*

$$|\operatorname{Cl}_{L/k}[\ell]| = O_{\epsilon,k,\epsilon_0}(\operatorname{Disc}(L/k)^{1/2-\delta+\epsilon}).$$

where

$$\delta = \delta_c(\eta,\ell,p) = \frac{\Delta(\ell,p)}{p(\eta+1)},$$

and $\eta = \eta(L/k) = \frac{\ln \operatorname{Disc}(K_2/k)}{\ln \operatorname{Disc}(K_1/k)}$.

Proof. We separate the discussion when K_1/k is $\Delta(\ell,p)$-bad or good with respect to c where c is a fixed absolute number satisfying $c < \frac{1}{p+1}$. The constant c will be fixed once and for all in the proof of the current theorem. By Lemma 11.4, we get

$$\operatorname{Disc}(K_1/k) \ge \operatorname{Disc}(L/k)^{1/p(\eta+1)} \ge \operatorname{Disc}(L/k)^{1/p(\eta_0(1+\epsilon_0)+1)}.$$

Note that a fixed integer $L_0 > 0$, there are only finitely many A-extensions L/k where $\operatorname{Disc}(L/k) \le L_0$, thus only finitely many L/k with $\operatorname{Disc}(K_1/k) \le K_0 = L_0^{1/p(\eta_0(1+\epsilon_0)+1)}$ and $\eta(L/k) \le \eta_0(1+\epsilon_0)$. So we can assume both L/k and K_1/k are sufficiently large.

If K_1/k is $\Delta(\ell,p)$-bad, then we are going to show that at least one of K_i/k is θ_i-good where

$$\theta_i := \Delta(\ell,p)\frac{\ln \operatorname{Disc}(K_1/k)}{\ln \operatorname{Disc}(K_i/k)} < \Delta(\ell,p),$$

for $2 \le i \le p+1$. Equivalently, we define θ_i so that $\operatorname{Disc}(K_1)^{\Delta(\ell,p)} = \operatorname{Disc}(K_i)^{\theta_i}$. Consider all primes p in k with $|p| < Y$ where $Y = \operatorname{Disc}(K_1/k)^{\Delta(\ell,p)}$. Since K_1/k is $\Delta(\ell,p)$-bad, there are at most $cY/\ln Y$ primes in k splitting in K_1/k. The number of primes in k that are ramified in L/k is bounded by

$$O_{\epsilon,k}(\operatorname{Disc}(L/k)^{\epsilon}) \le O_{\epsilon,k,\epsilon_0}(Y^{\epsilon}),$$

since $Y \ge \operatorname{Disc}(L/k)^{\Delta(\ell,p)/p(\eta_0(1+\epsilon_0)+1)}$. Therefore when L/k is sufficiently large,

$$\pi(Y;K_1/k,\hat{e}) = \pi(Y) - \pi(Y;K_1/k,e) - O_{\epsilon,k,\epsilon_0}(Y^{\epsilon}) \ge (1-c-\epsilon)\cdot\frac{Y}{\ln Y}, \tag{14.3}$$

where the last inequality holds whenever $Y \ge Y_0 = Y_0(\epsilon,\epsilon_0)$ with Y_0 depending at most on ϵ and ϵ_0. Since the decomposition group of A at an unramified prime is cyclic, a prime p in k that is inert in K_1/k and must be split in some K_i for $2 \le i \le p+1$. By pigeon hole principle, there exists at least one K_i/k satisfying

$$\pi(Y;K_i/k,e) \ge \frac{1-c-\epsilon}{p}\cdot\frac{Y}{\ln Y} \ge c\frac{Y}{\ln Y},$$

then K_i/k is θ_i-good. Let's say K_j/k with $j > 1$ is θ_j-good, then by Lemma 13.5, we get

$$|\operatorname{Cl}_{K_j/k}[\ell]| = O_{\epsilon,k}(\operatorname{Disc}(K_j/k)^{1/2-\theta_j+\epsilon}),$$

where we drop the dependence on c since we fix the absolute number $c < \frac{1}{p+1}$ from the beginning. Therefore by Lemma 11.1 and 11.3 and 11.4, when $\mathrm{Disc}(L/k) \geq L_0(\epsilon, \epsilon_0) = Y_0(\epsilon, \epsilon_0)^{p(\eta_0(1+\epsilon_0)+1)/\Delta(\ell,p)}$, we get

$$\begin{aligned} |\operatorname{Cl}_{L/k}[\ell]| =& \prod_i |\operatorname{Cl}_{K_i/k}[\ell]| = O_{\epsilon,k}(\mathrm{Disc}(K_j/k)^{1/2-\theta_i+\epsilon}) \prod_{i\neq j} \mathrm{Disc}(K_i/k)^{1/2+\epsilon} \\ =& O_{\epsilon,k}\Big(\frac{\mathrm{Disc}(L/k)^{1/2+\epsilon}}{\mathrm{Disc}(K_j/k)^{\theta_i}}\Big) = O_{\epsilon,k}(\mathrm{Disc}(L/k)^{1/2-\Delta(\ell,p)/p(\eta+1)+\epsilon}). \end{aligned} \tag{14.4}$$

If K_1 is $\Delta(\ell,p)$-good, then we get from Lemma 13.5 that

$$|\operatorname{Cl}_{K_1/k}[\ell]| = O_{\epsilon,k}(\mathrm{Disc}(K_1/k)^{1/2-\Delta(\ell,p)+\epsilon}).$$

Then similarly, by Lemma 11.1 and 11.3 and 11.4, we get

$$\begin{aligned} |\operatorname{Cl}_{L/k}[\ell]| =& \prod_i |\operatorname{Cl}_{K_i/k}[\ell]| = O_{\epsilon,k}\Big(\mathrm{Disc}(K_1/k)^{1/2-\Delta(\ell,p)+\epsilon}\Big) \prod_{i\neq 1} \mathrm{Disc}(K_i/k)^{1/2+\epsilon} \\ =& O_{\epsilon,k}\Big(\frac{\mathrm{Disc}(L/k)^{1/2+\epsilon}}{\mathrm{Disc}(K_1/k)^{\Delta(\ell,p)}}\Big) = O_{\epsilon,k}(\mathrm{Disc}(L/k)^{1/2-\Delta(\ell,p)/p(\eta+1)+\epsilon}). \end{aligned} \tag{14.5}$$

Since we assume L/k sufficiently large for later discussion, i.e., $\mathrm{Disc}(L/k) \geq L_0(\epsilon, \epsilon_0)$, in summary, we show that for any A-extension L/k

$$|\operatorname{Cl}_{L/k}[\ell]| = O_{\epsilon,k,\epsilon_0}(\mathrm{Disc}(L/k)^{1/2-\delta+\epsilon}),$$

with $\delta = \delta_c(\eta,\ell,p) = \frac{\Delta(\ell,p)}{p(\eta+1)}$. □

This gives a power saving on the pointwise bound of $\operatorname{Cl}_{L/k}[\ell]$ in terms of $\eta(L/k)$.

Remark 14.2. *Notice that here in Theorem 14.1 we only take the bound $\eta_0(\ell,p)_k \cdot (1+\epsilon_0)$ for η for simplicity. The same non-trivial saving $\delta = \delta_c(\eta,\ell,p)$ can be obtained with $\eta \leq M$ for arbitrary number M. In this scenario, the implied constant depends on M instead of ϵ_0.*

14.2 Incomparable Size

In this section, we will give another strategy when η is very large, equivalently when K_2 is much larger than K_1. We will also see the cut-off $\eta_0(\ell,p)_k$ from the following theorem. We will first prove the result over $\mathbb{Q}$ in Theorem 14.3 and then prove the result over a general number field k in Theorem 14.4.

Theorem 14.3. *Given $A = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ with odd p, an integer $\ell > 1$ with $(\ell,p) = 1$. Denote $\eta_0 = \eta_0(\ell,p) = ((p-1)\cdot\Delta(\ell,p)\cdot(1-2/p))^{-1}$. For any A-extension $L/\mathbb{Q}$ with $\eta = \eta(L/\mathbb{Q}) > \eta_0(1+\epsilon_0)$, we have the pointwise bound*

$$|\operatorname{Cl}_L[\ell]| = O_{\epsilon,\epsilon_0}(\mathrm{Disc}(L)^{1/2-\delta+\epsilon})$$

for some

$$\delta = \delta_{ic}(\eta,\ell,p) = \frac{\Delta(\ell,p)\eta}{p(\eta+1)}$$

where $\eta = \frac{\ln \mathrm{Disc}(K_2)}{\ln \mathrm{Disc}(K_1)}$.

Proof. By Lemma 11.4, we have $\mathrm{Disc}(K_2) \geq \mathrm{Disc}(L)^{\eta/p(\eta+1)} \geq \mathrm{Disc}(L)^{\eta_0(1+\epsilon_0)/p(\eta_0(1+\epsilon_0)+1)}$. Note that for a fixed integer $L_0 > 0$, there are only finitely many L with $\mathrm{Disc}(L) \leq L_0$, thus only finitely many L with $\mathrm{Disc}(K_2) \leq K_0 = L_0^{\eta_0(1+\epsilon_0)/p(\eta_0(1+\epsilon_0)+1)}$ and $\eta > \eta_0(1+\epsilon_0)$. So we can assume that both L and K_2 are sufficiently large.

We will show that at least one of K_i for $2 \leq i \leq p+1$ is θ_i-good for some $\theta_i > 0$ with respect to c where c is a fixed small number satisfying $c < \frac{(p-2)\epsilon_0}{2+p\epsilon_0}$. The constant $c = c(\epsilon_0)$ will be fixed once and for all for the current theorem.

If $\eta(L/\mathbb{Q}) > \eta_0(1+\epsilon_0)$, then we can apply Lemma 12.1 with

$$x = \mathrm{Disc}(K_2)^{\Delta(\ell,p)}, \qquad q = \mathrm{Cond}(K_1) \asymp \mathrm{Disc}(K_1)^{1/(p-1)},$$

to count the number of primes in $\mathbb{Q}$ splitting in $K_1/\mathbb{Q}$. By class field theory, this is equivalent to taking $\frac{\phi(q)}{p}$ residue classes $a \mod q$ and then adding up $\pi(x;q,a)$ over a. Therefore we have positive density of primes up to x in $\mathbb{Q}$ that are inert in $K_1/\mathbb{Q}$,

$$\begin{aligned}\pi(x;K_1/\mathbb{Q},\hat{e}) &= \pi(x) - \pi(x;K_1/\mathbb{Q},e) - O_\epsilon(\mathrm{Disc}(L)^\epsilon)\\ &\geq \pi(x) - \frac{2}{1-1/\Delta(\ell,p)(p-1)\eta}\cdot\frac{x}{p\ln x} - O_{\epsilon,\epsilon_0}(x^\epsilon),\\ &\geq C\frac{x}{\ln x}.\end{aligned} \tag{14.6}$$

The first inequality comes from Lemma 12.1 and $\mathrm{Disc}(K_2) \geq \mathrm{Disc}(L)^{\eta_0(1+\epsilon_0)/p(\eta_0(1+\epsilon_0)+1)}$. The second inequality holds when we take $C = 1 - \frac{2}{p}\frac{1}{1-1/\Delta(\ell,p)(p-1)\eta_0(1+\epsilon_0)} - \epsilon$ and $x \geq x_0 = x_0(\epsilon)$ with x_0 depending at most on ϵ. Primes that are inert in K_1 must be split in K_i for some $i > 1$. Therefore by pigeon hole principle, there exists at least one K_j for $2 \leq j \leq p+1$ satisfying

$$\pi(x;K_j,e) \geq \frac{C}{p}\cdot\frac{x}{\ln x} \geq c\frac{x}{\ln x}, \tag{14.7}$$

where the last inequality comes from the assumption $c < \frac{(p-2)\epsilon_0}{2+\epsilon_0}$. This K_j is θ_j-good for

$$\theta_j := \Delta(\ell,p)\cdot\frac{\ln\mathrm{Disc}(K_2)}{\ln\mathrm{Disc}(K_j)} \leq \Delta(\ell,p). \tag{14.8}$$

Then by Lemma 13.5, we get

$$|\mathrm{Cl}_{K_j}[\ell]| = O_{\epsilon,c}(\mathrm{Disc}(K_j)^{1/2-\theta_j+\epsilon}) = O_{\epsilon,\epsilon_0}(\mathrm{Disc}(K_j)^{1/2-\theta_j+\epsilon}),$$

since our constant c is a small number depending at most on ϵ_0. By Lemma 11.3 and 11.1 and 11.4, we have for every L that

$$|\mathrm{Cl}_L[\ell]| = O_{\epsilon,\epsilon_0}(\mathrm{Disc}(L)^{1/2-\Delta(\ell,p)\eta/p(\eta+1)+\epsilon}). \tag{14.9}$$

So we prove this theorem with

$$\delta_{ic}(\eta,\ell,p) = \frac{\Delta(\ell,p)\eta}{p(\eta+1)}.$$

□

Then we give the version over a general number field. The only distinction is that we will apply Lemma 12.3 instead of Lemma 12.1.

Theorem 14.4. *Given $A = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, an integer $\ell > 1$ with $(\ell, p) = 1$. Denote $\eta_0 = \eta_0(\ell,p)_k = \max\{\beta, \gamma + \Delta(\ell,p)\}/\Delta(\ell,p)$ where $\beta = \beta(k, \mathbb{Z}/p\mathbb{Z})$ and $\gamma = \gamma(k, \mathbb{Z}/p\mathbb{Z})$. For any A-extension L/k with $\eta(L/k) > \eta_0$, we have the pointwise bound*

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

where

$$\delta = \delta_{ic,k}(\eta, \ell, p) = \frac{(\Delta(\ell,p) - \gamma/\eta)\eta}{p(\eta+1)}.$$

Proof. Notice that by Lemma 11.4, we have

$$\operatorname{Disc}(K_2/k) \geq \operatorname{Disc}(L/k)^{\eta/p(\eta+1)} \geq \operatorname{Disc}(L/k)^{\eta_0/p(\eta_0+1)}.$$

Note that for a fixed integer $L_0 > 0$, there are only finitely many L/k with $\operatorname{Disc}(L/k) \leq L_0$, thus only finitely many L/k with $\operatorname{Disc}(K_2/k) \leq K_0 = L_0^{\eta_0/p(\eta_0+1)}$ and $\eta > \eta_0$. So we can assume that both K_2/k and L/k are sufficient large.

Firstly, we will show that there exist a lot of primes inert in K_1/k with the range of consideration $x = \operatorname{Disc}(K_2/k)^{\Delta(\ell,p)}$ when L/k is sufficiently large. We will apply Lemma 12.3 to K_1/k with $x = \operatorname{Disc}(K_2/k)^{\Delta(\ell,p)}$. Recall the absolute constant $D_0 = D_0(k)$ depending at most on k in Lemma 12.3.

If $\operatorname{Disc}(K_1/k) < D_0$, then it follows from the standard Chebotarev density theorem that for $C' = \frac{p-1}{p} - \epsilon$, we have

$$\pi(x; K_1/k, \hat{e}) \geq C' \frac{x}{\ln x} = \frac{C'}{\Delta(\ell,p)} \cdot \frac{\operatorname{Disc}(K_2/k)^{\Delta(\ell,p)}}{\ln \operatorname{Disc}(K_2/k)},$$

when x is sufficiently large comparing to D_0, say $x \geq x_0 = x_0(D_0, \epsilon) = x_0(k, \epsilon)$ where x_0 depends at most on D_0 and ϵ, thus depends at most on k and ϵ. If we take $K_0^{\Delta(\ell,p)} = x_0(k,\epsilon)$, then when $\operatorname{Disc}(L/k) \geq L_0(k,\epsilon) = K_0(k,\epsilon)^{p(\eta_0+1)/\eta_0}$ is sufficiently large, we know that if $\operatorname{Disc}(K_1/k) < D_0$ then $\pi(x; K_1/k, \hat{e}) \geq \frac{C'}{\Delta(\ell,p)} \cdot \frac{\operatorname{Disc}(K_2/k)^{\Delta(\ell,p)}}{\ln \operatorname{Disc}(K_2/k)}$.

If $\operatorname{Disc}(K_1/k) \geq D_0(k)$, then we apply Lemma 12.3. When $\eta > \eta_0$, we have $\operatorname{Disc}(K_2/k)^{\Delta(\ell,p)} \geq \max\{\operatorname{Disc}(K_1/k)^{\beta}, \operatorname{Disc}(K_1/k)^{\gamma}\}$ for $\beta = \beta(k, \mathbb{Z}/p\mathbb{Z})$ and $\gamma = \gamma(k, \mathbb{Z}/p\mathbb{Z})$ in Lemma 12.3. By Lemma 12.3 there exists some $C_k > 0$ such that

$$\pi(x; K_1/k, \hat{e}) \geq C_k \frac{1}{\operatorname{Disc}(K_1/k)^{\gamma}} \cdot \frac{x}{\ln x} \geq \frac{C_k}{\Delta(\ell,p)} \cdot \frac{\operatorname{Disc}(K_2/k)^{\Delta(\ell,p)-\gamma/\eta}}{\ln \operatorname{Disc}(K_2/k)}, \tag{14.10}$$

where C_k is some constant only depending on k. So in summary, as L/k is sufficiently large (i.e., $\operatorname{Disc}(L/k) \geq L_0(k,\epsilon) = K_0(k,\epsilon)^{p(\eta_0+1)/\eta_0}$), we show

$$\pi(x; K_1/k, \hat{e}) \geq \frac{C_k''}{\Delta(\ell,p)} \cdot \frac{\operatorname{Disc}(K_2/k)^{\Delta(\ell,p)-\gamma/\eta}}{\ln \operatorname{Disc}(K_2/k)},$$

where $C_k'' = \min\{C', C_k'\}$ depends only on k.

By pigeon hole principle, there exists at least one K_j/k for $2 \leq j \leq p+1$ where

$$\pi(x; K_j/k, e) \geq \frac{C_k''}{p\Delta(\ell,p)} \cdot \frac{\operatorname{Disc}(K_2/k)^{\Delta(\ell,p)-\gamma/\eta}}{\ln \operatorname{Disc}(K_2/k)}. \tag{14.11}$$

Finally by Lemma 13.5 and Lemma 11.4, we have for any L/k that

$$|\operatorname{Cl}_{L/k}[\ell]| \leq O_{\epsilon,k}(\operatorname{Disc}(L/k)^{1/2-\delta+\epsilon}), \tag{14.12}$$

where

$$\delta = \delta_{ic,k}(\eta, \ell, p) = \frac{(\Delta(\ell,p) - \gamma/\eta)\eta}{p(\eta+1)}.$$

□

Remark 14.5. *Here when $k = \mathbb{Q}$ and $p = 2$, we can apply Lemma 12.2 as a sub-case of Lemma 12.3 with $\gamma(\mathbb{Q}, \mathbb{Z}/2\mathbb{Z}) = 1/2 - \epsilon$, $\beta(\mathbb{Q}, \mathbb{Z}/2\mathbb{Z}) = 8$ and $D_0 = q_2$.*

14.3 Savings for Odd A with Rank 2

So combining Theorem 14.1 and 14.3 and (13.4) in Remark 13.3, we get the following theorem.

Theorem 14.6 (Odd Exponent, Rank 2, Over $\mathbb{Q}$)**.** *Given $A = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ with odd p and an integer $\ell > 1$ with $(\ell, p) = 1$. For any A-extension $L/\mathbb{Q}$, we have*

$$|\operatorname{Cl}_L[\ell]| = O_\epsilon(\operatorname{Disc}(L)^{1/2-\delta(\ell,p)+\epsilon}),$$

with

$$\delta(\ell,p) = \delta_c(\eta_0, \ell, p) = \frac{\Delta(\ell,p)}{p(1+\eta_0)},$$

where $\eta_0 = \frac{1}{(p-1)\Delta(\ell,p)(1-2/p)}$.

Proof. Combining Theorem 14.1 and Theorem 14.3, for every fixed small ϵ_0, we show that for every A-extension $L/\mathbb{Q}$

$$|\operatorname{Cl}_L[\ell]| = O_\epsilon(\operatorname{Disc}(L)^{1/2-\delta(\ell,p,\epsilon_0)+\epsilon}),$$

where $\delta(\ell, p, \epsilon_0) = \delta_c(\eta_0(1+\epsilon_0), \ell, p) = \frac{\Delta(\ell,p)}{p(1+\eta_0(1+\epsilon_0))}$. Since we can take arbitrarily small ϵ_0 and we also state the theorem with arbitrarily small ϵ, we can get

$$|\operatorname{Cl}_L[\ell]| = O_\epsilon(\operatorname{Disc}(L)^{1/2-\delta(\ell,p)+\epsilon}),$$

for $\delta(\ell,p) = \delta_c(\eta_0, \ell, p)$. □

For general number field k, similarly notice that since $\delta_{ic,k}(\eta, \ell, p)$ always increases as η increases and $\delta_c(\eta, \ell, p)$ always decreases as η increases. By comparing $\delta_c(\eta_0, \ell, p)$ and $\delta_{ic,k}(\eta_0, \ell, p)$ at $\eta_0 = \eta_0(\ell,p)_k = \max\{\beta(k, \mathbb{Z}/p\mathbb{Z}), \gamma(k, \mathbb{Z}/p\mathbb{Z}) + \Delta(\ell,p)\}/\Delta(\ell,p)$, we see that the smallest saving always happens at $\delta_c(\eta_0, \ell, p)_k$. So we are guaranteed to find the universal saving $\delta > 0$ for all ranges of η at the cut-off η_0.

Remark 14.7. *In the proof of Theorem 14.4, we can see that it suffices to take $\eta_0(\ell,p)_k$ to be $\max\{\beta(k, \mathbb{Z}/p\mathbb{Z}), \gamma(k, \mathbb{Z}/p\mathbb{Z})\}/\Delta(\ell,p)$. The reason that instead we take*

$$\eta_0(\ell,p)_k = \max\{\beta(k, \mathbb{Z}/p\mathbb{Z}), \gamma(k, \mathbb{Z}/p\mathbb{Z}) + \Delta(\ell,p)\}/\Delta(\ell,p),$$

is that it guarantees $\delta_{ic,k}(\eta_0, \ell, p) > \delta_c(\eta_0, \ell, p)$ and simplifies the final expression of the saving. However, notice that usually β is larger than γ in reality, see [Zam17] for example, so in such situations it will not change the actual value of $\eta_0(\ell,p)_k$ after plugging in β and γ.

Theorem 14.8 (Odd Exponent, Rank 2, Over k)**.** *Given $A = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ with odd p and an integer $\ell > 1$ with $(\ell, p) = 1$. For any A-extension L/k, we have*

$$|\operatorname{Cl}_L[\ell]| = O_{\epsilon,k}(\operatorname{Disc}(L)^{1/2-\delta_k(\ell,p)+\epsilon}),$$

where $\delta_k(\ell,p) = \delta_c(\eta_0, \ell, p) = \frac{\Delta(\ell,p)}{p(1+\eta_0)}$ and $\eta_0 = \eta_0(\ell,p)_k = \max\{\beta(k, \mathbb{Z}/p\mathbb{Z}), \gamma(k, \mathbb{Z}/p\mathbb{Z}) + \Delta(\ell,p)\}/\Delta(\ell,p)$.

14.4 Induction

In this section, we will derive the ℓ-torsion bound for every $A = (\mathbb{Z}/p\mathbb{Z})^r$ when $r > 2$ from the case $A = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Theorem 14.9 (Odd Exponent, Over k)**.** *Given $A = (\mathbb{Z}/p\mathbb{Z})^r$ with $r \geq 2$ and p odd. Given an arbitrary integer $\ell = \ell_{(p)} \cdot \ell_p$ where $\ell_{(p)}$ is the maximal factor of ℓ relatively prime to p. For any A-extension L/k, we have*

$$|\operatorname{Cl}_L[\ell]| = O_{k,\epsilon}(\operatorname{Disc}(L)^{1/2-\delta_k(\ell_{(p)},p)+\epsilon}),$$

where $\delta_{\mathbb{Q}}(\ell, p) = \delta(\ell, p)$ in Theorem 14.6 when $k = \mathbb{Q}$, and $\delta_k(\ell, p)$ in Theorem 14.8 for general k.

Proof. Firstly we assume $(\ell, p) = 1$. The result for $r = 2$ and (ℓ, p) is stated in Theorem 14.6 and 14.8. For $r > 2$ and $(\ell, p) = 1$, notice that

$$\begin{aligned}|\operatorname{Cl}_{L/k}[\ell]| = \prod_i |\operatorname{Cl}_{K_i/k}[\ell]| = \Big(\prod_j |\operatorname{Cl}_{M_j/k}[\ell]|\Big)^{1/(p+1)} = O_{\epsilon,k}\Big(\prod_j \operatorname{Disc}(M_j/k)^{1/2-\delta(\ell,p)+\epsilon}\Big)^{1/(p+1)} \\ = O_{\epsilon,k}\Big(\prod_j \operatorname{Disc}(M_j/k)^{1/(p+1)}\Big)^{1/2-\delta(\ell,p)+\epsilon} = O_{\epsilon,k}(\operatorname{Disc}(L/k)^{1/2-\delta(\ell,p)+\epsilon}).\end{aligned} \tag{14.13}$$

where K_i ranges over all degree p sub-extensions in L over $\mathbb{Q}$ and M_j ranges over all degree p^2 sub-extensions in L over $\mathbb{Q}$. The first equality comes from Lemma 11.1. The second equality comes from Corollary 11.2. The first inequality comes from Theorem 14.6. The last equality comes from (11.1). Finally it follows from (13.4) in Remark 13.3.

For general $\ell = \ell_{(p)}\ell_p$, notice that $|\operatorname{Cl}_L[\ell]| = |\operatorname{Cl}_L[\ell_{(p)}]| \cdot |\operatorname{Cl}_L[\ell_p]|$ and $|\operatorname{Cl}_L[\ell_p]| = O_\epsilon(\operatorname{Disc}(L)^\epsilon)$, we get $|\operatorname{Cl}_L[\ell]| = O_{k,\epsilon}(\operatorname{Disc}(L)^{1/2-\delta_k(\ell_{(p)},p)+\epsilon})$. □

Remark 14.10 (Odd Exponent, $\ell = 2$, Over k)**.** *When $\ell = 2$, we can obtain better results because of the pointwise result on 2-torsion from [BST+17]. It is proved that $|\operatorname{Cl}_F[2]| \leq O(\operatorname{Disc}(F)^{1/2-1/2d+\epsilon})$ where $d = [F : \mathbb{Q}]$ by [BST+17]. By (13.4) in Remark13.3, we get for K with $\operatorname{Gal}(K/k) = \mathbb{Z}/p\mathbb{Z}$, the 2-torsion is bounded*

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

Then the statement follows from a straight forward use of Lemma 11.1.

15 Even p

In this section, we will discuss the cases when A is an elementary abelian group with even exponent, i.e., when $A = (\mathbb{Z}/2\mathbb{Z})^r$ and $r > 1$. In section 15.1, we first give the result for $r = 2$. Then in order to get a better saving than that obtained in section 15.1, we focus on $r = 3$ in section 15.2, 15.3 and 15.4, and use an induction to get an overall better saving for $r > 3$ in section 15.5.

The main reason that we separate the discussion for p being odd and even is that in Theorem 14.3 we ask the constant c to be smaller than $\frac{(p-2)\epsilon_0}{2+\epsilon_0}$, which is only positive when p is odd. So when $p = 2$, we need to replace Theorem 14.3, and, more importantly, consequences of Theorem 14.3. The strategy for doing this is treat $r = 3$ as the initial case for $p = 2$, i.e., we replace Theorem 14.3 with Theorem 15.3 in this section.

15.1 Even Exponent with Rank 2

In this section, we work with $A = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. We will follow the notation introduced at the beginning of section 14. Recall that we have K_i for $i = 1, 2, 3$ where $\mathrm{Disc}(K_1/k) \leq \mathrm{Disc}(K_2/k) \leq \mathrm{Disc}(K_3/k)$, and $\eta(L/k) := \frac{\ln \mathrm{Disc}(K_2/k)}{\ln \mathrm{Disc}(K_1/k)}$. Again we split the discussion to η being small (the comparable case) and η being big (the incomparable case). We take

$$\eta_0 = \eta_0(\ell, 2)_k = \max\{\beta(k, \mathbb{Z}/p\mathbb{Z}), \gamma(k, \mathbb{Z}/p\mathbb{Z}) + \Delta(\ell, 2)\}/\Delta(\ell, 2)$$

in this section.

For the comparable case, we recall Theorem 14.1 (which is stated for all A, not just odd A), which states that

$$|\operatorname{Cl}_{L/k}[\ell]| = O_{\epsilon,k,\epsilon_0}(\mathrm{Disc}(L/k)^{1/2-\delta+\epsilon}),$$

where $\delta = \delta_c(\eta, \ell, 2) = \frac{\Delta(\ell,2)}{2(\eta+1)}$ and $\eta = \eta(L/k) = \frac{\ln \mathrm{Disc}(K_2/k)}{\ln \mathrm{Disc}(K_1/k)} \leq \eta_0(\ell, 2)_k(1 + \epsilon_0)$.

For the incomparable case, we recall Theorem 14.4 (which is stated for all A, not just odd A), which states that

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

where $\delta = \delta_{ic,k}(\eta, \ell, 2) = \frac{(\Delta(\ell,2)-1/\eta)\eta}{2(\eta+1)}$ when $\eta > \eta_0(\ell, 2)_k$. Combining the two cases, we get the following theorem.

Theorem 15.1 (Even Exponent, Rank 2, Over k)**.** *Given $A = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $\ell > 1$ an odd integer. For any A-extension L/k, we have*

$$|\operatorname{Cl}_L[\ell]| = O_{\epsilon,k}(\mathrm{Disc}(L)^{1/2-\delta_k(\ell,2)+\epsilon}),$$

with

$$\delta_k(\ell, 2) = \frac{\Delta(\ell, 2)}{p(\eta_0 + 1)},$$

where $\eta_0 = \max\{\beta(k, \mathbb{Z}/2\mathbb{Z}), \gamma(k, \mathbb{Z}/2\mathbb{Z}) + \Delta(\ell, 2)\}/\Delta(\ell, 2)$. In particular, when $k = \mathbb{Q}$, we have

$$\delta_{\mathbb{Q}}(\ell, 2) = \frac{\Delta(\ell, 2)}{p(\eta_0 + 1)} = \frac{1}{64\ell^2 + 4\ell}.$$

Proof. If $k = \mathbb{Q}$, by Lemma 12.2, we can take $\beta(\mathbb{Q}, \mathbb{Z}/2\mathbb{Z}) = 8$ and $\gamma(\mathbb{Q}, \mathbb{Z}/2\mathbb{Z}) = 1/2 - \epsilon$. Then $\eta_0(\ell, 2)_{\mathbb{Q}} = \frac{8}{\Delta(\ell,2)}$. By comparing $\frac{\Delta(\ell,2)}{p(\eta_0+1)}$ and $\frac{(\Delta(\ell,2)-\gamma(\mathbb{Q},\mathbb{Z}/2\mathbb{Z})/\eta_0)\eta_0}{p(\eta_0+1)}$, we see that a universal saving is

$$\delta_{\mathbb{Q}}(\ell, 2) = \frac{\Delta(\ell, 2)}{p(\eta_0 + 1)} = \frac{1}{64\ell^2 + 4\ell}.$$

Similarly, we have

$$\delta_k(\ell, 2) = \frac{\Delta(\ell, 2)}{p(\eta_0 + 1)},$$

where $\eta_0 = \max\{\beta(k, \mathbb{Z}/2\mathbb{Z}), \gamma(k, \mathbb{Z}/2\mathbb{Z}) + \Delta(\ell, 2)\}/\Delta(\ell, 2)$. □

15.2 Comparable Size for Rank 3

In this section, we work with $A = (\mathbb{Z}/2\mathbb{Z})^r$ with $r > 2$. In section 15.2, 15.3 and 15.4, we focus on the case $r = 3$ over $\mathbb{Q}$. In section 15.5, we apply the result we obtained for $r = 3$ to obtain results for $r > 3$. The main reason that we can get a better saving here for $r = 3$ over $\mathbb{Q}$ than $r = 2$ is that we can apply the Lemma 12.1 for the incomparable case of $A = (\mathbb{Z}/2\mathbb{Z})^3$ instead of Lemma 12.2.

We introduce the notation for the current section and section 15.3. For $A = (\mathbb{Z}/2\mathbb{Z})^3$, there are 7 index-2 subgroups and 7 index-4 subgroups. For an A-extension $L/\mathbb{Q}$, we denote M_1 to be the quartic subfield with smallest discriminant, and K_m to be the smallest quadratic field outside M_1. Denote K_i for $i = 1, 2, 3$ to be subfields of M_1 ordered by $\mathrm{Disc}(K_i)$. Denote K_i' to be the other quadratic subfield of the compositum $K_m K_i$. So we always have $\mathrm{Disc}(K_i') \geq \mathrm{Disc}(K_m)$. In this section and section 15.3 and 15.4, we will denote

$$\eta = \eta(L/k) := \frac{\ln \mathrm{Disc}(K_m)}{\ln \mathrm{Disc}(M_1)}, \qquad \eta_0 = \frac{1}{\Delta(\ell, 2)}. \tag{15.1}$$

See Theorem 15.3 for the reason on the choice of η_0. We will use $\delta_c'(\eta, \ell)$ and $\delta_{ic}'(\eta, \ell)$ to denote the savings in section 15.2 and 15.3 to distinguish from $\delta_c(\eta, \ell, 2)$ and $\delta_{ic}(\eta, \ell, 2)$ used in section 15.1.

Theorem 15.2. *Given $A = (\mathbb{Z}/2\mathbb{Z})^3$ and an odd integer $\ell > 1$. For any A-extension $L/\mathbb{Q}$ with $\eta(L/\mathbb{Q}) \leq \eta_0(1 + \epsilon_0) = \frac{1+\epsilon_0}{\Delta(\ell,2)}$, we have*

$$|\mathrm{Cl}_L[\ell]| = O_{\epsilon,\epsilon_0}(\mathrm{Disc}(L)^{1/2-\delta+\epsilon}),$$

for

$$\delta = \delta_c'(\eta, \ell) = \frac{\Delta(\ell, 4)}{4\eta + 2} > 0,$$

where $\eta = \frac{\ln \mathrm{Disc}(K_m)}{\ln \mathrm{Disc}(M_1)}$.

Proof. The proof is similar with that of Theorem 14.1. We separate the discussion for M_1 being $\Delta(\ell, 4)$-bad or not with respect to c where c is a fixed small number satisfying $c < 1/7$. We fix c once and for all for the current theorem. By Lemma 11.5, we have $\mathrm{Disc}(M_1) \geq \mathrm{Disc}(L)^{1/(4\eta+2)} \geq \mathrm{Disc}(L)^{1/(4\eta_0(1+\epsilon_0)+2)}$. Note that for a fixed $L_0 > 0$, there are only finitely many L/Q with $\mathrm{Disc}(L) \geq L_0$, thus only finitely many $\mathrm{Disc}(M_1) \geq M_0 = L_0^{1/(4\eta_0(1+\epsilon_0)+2)}$ with $\eta(L/\mathbb{Q}) \leq \eta_0(1 + \epsilon_0)$. So we can assume both M_1 and L are sufficiently large.

If M_1 is $\Delta(\ell, 4)$-good, then by Lemme 11.1 and Lemma 11.5, we have

$$|\mathrm{Cl}_L[\ell]| = |\mathrm{Cl}_{M_1}[\ell]| \prod_{K_i \not\subset M_1} |\mathrm{Cl}_{K_i}[\ell]| = O_\epsilon(\mathrm{Disc}(L)^{1/2-\Delta(\ell,4)/(4\eta+2)+\epsilon}). \tag{15.2}$$

If M_1 is $\Delta(\ell, 4)$-bad, then we have for $x = \mathrm{Disc}(M_1)^{\Delta(\ell,4)}$ that

$$\pi(x; M_1, \hat{e}) \geq (1 - c - \epsilon) \cdot \frac{x}{\ln x},$$

when $x \geq x_0(\epsilon, \epsilon_0)$ is sufficiently large with x_0 depending at most on ϵ and ϵ_0. These primes are inert in M_1/k, so will always split at exactly 2 of $\{K_m, K_1', K_2', K_3'\}$ not contained in M_1. Denote

$$\theta_i = \frac{\Delta(\ell, 4) \ln \mathrm{Disc}(M_1)}{\ln \mathrm{Disc}(K_i')}, \quad i = 1, 2, 3, \quad \theta_m = \frac{\Delta(\ell, 4) \ln \mathrm{Disc}(M_1)}{\ln \mathrm{Disc}(K_m)},$$

for K_i' $(i = 1, 2, 3)$ and K_m respectively. By pigeon hole principle, we get at least $\frac{1-c}{\binom{4}{2}} \frac{x}{\ln x}$ many primes that are all split in two of S. Since $c < 1/7$, we get at least two of K_i of S that are θ_i-good. Denote them by K_j for $j \in J$. Therefore when $\mathrm{Disc}(L/k) \geq L_0(\epsilon, \epsilon_0) = x_0(\epsilon, \epsilon_0)^{(4\eta_0(1+\epsilon_0)+2)/\Delta(\ell,2)}$, we always get for two K_j that

$$|\mathrm{Cl}_{K_j}[\ell]| = O_\epsilon(\mathrm{Disc}(K_j)^{1/2-\theta_j+\epsilon}),$$

and it follows that for every L we get

$$|\operatorname{Cl}_L[\ell]| = \prod_{i\notin J} |\operatorname{Cl}_{K_i}[\ell]| \prod_{j\in J} |\operatorname{Cl}_{K_j}[\ell]| = O_{\epsilon,\epsilon_0}(\operatorname{Disc}(L)^{1/2-2\Delta(\ell,4)/(4\eta+2)+\epsilon}), \tag{15.3}$$

where the last inequality follows from Lemma 11.5. Therefore we can always get a saving with

$$\delta_c'(\eta,\ell) = \frac{\Delta(\ell,4)}{4\eta+2}.$$

□

15.3 Incomparable Size for Rank 3

In this section, we will treat the case when $A = (\mathbb{Z}/2\mathbb{Z})^3$ and the base field is $\mathbb{Q}$, and $\eta(L/\mathbb{Q})$ is large.

Theorem 15.3. *Given $A = (\mathbb{Z}/2\mathbb{Z})^3$ and an odd integer $\ell > 1$. For any A-extension L/k, if $\eta > \eta_0(1+\epsilon_0) = \frac{1+\epsilon_0}{\Delta(\ell,2)}$, then*

$$|\operatorname{Cl}_L[\ell]| = O_{\epsilon,\epsilon_0}(\operatorname{Disc}(L)^{1/2-\delta+\epsilon}),$$

for

$$\delta = \delta_{ic}'(\eta,\ell) = \frac{\Delta(\ell,2)\eta}{2\eta+1} > 0.$$

Proof. Similarly with the proof of Theorem 14.3, by Lemma 11.5, we can assume both L and K_m are sufficiently large.

We will show that at least 2 of quadratic fields K_i in $\{K_m, K_1', K_2', K_3'\}$ are θ_i good for

$$\theta_i = \frac{\Delta(\ell,2)\ln\operatorname{Disc}(K_m)}{\ln\operatorname{Disc}(K_i')}, \quad i=1,2,3, \quad \theta_m = \Delta(\ell,2),$$

with respect to c where c is a small number satisfying $c < \frac{\epsilon_0}{6(1+2\epsilon_0)}$. We will fix $c = c(\epsilon_0)$ once and for all for the current theorem.

We apply Lemma 12.1 with

$$x = \operatorname{Disc}(K_m)^{\Delta(\ell,2)}, \qquad q = \operatorname{Cond}(M_1) \asymp \operatorname{Disc}(M_1)^{1/2},$$

to count the number of primes in $\mathbb{Q}$ that split in $M_1/\mathbb{Q}$. By class field theory, this is equivalent to take $\frac{\phi(q)}{p}$ residue classes $a \pmod q$ and then add up over a, and we get

$$\pi(x; M_1/\mathbb{Q}, e) \le \frac{2}{1-\ln q/\ln x}\cdot\frac{x}{4\ln x} = \frac{2}{1-1/2\Delta(\ell,2)\eta}\cdot\frac{x}{4\ln x}.$$

So we get a positive density C of primes that are inert in $M_1/\mathbb{Q}$

$$\pi(x; M_1/\mathbb{Q}, \hat{e}) \ge (1 - \frac{1}{2-1/\Delta(\ell,2)\eta} - \epsilon)\frac{x}{\ln x} = C\frac{x}{\ln x}, \tag{15.4}$$

when $x \ge x_0(\epsilon,\epsilon_0)$ is sufficiently large. Primes that are inertia in M_1 must be split in exactly two of K_j in $\{K_m, K_1', K_2', K_3'\}$. Therefore by pigeon hole principle, there exist at least two such K_j satisfy

$$\pi(x; K_j, e) \ge \frac{C}{\binom{4}{2}}\cdot\frac{x}{\ln x} \ge c\frac{x}{\ln x}, \tag{15.5}$$

which implies that K_j is θ_j-good. The second inequality comes from $\eta > \eta_0(1+\epsilon_0)$ and the assumption on c. Then by Lemma 13.5, we get

$$|\operatorname{Cl}_{K_j}[\ell]| = O_{\epsilon,\epsilon_0}(\operatorname{Disc}(K_j)^{1/2-\theta_j+\epsilon}).$$

By Lemma 11.3 and 11.1 and Lemma 11.5, we have for every L that

$$|\operatorname{Cl}_L[\ell]| \leq O_{\epsilon,\epsilon_0}(\operatorname{Disc}(L)^{1/2-2\Delta(\ell,2)\eta/(4\eta+2)+\epsilon}). \tag{15.6}$$

So we prove this theorem with

$$\delta'_{ic}(\eta,\ell) = \frac{\Delta(\ell,2)\eta}{(2\eta+1)}.$$

□

15.4 Savings for Even A with Rank 3

Finally combining Theorem 15.2 and 15.3, we get the following theorem.

Theorem 15.4. *Given $A = (\mathbb{Z}/2\mathbb{Z})^3$ and an odd prime integer ℓ. For any A-extension $L/\mathbb{Q}$, we have*

$$|\operatorname{Cl}_L[\ell]| = O_\epsilon(\operatorname{Disc}(L)^{1/2-\delta+\epsilon})$$

for some

$$\delta = \delta'_c(\eta_0,\ell) = \frac{\Delta(\ell,4)}{4\eta_0+2},$$

where $\eta_0 = \frac{1}{\Delta(\ell,2)}$.

Proof. Similarly with Theorem 14.6 we can take ϵ_0 arbitrarily small. Notice that $\delta'_c(\eta,\ell)$ decreases as η increases and $\delta'_{ic}(\eta,\ell)$ increases as η increases. We compare

$$\delta'_c(\eta_0,\ell) = \frac{1}{48\ell^2+12\ell}, \qquad \delta'_{ic}(\eta_0,\ell) = \frac{1}{4\ell+1}.$$

So the worst point in all range of η is the exactly at $\eta = \eta_0$. We can pick $\delta = \frac{\Delta(\ell,4)}{4\eta_0+2} = \frac{1}{48\ell^2+12\ell}$. □

Remark 15.5. *Comparing the saving we get in Theorem 15.1 and 15.4, here we get an improvement over $\mathbb{Q}$, i.e.,*

$$\frac{1}{48\ell^2+12\ell} > \frac{1}{64\ell^2+4\ell}$$

for arbitrary $\ell > 1$.

15.5 Induction

In this section, we will derive ℓ-torsion bound for every $A = (\mathbb{Z}/2\mathbb{Z})^r$ with $r > 2$. Following the Remark 15.5, we will use Theorem 15.4 to prove a point-wise saving for elementary 2-abelian group with rank greater than 3.

Theorem 15.6 (Even Exponent, Over $\mathbb{Q}$)**.** *Given $A = (\mathbb{Z}/2\mathbb{Z})^r$ with $r > 2$ and an arbitrary integer $\ell = \ell_{(2)}\ell_2 > 1$. For any A-extension $L/\mathbb{Q}$, we have the pointwise bound*

$$|\operatorname{Cl}_L[\ell]| = O_\epsilon(\operatorname{Disc}(L/k)^{1/2-\delta(\ell_{(2)})+\epsilon}),$$

for $\delta(\ell) = \frac{1}{48\ell^2+12\ell}$.

Proof. By a similar proof of Theorem 14.9,

$$|\operatorname{Cl}_L[\ell]| = \prod_s |\operatorname{Cl}_{F_s}[\ell]|^{1/7} = O_\epsilon(\prod_s \operatorname{Disc}(F_s)^{1/2-\delta+\epsilon})^{1/7} = O_\epsilon(\operatorname{Disc}(L)^{1/2-\delta+\epsilon}). \tag{15.7}$$

where F_s ranges over all degree 8 subfields of L. It follows directly from Corollary 11.2 and (11.1). Similarly with Theorem 14.9, we derive the results for general ℓ by $|\operatorname{Cl}_L[\ell]| = |\operatorname{Cl}_L[\ell_{(2)}]| \cdot |\operatorname{Cl}_L[\ell_2]|$. □

Remark 15.7 (Even Exponent, $\ell = 3$, Over $\mathbb{Q}$)**.** *When $\ell = 3$, we can do induction over an even better result from [EV07] that $|\operatorname{Cl}_F[3]| = O(\operatorname{Disc}(F)^{1/3+\epsilon})$ for any quadratic extension $F/\mathbb{Q}$. From a direct use of Corollary 11.2 and (11.1), we can take $\delta(3) = 1/3$.*

When $k \neq \mathbb{Q}$, we use the induction from $r = 2$. It follows from a similar proof with Theorem 14.9 directly:

Theorem 15.8 (Even Exponent, Over k)**.** *Given $A = (\mathbb{Z}/2\mathbb{Z})^r$ with $r \geq 2$ and an integer $\ell > 1$. For any A-extension L/k, we have the pointwise bound*

$$|\operatorname{Cl}_L[\ell]| = O_{\epsilon,k}(\operatorname{Disc}(L/k)^{1/2-\delta_k(\ell_{(2)})+\epsilon}),$$

for $\delta_k(\ell) = \delta_k(\ell, 2)$ in Theorem 15.1.

16 Acknowledgement

The author is supported by Foerster-Bernstein Fellowship at Duke University. I would like to thank Jürgen Klüners, Weitong Wang and Asif Zaman for providing helpful references. I would like to thank Dimitris Koukoulopoulos, Robert J. Lemke Oliver, Melanie Matchett Wood, Asif Zaman and Ruixiang Zhang for helpful conversations. I would like to thank Jordan Ellenberg, Melanie Matchett Wood and Yongqiang Zhao for suggestions on an earlier draft.

References

[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.

[CM87] H. Cohen and J. Martinet. Class groups of number fields: numerical heuristics. *Mathematics of Computation*, 48(177):123–137, 1987.

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

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

[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.

[Smi01] Bart De Smit. Brauer-Kuroda relations for S-class numbers. *Acta Arithmetica*, 98(2):133–146, 2001.

[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.

[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.

[Wan17] J. Wang. Malle's conjecture for $S_n \times A$ for $n = 3, 4, 5$. *arXiv: 1705.00044*, 2017.

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

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

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

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