A Heuristic for the Distribution of Ray Class Groups of Number Fields

Robin Ammon

Submitted in Fulfilment of the Requirements for the Degree of

Doctor of Philosophy

School of Mathematics & Statistics
College of Science & Engineering
University of Glasgow

September 2025

Abstract

We propose a conjecture for the distribution of the 'good part' of the ray class group $\mathrm{Cl}_K(\mathfrak{m})$ of a number field K, for K running over a natural family of Galois extensions of a fixed base number field F and fixed modulus $\mathfrak{m}$ given by an integral ideal of $\mathcal{O}_F$. It can be seen as a generalisation of earlier conjectures by Pagano–Sofos for the family of imaginary quadratic number fields and by Bartel–Pagano for the family of real quadratic number fields. Our conjecture is phrased in terms of the Arakelov ray class sequence of a number field introduced by Bartel–Pagano and postulates that the 'good part' of the latter behaves randomly in the sense of Cohen–Lenstra. To be able to state it, we develop a commensurability theory for automorphism groups of chain complexes, extending the commensurability theory of Bartel–Lenstra for automorphism groups of modules.

We show that our conjecture implies the Cohen–Lenstra–Martinet heuristics as reformulated by Bartel–Lenstra and predicts equidistribution of the reduction map $\mathcal{O}_K^\times \to (\mathcal{O}_K/\mathfrak{m})^\times$. We further obtain from our conjecture a general formula for the average ℓ-torsion, ℓ a good prime, of $\mathrm{Cl}_K(\mathfrak{m})$ in families of abelian extensions. We explicitly calculate the predicted average ℓ-torsion of ray class groups of cyclic cubic fields with fixed rational modulus for $\ell \neq 2, 3$.

Contents

Author's Declaration

I declare that, except where explicit reference is made to the contribution of others, this dissertation is the result of my own work and has not been submitted for any other degree at the University of Glasgow or any other institution.

1 Introduction

In number theory, the investigation of statistical questions has become an increasingly important research topic, stretching over many subdisciplines and dealing with objects of various kinds. Now known as *arithmetic statistics*, the modern origin of this area lies in H. Cohen and H. W. Lenstra's seminal paper [CL84], in which they took a new perspective on the previously poorly understood ideal class groups of number fields by studying them through their distribution in natural families of number fields. Their approach and the conjectures they made, known as the *Cohen–Lenstra heuristics*, laid the groundwork for plenty of subsequent research in number theory and beyond.

The present work is closely related to those roots of arithmetic statistics and is concerned with the distribution of ray class groups, which are a natural generalisation of the ideal class group and play an important role in global class field theory. First conjectures about the distribution of ray class groups of imaginary quadratic number fields and real quadratic number fields have been made by Pagano–Sofos [PS17] and Bartel–Pagano [BP25], respectively. In this thesis, we seek to generalise their work to the 'good part' of ray class groups in families of arbitrary Galois extensions of number fields. Building on the existing work for both class groups and ray class groups, we develop all theory necessary in order to make a natural conjecture about the distribution of ray class groups with fixed modulus. To further support our conjecture, we then derive several consequences of it, some of which rely on results that may be of independent interest.

1.1 Background

We discuss the context of this thesis in some more detail.

1.1.1 Arithmetic Statistics and the Distribution of Number-Theoretic Objects

The key philosophy of arithmetic statistics is that the statistical behaviour of mathematical objects mirrors their structural properties, the reason being that any structure will favour certain outcomes and even rule out others. In order to better understand the structure and nature of the objects one is interested in, the aim is thus to prove results on their statistics. This is also an instance of the common approach in mathematics to study objects of interest all at once, compared to individually. The nature of the area entails that statements in arithmetic statistics generally contain a lot of information and are not easy to prove, and making a good conjecture is an important part of the research.

A lot of the time, as is the case also for us with ray class groups, one is interested in the *distribution* of number-theoretic objects, since it encodes a great deal of information about them. What this means explicitly is that given a family of objects of interest X_i, $i \in I$, belonging to some set $\mathcal{X}$ – to be thought of as the set of 'outcomes' and assumed to be countable here – one wants to know how often every $Y \in \mathcal{X}$ occurs among the X_i, i.e. one wants to know what the probability is that for a randomly drawn X_i we have $X_i = Y$. If I is finite, it is clear what that probability should mean. However, if I is infinite, to make sense of that probability requires a height function $h\colon I \to \mathbb{R}_{\geq 0}$ with the property that $|\{\, i \in I \mid h(i) \leq n \,\}| < \infty$ for all $n \in \mathbb{Z}_{>0}$. Using h to induce an ordering on I, the probability that a random X_i equals Y can then be expressed as

$$\mathbb{P}_h(X_i = Y) = \lim_{n\to\infty} \frac{|\{\, i \in I \mid h(i) \leq n, X_i = Y \,\}|}{|\{\, i \in I \mid h(i) \leq n \,\}|}.$$

Note that this probability may depend on h and that the limit may not exist. Studying the distribution of the X_i (with respect to h) means to study $\mathbb{P}_h$. Obtaining meaningful number-theoretic statements requires sensible choices of family I, outcomes $\mathcal{X}$, height function h and possibly even objects X_i.

In practice, determining the distribution of objects X_i as above requires deep knowledge about them. A common approach when investigating that distribution is to compare it with the distribution of a random object of the same kind, provided one can make sense of the latter. The idea behind this is that if the X_i behave like a random object of a certain type T, this means that all the structure the X_i have is that of an object of type T, since additional structure would cause them to behave differently. In that case, the structure of the objects X_i can be regarded as fully understood! On the other hand, if the X_i do not behave like a random object of type T, this indicates that they carry additional structure, which had not yet been taken into account. A strategy to understand the X_i from a macroscopic view is thus to 'extract' all their structure until one can prove that they behave like a random object of exactly that structure.

Requisite for the above strategy is to know what the distribution of a random object looks like. Often, the objects X_i will be certain algebraic structures determined up to some notion of isomorphism and the set of outcomes $\mathcal{X}$ will be a full set of representatives for the set of isomorphism classes of these structures. In that case, there is a well-established principle for the distribution of random such objects, pioneered by Cohen and Lenstra:

Principle 1.1 (Cohen–Lenstra Principle)**.** *Suppose that objects of type T admit a notion of isomorphism. The probability that a randomly drawn object of type T is isomorphic to a given object Y of type T is proportional to* $1/|\operatorname{Aut} Y|$.

The factor $1/|\operatorname{Aut} Y|$ is, as Cohen and Lenstra write, 'a very natural and common weighting factor', and the principle conforms with several natural ways of generating random objects, for example when generating a random group of order n by writing down a random $n \times n$ multiplication table [CL84, page 54] or when generating a random finite abelian p-group as the cokernel of a random (with respect to Haar measure) full rank square matrix over $\mathbb{Z}_p$ [FW89].

1.1.2 Previous Work on the Distribution of Ideal Class Groups

Before contemplating the distribution of ray class groups, it is imperative to first understand the situation for the ideal class group Cl_K of a number field K. This finite abelian group is a central object in number theory, but – despite its prominent position – for a long time there had not been known much about its behaviour. Given K, there existed algorithms to compute Cl_K, but general structural results were scarce and there was little hope for advancement. Motivated by this lack of knowledge and by newly available computational data, Cohen and Lenstra [CL84] began to study the distribution of class groups in families of number fields, in line with the ideas described above.

In doing so, working in the setting of a Galois extension K/F of number fields with Galois group G, the class group Cl_K is subject to the following considerations. First of all, it naturally is a G-module and therefore should be understood as such rather than merely as an abelian group. Secondly, it is known that genus theory restricts the structure of the p-Sylow subgroup $\mathrm{Cl}_K[p^\infty]$ for primes p dividing $|K : F| = |G|$. For this reason, Cohen and Lenstra consider only the S-part $\mathrm{Cl}_K[S^\infty] = \bigoplus_{p \in S} \mathrm{Cl}_K[p^\infty]$ of the class group for a set S of primes not dividing $|K : F|$. Finally, for such S, by [Neu99, Proposition III.1.6 (ii) and (iv)], extension of ideals gives an isomorphism $\mathrm{Cl}_F[S^\infty] \xrightarrow{\sim} \mathrm{Cl}_K[S^\infty]^G = (\sum_{g \in G} g)\,\mathrm{Cl}_K[S^\infty]$, fixing part of $\mathrm{Cl}_K[S^\infty]$. Taking the above information into account, Cohen and Lenstra make conjectures for the distribution of $\mathrm{Cl}_K[S^\infty]$ for imaginary quadratic number fields and totally real abelian extensions of $F = \mathbb{Q}$, ordered by absolute discriminant.

We describe in some more detail the conjectures for quadratic number fields. Here, the Galois group acts on Cl_K by -1, so neither the Galois module structure nor the Galois fixed points impose any structural restrictions on the group structure on the odd part of the class group. Hence, the latter is investigated just as an abelian group. The existing data indicated a close relation of the behaviour of the odd part of Cl_K to that of a random finite abelian group of odd order in the sense of Principle 1.1. Cohen and Lenstra turned this observation into a conjecture as follows. Let S be a set of primes. Call a group an S-group if the order of every element is a product of primes in S. For finite S, $u \in \mathbb{Z}_{\geq 0}$ and $\mathcal{H}_S$ a full set of representatives for the isomorphism classes of finite abelian S-groups, they prove that $c_{S,u} := \sum_{H \in \mathcal{H}_S} \frac{1}{|H|^u \cdot |\mathrm{Aut}\, H|} < \infty$. Their conjecture for imaginary quadratic fields then is:

Conjecture 1.2 ([CL84, Fundamental Assumptions 8.1 (1)])**.** *Let S be a finite set of odd primes. For $B \in \mathbb{R}_{>0}$ write $\mathcal{K}^-_{\leq B}$ for the set of imaginary quadratic number fields with absolute value of their discriminant bounded by B. Let $f \colon \mathcal{H}_S \to \mathbb{C}$ be 'reasonable'. Then*

$$\lim_{B \to \infty} \frac{\sum_{K \in \mathcal{K}^-_{\leq B}} f(\mathrm{Cl}_K[S^\infty])}{\left|\mathcal{K}^-_{\leq B}\right|} = \lim_{B \to \infty} \sum_{H \in \mathcal{H}_S, |H| \leq B} f(H) \cdot \frac{1}{c_{S,0}} \cdot \frac{1}{|\mathrm{Aut}\, H|}.$$

They do not make precise what 'reasonable' should mean. In this form, the conjecture is more general than just a statement on the distribution of $\mathrm{Cl}_K[S^\infty]$; one obtains the latter by taking f to be the indicator function of $H \in \mathcal{H}_S$, in which case the conjecture reads

$$\lim_{B\to\infty} \frac{\left|\left\{ K \in \mathcal{K}^-_{\leq B} \;\middle|\; \mathrm{Cl}_K[S^\infty] \cong H \right\}\right|}{\left|\mathcal{K}^-_{\leq B}\right|} = \frac{1}{c_{S,0}} \cdot \frac{1}{|\mathrm{Aut}\, H|}.$$

In terms of the ideas of Section 1.1.1, Conjecture 1.2 thus postulates that the only structure on $\mathrm{Cl}_K[S^\infty]$ for a generic imaginary quadratic number field K is the abelian group structure. For real quadratic number fields, the conjecture is slightly different.

Conjecture 1.3 ([CL84, Fundamental Assumptions 8.1 (2)]). *Let S be a finite set of odd primes. For $B \in \mathbb{R}_{>0}$ write $\mathcal{K}^+_{\leq B}$ for the set of real quadratic number fields with absolute value of their discriminant bounded by B. Let $f\colon \mathcal{H}_S \to \mathbb{C}$ be 'reasonable'. Then*

$$\lim_{B\to\infty} \frac{\sum_{K\in\mathcal{K}^+_{\leq B}} f(\mathrm{Cl}_K[S^\infty])}{\left|\mathcal{K}^+_{\leq B}\right|} = \lim_{B\to\infty} \sum_{H\in\mathcal{H}_S, |H|\leq B} f(H) \cdot \frac{1}{c_{S,1}} \cdot \frac{1}{|H| \cdot |\mathrm{Aut}\, H|}.$$

The above indicates that the odd part of the class group of real quadratic fields carries some sort of additional structure to the abelian group structure. Cohen and Lenstra attribute the different behaviour to the difference in the rank of $\mathcal{O}_K^\times$. They also make slightly more general versions of the above conjectures allowing infinite S.

The Cohen–Lenstra heuristics have been generalised by Cohen and Martinet [CM90] to arbitrary Galois extensions of number fields, again ordered by absolute discriminant. Cohen–Martinet also consider only the S-part $\mathrm{Cl}_K[S^\infty]$ of the class group for a possibly infinite set S of so-called 'good primes'. Here, the general conception is that there is a notion of such 'good primes' for which the 'good part' $\mathrm{Cl}_K[S^\infty]$ behaves well in the sense that it has minimal structural restrictions and distribution given by a law of the kind as proposed by Cohen and Lenstra. The notion of 'good primes' that Cohen and Martinet use is slightly more general than the one used by Cohen and Lenstra. Analogous as before, their conjectured distribution for the 'good part' of the class group weighs an outcome Y by a factor of the form $1/(|Y|^{\underline{u}} \cdot |\mathrm{Aut}\, Y|)$ with $\underline{u}$ determined by the rank of $\mathcal{O}_K^\times$. Cohen and Martinet moreover outline how to obtain statements on non-Galois extensions from their conjecture. See also [WW21], which further discusses their work.

Over time, certain flaws in the Cohen–Lenstra–Martinet heuristics have been found. Malle [Mal08] indicated that the conjecture for the distribution of $\mathrm{Cl}_K[p^\infty]$ for K running over a family of Galois extensions of F does not seem to hold when the base field F contains the p-th roots of unity. Later on, Bartel and Lenstra [BL20] gave two explicit counterexamples to the heuristics, revealing problems with ordering number fields by discriminant and with allowing infinite S. They also proposed a corrected version of the heuristics, which we are now going to explain in some more detail, as it is one of the starting points for our conjecture on ray class groups.

Besides dealing with the issues mentioned above, Bartel and Lenstra also achieved to reformulate the Cohen–Lenstra–Martinet heuristics in a way which captures the influence of the unit group on the class group that causes the non-random behaviour of the latter. They do so by considering the Arakelov class group Pic^0_K of a number field K in place of the class group Cl_K. The Arakelov class group is a compact real abelian Lie group, whose definition 'adds' the infinite places to the class group, and which naturally comes with a short exact sequence

$$0 \longrightarrow \mathcal{O}_K^\times \otimes_{\mathbb{Z}} \mathbb{R}/\mathbb{Z} \longrightarrow \mathrm{Pic}^0_K \longrightarrow \mathrm{Cl}_K \longrightarrow 0. \tag{1.4}$$

Bartel and Lenstra show that the Cohen–Lenstra–Martinet heuristics are equivalent to the conjecture that the 'good part' of the Arakelov class group behaves like a random object in the sense of Principle 1.1. In the philosophy of Section 1.1.1, Pic^0_K thus incorporates the structure on the 'good part' of the class group related to the unit group – as is also suggested by the short exact sequence (1.4) – and there is no additional structure. This also conforms with the viewpoint that in order to get a complete picture in questions regarding number fields, it is necessary to take into account not only the finite but also the infinite places.

We now discuss some of the aspects and details of Bartel and Lenstra's conjecture that we will refer back to later. They work in the following setup.

Setup 1.5. Let F be a number field and fix an algebraic closure $\overline{F}$ of F. Let G be a finite group. Let A be the quotient of $\mathbb{Q}G$ by a two-sided ideal containing $\sum_{g\in G} g$ and let V be a finitely generated A-module. Let S be a finite set of primes that are good for A (see Definition 7.1) and let $R := \mathrm{im}(\mathbb{Z}_{(S)}G \to A)$, where $\mathbb{Z}_{(S)}$ denotes the localisation of $\mathbb{Z}$ at $\mathbb{Z} \setminus \bigcup_{p\in S} p\mathbb{Z}$. Let $\mathcal{M}_V$ be a full set of representatives for the isomorphism classes of finitely generated R-modules M with $A \otimes_R M \cong V$.

Let $\mathcal{K}^{\mathrm{BL}}$ be the family of pairs (K, ι) where $K \subseteq \overline{F}$ is a Galois extension of F not containing a primitive p-th root of unity for any $p \in S$ and ι is an isomorphism $G \xrightarrow{\sim} \mathrm{Gal}(K/F)$ that induces an isomorphism $A \otimes_{\mathbb{Z}G} \mathcal{O}_K^\times \cong V$ of A-modules. Assume that $\mathcal{K}^{\mathrm{BL}}$ is infinite. Let $C\colon \mathcal{K}^{\mathrm{BL}} \to \mathbb{R}_{\geq 0}$ be the function which for (K, ι) is given by the absolute norm of the product of the prime ideals of $\mathcal{O}_F$ that ramify in K. For $B \in \mathbb{R}_{>0}$ denote by $\mathcal{K}^{\mathrm{BL}}_{C\leq B}$ the set of $(K, \iota) \in \mathcal{K}^{\mathrm{BL}}$ with $C(K, \iota) \leq B$.

In the definition of the family $\mathcal{K}^{\mathrm{BL}}$, the fields are not allowed to contain primitive p-th roots of unity for primes $p \in S$ in order to avoid the issues with roots of unity discussed above. The assumption that $\mathcal{K}^{\mathrm{BL}}$ be infinite is there to be able to reasonably apply Principle 1.1. Ordering the fields by C is believed to be better behaved than ordering by the discriminant, cf. [BL20, page 929].

Instead of working with the compact group Pic^0_K, Bartel and Lenstra consider its Pontryagin dual $(\operatorname{Pic}^0_K)^\vee$. If K/F is a Galois extension with Galois group G, then $(\operatorname{Pic}^0_K)^\vee$ naturally is a G-module. The significance of the ring R is to remove the structural restrictions on $(\operatorname{Pic}^0_K)^\vee$ given by genus theory and Galois fixed points by considering $R \otimes_{\mathbb{Z}G} (\operatorname{Pic}^0_K)^\vee$ for $(K, \iota) \in \mathcal{K}^{\mathrm{BL}}$. The set S is assumed to be finite to circumvent the problems with infinite S discussed earlier. The requirement that $\sum_{g \in G} g = 0 \in A$ ensures that tensoring with R removes the Galois fixed points; in defining A, one may quotient out more components of $\mathbb{Q}G$, which allows to remove the corresponding components of $(\operatorname{Pic}^0_K)^\vee$ if wanted.

We remark that R is flat over $\mathbb{Z}G$ and that the dual of (1.4) tensored with R splits, so that the resulting sequence adds no additional piece of structure to $R \otimes_{\mathbb{Z}G} (\operatorname{Pic}^0_K)^\vee$. Moreover, if $(K, \iota) \in \mathcal{K}^{\mathrm{BL}}$, then $R \otimes_{\mathbb{Z}G} (\operatorname{Pic}^0_K)^\vee$ is a finitely generated R-module satisfying $A \otimes_R R \otimes_{\mathbb{Z}G} (\operatorname{Pic}^0_K)^\vee \cong V$, which means that one can uniquely identify $R \otimes_{\mathbb{Z}G} (\operatorname{Pic}^0_K)^\vee$ with an element of $\mathcal{M}_V$. Thus, the desired conjecture to make is that the 'good part' $R \otimes_{\mathbb{Z}G} (\operatorname{Pic}^0_K)^\vee$ of Pic^0_K behaves like a random element of $\mathcal{M}_V$. When trying to formalise this in terms of Principle 1.1, one encounters the major issue that the automorphism group of $R \otimes_{\mathbb{Z}G} (\operatorname{Pic}^0_K)^\vee$ is in general not finite. Bartel and Lenstra manage to resolve this problem by developing a theory of commensurability of automorphism groups in [BL17], which allows to make sense of the index of automorphism groups, even when those groups are infinite. Their crucial result is [BL17, Theorem 1.2], which in the special case of the setting above gives the following.

Theorem 1.6. *Use Setup 1.5 and let*

$$\mathcal{S} := \{\, L \text{ finitely generated } R\text{-module} \mid A \otimes_R L \cong V \,\}.$$

There is a unique function $\mathrm{ia}\colon \mathcal{S} \times \mathcal{S} \to \mathbb{Q}_{>0}$ *such that:*

(i) If $L, L', M, M' \in \mathcal{S}$ and $L \cong L'$ and $M \cong M'$, then $\mathrm{ia}(L, M) = \mathrm{ia}(L', M')$.

(ii) If $L, M, N \in \mathcal{S}$, then $\mathrm{ia}(L, M) \cdot \mathrm{ia}(M, N) = \mathrm{ia}(L, N)$.

(iii) If $L, M \in \mathcal{S}$ and there is a monomorphism $L \hookrightarrow M$ with finite cokernel, then with $H := \{\, \mu \in \operatorname{Aut} M \mid \mu L = L \,\}$ and $\rho\colon H \to \operatorname{Aut} L$, $\mu \mapsto \mu|_L$ one has

$$\mathrm{ia}(L, M) = \frac{|\operatorname{Aut} M : H| \cdot |\ker \rho|}{|\operatorname{Aut} L : \operatorname{im} \rho|}.$$

Here, ia stands for 'index of automorphism groups'. Accordingly, the value $\mathrm{ia}(L, M)$ should be thought of as $|\operatorname{Aut} M : \operatorname{Aut} L|$, which it indeed equals if $\operatorname{Aut} L$ and $\operatorname{Aut} M$ are finite. With $\mathrm{ia}(L, M)$ for fixed M acting as a replacement of $1/\,|\operatorname{Aut} L|$, Bartel and Lenstra then show that $\sum_{N \in \mathcal{M}_V} \mathrm{ia}(N, M) < \infty$ and construct the probability distribution

$$\mathbb{P}^{\mathrm{BL}}\colon \mathcal{M}_V \to [0, 1],\ L \mapsto \frac{1}{\sum_{N \in \mathcal{M}_V} \mathrm{ia}(N, M)} \cdot \mathrm{ia}(L, M)$$

that can be thought of as weighing each $L \in \mathcal{M}_V$ by a weight proportional to the inverse of the size of its automorphism group. Note that $\mathbb{P}^{\mathrm{BL}}$ is independent of M by part (ii) of the above theorem. They propose the following conjecture, a corrected version of the Cohen–Lenstra–Martinet heuristics.

Conjecture 1.7 ([BL20, Conjecture 1.5])**.** *Use Setup 1.5. Let $f\colon \mathcal{M}_V \to \mathbb{C}$ be a 'reasonable' function. Then the limit*

$$\mathrm{Av}(f) := \lim_{B\to\infty} \frac{\sum_{(K,\iota)\in\mathcal{K}^{\mathrm{BL}}_{C\le B}} f(R \otimes_{\mathbb{Z}G} (\mathrm{Pic}^0_K)^\vee)}{\left|\mathcal{K}^{\mathrm{BL}}_{C\le B}\right|}$$

exists, the sum

$$\mathbb{E}(f) := \sum_{M\in\mathcal{M}_V} f(M)\cdot \mathbb{P}^{\mathrm{BL}}(M)$$

converges absolutely, and both expressions are equal.

Bartel and Lenstra also discuss which functions may be considered reasonable.

In a similar direction, the paper [WW21] also reformulates the Cohen–Lenstra–Martinet heuristics in a way that aligns with Principle 1.1, but using a different object than the Arakelov ray class group. Going further, Bartel–Johnston–Lenstra [BJL24] make conjectures for infinite S, and Sawin–Wood [SW23] make conjectures in the case when p-th roots of unity are present in the base field for $p \in S$.

We remark that for the most part, the conjectures above rely on computational data and the ideas from Section 1.1.1. To this date, the only proven cases of the Cohen–Lenstra–Martinet heuristics are those of the average 3-torsion (i.e. for the function $f(M) = |M[3]|$) of class groups of quadratic extensions of number fields [DH71, DW88] and of the average 3-torsion of class groups of certain 2-extensions [LOWW25].

The conjectures discussed above all deal with the 'good part' of the class group, the analogue of which we will be concerned with in our investigations of ray class groups. We remark that there has also been research on the 'bad part' of Cl_K. In fact, here, more statements have been proved. See [Ger87], [FK07], [Smi26a], [Smi26b].

1.1.3 Previous Work on the Distribution of Ray Class Groups

For a number field K and a modulus $\mathfrak{m}$ in K, that is, a pair $\mathfrak{m} = (\mathfrak{m}_0, \mathfrak{m}_\infty)$ where $\mathfrak{m}_0$ is a nonzero integral ideal of $\mathcal{O}_K$ and $\mathfrak{m}_\infty$ is a set of real places of K, we denote by $\mathrm{Cl}_K(\mathfrak{m})$ the ray class group of K with modulus $\mathfrak{m}$. It is a finite abelian group that generalises the ideal class group in the sense that $\mathrm{Cl}_K(\mathcal{O}_K, \varnothing) = \mathrm{Cl}_K$. The ray class group naturally comes with a short exact sequence

$$\mathrm{S}^{\mathrm{fin}}_K(\mathfrak{m})\colon \qquad 0 \longrightarrow \frac{(\mathcal{O}_K/\mathfrak{m}_0)^\times \times \{\pm 1\}^{\mathfrak{m}_\infty}}{\rho(\mathcal{O}_K^\times)} \longrightarrow \mathrm{Cl}_K(\mathfrak{m}) \longrightarrow \mathrm{Cl}_K \longrightarrow 0$$

where $\rho\colon \mathcal{O}_K^\times \to (\mathcal{O}_K/\mathfrak{m}_0)^\times \times \{\pm 1\}^{\mathfrak{m}_\infty}$ sends u to the tuple consisting of $\overline{u}$ and the signs of u under each of the real embeddings in $\mathfrak{m}_\infty$. To be able to ask statistical questions about $\mathrm{Cl}_K(\mathfrak{m})$ for K running over a family of extensions of a number field F, we will always consider a fixed modulus of the form $\mathfrak{m} = (\mathfrak{m}_F, \varnothing)$, where $\mathfrak{m}_F$ is a nonzero integral ideal of $\mathcal{O}_F$, which for an extension K/F we regard as an ideal of $\mathcal{O}_K$ by extension of ideals.

The story of the investigations of the distribution of ray class groups begins with Varma's paper [Var22], in which they prove an explicit formula for the average 3-torsion of ray class groups of imaginary and real quadratic fields with fixed rational modulus. The result shows that ray class groups with nontrivial modulus behave fundamentally differently to class groups, and thus set the task to find a model for the distribution of ray class groups that both explains this behaviour and naturally extends the Cohen–Lenstra–Martinet heuristics.

The first work in this direction is that of Pagano and Sofos [PS17], who make a conjecture for the distribution of ray class groups of imaginary quadratic number fields ordered by discriminant. Their key idea is to not consider the ray class group on its own, but rather the whole exact sequence $\mathrm{S}_K^{\mathrm{fin}}(\mathfrak{m})$ naturally associated with it. This again is in line with the ideas from Section 1.1.1 that all information on the objects of interest has to be taken into account to determine their distribution, the sequence $\mathrm{S}_K^{\mathrm{fin}}(\mathfrak{m})$ imposing restrictions on the structure of $\mathrm{Cl}_K(\mathfrak{m})$. They also make a conjecture for the distribution of the 'bad' part at $p = 2$ and prove a result on the distribution of 4-ranks of ray class groups of imaginary quadratic fields.

Taking up the work described above, Bartel and Pagano [BP25] examined the good part of $\mathrm{S}_K^{\mathrm{fin}}(\mathfrak{m})$ for quadratic fields, rephrasing the conjecture of Pagano and Sofos for imaginary quadratic K in terms of Principle 1.1, and proposing a conjecture for real quadratic K. Crucially, they introduce the *Arakelov ray class group* $\mathrm{Pic}_K^0(\mathfrak{m})$ of a number field K associated to a modulus $\mathfrak{m}$ in K, a natural generalisation of Pic_K^0 that is related to $\mathrm{Cl}_K(\mathfrak{m})$ as Pic_K^0 is to Cl_K. It is again a compact real abelian Lie group and has a natural short exact sequence

$$\mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})\colon \qquad 0 \longrightarrow \frac{(\mathcal{O}_K/\mathfrak{m}_0)^\times \times \{\pm 1\}^{\mathfrak{m}_\infty}}{\rho(\mu(K))} \longrightarrow \mathrm{Pic}_K^0(\mathfrak{m}) \longrightarrow \mathrm{Pic}_K^0 \longrightarrow 0$$

attached to it. Combining the ideas of [BL20] and [PS17], Bartel and Pagano conjecture that for K running over either imaginary or real quadratic fields, ordered by conductor, and modulus given by a fixed rational integer, the S-part $\mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})[S^\infty]$ is distributed like a random suitable short exact sequence. Here, an automorphism of a short exact sequence means an automorphism in the category of chain complexes. Besides showing that their conjecture is consistent with the Cohen–Lenstra–Martinet heuristics for quadratic fields, Bartel and Pagano derive several other implications of which we briefly describe two. Once again extending the work of Pagano–Sofos, they deduce from their postulate a formula for the average p-torsion of $\mathrm{Cl}_K(\mathfrak{m})$, p odd, also for real quadratic fields, which recovers Varma's result for $p = 3$. Moreover, they show that the sequence $\mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})$ 'knows about' the reduction map $\rho\colon \mathcal{O}_K^\times \to (\mathcal{O}_K/\mathfrak{m}_0)^\times$ and obtain from this an equidistribution prediction for the image of the fundamental unit of K under ρ.

1.2 Main Results

The purpose of this thesis is to extend the work on the distribution of ray class groups outlined above. We propose a conjecture for the distribution of the good part of $\mathrm{Cl}_K(\mathfrak{m})$ for K running over a natural family of Galois extensions of a fixed base number field F and fixed modulus $\mathfrak{m}$ given by an integral ideal of $\mathcal{O}_F$. The conjecture rests on the ideas described in the previous sections and forms a natural generalisation of the existing conjectures on the distribution of ideal class groups and ray class groups. The core principle is to continue the direction of [BP25] and fuse the extensions approach from [PS17] with the Arakelov approach from [BL20]. In further support of our heuristics, we deduce several consequences of it, amongst them an equidistribution statement for the good part of reduction map $\mathcal{O}_K^\times \to (\mathcal{O}_K/\mathfrak{m})^\times$ and a general formula for the average ℓ-torsion of $\mathrm{Cl}_K(\mathfrak{m})$ for abelian extensions K/F and good primes ℓ.

1.2.1 The Main Conjecture

We work in a similar setting as Setup 1.5.

Setup 1.8. Fix a number field F, an algebraic closure $\overline{F}$ of F and an ideal $\mathfrak{m}_F \trianglelefteq \mathcal{O}_F$. Let G be a finite group and let W be a finitely generated $\mathbb{Q}G$-module. Let A be the quotient of $\mathbb{Q}G$ by a two-sided ideal containing $\sum_{g\in G} g$ and let S be a finite set of primes that are good for A in the sense of [BL20] (see Definition 7.1). Let $R := \mathrm{im}(\mathbb{Z}_{(S)}G \to A)$ and let $V := A \otimes_{\mathbb{Q}G} W$. Let $\mathcal{M}_V$ be a full set of representatives for the isomorphism classes of finitely generated R-modules M with $A \otimes_R M \cong V$.

We consider the family $\mathcal{K}$ of Galois extensions of F that is defined as the family $\mathcal{K}^{\mathrm{BL}}$ from Setup 1.5, except with the condition $A \otimes_R \mathcal{O}_K^\times \cong V$ replaced by the more general condition that $\mathbb{Q} \otimes_{\mathbb{Z}} \mathcal{O}_K^\times \cong W$ as $\mathbb{Q}G$-modules. Assume that $\mathcal{K}$ is infinite. For $(K, \iota) \in \mathcal{K}$ use the notation $\mathfrak{m} := (\mathfrak{m}_F, \varnothing)$. For nonabelian G let $C\colon \mathcal{K} \to \mathbb{R}_{\geq 0}$ be the function that maps (K, ι) to the absolute norm of the product of the prime ideals of $\mathcal{O}_F$ that ramify in K. For abelian G let $C\colon \mathcal{K} \to \mathbb{R}_{\geq 0}$ be any fair counting function as defined in [Woo10] (see Definition 8.10). Then for $B \in \mathbb{R}_{>0}$ write $\mathcal{K}_{C\leq B}$ for the set of $(K, \iota) \in \mathcal{K}$ with $C(K, \iota) \leq B$.

In accordance with the philosophy from Section 1.1.1, our goal is to package all structure of the good part of $\mathrm{Cl}_K(\mathfrak{m})$ for $(K, \iota) \in \mathcal{K}$ into one object and then conjecture that this object behaves randomly in the sense of Principle 1.1. Borrowing from [BP25], we postulate that the desired object is given by the good part of the Arakelov ray class sequence $\mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})$ with component of the trivial character removed. We 'extract' that part from $\mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})$ as in [BL20]: Consider in a first step equivalently the Pontryagin dual sequence $\mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee$. Then form the sequence $R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee$, which is given as

$$0 \longrightarrow R \otimes_{\mathbb{Z}G} (\mathrm{Pic}_K^0)^\vee \longrightarrow R \otimes_{\mathbb{Z}G} \mathrm{Pic}_K^0(\mathfrak{m})^\vee \longrightarrow R \otimes_{\mathbb{Z}G} ((\mathcal{O}_K/\mathfrak{m}_F)^\times)^\vee \longrightarrow 0,$$

and which is again exact by flatness of R. To formalise our conjecture, we wish to find a suitable space of outcomes for these sequences and then define a probability distribution on that space that weighs each outcome proportional to the inverse of the size of its automorphism group. For this, we make use of the fact that short exact sequences are parametrised by Ext^1. As before, we have that the left hand term $R \otimes_{\mathbb{Z}G} (\mathrm{Pic}_K^0)^\vee$ is isomorphic to a unique element of $\mathcal{M}_V$. Following the previous works [PS17] and [BP25], we next partition the family $\mathcal{K}$ into finitely many natural subfamilies such that the right hand side of $R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee$ constant in each subfamily.

Setup 1.9. Use Setup 1.8. Further let $T = (T_\mathfrak{p})_{\mathfrak{p} \mid \mathfrak{m}_F}$ be a collection of degree $|G|$ etale $F_\mathfrak{p}$-algebras $T_\mathfrak{p}$ with an inclusion $G \hookrightarrow \mathrm{Aut}_{F_\mathfrak{p}} T_\mathfrak{p}$ such that G acts transitively on the set of primitive idempotents of $T_\mathfrak{p}$. Assume that T is *viable*, i.e. that there is an extension K/F with Galois group isomorphic to G in such a way that for all $\mathfrak{p} \mid \mathfrak{m}_F$ there is a G-equivariant $F_\mathfrak{p}$-algebra isomorphism $K \otimes_F F_\mathfrak{p} \cong T_\mathfrak{p}$. Define $\mathcal{K}^T$ to be the set of $(K, \iota) \in \mathcal{K}$ with $K \otimes_F F_\mathfrak{p} \cong T_\mathfrak{p}$ for all $\mathfrak{p} \mid \mathfrak{m}_F$. For $B \in \mathbb{R}_{>0}$ write $\mathcal{K}^T_{C \leq B}$ for the set of $(K, \iota) \in \mathcal{K}^T$ with $C(K, \iota) \leq B$.

We will show that each $T_\mathfrak{p}$ has a unique maximal $\mathcal{O}_{F_\mathfrak{p}}$-order $\mathcal{O}_{T_\mathfrak{p}}$ and that for $(K, \iota) \in \mathcal{K}^T$ there is a G-equivariant $\mathcal{O}_F$-algebra isomorphism $\mathcal{O}_K/\mathfrak{m}_F \cong \mathcal{O}_T/\mathfrak{m}_F$, where $\mathcal{O}_T := \prod_{\mathfrak{p} \mid \mathfrak{m}_F} \mathcal{O}_{T_\mathfrak{p}}$. Let $U_T := (\mathcal{O}_T/\mathfrak{m}_F)^\times$ and $U_{T,R} := R \otimes_{\mathbb{Z}G} (\mathcal{O}_T/\mathfrak{m}_F)^\times$. We denote by $\mathrm{Aut}_{G\text{-eq. alg.}}(U_{T,R}^\vee)$ the set of automorphisms of $U_{T,R}^\vee$ that are induced by a G-equivariant $\mathcal{O}_F$-algebra automorphism of $\mathcal{O}_T/\mathfrak{m}_F$.

Definition 1.10. Let $N \in \mathcal{M}_V$.

(a) Let $\Theta, \Theta' \in \mathrm{Ext}^1_R(U_{T,R}^\vee, N)$. A triple (f_1, f_0, f_{-1}) is an $(\mathrm{Aut}_{G\text{-eq. alg.}}(U_{T,R}^\vee) \times \mathrm{Aut}\, N)$-*isomorphism* from Θ to Θ' if (f_1, f_0, f_{-1}) is an isomorphism from Θ to Θ' when regarding them as chain complexes concentrated in degrees 1, 0 and -1, and if additionally $f_{-1} \in \mathrm{Aut}_{G\text{-eq. alg.}}(U_{T,R}^\vee)$. Write $[\Theta]_{G\text{-eq. alg.}}$ for the $(\mathrm{Aut}_{G\text{-eq. alg.}}(U_{T,R}^\vee) \times \mathrm{Aut}\, N)$-isomorphism class of Θ and write $\mathrm{Aut}_{G\text{-eq. alg.}}(\Theta)$ for the group of all $(\mathrm{Aut}_{G\text{-eq. alg.}}(U_{T,R}^\vee) \times \mathrm{Aut}\, N)$-automorphisms of Θ.

(b) Let $\mathcal{E}(U_{T,R}^\vee, N)$ be a full set of representatives for the $(\mathrm{Aut}_{G\text{-eq. alg.}}(U_{T,R}^\vee) \times \mathrm{Aut}\, N)$-isomorphism classes in $\mathrm{Ext}^1_R(U_{T,R}^\vee, N)$. Put $\mathcal{E}(U_{T,R}^\vee, \mathcal{M}_V) := \coprod_{N' \in \mathcal{M}_V} \mathcal{E}(U_{T,R}^\vee, N')$.

We will show that we naturally have $R \otimes_{\mathbb{Z}G} ((\mathcal{O}_K/\mathfrak{m}_F)^\times)^\vee \cong (R \otimes_{\mathbb{Z}G} (\mathcal{O}_K/\mathfrak{m}_F)^\times)^\vee$. Thus for $(K, \iota) \in \mathcal{K}^T$, via an isomorphism $R \otimes_{\mathbb{Z}G} (\mathrm{Pic}_K^0)^\vee \cong N$ for $N \in \mathcal{M}_V$ and a G-equivariant $\mathcal{O}_F$-algebra isomorphism $\mathcal{O}_K/\mathfrak{m}_F \cong \mathcal{O}_T/\mathfrak{m}_F$, we may identify $R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee$ with a unique element $[R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee]$ of $\mathcal{E}(U_{T,R}^\vee, \mathcal{M}_V)$, independently of the choices of isomorphisms made. The space $\mathcal{E}(U_{T,R}^{\vee}, \mathcal{M}_V)$ is our space of outcomes for the sequences $R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^{\vee}$ for $(K, \iota) \in \mathcal{K}^T$.

When trying to define a probability distribution on $\mathcal{E}(U_{T,R}^{\vee}, \mathcal{M}_V)$ that weighs each element Θ by the inverse of the size of $\mathrm{Aut}_{G\text{-eq. alg.}}(\Theta)$, one runs into the problem that the latter group typically has infinite order. To resolve this issue, we follow the approach of [BL20], and in a first step generalise the commensurability theory of automorphism groups from [BL17] to chain complexes. The following statement is obtained as a consequence of Theorem 5.42:

Theorem 1.11. *For $N \in \mathcal{M}_V$ denote by $\mathcal{T}(N)$ the set of chain complexes of the form*

$$\cdots \longrightarrow 0 \longrightarrow 0 \longrightarrow N \longrightarrow L \longrightarrow U_{T,R}^{\vee} \longrightarrow 0 \longrightarrow 0 \longrightarrow \cdots$$

where N is in degree 1 and L is a finitely generated R-module, and which become isomorphic to $0 \to V \xrightarrow{\mathrm{id}} V \to 0 \to 0$ after applying $A \otimes_R -$. Define $(\mathrm{Aut}_{G\text{-eq. alg.}}(U_{T,R}^{\vee}) \times \mathrm{Aut}\, N)$-isomorphism of elements of $\mathcal{T}(N)$ as above. Let $\mathcal{T} := \bigcup_{N \in \mathcal{M}_V} \mathcal{T}(N)$. There is a unique function $\mathrm{ia}_{G\text{-eq. alg.}} \colon \mathcal{T} \times \mathcal{T} \to \mathbb{Q}_{>0}$ such that:

(i) If $\Theta, \Delta \in \mathcal{T}(N)$ are $(\mathrm{Aut}_{G\text{-eq. alg.}}(U_{T,R}^{\vee}) \times \mathrm{Aut}\, N)$-isomorphic and $\Theta', \Delta' \in \mathcal{T}(M)$ are $(\mathrm{Aut}_{G\text{-eq. alg.}}(U_{T,R}^{\vee}) \times \mathrm{Aut}\, M)$-isomorphic, then it holds that $\mathrm{ia}_{G\text{-eq. alg.}}(\Theta, \Theta') = \mathrm{ia}_{G\text{-eq. alg.}}(\Delta, \Delta')$.

(ii) If $\Theta, \Theta', \Theta'' \in \mathcal{T}$, then $\mathrm{ia}_{G\text{-eq. alg.}}(\Theta, \Theta') \cdot \mathrm{ia}_{G\text{-eq. alg.}}(\Theta', \Theta'') = \mathrm{ia}_{G\text{-eq. alg.}}(\Theta, \Theta'')$.

(iii) If $\Theta, \Theta' \in \mathcal{T}$ and there is a monomorphism $\Theta \hookrightarrow \Theta'$ with finite cokernel, then with

$$H := \left\{ \sigma \in \mathrm{Aut}_{G\text{-eq. alg.}}(\Theta') \;\middle|\; \sigma\Theta = \Theta, \exists\, \tau \in \mathrm{Aut}_{G\text{-eq. alg.}}(\Theta) : \sigma\big|_{\Theta} = \tau \right\}$$

and $\rho \colon H \to \mathrm{Aut}_{G\text{-eq. alg.}}(\Theta)$, $\sigma \mapsto \sigma|_{\Theta}$ one has

$$\mathrm{ia}_{G\text{-eq. alg.}}(\Theta, \Theta') = \frac{|\mathrm{Aut}_{G\text{-eq. alg.}}(\Theta') : H| \cdot |\ker \rho|}{|\mathrm{Aut}_{G\text{-eq. alg.}}(\Theta) : \mathrm{im}\, \rho|}.$$

In fact, in Theorem 5.42 we will prove a much more general statement on the commensurability of subgroups of automorphism groups of certain chain complexes. The theorem above provides us with a function

$$\mathrm{ia}_{G\text{-eq. alg.}} \colon \mathcal{E}(U_{T,R}^{\vee}, \mathcal{M}_V) \times \mathcal{E}(U_{T,R}^{\vee}, \mathcal{M}_V) \to \mathbb{Q}_{>0}$$

which analogously as the function ia from Theorem 1.6 should be thought of as outputting $\mathrm{ia}_{G\text{-eq. alg.}}(\Theta, \Theta') = |\mathrm{Aut}_{G\text{-eq. alg.}}(\Theta') : \mathrm{Aut}_{G\text{-eq. alg.}}(\Theta)|$. Using $\mathrm{ia}_{G\text{-eq. alg.}}$, we construct the desired probability distribution on $\mathcal{E}(U_{T,R}^{\vee}, \mathcal{M}_V)$.

Theorem 1.12 (Theorem 8.34)**.** *There is a unique discrete probability distribution* $\mathbb{P}_T$ *on* $\mathcal{E}(U_{T,R}^\vee, \mathcal{M}_V)$ *with the property that for all* $\Theta, \Theta' \in \mathcal{E}(U_{T,R}^\vee, \mathcal{M}_V)$ *we have*

$$\frac{\mathbb{P}_T(\Theta)}{\mathbb{P}_T(\Theta')} = \mathrm{ia}_{G\text{-eq. alg.}}(\Theta, \Theta').$$

This distribution also has the following properties:

(i) If $\Theta, \Theta' \in \mathcal{E}(U_{T,R}^\vee, \mathcal{M}_V)$ *and* Φ *is a short exact sequence of finite* R*-modules with* $\Theta \oplus \Phi \cong \Theta'$*, then*

$$\mathbb{P}_T(\Theta) = \left|\mathrm{Aut}_{G\text{-eq. alg.}}(\Theta') : \mathrm{Aut}_{G\text{-eq. alg.}}(\Theta)\right| \cdot \mathbb{P}_T(\Theta')$$

where the inclusion $\mathrm{Aut}_{G\text{-eq. alg.}}(\Theta) \hookrightarrow \mathrm{Aut}_{G\text{-eq. alg.}}(\Theta')$ *is given by* $f \mapsto f \oplus \mathrm{id}_\Phi$*.*

(ii) If $\Theta \in \mathcal{E}(U_{T,R}^\vee, \mathcal{M}_V)$ *is given by*

$$0 \longrightarrow N \longrightarrow L \longrightarrow U_{T,R}^\vee \longrightarrow 0,$$

then we have

$$\mathbb{P}_T(\Theta) = \mathbb{P}^{\mathrm{BL}}(N) \cdot \frac{|[\Theta]_{G\text{-eq. alg.}}|}{\left|\mathrm{Ext}_R^1(U_{T,R}^\vee, N)\right|}.$$

For $f\colon \mathcal{E}(U_{T,R}^\vee, \mathcal{M}_V) \to \mathbb{C}$ define

$$\mathbb{E}(f) := \sum_{\Theta \in \mathcal{E}(U_{T,R}^\vee, \mathcal{M}_V)} f(\Theta) \cdot \mathbb{P}_T(\Theta)$$

if the sum converges absolutely. We propose the following conjecture for the distribution of the good part of Arakelov ray class sequences.

Conjecture 1.13 (Conjecture 8.38)**.** *Use Setup 1.9. Let* $f\colon \mathcal{E}(U_{T,R}^\vee, \mathcal{M}_V) \to \mathbb{C}$ *be 'reasonable'. Then the limit*

$$\mathrm{Av}(f) := \lim_{B \to \infty} \frac{\sum_{(K,\iota) \in \mathcal{K}_{C \le B}^T} f([R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee])}{\left|\mathcal{K}_{C \le B}^T\right|}$$

exists and equals $\mathbb{E}(f)$*.*

1.2.2 Implications of the Main Conjecture and Other Results

Apart from it being a natural prediction to be made, we will further reinforce Conjecture 1.13 by showing that it has many pleasing consequences for the statistical behaviour of certain of those objects attached to $(K, \iota) \in \mathcal{K}^T$, information on which is contained in the sequence $R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee$.

Ideal class groups. As an immediate consequence of Theorem 1.12 we obtain that for the trivial modulus, Conjecture 1.13 reduces to the Cohen–Lenstra–Martinet heuristics.

Corollary 1.14. *Assume that Conjecture 1.13 holds. Then Conjecture 1.7 holds.*

We also obtain a finer version of Conjecture 1.7, namely for (K, ι) running over the family $\mathcal{K}^T$ instead of $\mathcal{K}$; see Corollary 9.3.

Equidistribution results. We obtain the following predictions of equidistribution of key objects related to $R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee$. To avoid much of the glut of technical language needed for precise statements, we state them in a vague and more conceptual manner and refer to the statements in brackets and the respective sections of Chapter 9 for the omitted details.

Corollary 1.15. *Use the notation from Section 1.2.1. Assume that Conjecture 1.13 holds. Then the following hold.*

(i) (Corollary 9.7.) Let $N \in \mathcal{M}_V$ and let $\mathcal{K}^T(N)$ be the set of $(K, \iota) \in \mathcal{K}^T$ with $R \otimes_{\mathbb{Z}G} (\mathrm{Pic}_K^0)^\vee \cong N$. As (K, ι) runs over $\mathcal{K}^T(N)$, the sequence $R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee$ is equidistributed in $\mathcal{E}(U_{T,R}^\vee, N)$.

(ii) (Corollary 9.23.) Let $N \in \mathcal{M}_V$ and let $\omega \in \mathrm{Hom}_R(U_{T,R}^\vee, \mathrm{Hom}_{\mathbb{Z}_{(S)}}(N/N_{\mathrm{tors}}, \mathbb{Z}_{(S)})^\vee)$. Let $\mathcal{K}^T(N, \omega) \subseteq \mathcal{K}^T(N)$ be as in Definition 9.8. As (K, ι) runs over $\mathcal{K}^T(N, \omega)$, the sequence $R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{fin}}(\mathfrak{m})^\vee$ is equidistributed in its space of outcomes.

(iii) (Corollary 9.29.) For $(K, \iota) \in \mathcal{K}^T$ let $\overline{\rho_K(\mathfrak{m})}\colon \mathcal{O}_K^\times/\mu(K) \to (\mathcal{O}_K/\mathfrak{m}_F)^\times/\rho(\mu(K))$ be the reduction map. As (K, ι) runs over $\mathcal{K}^T$, the local reduction map $\mathrm{id}_R \otimes \overline{\rho_K(\mathfrak{m})}$ is equidistributed in its space of outcomes.

(iv) (Proposition 9.30.) As (K, ι) runs over $\mathcal{K}^T$, the distribution of $R \otimes_{\mathbb{Z}G} (\mathrm{Pic}_K^0)^\vee$ and the distribution of $\mathrm{id}_R \otimes \overline{\rho_K(\mathfrak{m})}$ are independent of each other.

Here, we use the term associated space of outcomes to mean the natural respective set of outcomes from Chapter 9 with the property that for (K, ι) in the respective subfamily of $\mathcal{K}^T$, the object in question can uniquely be identified with an element of the set of outcomes. The above statements can be seen as generalisations of the statements (b) to (e) of [BP25, Theorem 1.8]. They are generally obtained in an analogous manner as in loc. cit. The hardest to derive from Conjecture 1.13 is statement (iii). It builds on the remarkable statement from [BP25] mentioned above that the Arakelov ray class sequence $\mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})$ 'knows about' the reduction map $\overline{\rho_K(\mathfrak{m})}$. By generalising Bartel and Pagano's method, we show in Proposition 7.26 that the local reduction map $\mathrm{id}_R \otimes \overline{\rho_K(\mathfrak{m})}$ can be obtained from $R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee$ by means of a general construction on short exact sequences. A key ingredient for this construction is an explicit description of the Pontryagin dual of $\mathbb{Z}_{(S)}$ regarded with the discrete topology. We provide such a description in Theorem 4.34 for S being any nonempty subset of the union of $\{0\}$ and the set of rational primes. It makes explicit isomorphisms appearing in [CEW97] and generalises the well-known isomorphisms $\mathbb{Z}^\vee \cong \mathbb{R}/\mathbb{Z}$ and $\mathbb{Q}^\vee \cong \mathbb{A}_\mathbb{Q}/\mathbb{Q}$.

Average torsion of ray class groups. Analogous as in [PS17] and [BP25], Conjecture 1.13 leads to a prediction for the average torsion of ray class groups. In Corollary 9.43 we first derive a general formula for certain average torsion of $\mathrm{Cl}_K(\mathfrak{m})$ on $\mathcal{K}^T$ and then as an immediate consequence obtain the below result.

Corollary 1.16 (Corollary 9.44)**.** *Use Setup 1.8 with G abelian and $S = \{\ell\}$ where ℓ is a prime with $\ell \nmid |\mathrm{Cl}_F| \cdot |G|$. Denote the simple components of A by $A_1, \dots, A_c$. For $i \in \{1, \dots, c\}$ denote by K_i the centre of A_i and by V_i the i-th isotypical component of the A-module V. Assume that Conjecture 1.13 holds for all viable collections $T = (T_\mathfrak{p})_{\mathfrak{p}|\mathfrak{m}_F}$. Then the limit*

$$\lim_{B\to\infty} \frac{\sum_{(K,\iota)\in\mathcal{K}_{C\leq B}} |\mathrm{Cl}_K(\mathfrak{m})[\ell]|}{|\mathcal{K}_{C\leq B}|}$$

exists and equals

$$\sum_{\substack{T=(T_\mathfrak{p})_{\mathfrak{p}|\mathfrak{m}_F}\\ \text{viable }/\cong}} \mathrm{Pr}_C(T)\cdot \left|U_T[\ell]^G\right| \cdot \prod_{i=1}^{c} \prod_{\substack{\mathfrak{q}\in\mathrm{Max}(\mathcal{O}_{K_i})\\ \mathfrak{q}|\ell}} \left(\frac{|U_T[\ell]_i[\mathfrak{q}^\infty]|}{\ell^{f(\mathfrak{q}|\ell)\cdot\dim_{K_i}(V_i)}} + 1\right),$$

where: $U_T[\ell]_i$ denotes the i-th isotypical component of the $\mathbb{Z}_{(\ell)}G$-module $U_T[\ell]$; $U_T[\ell]_i[\mathfrak{q}^\infty]$ denotes the set of $x \in U_T[\ell]_i$ with $\mathrm{ann}_{\mathcal{O}_{K_i}}(x) = \mathfrak{q}^r$ for some $r \in \mathbb{Z}_{\geq 0}$; for $T = (T_\mathfrak{p})_{\mathfrak{p}|\mathfrak{m}_F}$,

$$\mathrm{Pr}_C(T) := \lim_{B\to\infty} \frac{\left|\left\{ (K,\iota) \in \widetilde{\mathcal{K}} \;\middle|\; K \otimes_F F_\mathfrak{p} \cong T_\mathfrak{p} \text{ for all } \mathfrak{p} \mid \mathfrak{m}_F, C(K) \leq B \right\}\right|}{\left|\left\{ (K,\iota) \in \widetilde{\mathcal{K}} \;\middle|\; C(K) \leq B \right\}\right|},$$

with $\widetilde{\mathcal{K}}$ the set of pairs (K,ι) where $K \subseteq \overline{F}$ is a Galois extension of F and ι is an isomorphism $G \xrightarrow{\sim} \mathrm{Gal}(K/F)$.

We will show that the limit $\mathrm{Pr}_C(T)$ always exists under the assumptions above and provide means to calculate it in certain cases. As a special case, the above result recovers the formulas from [PS17] and [BP25] for the average ℓ-torsion, ℓ odd, of $\mathrm{Cl}_K(\mathfrak{m})$ for K imaginary quadratic and K real quadratic, respectively. In particular, Conjecture 1.13 implies Varma's [Var22] results on the average 3-torsion of ray class groups of quadratic fields.

Extending beyond the quadratic case, in Chapter 10 we explicitly calculate all the terms of the formula in Corollary 1.16 for $F = \mathbb{Q}$, $G = C_q$, q prime, and certain values of ℓ. In particular, we obtain an explicit formula for the average ℓ-torsion of the ray class groups of cyclic cubic fields for $\ell \neq 2, 3$. We state the case of $\ell \equiv 2 \mod 3$ below. A formula for $\ell \equiv 1 \mod 3$ can also be obtained but is more complicated.

Corollary 1.17 (Corollary 10.25)**.** *Denote by $\mathcal{K}^{C_3}$ the family of pairs (K, ι) where $K \subseteq \overline{\mathbb{Q}}$ is a Galois extension of $\mathbb{Q}$ and ι is an isomorphism $C_3 \xrightarrow{\sim} \mathrm{Gal}(K/\mathbb{Q})$. Let $\mathfrak{m}_{\mathbb{Q}}$ be a positive integer. For $a, b \in \mathbb{Z}$ define $\mathcal{P}(a, b) := \{p \mid \mathfrak{m}_{\mathbb{Q}} : p \equiv a \mod b\}$. For $(K, \iota) \in \mathcal{K}^{C_3}$ let $C(K, \iota)$ be the norm of the product of the primes of $\mathbb{Q}$ that ramify in K. Let $2 \neq \ell$ be a prime with $\ell \equiv 2 \mod 3$. Assume that Conjecture 1.13 holds. Then the limit*

$$\lim_{B\to\infty} \frac{\sum_{(K,\iota)\in\mathcal{K}^{C_3}_{C\leq B}} |\mathrm{Cl}_K(\mathfrak{m}_{\mathbb{Q}}, \varnothing)[\ell]|}{\left|\mathcal{K}^{C_3}_{C\leq B}\right|}$$

exists and equals

$$\begin{cases} \ell^{|\mathcal{P}(1,\ell)|}\left(1 + \frac{1}{\ell^2}\left(\frac{\ell^2+2}{3}\right)^{|\mathcal{P}(2\ell+1,3\ell)|} \prod_{p\in\mathcal{P}(1,3\ell)} \frac{p(\ell^2+2)+6}{3p+6}\right), & \ell^2 \nmid \mathfrak{m}_{\mathbb{Q}}, \\ \ell^{|\mathcal{P}(1,\ell)|+1}\left(1 + \left(\frac{\ell^2+2}{3}\right)^{|\mathcal{P}(2\ell+1,3\ell)|} \prod_{p\in\mathcal{P}(1,3\ell)} \frac{p(\ell^2+2)+6}{3p+6}\right), & \ell^2 \mid \mathfrak{m}_{\mathbb{Q}}. \end{cases}$$

We remark that while Corollary 1.16 is in the same spirit as [PS17, Conjecture 2.15] and [BP25, Proposition 4.15], to prove it, we introduce some new ideas. What remains the same is the key ingredient we use, which is the map described below.

Let Z be a commutative ring, let R be a Z-algebra and let $a \in Z$. Let M and N be R-modules and let $\Theta \in \mathrm{Ext}^1_R(M, N)$. The snake lemma applied to the commutative diagram with two rows, each given by Θ, and vertical maps given by multiplication by a, yields a homomorphism $\delta_a^{M,N}(\Theta) \colon M[a] \to N/aN$. This construction gives rise to a map

$$\delta_a^{M,N} \colon \mathrm{Ext}^1_R(M, N) \to \mathrm{Hom}_R(M[a], N/aN), \; \Theta \mapsto \delta_a^{M,N}(\Theta).$$

In our proof of Corollary 1.16, we use the following new result on $\delta_a^{M,N}$, which is a consequence of Theorem 3.26.

Theorem 1.18. *Let Z be a Dedekind domain with fraction field K, let A be a separable K-algebra and let R be a maximal Z-order in A. Let $a \in Z$. Assume that A is commutative, that a has no square prime divisors in Z and that the integral closure of Z in any simple component of A is unramified over Z at all prime divisors of a in Z. Then $\delta_a^{M,N}$ is surjective for all finitely generated R-modules M and N.*

In fact, Theorem 3.26 provides a precise characterisation of the surjectivity of $\delta_a^{M,N}$ in the same setting as in the theorem above but without the assumptions on A, a and Z, and may be of independent interest.

1.3 Organisation of the Material

Chapters 2 through 7 can all be seen as preparations for Conjecture 1.13 and are mostly self-contained. The first three of these contain some more general background material. In Chapter 2 we discuss Ext groups and in particular the relation between Ext^1 and short exact sequences. Chapter 3 is concerned mainly with modules over maximal orders. Here, we investigate properties of torsion and torsionfree modules and give a proof of Theorem 1.18. Chapter 4 discusses Pontryagin duality for locally compact Hausdorff abelian groups that are also modules over a locally compact ring. This more general setting of duality is crucial for us as we need to respect Galois module structures when dualising. We also give some more specific results on duality for modules over a $\mathbb{Z}_{(S)}$-order.

The chapters thereafter are more geared to our context. In Chapter 5 we develop a commensurability theory for subgroups of automorphism groups of chain complexes that allows us to prove Theorem 1.11. In Chapter 6 we recall the definition and some properties of the central object for our conjecture, the Arakelov ray class group. Chapter 7 formalises the process of picking out good components from the Arakelov ray class sequence and establishes important properties of this construction.

In Chapter 8 we establish the setup for Conjecture 1.13, filling in all details omitted above. We then prove Theorem 1.12 and state the main heuristic again. The final two chapters are concerned with implications of Conjecture 1.13. In Chapter 9 we derive Corollaries 1.14, 1.15 and 1.16. Finally, in Chapter 10, we specify to families of cyclic extensions of prime degree. We explicitly determine all the terms appearing in the formula for the average torsion in some specific cases and in particular prove Corollary 1.17.

1.4 Notation and Conventions

Rings and Modules

All rings are unital. Unless otherwise specified, by module we mean left module.

For a ring R, we denote by $R^\times$ its unit group and by $\mathfrak{Z}(R)$ its centre. If $\varphi\colon R \to T$ is a ring homomorphism, then we denote by $\varphi^\times$ the induced group homomorphism $R^\times \to T^\times$.

Suppose that $R = R_1 \times \cdots \times R_n$ is a product of rings and that M is an R-module. Then for $i \in \{1, \ldots, n\}$ we denote by $M_i := e_i M$ the i-th isotypical component of M, where $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ with 1 in i-th position. Note that M_i is an R-submodule of M as well as an R_i-module and that $M = \bigoplus_{i=1}^n M_i$.

Categories

If $\mathcal{C}$ is a category, then by writing $C \in \mathcal{C}$ we mean that C is an object of $\mathcal{C}$.

Let $\mathcal{C}$ be a category and let $L, M, N \in \mathcal{C}$. Let $f\colon L \to M$ and $g\colon N \to M$ be morphisms. If the fibre product of f and g exists, then we denote it by $L \times_M N$ and denote by $\pi_L\colon L \times_M N \to L$ and $\pi_N\colon L \times_M N \to N$ its associated morphisms. Note that if $\mathcal{C} = {}_R\mathsf{Mod}$, then the fibre product exists and is given by

$$L \times_M N = \{\, (l, n) \in L \times N \mid f(l) = g(n) \,\}$$

together with the canonical projections. Now let $h\colon M \to L$ and $k\colon M \to N$ be morphisms. If the pushout of h and k exists, then we denote it by $L +_M N$ and denote by $\iota_L\colon L \to L +_M N$ and $\iota_N\colon N \to L +_M N$ its associated morphisms. Note that if $\mathcal{C} = {}_R\mathsf{Mod}$, then the pushout exists and is given by

$$L +_M N = L \oplus N / \{\, (h(m), -k(m)) \mid m \in M \,\}$$

together with the maps induced by the canonical inclusions $L \to L \oplus N$ and $N \to L \oplus N$.

We use the following notation for categories:

Grp	Groups
Ab	Abelian groups
Ring	Rings (with unit)
${}_R\mathsf{Mod}$	Left modules over the ring R
${}_R\mathsf{mod}$	Finitely generated left modules over the ring R
$\mathsf{Ch}(\mathcal{C})$	Chain complexes in the abelian category $\mathcal{C}$
$\mathsf{Ch}(\mathcal{C})^b$	Bounded chain complexes in the abelian category $\mathcal{C}$
LCA	LCA groups
${}_R\mathsf{LCA}$	LCA modules over the locally compact ring R

Localisation and Completion

For a commutative ring Z, we denote by $\mathrm{Max}(Z)$ the set of maximal ideals of Z. If $\mathfrak{p}$ is a prime ideal of Z, then we denote by $Z_\mathfrak{p}$ the localisation of Z at $\mathfrak{p}$ and by $\widehat{Z}_\mathfrak{p}$ the completion of Z at $\mathfrak{p}$ (if $\mathfrak{p}$ is maximal, this is the same as the completion of $Z_\mathfrak{p}$ at $\mathfrak{p}Z_\mathfrak{p}$). If further M is a Z-module, then we denote by $M_\mathfrak{p} := (Z \setminus \mathfrak{p})^{-1}M \cong Z_\mathfrak{p} \otimes_Z M$ the localisation of M at $\mathfrak{p}$ and by $\widehat{M_\mathfrak{p}}$ the completion of M at $\mathfrak{p}$. Note that if Z is noetherian and M is finitely generated, then the natural map $\widehat{Z}_\mathfrak{p} \otimes_Z M \to \widehat{M_\mathfrak{p}}$ is an isomorphism [AM69, Proposition 10.13].

Let S be a nonempty subset of the union of $\{0\}$ and the set of rational primes. We denote the localisation of $\mathbb{Z}$ at $\mathbb{Z} \setminus \bigcup_{p \in S} p\mathbb{Z}$ by

$$\mathbb{Z}_{(S)} := (\mathbb{Z} \setminus \textstyle\bigcup_{p \in S} p\mathbb{Z})^{-1}\mathbb{Z} = \left\{ \frac{a}{b} \,\middle|\, a, b \in \mathbb{Z}, b \notin \textstyle\bigcup_{p \in S} p\mathbb{Z} \right\}.$$

We always consider $\mathbb{Z}_{(S)}$ with the discrete topology. The nonzero prime ideals of $\mathbb{Z}_{(S)}$ are the $p\mathbb{Z}_{(S)}$ for $p \in S \setminus \{0\}$, and the localisation of $\mathbb{Z}_{(S)}$ at $p\mathbb{Z}_{(S)}$ is just $\mathbb{Z}_{(p)}$. Note that if $S' \subseteq S$, then $\mathbb{Z}_{(S)} \subseteq \mathbb{Z}_{(S')}$. Moreover, $\mathbb{Z}_{(S)} = \bigcap_{p \in S} \mathbb{Z}_{(p)}$. If S is the set of all rational primes, then $\mathbb{Z}_{(S)} = \mathbb{Z}$, and if $S = \{0\}$, then $\mathbb{Z}_{(S)} = \mathbb{Q}$.

Torsion

Let Z be an integral domain. Let M be a Z-module. We say that an element $m \in M$ is a *Z-torsion element* if $\operatorname{ann}_Z(m) \neq 0$, that is, if there is $0 \neq z \in Z$ such that $zm = 0$. We denote by $\operatorname{tors}_Z(M)$ or simply M_{tors} the Z-torsion submodule of M. We say that M is *Z-torsionfree* if $M_{\mathrm{tors}} = 0$ and that it is *Z-torsion* if $M = M_{\mathrm{tors}}$.

For $a \in Z$ we denote by $M[a] := \{\, m \in M \mid am = 0 \,\}$ the a-torsion submodule of M. If Z is a Dedekind domain and $\mathfrak{p}$ is a maximal ideal of Z, then we denote by

$$M[\mathfrak{p}^\infty] := \{\, m \in M \mid \operatorname{ann}_Z(m) = \mathfrak{p}^r \text{ for some } r \in \mathbb{Z}_{\geq 0} \,\}$$

the $\mathfrak{p}$-primary component of M. More generally, if S is a set of maximal ideals of Z, then we write $M[S^\infty]$ for the set of elements of M whose annihilator is a product of primes in S.

These notions will often come up in the context where R is a Z-order (in some finite dimensional algebra over the fraction field of Z) and M is an R-module. We make the convention that in this case, by torsion we always mean Z-torsion.

Maximal Orders over Dedekind Domains

Let Z be a Dedekind domain with fraction field K, let A be a separable K-algebra and let R be a maximal Z-order in A. In this context, we will use the following notation, which is based on the one from [CM90].

Let $A = A_1 \times \cdots \times A_c$ be the decomposition of A into simple components and let $R = R_1 \times \cdots \times R_c$ be the associated decomposition of R. For $i \in \{1, \ldots, c\}$ define $K_i := \mathfrak{Z}(A_i)$ and let Z_i be the integral closure of Z in K_i. Then R_i is a maximal Z_i-order in A_i by [Rei03, Theorem 10.5]. There are a unique $l_i \in \mathbb{Z}_{\geq 1}$ and a unique division ring D_i with centre K_i such that $A_i \cong \operatorname{Mat}_{l_i}(D_i)$. In a diagram,

$$\begin{tikzcd}
K_i \arrow[r, hook] & D_i \arrow[r, hook] & \operatorname{Mat}_{l_i}(D_i) \cong A_i \\
Z_i \arrow[u, hook] \arrow[rr, hook] & & R_i, \arrow[u, hook, "\text{m.o.}"']
\end{tikzcd}$$

where 'm.o.' means maximal order. Now let $\mathfrak{p}$ be a maximal ideal of Z_i. Let $K_{i,\mathfrak{p}}$ be the completion of K_i at $\mathfrak{p}$ and let $\widehat{Z}_{i,\mathfrak{p}}$ be the completion of Z_i at $\mathfrak{p}$, a complete discrete valuation ring. Denote by $\widehat{\mathfrak{p}}$ the unique maximal ideal of $\widehat{Z}_{i,\mathfrak{p}}$. Let $A_{i,\mathfrak{p}} := K_{i,\mathfrak{p}} \otimes_{K_i} A_i$, a central simple $K_{i,\mathfrak{p}}$-algebra. There are a unique $l_{i,\mathfrak{p}} \in \mathbb{Z}_{\geq 1}$ and a unique division ring $D_{i,\mathfrak{p}}$ with centre $K_{i,\mathfrak{p}}$ such that $A_{i,\mathfrak{p}} \cong \mathrm{Mat}_{l_{i,\mathfrak{p}}}(D_{i,\mathfrak{p}})$.

Denote by $v_{i,\mathfrak{p}}$ the valuation on $K_{i,\mathfrak{p}}$. By [Rei03, Theorems 12.6 and 12.10], it extends uniquely to a valuation on $D_{i,\mathfrak{p}}$. Let $v_{D_{i,\mathfrak{p}}} = e(D_{i,\mathfrak{p}}/K_{i,\mathfrak{p}}) \cdot v_{i,\mathfrak{p}}$ be the associated normalised valuation on $D_{i,\mathfrak{p}}$. We write $e_{i,\mathfrak{p}} := e(D_{i,\mathfrak{p}}/K_{i,\mathfrak{p}})$ and $f_{i,\mathfrak{p}} := f(D_{i,\mathfrak{p}}/K_{i,\mathfrak{p}})$. By [Rei03, Theorem 12.8], the ring $\Delta_{i,\mathfrak{p}} := \{ x \in D_{i,\mathfrak{p}} \mid v_{i,\mathfrak{p}}(x) \geq 0 \}$ is the unique maximal $\widehat{Z}_{i,\mathfrak{p}}$-order $\Delta_{i,\mathfrak{p}}$ in $D_{i,\mathfrak{p}}$. Let $\pi_{D_{i,\mathfrak{p}}} \in \Delta_{i,\mathfrak{p}}$ such that $v_{D_{i,\mathfrak{p}}}(\pi_{D_{i,\mathfrak{p}}}) = 1$ and let $\mathfrak{p}' := \pi_{Di,\mathfrak{p}} \Delta_{i,\mathfrak{p}}$. By [Rei03, Theorem 13.2], $\mathfrak{p}'$ is the unique maximal left ideal of $\Delta_{i,\mathfrak{p}}$ and every non-zero one-sided ideal of $\Delta_{i,\mathfrak{p}}$ is a two-sided ideal and is a power of $\mathfrak{p}'$.

Let $\widehat{R}_{i,\mathfrak{p}} := \widehat{Z}_{i,\mathfrak{p}} \otimes_{Z_i} R_i$, a maximal $\widehat{Z}_{i,\mathfrak{p}}$-order in $A_{i,\mathfrak{p}}$. By [Rei03, Theorem 17.3] we may choose the isomorphism $A_{i,\mathfrak{p}} \cong \mathrm{Mat}_{l_{i,\mathfrak{p}}}(D_{i,\mathfrak{p}})$ in such a way that it carries $\widehat{R}_{i,\mathfrak{p}}$ onto $\mathrm{Mat}_{l_{i,\mathfrak{p}}}(\Delta_{i,\mathfrak{p}})$. In a diagram,

$$\begin{tikzcd}
K_{i,\mathfrak{p}} \arrow[r, hook, "\text{cent.}"] & D_{i,\mathfrak{p}} \arrow[r, hook] & \mathrm{Mat}_{l_{i,\mathfrak{p}}}(D_{i,\mathfrak{p}}) \arrow[r, "\sim"] & A_{i,\mathfrak{p}} \\
\widehat{Z}_{i,\mathfrak{p}} \arrow[u, hook] \arrow[r, hook, "\text{int.cls.}"'] & \Delta_{i,\mathfrak{p}} \arrow[u, hook, "\text{! m.o.}"] \arrow[r, hook] & \mathrm{Mat}_{l_{i,\mathfrak{p}}}(\Delta_{i,\mathfrak{p}}) \arrow[u, hook, "\text{m.o.}"] \arrow[r, "\sim"] & \widehat{R}_{i,\mathfrak{p}}, \arrow[u, hook, "\text{m.o.}"]
\end{tikzcd}$$

where '! m.o.' means unique maximal order. If M is an R-module, write M_i for the i-th isotypical component, which is an R_i-module. Further define $\widehat{M_{i,\mathfrak{p}}} := \widehat{Z}_{i,\mathfrak{p}} \otimes_{Z_i} M_i$, an $\widehat{R}_{i,\mathfrak{p}}$-module.

Topological Groups

If M is a topological group, then we denote by M_0 its connected component of the identity. If N is another topological group, then we denote by $\mathrm{Hom}_{\mathrm{cts}}(M, N)$ the set of continuous group homomorphisms from M to N. Given a compact subset $K \subseteq M$ and an open subset $U \subseteq N$, define

$$W(K, U) := \{ \varphi \in \mathrm{Hom}_{\mathrm{cts}}(M, N) \mid \varphi(K) \subseteq U \}.$$

Then the $W(K, U)$ are a subbasis for a topology on $\mathrm{Hom}_{\mathrm{cts}}(M, N)$. This topology is called the *compact-open topology* on $\mathrm{Hom}_{\mathrm{cts}}(M, N)$, and we will always consider $\mathrm{Hom}_{\mathrm{cts}}(M, N)$ as a topological space equipped with it.

2 Ext Groups and Extensions

Throughout this chapter, let R be a ring.

We collect some theorems and definitions from the theory of Ext groups, most of which are well-known and stated here for convenience and later use. We assume familiarity with basic properties of Ext groups, for which we refer to [Wei94, Chapter 3]. Having in mind our later applications to homomorphisms and short exact sequences, we are mostly concerned with $\mathrm{Ext}^0 = \mathrm{Hom}$ and Ext^1.

2.1 Ext Groups

For left R-modules M and N both the functors $\mathrm{Hom}_R(M,-)\colon\ {}_R\mathsf{Mod} \to \mathsf{Ab}$ as well as $\mathrm{Hom}_R(-,N)\colon\ {}_R\mathsf{Mod}^{\mathrm{op}} \to \mathsf{Ab}$ are left exact but not right exact. Their right derived functors are the Ext functors $\mathrm{Ext}^n_R(M,-)\colon\ {}_R\mathsf{Mod} \to \mathsf{Ab}$ and $\mathrm{Ext}^n_R(-,N)\colon\ {}_R\mathsf{Mod}^{\mathrm{op}} \to \mathsf{Ab}$. These constitute bifunctors

$$\mathrm{Ext}^n_R(-,-)\colon\ {}_R\mathsf{Mod}^{\mathrm{op}} \times {}_R\mathsf{Mod} \to \mathsf{Ab}$$

which are the right derived functors of $\mathrm{Hom}_R(-,-)\colon\ {}_R\mathsf{Mod}^{\mathrm{op}} \times {}_R\mathsf{Mod} \to \mathsf{Ab}$. Note that if S is another ring and M is an (R,S)-bimodule, then $\mathrm{Ext}^n_R(M,N)$ is naturally a left S-module, and if N is an (R,S)-bimodule, then $\mathrm{Ext}^n_R(M,N)$ is naturally a right S-module, cf. [Rei03, page 9].

If $f\colon M' \to M$ is an R-module homomorphism, we denote by f^* the induced homomorphism $\mathrm{Ext}^n_R(M,N) \to \mathrm{Ext}^n_R(M',N)$, and if $g\colon N \to N'$ is an R-module homomorphism, we denote by g_* the induced homomorphism $\mathrm{Ext}^n_R(M,N) \to \mathrm{Ext}^n_R(M,N')$.

We state the following proposition for convenience as it will be used repeatedly.

Proposition 2.1 ([Rei03, Theorem 2.39]). *Let Z be a commutative ring. Let Z' be a Z-algebra that is flat as a Z-module and let R be a Z-algebra that is left noetherian. Let M be a finitely generated R-module and let N be any R-module. Then the map*

$$\begin{gathered} Z' \otimes_Z \mathrm{Hom}_R(M,N) \to \mathrm{Hom}_{Z'\otimes_Z R}(Z' \otimes_Z M, Z' \otimes_Z N), \\ a \otimes \varphi \mapsto (b \otimes m \mapsto ba \otimes \varphi(m)), \end{gathered}$$

is an isomorphism of Z'-bimodules. This isomorphism is the first of a family of Z'-bimodule isomorphisms

$$Z' \otimes_Z \mathrm{Ext}^n_R(M,N) \cong \mathrm{Ext}^n_{Z'\otimes_Z R}(Z' \otimes_Z M, Z' \otimes_Z N)$$

for $n \in \mathbb{Z}_{\geq 0}$.

We will need a different version of change of rings as well.

Proposition 2.2. *Let $S \to R$ be a flat ring homomorphism. Let $n \in \mathbb{Z}_{\geq 0}$ and let M and N be S-modules. Then the functor $R \otimes_S -$ induces a homomorphism*

$$\operatorname{Ext}^n_S(M, N) \to \operatorname{Ext}^n_R(R \otimes_S M, R \otimes_S N)$$

which is natural in M and N and compatible with the connecting homomorphisms.

Proof. See [HS97, Section IV.12]. □

2.2 Ext and Extensions

What makes Ext groups so important for us is that Ext^1_R provides a nice algebraic framework for working with short exact sequences of R-modules. We now explain this relation in detail.

Definition 2.3. Let M and N be R-modules.

(a) An *extension* of M by N is a short exact sequence $0 \to N \to L \to M \to 0$ of R-modules.

(b) We say that two extensions $0 \to N \to L \to M \to 0$ and $0 \to N \to L' \to M \to 0$ of M by N are *equivalent* if there is a homomorphism $f\colon L \to L'$ that makes the diagram

$$\begin{tikzcd}
0 \arrow[r] & N \arrow[r] \arrow[d, equal] & L \arrow[r] \arrow[d, "f"] & M \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & N \arrow[r] & L' \arrow[r] & M \arrow[r] & 0
\end{tikzcd}$$

commute. We denote by $E_R(M, N)$ the set of equivalence classes of extensions of M by N.

(c) Given two extensions $\Theta\colon 0 \to N \xrightarrow{\alpha} L \xrightarrow{\beta} M \to 0$ and $\Theta'\colon 0 \to N \xrightarrow{\alpha'} L' \xrightarrow{\beta'} M \to 0$ of M by N, their *Baer sum* is defined to be the extension

$$0 \longrightarrow N \longrightarrow (L \times_M L')/\{\, (\alpha(n), -\alpha'(n)) \mid n \in N \,\} \longrightarrow M \longrightarrow 0,$$

where the left hand map is given by $n \mapsto \overline{(\alpha(n), 0)} = \overline{(0, \alpha'(n))}$ and the right hand map is given by $\overline{(l, l')} \mapsto \beta(l) = \beta'(l')$. We will denote this extension by $\Theta + \Theta'$.

Construction 2.4. Let M and N be R-modules. Construct a map $\varepsilon\colon E_R(M, N) \to \operatorname{Ext}^1_R(M, N)$ as follows. Let $\Theta\colon 0 \to N \to L \to M \to 0$ be an extension of M by N. Apply $\operatorname{Ext}_R(M, -)$ to obtain a connecting homomorphism $\delta_\Theta\colon \operatorname{Hom}_R(M, M) \to \operatorname{Ext}^1_R(M, N)$ and define $\varepsilon(\Theta) := \delta_\Theta(\mathrm{id}_M)$.

Proposition 2.5. *Let M and N be R-modules. The set $E_R(M,N)$ forms an abelian group with respect to Baer sum and the map*

$$\varepsilon\colon E_R(M,N) \to \operatorname{Ext}^1_R(M,N)$$

is a group isomorphism.

Proof. See [Wei94, Section 3.4] or [HS97, Section III.2]. □

This different perspective on $\operatorname{Ext}^1_R(M,N)$ will play a central role in our work.

Remark 2.6. There is a similar description of $\operatorname{Ext}^n_R(M,N)$ for any n, using so-called *n-extensions*, see [HS97, Section IV.9]. We will not need this here, however.

Via the isomorphism from Proposition 2.5, the constructions on $\operatorname{Ext}^1_R(M,N)$ from the previous sections correspond to constructions on extensions, and we now describe the latter. We will generally omit any notation signifying that the elements of $E_R(M,N)$ are equivalence classes. This is because later we will also work with another, weaker, equivalence relation on extensions.

The functoriality of Ext behaves in the following way for extensions, cf. [HS97, Sections III.1 and III.2] or [Rot09, Section 7.2.1].

Construction 2.7. Let M and N be R-modules. Let $\Theta \in E_R(M,N)$ be given by

$$0 \longrightarrow N \xrightarrow{\alpha} L \xrightarrow{\beta} M \longrightarrow 0.$$

(a) Let $f\colon M' \to M$ be an R-module homomorphism. Then there is a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & N \arrow[r, "\alpha'"] \arrow[d, equal] & L \times_M M' \arrow[r, "\pi_{M'}"] \arrow[d, "\pi_L"] & M' \arrow[r] \arrow[d, "f"] & 0 \\
0 \arrow[r] & N \arrow[r, "\alpha"'] & L \arrow[r, "\beta"'] & M \arrow[r] & 0
\end{tikzcd}$$

with exact rows, where $\alpha'(m) = (\alpha(m), 0)$. The extension $f^*(\Theta) \in E_R(M',N)$ is given by the upper sequence.

(b) Let $g\colon N \to N'$ be an R-module homomorphism. Then there is a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & N \arrow[r, "\alpha"] \arrow[d, "g"] & L \arrow[r, "\beta"] \arrow[d, "\iota_L"] & M \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & N' \arrow[r, "\iota_{N'}"'] & N' +_N L \arrow[r, "\beta'"'] & M \arrow[r] & 0
\end{tikzcd}$$

with exact rows, where $\beta'(\overline{(n',l)}) = \beta(l)$. The extension $g_*(\Theta) \in E_R(M,N')$ is given by the lower sequence.

The change of rings homomorphism from Proposition 2.2 has the expected description in terms of extensions:

Proposition 2.8. *Let $S \to R$ be a flat ring homomorphism. Let M and N be S-modules. Then under the isomorphism from Proposition 2.5, the map*

$$E_S(M,N) \to E_R(R \otimes_S M, R \otimes_S N),\ \Theta \mapsto R \otimes_S \Theta$$

corresponds to the homomorphism from Proposition 2.2.

Proof. We have to check that the diagram

$$\begin{tikzcd}
E_S(M,N) \arrow[r] \arrow[d, "\varepsilon_S"] & E_R(R \otimes_S M, R \otimes_S N) \arrow[d, "\varepsilon_R"] \\
\operatorname{Ext}^1_S(M,N) \arrow[r, "\tau"] & \operatorname{Ext}^1_R(R \otimes_S M, R \otimes_S N)
\end{tikzcd}$$

commutes, where τ is the homomorphism from Proposition 2.2. Let $\Theta\colon 0 \to N \to L \to M \to 0$ be an extension of M by N. Denote by $\delta_\Theta\colon \operatorname{Hom}_S(M,M) \to \operatorname{Ext}^1_S(M,N)$ the connecting homomorphism when applying $\operatorname{Ext}_S(M,-)$ to Θ, and by $\delta_{R\otimes_S\Theta}\colon \operatorname{Hom}_R(R\otimes_S M, R\otimes_S M) \to \operatorname{Ext}^1_R(R \otimes_S M, R \otimes_S N)$ the connecting homomorphsim when applying $\operatorname{Ext}_R(R \otimes_S M, -)$ to $R \otimes_S \Theta$. Since τ is compatible with connecting homomorphisms, we have a commutative diagram

$$\begin{tikzcd}
\operatorname{Hom}_S(M,M) \arrow[r, "\delta_\Theta"] \arrow[d, "R\otimes_S -"] & \operatorname{Ext}^1_S(M,N) \arrow[d, "\tau"] \\
\operatorname{Hom}_R(R \otimes_S M, R \otimes_S M) \arrow[r, "\delta_{R\otimes_S\Theta}"'] & \operatorname{Ext}^1_R(R \otimes_S M, R \otimes_S N).
\end{tikzcd}$$

The claim follows immediately from this and the construction of ε. □

In the following, when dealing with $\operatorname{Ext}^1_R(M,N)$ or $E_R(M,N)$, we will always use the notation $\operatorname{Ext}^1_R(M,N)$ and use the homological and the extension description interchangeably, without further comment.

2.3 Isomorphism of Extensions

We will later investigate the statistical behaviour of certain homomorphisms and short exact sequences, whose underlying modules vary over the family under consideration. In our context, asking statistical questions about these objects will only make sense when regarding the involved modules up to isomorphism. This leads to the following notion of isomorphism of homomorphisms and extensions that was already used in the introduction.

Definition 2.9. Let M and N be R-modules. Let $H \leq \operatorname{Aut} M \times \operatorname{Aut} N$.

(a) Let $\varphi, \varphi' \in \operatorname{Hom}_R(M, N)$. An *$H$-isomorphism* from φ to φ' is a pair $(\mu, \nu) \in H$ with the property that the diagram

$$\begin{tikzcd}
M \arrow[r, "\varphi"] \arrow[d, "\mu"] & N \arrow[d, "\nu"] \\
M \arrow[r, "\varphi'"'] & N
\end{tikzcd}$$

commutes.

(b) Let $\Theta\colon 0 \to N \to L \to M \to 0$ and $\Theta'\colon 0 \to N \to L' \to M \to 0$ be two extensions of M by N. An *H-isomorphism* from Θ to Θ' is a tuple $((\mu, \nu), \lambda) \in H \times \operatorname{Hom}_R(L, L')$ with the property that the diagram

$$\begin{tikzcd}
0 \arrow[r] & N \arrow[r] \arrow[d, "\nu"] & L \arrow[r] \arrow[d, "\lambda"] & M \arrow[r] \arrow[d, "\mu"] & 0 \\
0 \arrow[r] & N \arrow[r] & L' \arrow[r] & M \arrow[r] & 0
\end{tikzcd}$$

commutes.

Now let $n \in \{0, 1\}$ and let $x, x' \in \operatorname{Ext}_R^n(M, N)$. If there is an H-isomorphism from x to x', we say that x and x' are *H-isomorphic* and write $x \cong_H x'$. We denote by $\operatorname{Aut}_H(x)$ the H-automorphism group of x and by $[x]_H \subseteq \operatorname{Ext}_R^n(M, N)$ its H-isomorphism class. In the case $H = \operatorname{Aut} M \times \operatorname{Aut} N$, we simply speak of *isomorphisms* and omit the H in the notation.

Note that the notion of isomorphism of extensions agrees with the notion of isomorphism when considering them as objects in the category of chain complexes. It is clear that being equivalent in the sense of Definition 2.3 implies being H-isomorphic, which in turn implies being isomorphic. So it makes sense to speak of (H-)isomorphism of extensions even when considering them as elements of $\operatorname{Ext}_R^1(M, N)$.

We now link the notions of isomorphism of homomorphisms and extensions to the following natural action. This is inspired by [PS17] and [BP25].

Definition 2.10. Let $n \in \mathbb{Z}_{\geq 0}$. Let M and N be R-modules. Let $(\mu, \nu) \in \operatorname{Aut} M \times \operatorname{Aut} N$ and $x \in \operatorname{Ext}_R^n(M, N)$. Then we put

$$(\mu, \nu).x := (\mu^{-1})^* \circ \nu_*(x) = \nu_* \circ (\mu^{-1})^*(x),$$

which defines an action of $\operatorname{Aut} M \times \operatorname{Aut} N$ on $\operatorname{Ext}_R^n(M, N)$. If $H \leq \operatorname{Aut} M \times \operatorname{Aut} N$, we denote by $\operatorname{Stab}_H(x)$ and $O_H(x)$ the stabiliser and orbit of x, respectively, with respect to the action of H on $\operatorname{Ext}_R^1(M, N)$. As before, we omit the subscript H if $H = \operatorname{Aut} M \times \operatorname{Aut} N$.

Note that in the case $n = 0$, the action of $(\mu, \nu) \in \operatorname{Aut} M \times \operatorname{Aut} N$ on $\varphi \in \operatorname{Ext}^0_R(M, N) = \operatorname{Hom}_R(M, N)$ is simply given by

$$(\mu, \nu).\varphi = \nu \circ \varphi \circ \mu^{-1}.$$

Hence, $\varphi' \cong_H \varphi$ if and only if $\varphi' \in O_H(\varphi)$, so that $[\varphi]_H = O_H(\varphi)$. Moreover, $\operatorname{Aut}_H(\varphi) = \operatorname{Stab}_H(\varphi)$. We now consider the case of extensions and derive similar results.

Lemma 2.11. *Let M and N be R-modules. Let $(\mu, \nu) \in \operatorname{Aut} M \times \operatorname{Aut} N$. Let $\Theta, \Theta' \in \operatorname{Ext}^1_R(M, N)$ and write $\Theta\colon 0 \to N \to L \to M \to 0$ and $\Theta'\colon 0 \to N \to L' \to M \to 0$. Then $(\mu, \nu).\Theta$ is given by the exact sequence*

$$0 \longrightarrow N \xrightarrow{\alpha\circ\nu^{-1}} L \xrightarrow{\mu\circ\beta} M \longrightarrow 0.$$

In particular, $(\mu, \nu).\Theta = \Theta'$ if and only if there is $\lambda \in \operatorname{Hom}_R(L, L')$ such that $((\mu, \nu), \lambda)$ is an isomorphism from Θ to Θ'.

Proof. This follows easily from Construction 2.7. □

Proposition 2.12. *Let M and N be R-modules and let $\Theta, \Theta' \in \operatorname{Ext}^1_R(M, N)$. Let $H \leq \operatorname{Aut} M \times \operatorname{Aut} N$. Then the following hold:*

(i) We have $\Theta' \cong_H \Theta$ if and only if $\Theta' \in O_H(\Theta)$. In particular, $[\Theta]_H = O_H(\Theta)$.

(ii) Let $\rho\colon \operatorname{Aut}_H \Theta \to H$ be the natural map. Then $\operatorname{im} \rho = \operatorname{Stab}_H(\Theta)$ and $\ker \rho \cong \operatorname{Hom}_R(M, N)$.

Proof. Claim (i) and the equality $\operatorname{im} \rho = \operatorname{Stab}_H(\Theta)$ in part (ii) are immediate from Lemma 2.11. It remains to prove that $\ker \rho \cong \operatorname{Hom}_R(M, N)$. Suppose that Θ is given by the extension $0 \to N \xrightarrow{\alpha} L \xrightarrow{\beta} M \to 0$. It is then easy to check that the map

$$\operatorname{Hom}_R(M, N) \to \operatorname{Aut}_H \Theta, \ \gamma \mapsto (\mathrm{id}_N, \mathrm{id}_L + \alpha\gamma\beta, \mathrm{id}_M)$$

is an injective homomorphism whose image is precisely $\ker \rho$. □

In certain cases, we can compare isomorphism class and stabiliser sizes for different subgroups of $\operatorname{Aut} M \times \operatorname{Aut} N$.

Corollary 2.13. *Let M and N be R-modules and let $\Theta \in \operatorname{Ext}^1_R(M, N)$. Let $H \leq H' \leq \operatorname{Aut} M \times \operatorname{Aut} N$ and suppose that $|H' : H| < \infty$. Then*

$$|\operatorname{Stab}_{H'}(\Theta) : \operatorname{Stab}_H(\Theta)| = |\operatorname{Aut}_{H'}(\Theta) : \operatorname{Aut}_H(\Theta)| < \infty.$$

If moreover one of $[\Theta]_H$ and $[\Theta]_{H'}$ is finite, then so is the other one, and it holds that

$$\frac{|[\Theta]_{H'}|}{|[\Theta]_H|} = \frac{|H' : H|}{|\operatorname{Aut}_{H'}(\Theta) : \operatorname{Aut}_H(\Theta)|}.$$

Proof. Note that we have a natural injection

$$\operatorname{Aut}_{H'}(\Theta)/\operatorname{Aut}_H(\Theta) \hookrightarrow H'/H$$

which shows $|\operatorname{Aut}_{H'}(\Theta) : \operatorname{Aut}_H(\Theta)| < \infty$. By Proposition 2.12, there is a commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & \operatorname{Hom}_R(M,N) \arrow[r] \arrow[d, equal] & \operatorname{Aut}_H(\Theta) \arrow[r] \arrow[d, hook] & \operatorname{Stab}_H(\Theta) \arrow[r] \arrow[d, hook] & 1 \\
1 \arrow[r] & \operatorname{Hom}_R(M,N) \arrow[r] & \operatorname{Aut}_{H'}(\Theta) \arrow[r] & \operatorname{Stab}_{H'}(\Theta) \arrow[r] & 1
\end{tikzcd}$$

of groups with exact rows. The snake lemma then yields the first claim. For the isomorphism classes simply note that

$$\left|H' : \operatorname{Stab}_{H'}(\Theta)\right| \cdot |\operatorname{Stab}_{H'}(\Theta) : \operatorname{Stab}_H(\Theta)| = \left|H' : H\right| \cdot |H : \operatorname{Stab}_H(\Theta)| \,.$$

Then use the orbit-stabiliser theorem and the first claim. □

3 Torsion and Lattices over (Maximal) Orders

In this chapter, we collect statements related to torsion and lattices, in the context of (maximal) orders. The first two subsections contain well-known properties of the torsion submodule and of lattices, which will be useful throughout. For the most part, these are compiled from [Rei03]. In Section 3.3 we prove a classification of the finitely generated torsion modules over a maximal order over a complete discrete valuation ring. This theory will then be used in Section 3.4 as a key foundation for the proof of the characterisation of surjectivity of the map $\delta_a^{M,N}$ from the introduction. Finally, in the last subsection, we establish some results on the cardinality of certain Ext groups.

3.1 Torsion and Lattices over Orders

In this section, let Z be an integral domain with fraction field K and let R be a Z-order (in some finite-dimensional K-algebra).

We collect some basic results on torsion that will be used frequently. See Section 1.4 for relevant notation regarding torsion and recall that by torsion of an R-module we always mean Z-torsion.

Lemma 3.1. *Let M be a Z-module. Let $x \in K^\times$ and $m \in M$. Then:*

$$x \otimes m = 0 \in K \otimes_Z M \qquad \Longleftrightarrow \qquad m \in M_{\text{tors}}.$$

In particular, M_{tors} is the kernel of $M \to K \otimes_Z M$.

Proof. Suppose that $m \in M_{\text{tors}}$. Then there is $0 \neq z \in Z$ with $zm = 0$. It follows that $x \otimes m = \frac{x}{z} \otimes zm = 0$. Conversely, suppose that $x \otimes m = 0$. Write $x = \frac{a}{b}$ with $a, b \in Z \setminus \{0\}$. We have $0 = \frac{am}{b} \in (Z \setminus \{0\})^{-1}M$ which means that there is $c \in Z \setminus \{0\}$ with $cam = 0$. Hence, $m \in M_{\text{tors}}$. □

Thus, if M is Z-torsionfree, then we can identify it with its image in $K \otimes_Z M$.

Lemma 3.2. *Let M be a Z-module. Suppose that Z' is an integral domain that is flat as a Z-module. Then $(Z' \otimes_Z M)_{\text{tors}} = Z' \otimes_Z M_{\text{tors}}$ and the natural map*

$$(Z' \otimes_Z M)/(Z' \otimes_Z M)_{\text{tors}} \to Z' \otimes_Z M/M_{\text{tors}}$$

is an isomorphism.

Proof. Since Z' is Z-flat, the exact sequence $0 \to M_{\mathrm{tors}} \to M \to M/M_{\mathrm{tors}} \to 0$ of Z-modules gives rise to an exact sequence

$$0 \longrightarrow Z' \otimes_Z M_{\mathrm{tors}} \longrightarrow Z' \otimes_Z M \longrightarrow Z' \otimes_Z M/M_{\mathrm{tors}} \longrightarrow 0$$

of Z'-modules. It is clear that $Z' \otimes_Z M_{\mathrm{tors}} \subseteq (Z' \otimes_Z M)_{\mathrm{tors}}$. The converse follows from the above exact sequence and the fact that $Z' \otimes_Z M/M_{\mathrm{tors}}$ is Z'-torsionfree by [Sta25, Tag 0AXM]. The second claim is immediate. □

We now switch perspective to R-modules. Note that if M is an R-module and $a \in Z$, then M_{tors} and $M[a]$ are R-submodules of M, and M/M_{tors} is torsionfree. If moreover Z is a Dedekind domain and $\mathfrak{p}$ is a maximal ideal of Z, then also the $\mathfrak{p}$-primary component $M[\mathfrak{p}^\infty]$ is an R-submodule of M. We have the following generalisation of the decomposition of a torsion abelian group into the direct sum of its Sylow subgroups (which holds for any Z-algebra R).

Lemma 3.3. *Suppose that Z is a Dedekind domain. Let M be an R-module. Then the following hold:*

(i) We have

$$M_{\mathrm{tors}} = \bigoplus_{\mathfrak{p} \in \mathrm{Max}(Z)} M[\mathfrak{p}^\infty],$$

and if $zM_{\mathrm{tors}} = 0$ for $z \in Z$ with $(z) = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_k^{r_k} \subseteq Z$, then $M_{\mathrm{tors}} = \bigoplus_{i=1}^{k} M[\mathfrak{p}_i^\infty]$.

Assume now that M_{tors} is finitely generated as a Z-module. Let $\mathfrak{p}$ and $\mathfrak{q}$ be maximal ideals of Z. Then we further have:

(ii) $M[\mathfrak{p}^\infty]$ is naturally a $Z_{\mathfrak{p}}$-module and an $R_{\mathfrak{p}}$-module.

(iii) There is a natural isomorphism

$$Z_{\mathfrak{p}} \otimes_Z M[\mathfrak{p}^\infty] \cong M[\mathfrak{p}^\infty], \quad \begin{matrix} a \otimes m \mapsto am, \\ 1 \otimes m \leftarrow\!\shortmid m \end{matrix}$$

of $R_{\mathfrak{p}}$-modules.

(iv) If $\mathfrak{q} \neq \mathfrak{p}$, then $Z_{\mathfrak{p}} \otimes_Z M[\mathfrak{q}^\infty] = 0$.

(v) We have

$$Z_{\mathfrak{p}} \otimes_Z M_{\mathrm{tors}} \cong Z_{\mathfrak{p}} \otimes_Z M[\mathfrak{p}^\infty] \cong M[\mathfrak{p}^\infty]$$

as $R_{\mathfrak{p}}$-modules.

All statements above also hold with $Z_{\mathfrak{p}}$ replaced by $\widehat{Z}_{\mathfrak{p}}$, the completion of Z at $\mathfrak{p}$, and $R_{\mathfrak{p}}$ replaced by $\widehat{R}_{\mathfrak{p}} = \widehat{Z}_{\mathfrak{p}} \otimes_Z R$.

Proof. To show that the sum in (i) is direct, let $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ be maximal ideals of Z and let $m_i \in M[\mathfrak{p}_i^\infty]$ with $0 = m_1 + \dots + m_n$. Suppose that $\operatorname{ann}_Z(m_i) = \mathfrak{p}_i^{s_i}$ with $s_i \in \mathbb{Z}_{\geq 0}$. Let $l \in \{1, \dots, n\}$. We show that $m_l = 0$. Let $w \in \prod_{i \neq l} \mathfrak{p}_i^{s_i}$. Then $0 = w(m_1 + \dots + m_n) = wm_l$, so $w \in \mathfrak{p}_l^{s_l}$. This shows that $\prod_{i \neq l} \mathfrak{p}_i^{s_i} \subseteq \mathfrak{p}_l^{s_l}$ which forces $s_l = 0$. Hence, $m_l = 1 \cdot m_l = 0$.

Next, let $m \in M_{\text{tors}}$ and let $0 \neq z \in Z$ with $zm = 0$. Let $(z) = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_k^{r_k}$ be the factorisation of (z) into maximal ideals. Since Z is a Dedekind domain, we can find $z_i \in \prod_{j \neq i} \mathfrak{p}_j^{r_j}$ with $1 = z_1 + \dots + z_k$. Then we see that

$$m = z_1 m + \dots + z_k m \in M[\mathfrak{p}_1^\infty] \oplus \dots \oplus M_{[}\mathfrak{p}_k^\infty].$$

This proves (i).

Now assume that M_{tors} is finitely generated as a Z-module and let $\mathfrak{p}$ and $\mathfrak{q}$ be maximal ideals of Z. Then there is $k \in \mathbb{Z}_{\geq 0}$ with $\mathfrak{p}^k M[\mathfrak{p}^\infty] = 0$. The $Z_\mathfrak{p}$-module structure on $M[\mathfrak{p}^\infty]$ is induced by the isomorphism $Z_\mathfrak{p}/\mathfrak{p}^k Z_\mathfrak{p} \cong Z/\mathfrak{p}^k Z$. Since Z is central in R, the $Z_\mathfrak{p}$-module structure also gives rise to an $R_\mathfrak{p}$-module structure.

For part (iii) note that for $a \in Z_\mathfrak{p}$ and $m \in M[\mathfrak{p}^\infty]$ we have that $a \otimes m = 1 \otimes am$: If we let $z \in Z$ such that $a - z \in \mathfrak{p}^n Z_\mathfrak{p}$, then by definition, $am = zm$, so

$$1 \otimes am = 1 \otimes zm = z \otimes m = a \otimes m - (a - z) \otimes m = a \otimes m.$$

Claim (iv) is clear as we can invert elements of $\mathfrak{q}$ in $Z_\mathfrak{p}$. Finally, (v) is immediate from (i), (iii) and (iv). □

Finitely generated torsionfree modules will play an important role.

Definition 3.4 ([Rei03, pages 44 and 129])**.** A *Z-lattice* is a finitely generated Z-torsionfree Z-module. An *R-lattice* is an R-module that is a Z-lattice.

Remark 3.5. Some authors, e.g. [CR81], define a Z-lattice to be a finitely generated projective Z-module. This definition agrees with the one given above if Z is a Dedekind domain (see Proposition 3.9 below), which is the case that we will be interested in.

We end this section by briefly discussing the dual of an R-module, a notion especially useful for lattices. As before, we always regard Z as understood from the context.

Definition 3.6 ([Rei03, Exercise 40.2])**.** Let M be an R-module. Then the *dual* of M is $M^* := \operatorname{Hom}_Z(M, Z)$.

Proposition 3.7 ([Rei03, Exercise 40.2])**.** *Let M be an R-module. Then M^* is an R^{op}-module via $(r.f)(m) := f(rm)$ for $r \in R^{\text{op}}$, $f \in M^*$ and $m \in M$. Moreover, the following hold:*

(i) If N is another R-module and $\varphi\colon M \to N$ is an R-homomorphism, then the map $\varphi^*\colon N^* \to M^*$, $f \mapsto f \circ \varphi$ is an R^{op}-homomorphism, and this construction behaves functorially.

(ii) The map

$$M \to M^{**},\ m \mapsto (f \mapsto f(m))$$

is a homomorphism of R-modules, which is natural in M.

(iii) M^* is Z-torsionfree. In particular, if Z is noetherian and M is an R-lattice, then M^* is an R^{op}-lattice.

(iv) If Z is a Dedekind domain and M is an R-lattice, then the map from (ii) is an isomorphism of R-modules.

Note also that taking the dual is clearly compatible with direct sums. Moreover, in a similar direction, we have:

Lemma 3.8. *Let M be an R-module. Suppose that $R = R_1 \times \cdots \times R_n$ is a product of rings and let $M = M_1 \oplus \cdots \oplus M_n$ be the decomposition into isotypical components.*

Then $R^{\mathrm{op}} = R_1^{\mathrm{op}} \times \cdots \times R_n^{\mathrm{op}}$ and there is an isomorphism of R^{op}-modules

$$M^* \cong (M_1)^* \oplus \cdots \oplus (M_n)^*, \quad \begin{array}{l} f \mapsto \big(f\big|_{M_i}\big)_i \\ \big(m_1 + \cdots + m_n \mapsto f_1(m_1) + \cdots + f_n(m_n)\big) \leftarrow\!\shortmid (f_1, \ldots, f_n) \end{array}$$

where the duals on the right hand side are taken as R-modules. Moreover, $(M_i)^*$ lies in block R_i^{op} and we have isomorphisms

$$(M^*)_i \cong (M_i)^*, \quad \begin{array}{l} f \mapsto f\big|_{M_i} \\ \big(m_1 + \cdots + m_n \mapsto f_i(m_i)\big) \leftarrow\!\shortmid f_i \end{array}$$

of R^{op}-modules.

Proof. This is clear. □

3.2 Lattices over Maximal Orders

In this section, Z is a Dedekind domain with fraction field K and A is a separable K-algebra. We discuss some fundamental results for lattices over maximal Z-orders in A.

Proposition 3.9 ([Rei03, Corollary 21.5])**.** *Let R be a maximal Z-order in A. Then every R-lattice is R-projective. In particular, if M is a finitely generated R-module, then $M \cong M_{\mathrm{tors}} \oplus M/M_{\mathrm{tors}}$.*

Proposition 3.10. *Suppose that Z only has a finite number of maximal ideals. Let R be a Z-order in A and let M and N be R-lattices. Then the following are equivalent:*

(i) $M \cong N$ *as R-modules,*

(ii) $R_\mathfrak{p} \otimes_R M \cong R_\mathfrak{p} \otimes_R N$ *as $R_\mathfrak{p}$-modules for all maximal ideals $\mathfrak{p}$ of Z,*

(iii) $\widehat{R}_\mathfrak{p} \otimes_R M \cong \widehat{R}_\mathfrak{p} \otimes_R N$ *as $\widehat{R}_\mathfrak{p}$-modules for all maximal ideals $\mathfrak{p}$ of Z.*

If R is in fact a maximal Z-order in A, these are also equivalent to:

(iv) $A \otimes_R M \cong A \otimes_R N$ *as A-modules.*

Proof. The equivalence of (i) and (ii) is [Rei03, Exercise 18.3]. The equivalence of (ii) and (iii) follows from [Rei03, Theorem 18.2].

Now suppose that R is a maximal order and let $\mathfrak{p}$ be a maximal ideal of Z. Then $R_\mathfrak{p}$ is a maximal $Z_\mathfrak{p}$-order in A by [Rei03, Corollary 11.2] and $R_\mathfrak{p} \otimes_R M$ and $R_\mathfrak{p} \otimes_R N$ are $R_\mathfrak{p}$-lattices by Lemma 3.2. Hence, the equivalence of (ii) and (iv) follows from [Rei03, Theorem 18.10]. □

Corollary 3.11. *Suppose that Z only has a finite number of maximal ideals. Let R be a maximal Z-order in A and let M and N be two finitely generated R-modules. Then the following are equivalent:*

(i) $M \cong N$ *as R-modules,*

(ii) $R_\mathfrak{p} \otimes_R M \cong R_\mathfrak{p} \otimes_R N$ *as $R_\mathfrak{p}$-modules for all maximal ideals $\mathfrak{p}$ of Z,*

(iii) $\widehat{R}_\mathfrak{p} \otimes_R M \cong \widehat{R}_\mathfrak{p} \otimes_R N$ *as $\widehat{R}_\mathfrak{p}$-modules for all maximal ideals $\mathfrak{p}$ of Z.*

Proof. The equivalence of (ii) and (iii) follows from [Rei03, Theorem 18.2]. It is clear that (i) implies (ii).

We show that (ii) implies (i). Suppose that $R_\mathfrak{p} \otimes_R M \cong R_\mathfrak{p} \otimes_R N$ as $R_\mathfrak{p}$-modules for all maximal ideals $\mathfrak{p}$ of Z. Then by Lemma 3.2 we have $R_\mathfrak{p} \otimes_R M_{\text{tors}} \cong R_\mathfrak{p} \otimes_R N_{\text{tors}}$ and $R_\mathfrak{p} \otimes_R M/M_{\text{tors}} \cong R_\mathfrak{p} \otimes_R N/N_{\text{tors}}$ for all maximal ideals $\mathfrak{p}$ of Z. By Lemma 3.3, the former implies that $M_{\text{tors}} \cong N_{\text{tors}}$ as R-modules, whereas by Proposition 3.10 the latter implies that $M/M_{\text{tors}} \cong N/N_{\text{tors}}$ as R-modules. We conclude from Proposition 3.9 that $M \cong N$ as R-modules. □

3.3 Torsion Modules over Maximal Orders

We aim to give a description of finitely generated torsion modules over maximal orders over a complete discrete valuation ring that is similar to the description of finitely generated torsion modules over a PID in terms of elementary divisors.

3.3.1 Maximal Orders over Dedekind Domains

Proposition 3.12. *Let Z be a Dedekind domain with fraction field K, let A be a separable K-algebra and let R be a maximal Z-order in A. Let M be a finitely generated torsion R-module. Then there are $n \in \mathbb{Z}_{\geq 0}$ and left ideals $J_i \subseteq I_i$ of R, $i = 1, \ldots, n$, with $KI_i = KJ_i = A$ for all i such that*

$$M \cong \bigoplus_{i=1}^{n} I_i/J_i$$

as R-modules. If Z is a discrete valuation ring, then moreover there are $x_i \in R \cap A^\times$ with $I_i/J_i \cong R/Rx_i$.

Proof. The first claim follows from [Kne67, Satz 1]. Now suppose that Z is a discrete valuation ring. Then by [Rei03, Theorem 18.10], every left ideal of R is principal, so there are $x_i, y_i \in R$ such that $I_i = Ry_i$ and $J_i = Rx_iy_i$, $i = 1, \ldots, n$. Since $KI_i = KJ_i = A$ and $KR = A$, we have $x_i, y_i \in A^\times$, from which it follows that $I_i/J_i \cong R/Rx_i$. □

3.3.2 Matrix Orders over Complete Discrete Valuation Rings

In this subsection, Z is a complete discrete valuation ring with normalised valuation v and fraction field K. Let further D be a division ring whose centre contains K with $|D : K| < \infty$. By [Rei03, Theorems 12.6 and 12.10], v extends uniquely to a valuation on D, which we will also denote by v. Similarly as in Section 1.4 we denote by $\Delta := \{\, x \in D \mid v(x) \geq 0 \,\}$ the unique maximal Z-order in D and by v_D the normalised valuation on D associated to v. Let $\pi_D \in \Delta$ be a uniformiser for v_D. Let $l \in \mathbb{Z}_{\geq 1}$ and let $R := \mathrm{Mat}_l(\Delta)$.

The following proposition will be crucial.

Proposition 3.13 ([Rei03, Theorem 17.7])**.** *Let $x \in R$. Then there are $u, v \in \mathrm{GL}_l(\Delta)$ such that*

$$uxv = \mathrm{diag}(\pi_D^{a_1}, \ldots, \pi_D^{a_l}), \qquad \text{where } 0 \leq a_1 \leq \cdots \leq a_l \leq \infty$$

(where π_D^∞ is interpreted as 0). The a_i are uniquely determined by x.

Lemma 3.14. *The following hold:*

(i) For $h \in \mathbb{Z}_{\geq 0}$, the set of column vectors $(\Delta/\pi_D^h)^l$ is naturally an R-module.

(ii) Let $x \in R$ and let $0 \leq a_1 \leq \cdots \leq a_l \leq \infty$ be the integers from Proposition 3.13 associated to x. Then

$$R/Rx \cong (\Delta/\pi_D^{a_1})^l \oplus \cdots \oplus (\Delta/\pi_D^{a_l})^l$$

as R-modules.

(iii) Let $x, y \in R$ and let $0 \leq a_1 \leq \cdots \leq a_l \leq \infty$ and $0 \leq b_1 \leq \cdots \leq b_l \leq \infty$ be the integers from Proposition 3.13 associated to x and y, respectively. Then $R/Rx \cong R/Ry$ as R-modules if and only if $a_i = b_i$ for all i.

Proof. Statement (i) is clear. Now let x and a_i be as in (ii). By Proposition 3.13, there are $u, v \in \mathrm{GL}_l(\Delta)$ such that $uxv = \mathrm{diag}(\pi_D^{a_1}, \dots, \pi_D^{a_l})$. Notice that the R-module isomorphism $R \to R$, $r \mapsto rv$ induces an isomorphism $R/Rx \xrightarrow{\sim} R/Rxv$ and that $Rxv = Ru^{-1}uxv = Ruxv$. So we may from now on assume that $x = \mathrm{diag}(\pi_D^{a_1}, \dots, \pi_D^{a_l})$. For $w \in R = \mathrm{Mat}_l(\Delta)$ denote by w_i the columns of w, so that $w = (w_1 \mid \cdots \mid w_l)$. It is easy to see that the map $\overline{w} \mapsto (\overline{w_1}, \dots, \overline{w_l})$ gives the desired isomorphism.

Finally, let x, y, a_i, b_i be as in (iii). Let $X := R/Rx$ and $Y := R/Ry$. It is clear from (ii) that if $a_i = b_i$ for all i, then $X \cong Y$. Conversely, suppose that we have $X \cong Y$. Assume that there is i with $a_i \neq b_i$. Let t be maximal with $a_t \neq b_t$. Without loss of generality, $a_t > b_t$. Note that $\pi_D^{b_t}X$ and $\pi_D^{b_t}Y$ are submodules of X and Y, respectively. By (ii) and assumption, we have

$$\begin{aligned} \pi_D^{b_t}X &\cong \pi_D^{b_t}(\Delta/\pi_D^{a_1})^l \oplus \cdots \oplus \pi_D^{b_t}(\Delta/\pi_D^{a_t})^l \oplus \pi_D^{b_t}(\Delta/\pi_D^{a_{t+1}})^l \oplus \cdots \oplus \pi_D^{b_t}(\Delta/\pi_D^{a_l})^l \\ \pi_D^{b_t}Y &\cong \pi_D^{b_t}(\Delta/\pi_D^{a_{t+1}})^l \oplus \cdots \oplus \pi_D^{b_t}(\Delta/\pi_D^{a_l})^l \end{aligned}$$

as R-modules. Then by [Rei03, Exercise 6.7] we must have

$$\pi_D^{b_t}(\Delta/\pi_D^{a_1})^l = \cdots = \pi_D^{b_t}(\Delta/\pi_D^{a_t})^l = 0.$$

This implies $b_t \geq a_t$, a contradiction. □

Note that if M is an R-module, then by [Rei03, Exercise 6.5], M is indecomposable if and only if $\mathrm{End}_R(M)$ is a local ring. In particular, the Krull–Schmidt Theorem holds for R-modules (cf. [Rei03, Exercise 6.6] or [Lam91, Theorem 19.21]).

Proposition 3.15. *The modules*

$$M_h := R/R\,\mathrm{diag}(1, \dots, 1, \pi_D^h), \qquad h \in \mathbb{Z}_{\geq 1},$$

form a full set of representatives for the isomorphism classes of indecomposable finitely generated torsion R-modules.

Proof. Let $h \in \mathbb{Z}_{\geq 1}$. Since M_h is annihilated by π_D^h, it will also be annihilated by a high enough power of a uniformiser for v in Z, so it is a torsion module. To prove that M_h is indecomposable, we will show that $\mathrm{End}_R(M_h)$ is a local ring. Let $x := \mathrm{diag}(1, \dots, 1, \pi_D^h)$. We have an isomorphism of abelian groups

$$E_x := \{\, \overline{w} \in R/Rx \,|\, \overline{xw} = 0 \,\} \xleftrightarrow{\sim} \mathrm{End}_R(R/Rx)$$

given by sending $\overline{w} \in E_x$ to the map $\overline{r} \mapsto \overline{rw}$ and by sending $\varphi \in \mathrm{End}_R(R/Rx)$ to $\varphi(\overline{1})$. This becomes a ring isomorphism with the ring structure on E_x defined by $\overline{v} \cdot \overline{w} := \overline{wv}$

for $\overline{v}, \overline{w} \in E_x$. Note that for $w = (w_{ij}) \in R$ we have $\overline{w} \in E_x$ if and only if $v_D(w_{il}) \geq h$ for $i = 1, \dots, l-1$. We claim that

$$E_x^\times = \left\{ \overline{w} = \overline{(w_{ij})} \in E_x \,\middle|\, v_D(w_{ll}) = 0 \right\}.$$

Suppose that $\overline{w} = \overline{(w_{ij})} \in E_x$ satisfies $v_D(w_{ll}) = 0$. Define $v = (v_{ij}) \in R$ by $v_{ll} := w_{ll}^{-1}$ and $v_{ij} := 0$ otherwise. Then $\overline{v} \in E_x$ and one easily checks that $vw - 1 \in Rx$ and $wv - 1 \in Rx$, that is $\overline{w} \cdot \overline{v} = \overline{v} \cdot \overline{w} = \overline{1}$. Conversely, let $\overline{w} = \overline{(w_{ij})} \in E_x^\times$. Then there is $\overline{v} = \overline{(v_{ij})} \in E_x$ with $\overline{w} \cdot \overline{v} = \overline{v} \cdot \overline{w} = \overline{1}$. In particular, we have

$$(vw - 1)_{ll} = \sum_{k=1}^{l-1} v_{lk} w_{kl} + v_{ll} w_{ll} - 1 \in \pi_D^h \Delta.$$

But $v_D(w_{kl}) \geq h$ for $k = 1, \dots, l-1$, so we must have $v_D(v_{ll} w_{ll} - 1) \geq h$. This forces $v_D(v_{ll}) = v_D(w_{ll}) = 0$, and the claim on $E_x^\times$ is proven. We obtain

$$E_x \setminus E_x^\times = \left\{ \overline{w} = \overline{(w_{ij})} \in E_x \,\middle|\, v_D(w_{ll}) \geq 1 \right\}.$$

It is easily seen that this is a two-sided ideal of E_x, so E_x is a local ring and therefore $M_h = R/Rx$ is indecomposable.

It is clear by Lemma 3.14 (iii) that M_h and $M_{h'}$ are not isomorphic if $h \neq h'$. Now suppose that M is an indecomposable finitely generated torsion R-module. By [Rei03, Theorem 17.3], R is a maximal Z-order in $\mathrm{Mat}_l(D)$, so by Proposition 3.12 we have $M \cong R/Rx$ for some $x \in R \cap \mathrm{Mat}_l(D)^\times$. Let $0 \leq a_1 \leq \dots \leq a_l < \infty$ be the integers from Proposition 3.13 associated to x; note that $a_l < \infty$ as $x \in \mathrm{Mat}_l(D)^\times$. Since M is indecomposable, Lemma 3.14 (ii) forces $a_1 = \dots = a_{l-1} = 0$. Then by part (iii) of the same lemma, we have $M \cong M_{a_l}$. □

3.3.3 Maximal Orders over Complete Discrete Valuation Rings

Let again Z be a complete discrete valuation ring with normalised valuation v and fraction field K. Let A be a central simple K-algebra and let R be a maximal Z-order in A. We generalise the statements above from $\mathrm{Mat}_l(\Delta)$ to R.

Construction 3.16. We use notation as in Section 1.4: There are a unique $l \in \mathbb{Z}_{\geq 1}$ and a unique division ring D with centre K such that $A \cong \mathrm{Mat}_l(D)$. Let Δ be the unique maximal Z-order in D. We may choose the isomorphism $A \cong \mathrm{Mat}_l(D)$ in such a way that it carries R onto $\mathrm{Mat}_l(\Delta)$, giving us a ring isomorphism $\varphi\colon R \xrightarrow{\sim} \mathrm{Mat}_l(\Delta)$.

Let $x \in R$. By Proposition 3.13 we can uniquely associate integers $0 \leq a_1 \leq \dots \leq a_l \leq \infty$ to $\varphi(x)$. These integers are independent of the choice of ring isomorphism $R \cong \mathrm{Mat}_l(\Delta)$: If $\psi\colon R \xrightarrow{\sim} \mathrm{Mat}_l(\Delta)$ is another such isomorphism, then $\psi \circ \varphi^{-1}$ is an automorphism of $\mathrm{Mat}_l(\Delta)$, so is given by conjugation by an element of $\mathrm{GL}_l(\Delta)$. It follows that $\varphi(x)$ and $\psi(x) = \psi \circ \varphi^{-1}(\varphi(x))$ have the same associated integers. Thus, we can uniquely associate integers $0 \leq a_1 \leq \dots \leq a_l \leq \infty$ to x in this way. Call these the *invariants* of x.

Corollary 3.17. *The following hold:*

(i) Let $x, y \in R$ and let $0 \leq a_1 \leq \cdots \leq a_l \leq \infty$ and $0 \leq b_1 \leq \cdots \leq b_l \leq \infty$ be the invariants of x and y, respectively. Then $R/Rx \cong R/Ry$ as R-modules if and only if $a_i = b_i$ for all i.

(ii) For each $h \in \mathbb{Z}_{\geq 1}$ let $x^{(h)} \in R$ be an element whose invariants are $0, \ldots, 0, h$. Then the modules $R/Rx^{(h)}$, $h \in \mathbb{Z}_{\geq 1}$, form a full set of representatives for the isomorphism classes of indecomposable finitely generated torsion R-modules.

Proof. After choosing an isomorphism $\varphi\colon R \xrightarrow{\sim} \mathrm{Mat}_l(\Delta)$ as in Construction 3.16 to regard R-modules as $\mathrm{Mat}_l(\Delta)$-modules, this follows from the corresponding statements in Propositions 3.12 and 3.15. □

Definition 3.18. Let M be a finitely generated torsion R-module. Then by the Krull–Schmidt Theorem and by Corollary 3.17 we may uniquely associate to M a list of elements of $\mathbb{Z}_{\geq 1}$, namely the labels of its indecomposable summands. Call these the *elementary invariants* of M.

By Proposition 3.12, every finitely generated torsion R-module can be decomposed into a direct sum of modules of the form R/Rx for $x \in R \cap A^\times$. From this decomposition, one can easily read off the elementary invariants as follows:

Lemma 3.19. *Let $x \in R \cap A^\times$. Then the elementary invariants of R/Rx are the nonzero invariants of x.*

Proof. We may assume that $R = \mathrm{Mat}_l(\Delta)$ where l and Δ are as in Construction 3.16. The claim follows immediately from Lemma 3.14 (ii): If

$$a_1 = \cdots = a_{t-1} = 0 < a_t \leq \cdots \leq a_l < \infty,$$

where $t \geq 1$, are the invariants of x, then

$$R/Rx \cong M_{a_t} \oplus \cdots \oplus M_{a_l}.$$

Hence, the elementary invariants of R/Rx are $a_t, \ldots, a_l$. □

Remark 3.20. Elementary invariants are related to elementary divisors as follows. Suppose that T is a PID and let M be a finitely generated torsion Z-module. Then we have

$$M \cong T/\mathfrak{p}_1^{r_{1,1}} \oplus \cdots \oplus T/\mathfrak{p}_1^{r_{1,t_1}} \oplus \cdots \oplus T/\mathfrak{p}_k^{r_{k,1}} \oplus \cdots \oplus T/\mathfrak{p}_k^{r_{k,t_k}}$$

for distinct maximal ideals $\mathfrak{p}_j = (p_j)$ of T and positive integers $r_{j,n}$. The elementary divisors of M are

$$p_1^{r_{1,1}}, \ldots, p_1^{r_{1,t_1}}, \ldots, p_k^{r_{k,1}}, \ldots, p_k^{r_{k,t_k}}.$$

Let $j \in \{1, \dots, k\}$. Then $\widehat{T}_{\mathfrak{p}_j}$ is a complete discrete valuation ring and we have

$$\widehat{M_{\mathfrak{p}_j}} \cong \widehat{T}_{\mathfrak{p}_j}/p_j^{r_{j,1}} \oplus \cdots \oplus \widehat{T}_{\mathfrak{p}_j}/p_j^{r_{j,t_j}}$$

as $\widehat{T}_{\mathfrak{p}_j}$-modules. In the above language, with $Z = R = \widehat{T}_{\mathfrak{p}_j}$ and $A = K$ the fraction field of $\widehat{T}_{\mathfrak{p}_j}$, Lemma 3.19 gives that the elementary invariants of $\widehat{M_{\mathfrak{p}_j}}$ are $r_{j,1}, \dots, r_{j,t_j}$. So knowing the elementary invariants of all $\widehat{M_{\mathfrak{p}_j}}$ is equivalent to knowing the elementary divisors of M.

3.4 The Connecting Homomorphism of Torsion of a Short Exact Sequence

This section is concerned with the map constructed below, which will come into play later on in the proof of Theorem 9.42 when investigating the average torsion of ray class groups. It has already appeared in [PS17, Section 2.1] and [BP25, Section 4.2].

Construction 3.21. Let Z be a commutative ring and let R be a Z-algebra. Let $a \in Z$. Let M and N be R-modules. Let $\Theta \in \operatorname{Ext}^1_R(M, N)$ and write

$$\Theta\colon \qquad \begin{tikzcd} 0 \arrow[r] & N \arrow[r, "\alpha"] & L \arrow[r, "\beta"] & M \arrow[r] & 0. \end{tikzcd}$$

Then we have a commutative diagram of R-modules with exact rows

$$\begin{tikzcd} 0 \arrow[r] & N \arrow[r, "\alpha"] \arrow[d, "\cdot a"] & L \arrow[r, "\beta"] \arrow[d, "\cdot a"] & M \arrow[r] \arrow[d, "\cdot a"] & 0 \\ 0 \arrow[r] & N \arrow[r, "\alpha"] & L \arrow[r, "\beta"] & M \arrow[r] & 0, \end{tikzcd}$$

from which the snake lemma yields a homomorphism

$$\delta_a(\Theta) := \delta_{a,R}(\Theta) := \delta_{a,R}^{M,N}(\Theta)\colon M[a] \to N/aN$$

which is defined as follows: Let $m \in M[a]$. Pick $l \in L$ with $\beta(l) = m$. Then $al \in \ker(\beta) = \operatorname{im}(\alpha)$, so we may pick $n \in N$ with $\alpha(n) = al$. Then $\delta_a(\Theta)(m) = \overline{n}$. (This is well-defined by the snake lemma.)

Naturality of the connecting homomorphism in the snake lemma (cf. [HS97, page 100]) implies that $\delta_a(\Theta)$ does not depend on the chosen representative for Θ, so that we get a map

$$\delta_a\colon \operatorname{Ext}^1_R(M, N) \to \operatorname{Hom}_R(M[a], N/aN),\ \Theta \mapsto \delta_a(\Theta).$$

We are interested in the question when δ_a is surjective. First statements in this direction are [PS17, Proposition 2.7] and [BP25, Lemma 4.12]. Below, we vastly generalise these results, working with new ideas. We will give a characterisation of surjectivity for maximal orders over Dedekind domains. We first collect some general properties and auxiliary results for our endeavour.

Proposition 3.22. *Let Z be a commutative ring and let R be a Z-algebra. Let $a \in Z$. Let M and N be R-modules. The map δ_a is a group homomorphism which is natural in M and N.*

Proof. It is a straightforward computation to show that δ_a is a group homomorphism. Naturality follows from the explicit description of the induced maps on extensions in Construction 2.7 and from naturality of the connecting homomorphism in the snake lemma. □

In particular, δ_a is compatible with direct sums, so for example we have a commutative diagram

$$\begin{tikzcd}
\operatorname{Ext}^1_R(M, N \oplus N') \arrow[r, "\delta_a^{M,N\oplus N'}"] \arrow[d, "\wr"] & \operatorname{Hom}_R(M[a], (N \oplus N')/a(N \oplus N')) \arrow[d, "\wr"] \\
\operatorname{Ext}^1_R(M, N) \oplus \operatorname{Ext}^1_R(M, N') \arrow[r, "{(\delta_a^{M,N}, \delta_a^{M,N'})}"'] & \operatorname{Hom}_R(M[a], N/aN) \oplus \operatorname{Hom}_R(M[a], N'/aN').
\end{tikzcd}$$

Moreover, δ_a is compatible with flat base change.

Lemma 3.23. *Let Z be a commutative ring and let R be a Z-algebra. Let S be another Z-algebra and let $S \to R$ be a Z-algebra homomorphism that is flat as a ring homomorphism. Let $a \in Z$ and let M and N be S-modules. Then the diagram*

$$\begin{tikzcd}
\operatorname{Ext}^1_S(M, N) \arrow[r, "\delta_{a,S}"] \arrow[d, "R\otimes_S -"'] & \operatorname{Hom}_S(M[a], N/aN) \arrow[d, "R\otimes_S -"] \\
\operatorname{Ext}^1_R(R \otimes_S M, R \otimes_S N) \arrow[r, "\delta_{a,R}"'] & \operatorname{Hom}_R(R \otimes_S M[a], R \otimes_S N/aN)
\end{tikzcd}$$

commutes.

Proof. This again follows from naturality of the connecting homomorphism in the snake lemma. □

We will make use of the following generalisation of [Rot09, Example 7.23 (i)].

Lemma 3.24. *Let R be a ring. Let $x \in R$ be right regular (i.e. the map $R \to R$, $r \mapsto rx$ is injective). Let N be an R-module. Then there is an isomorphism of abelian groups*

$$N/xN \xrightarrow{\sim} \operatorname{Ext}^1_R(R/Rx, N).$$

For $n \in N$, the isomorphism maps $\overline{n} \in N/xN$ to the extension

$$0 \longrightarrow N \xrightarrow{\iota_N} N \oplus R/\{\,(rn, -rx) \,|\, r \in R\,\} \xrightarrow{\pi} R/Rx \longrightarrow 0$$

where $\iota_N(n) = \overline{(n,0)}$ and $\pi(\overline{(n,r)}) = \overline{r}$.

Proof. By assumption, we have a short exact sequence of R-modules

$$0 \longrightarrow R \xrightarrow{\cdot x} R \longrightarrow R/Rx \longrightarrow 0.$$

Applying the functor $\operatorname{Ext}_R(-,N)$ yields an exact sequence

$$0 \longrightarrow \operatorname{Hom}_R(R/Rx,N) \longrightarrow \operatorname{Hom}_R(R,N) \overset{(\cdot x)^*}{\longrightarrow} \operatorname{Hom}_R(R,N) \overset{\omega}{\longrightarrow} \operatorname{Ext}^1_R(R/Rx,N) \longrightarrow 0.$$

By [ML63, page 73] it holds that if $\varphi \in \operatorname{Hom}_R(R,N)$, then $\omega(\varphi)$ is given by the extension

$$0 \longrightarrow N \xrightarrow{\iota_N} N \oplus R/\{\,(\varphi(r),-rx)\,|\,r \in R\,\} \xrightarrow{\pi} R/Rx \longrightarrow 0$$

where $\iota_N(n) = \overline{(n,0)}$ and $\pi(\overline{(n,r)}) = \overline{r}$. Now under the isomorphism of abelian groups

$$N \xrightarrow{\sim} \operatorname{Hom}_R(R,N), \quad \begin{array}{l} n \mapsto (r \mapsto rn), \\ \varphi(1) \leftarrow\!\shortmid \varphi, \end{array}$$

we get an exact sequence

$$0 \longrightarrow \operatorname{Hom}_R(R/Rx,N) \longrightarrow N \xrightarrow{x\cdot} N \xrightarrow{\omega'} \operatorname{Ext}^1_R(R/Rx,N) \longrightarrow 0$$

where $\omega'(n)$ is given by the extension

$$0 \longrightarrow N \xrightarrow{\iota_N} N \oplus R/\{\,(rn,-rx)\,|\,r \in R\,\} \xrightarrow{\pi} R/Rx \longrightarrow 0.$$

The claim follows. □

Lemma 3.25. *Let Z be a commutative ring and let R be a Z-algebra. Let $a \in Z$ and let $x \in R$ be right regular. Let N be an R-module. Denote by*

$$\xi\colon N \to N/xN \xrightarrow{\sim} \operatorname{Ext}^1_R(R/Rx,N)$$

the surjective homomorphism of abelian groups which is the concatenation of the natural projection with the isomorphism from Lemma 3.24. Then for $n \in N$ and $\overline{r} \in R/Rx[a]$ it holds that

$$(\delta_a^{R/Rx,N} \circ \xi)(n)(\overline{r}) = \overline{r'n}$$

where $r' \in R$ is the unique element such that $ar = r'x$.

Proof. This is an easy calculation. In the sequence $\xi(n)$, $\overline{(0,r)}$ is a preimage of $\overline{r}$. We have

$$a \cdot \overline{(0,r)} = \overline{(0,ar)} = \overline{(0,ar)} + \overline{(r'n,-r'x)} = \overline{(r'n,0)} = \iota_N(r'n)$$

from which the claim follows by definition of δ_a. □

The explicit description of $\delta_a^{R/Rx,N} \circ \xi$ and the fact that $\delta_a^{R/Rx,N}$ is surjective if and only if $\delta_a^{R/Rx,N} \circ \xi$ is surjective will be important ingredients in the proof of the main theorem of this section, which is the following.

Theorem 3.26. *Let Z be a Dedekind domain with fraction field K, let A be a separable K-algebra and let R be a maximal Z-order in A. Let $a \in Z$ and let M and N be finitely generated R-modules. Use the notation from Section 1.4. Then the following are equivalent:*

(i) $\delta_{a,R}^{M,N}$ is surjective.

(ii) For all $i \in \{1, \dots, c\}$ and all maximal ideals $\mathfrak{p}$ of Z_i we have that either all elementary invariants of $(\widehat{M_{\text{tors}}})_{i,\mathfrak{p}}$ or all elementary invariants of $(\widehat{N_{\text{tors}}})_{i,\mathfrak{p}}$ are $\geq v_{i,\mathfrak{p}}(a) e_{i,\mathfrak{p}}$.

Proof. We split up the proof into six steps.

Step 1: Reduce to the case M torsion. If M is Z-torsionfree, then the domain and codomain of $\delta_{a,R}^{M,N}$ are both zero, so $\delta_{a,R}^{M,N}$ is clearly surjective. Thus by compatibility of δ_a with direct sums and by Proposition 3.9, we may from now on assume that M is a torsion module.

Step 2: Reduce to the case Z complete discrete valuation ring, A central simple. By naturality of δ_a we have that $\delta_{a,R}^{M,N}$ is surjective if and only if $\delta_{a,R_i}^{M_i,N_i}$ is surjective for all $i \in \{1, \dots, c\}$. Let $i \in \{1, \dots, c\}$. Then by compatibility of δ_a with direct sums and by Lemma 3.3 we have that $\delta_{a,R_i}^{M_i,N_i}$ is surjective if and only if $\delta_{a,R_i}^{M_i[\mathfrak{p}^\infty],N_i}$ is surjective for all maximal ideals $\mathfrak{p}$ of Z_i. Let $\mathfrak{p}$ be a maximal ideal of Z_i. Then by [Wei94, Lemma 3.3.6], the Z_i-modules $\operatorname{Ext}^1_{R_i}(M_i[\mathfrak{p}^\infty], N_i)$ and $\operatorname{Hom}_{R_i}(M_i[\mathfrak{p}^\infty][a], N_i/aN_i)$ are annihilated by a power of $\mathfrak{p}$. Hence, by Lemmas 3.3 and 3.23 and Proposition 2.1 it holds that $\delta_{a,R_i}^{M_i[\mathfrak{p}^\infty],N_i}$ is surjective if and only if $\delta_{a,\widehat{R}_{i,\mathfrak{p}}}^{\widehat{M}_{i,\mathfrak{p}},\widehat{N}_{i,\mathfrak{p}}}$ is surjective.

This means that to prove the equivalence we may assume that Z is a complete discrete valuation ring and A is a central simple K-algebra. We denote by v the valuation on Z, by π a uniformiser in Z and by $\mathfrak{p} = (\pi)$ the maximal ideal of Z. We may assume that $a = \pi^{v(a)}$. We have $A \cong \operatorname{Mat}_l(D)$ for a unique integer $l \in \mathbb{Z}_{\geq 1}$ and division ring D with centre K. The valuation v extends uniquely to D and we denote by $v_D = e(D/K)v$ the associated normalised valuation. Write $e := e(D/K)$. Denote by Δ the unique maximal Z-order in D. Let $\pi_D \in \Delta$ with $v_D(\pi_D) = 1$. We choose the isomorphism $A \cong \operatorname{Mat}_l(D)$ such that it carries R onto $\operatorname{Mat}_l(\Delta)$. So from now on we may assume that $A = \operatorname{Mat}_l(D)$ and $R = \operatorname{Mat}_l(\Delta)$.

Step 3: Reduce to the case N torsion. We show that $\delta_a^{M,N}$ is surjective if N is torsionfree. For this, by Proposition 3.15 we may assume that $M = M_h = R/Rx$ for some $h \in \mathbb{Z}_{\geq 1}$, where $x = \operatorname{diag}(1,\dots,1,\pi_D^h)$. Then by Lemma 3.25, $\delta_a^{M,N}$ is surjective if and only if the map

$$\widetilde{\delta}\colon N \to \operatorname{Hom}_R(R/Rx[\pi^{v(a)}], N/\pi^{v(a)}N),\ n \mapsto (\overline{r} \mapsto \overline{r'n}),$$

is surjective, where $r' \in R$ is the unique element such that $\pi^{v(a)}r = r'x$. By [Rei03, Theorem 17.3], every left ideal of R is principal, so there is $y \in R$ with $Rx \leq Ry \leq R$ such that $R/Rx[\pi^{v(a)}] = Ry/Rx = \langle \overline{y} \rangle$. Let $s \in R$ such that $x = sy$. Note that since $x \in A^\times$ we also have $y \in A^\times$ and $s \in A^\times$. It holds that

$$\pi^{v(a)}y = \pi^{v(a)}yx^{-1}x = \pi^{v(a)}s^{-1}x$$

where $\pi^{v(a)}s^{-1} = \pi^{v(a)}yx^{-1} \in R$ as $\pi^{v(a)}y \in Rx$. So $\widetilde{\delta}(n)(\overline{y}) = \overline{\pi^{v(a)}s^{-1}n}$. Now let $\varphi \in \operatorname{Hom}_R(R/Rx[\pi^{v(a)}], N/\pi^{v(a)}N)$ and suppose $\varphi(\overline{y}) = \overline{n_\varphi}$ where $n_\varphi \in N$. We need to find $n \in N$ such that $\overline{\pi^{v(a)}s^{-1}n} = \overline{n_\varphi} \in N/\pi^{v(a)}N$. We have

$$0 = \varphi(\overline{x}) = s\varphi(\overline{y}) = \overline{sn_\varphi} \in N/\pi^{v(a)}N,$$

so there is $n \in N$ with $sn_\varphi = \pi^{v(a)}n$. Since N is torsionfree, Lemma 3.1 shows that the natural map

$$\iota\colon N \hookrightarrow K \otimes_Z N = A \otimes_R N$$

provides an embedding of N into an A-module. It holds that

$$s\iota(n_\varphi) = \iota(sn_\varphi) = \iota(\pi^{v(a)}n) = \pi^{v(a)}\iota(n)$$

which implies

$$\iota(n_\varphi) = s^{-1}s\iota(n_\varphi) = s^{-1}\pi^{v(a)}\iota(n) = \iota(\pi^{v(a)}s^{-1}n)$$

as $\pi^{v(a)}s^{-1} \in R$. Since ι is injective, it follows that $n_\varphi = \pi^{v(a)}s^{-1}n$. Hence, $\delta_a^{M,N}$ is surjective if N is torsionfree. So from now on we may assume that N is a torsion module.

Step 4: Reduce to the case M and N indecomposable and rewrite $\widetilde{\delta}$. To prove the equivalence of (i) and (ii), by Proposition 3.15 it suffices to consider the case $M = M_h = R/Rx$ and $N = N_{h'} = R/Rz$ for some $h, h' \in \mathbb{Z}_{\geq 1}$, where $x = \operatorname{diag}(1,\dots,1,\pi_D^h)$ and $z = \operatorname{diag}(1,\dots,1,\pi_D^{h'})$. We use the notation y, s, $\widetilde{\delta}$ from above; surjectivity of $\delta_a^{M,N}$ is equivalent to surjectivity of $\widetilde{\delta}$. Note that by definition of e, there are units $u', u'' \in \Delta^\times$ such that $\pi^{v(a)} = \pi_D^{v(a)e}u'$ and $\pi^{v(a)} = u''\pi_D^{v(a)e}$. It is then easy to see that we may take

$$y = \operatorname{diag}(1,\dots,1,\pi_D^{\max(h-v(a)e,0)}).$$

Accordingly,

$$s = xy^{-1} = \operatorname{diag}(1,\dots,1,\pi_D^{\min(v(a)e,h)})$$

and

$$\pi^{v(a)}s^{-1} = u''\pi_D^{v(a)e}s^{-1} = u''\operatorname{diag}(\pi_D^{v(a)e},\dots,\pi_D^{v(a)e},\pi_D^{v(a)e-\min(v(a)e,h)}).$$

Moreover, we have $\pi^{v(a)}(R/Rz) = (\pi^{v(a)}R + Rz)/Rz$, so

$$N/\pi^{v(a)}N = \frac{R/Rz}{(\pi^{v(a)}R + Rz)/Rz} \cong \frac{R}{\pi^{v(a)}R + Rz} = \frac{R}{R\pi_D^{v(a)e} + Rz}.$$

Now

$$R\pi_D^{v(a)e} + Rz = \mathrm{Mat}_l(\Delta)\pi_D^{v(a)e} + \mathrm{Mat}_l(\Delta)z = \mathrm{Mat}_l(\Delta)z'$$

where

$$z' = \mathrm{diag}(1, \dots, 1, \pi_D^{\min(v(a)e, h')}).$$

Notice also that we have an isomorphism $R/Rs \xrightarrow{\sim} Ry/Rx$, $\overline{r} \mapsto \overline{ry}$. With this, statement (i) is equivalent to surjectivity of the map

$$\widetilde{\delta}\colon R/Rz \to \mathrm{Hom}_R(R/Rs, R/Rz'),\ \overline{r} \mapsto (\overline{1} \mapsto \pi^{v(a)}s^{-1}\overline{r}).$$

Step 5: Via $\widetilde{\delta}$, give explicit characterisation of (i) in terms of elements of Δ. Our next aim is to explicitly characterise surjectivity of $\widetilde{\delta}$. To do so, we analyse the space $\mathrm{Hom}_R(R/Rs, R/Rz')$. There is a bijection

$$\left\{ \overline{w} \in R/Rz' \,\middle|\, \overline{sw} = 0 \right\} \to \mathrm{Hom}_R(R/Rs, R/Rz'),\ \overline{w} \mapsto (\overline{1} \mapsto \overline{w}).$$

It is easy to see from the explicit descriptions of s and z' that for $w = (w_{ij}) \in R = \mathrm{Mat}_l(\Delta)$ we have $sw \in Rz'$ if and only if

$$\begin{aligned} v_D(w_{il}) &\geq \min(v(a)e, h') && \text{for } i = 1, \dots, l-1, \\ v_D(w_{ll}) &\geq \min(v(a)e, h') - \min(v(a)e, h). \end{aligned} \tag{3.27}$$

The element in $\mathrm{Hom}_R(R/Rs, R/Rz')$ defined by such a w is in the image of $\widetilde{\delta}$ if and only if there is $r = (r_{ij}) \in R = \mathrm{Mat}_l(\Delta)$ with $\pi^{v(a)}s^{-1}\overline{r} = \overline{w} \in R/Rz'$. Now

$$\pi^{v(a)}s^{-1}r - w = u'' \begin{pmatrix} \pi_D^{v(a)e}r_{11} - w_{11} & \dots & \pi_D^{v(a)e}r_{1l} - w_{1l} \\ \vdots & & \vdots \\ \pi_D^{v(a)e}r_{l-1,1} - w_{l-1,1} & \dots & \pi_D^{v(a)e}r_{l-1,l} - w_{l-1,l} \\ \pi_D^{v(a)e-\min(v(a)e,h)}r_{l1} - w_{l1} & \dots & \pi_D^{v(a)e-\min(v(a)e,h)}r_{ll} - w_{ll} \end{pmatrix},$$

so there is such an r if and only if there are $r_{ij} \in \Delta$ with

$$\begin{aligned} v_D(\pi_D^{v(a)e}r_{il} - w_{il}) &\geq \min(v(a)e, h') \qquad \text{for } i = 1, \dots, l-1, \\ v_D(\pi_D^{v(a)e-\min(v(a)e,h)}r_{ll} - w_{ll}) &\geq \min(v(a)e, h'). \end{aligned} \tag{3.28}$$

Note that by the properties of w we may always choose $r_{il} = 0$ for $i = 1, \dots, l-1$ to satisfy the first set of equations. In conclusion, statement (i) is equivalent to the following statement: For any $w_{ll} \in \Delta$ satisfying (3.27) there is $r_{ll} \in \Delta$ such that (3.28) holds.

Step 6: Conclude using step 5. We now finally prove the equivalence of (i) and (ii). Suppose that (ii) holds, that is, either $h \geq v(a)e$ or $h' \geq v(a)e$. Suppose first that $h \geq v(a)e$. If w_{ll} satisfies (3.27) we may simply take $r_{ll} = w_{ll}$. Now suppose that $h' \geq v(a)e$. By the first case, we may assume that $h < v(a)e$. Then if w_{ll} satisfies (3.27), this means $v_D(w_{ll}) \geq v(a)e - h$, so there is $\widetilde{w_{ll}} \in \Delta$ such that $w_{ll} = \pi_D^{v(a)e-h}\widetilde{w_{ll}}$. Now clearly $r_{ll} = \widetilde{w_{ll}}$ satisfies (3.28).

Conversely, suppose that (i) holds. Assume that statement (ii) fails, that is, $h, h' < v(a)e$. Consider $w_{ll} := \pi_D^{\max(h'-h,0)} \in \Delta$. This clearly satisfies (3.27) by our assumption, so there is $r_{ll} \in \Delta$ such that (3.28) holds. Note that

$$v_D(\pi_D^{v(a)e-h} r_{ll} - \pi_D^{\max(h'-h,0)}) = \max(h' - h, 0),$$

which shows

$$h' > \max(h' - h, 0) = v_D(\pi_D^{v(a)e-h} r_{ll} - w_{ll}) \geq \min(v(a)e, h') = h',$$

a contradiction. So (ii) must hold. □

Corollary 3.29. *Let Z be a Dedekind domain with fraction field K, let A be a separable K-algebra and let R be a maximal Z-order in A. Let $a \in Z$. Use the notation from Section 1.4. If $v_{i,\mathfrak{p}}(a) \leq 1$ and $e_{i,\mathfrak{p}} = 1$ for all $i \in \{1, \dots, c\}$ and all maximal ideals $\mathfrak{p}$ of Z_i, then $\delta_{a,R}^{M,N}$ is surjective for all finitely generated R-modules M and N.*

Note that for $a \in Z$ we have $v_{i,\mathfrak{p}}(a) \leq 1$ for all $i \in \{1, \dots, c\}$ and all maximal ideals $\mathfrak{p}$ of Z_i if and only if a has no square prime divisors in Z and Z_i/Z is unramified at all prime divisors of a in Z for all $i \in \{1, \dots, c\}$. Notice also that if A happens to be commutative, then $K_i = A_i$ for all $i \in \{1, \dots, c\}$, so that $e_{i,\mathfrak{p}} = 1$ for all $i \in \{1, \dots, c\}$ and all maximal ideals $\mathfrak{p}$ of Z_i.

We close this section by recording the following special case of Theorem 3.26 for PIDs, taking into account Remark 3.20.

Corollary 3.30. *Suppose that Z is a PID. Let $a \in Z$ and let M and N be finitely generated Z-modules. Then the following are equivalent:*

(i) $\delta_{a,Z}^{M,N}$ is surjective.

(ii) For all primes $p \mid a$, either the least power with which p occurs as an elementary divisor of M is $\geq v_p(a)$ or the least power with which p occurs as an elementary divisor of N is $\geq v_p(a)$ (if there is no such power, we take it to be ∞).

3.5 Cardinality Results for Ext Groups over Maximal Orders

We prove some results on the cardinality of certain Ext groups over maximal orders over Dedekind domains that will be needed later on.

Lemma 3.31. *Let Z be a Dedekind domain such that $Z/\mathfrak{p}$ is finite for every maximal ideal $\mathfrak{p}$ of Z. Let R be a Z-algebra that is finitely generated as a Z-module. Let M and N be finitely generated R-modules and suppose that M or N is a Z-torsion module. Then $\operatorname{Ext}_R^n(M,N)$ is finite for all $n \in \mathbb{Z}_{\geq 0}$.*

Proof. Let $n \in \mathbb{Z}_{\geq 0}$. By [Rei03, Theorem 2.34], $\operatorname{Ext}_R^n(M,N)$ is a finitely generated Z-module. But it is also a Z-torsion module by assumption and [Wei94, Lemma 3.3.6]. Hence, there are maximal ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ of Z and positive integers $r_1, \ldots, r_k$ such that

$$\operatorname{Ext}_R^n(M,N) \cong Z/\mathfrak{p}_1^{r_1} \oplus \cdots \oplus Z/\mathfrak{p}_k^{r_k}.$$

By assumption, $|Z/\mathfrak{p}_i^{r_i}| = |Z/\mathfrak{p}_i|^{r_i}$ is finite for all i, so $\operatorname{Ext}_R^n(M,N)$ is finite. □

Proposition 3.32. *Let Z be a Dedekind domain with fraction field K, let A be a separable K-algebra and let R be a maximal Z-order in A. Let M be a finitely generated R-module that is a Z-torsion module and let N be a finite R-module. Then*

$$|\operatorname{Hom}_R(M,N)| = \left|\operatorname{Ext}_R^1(M,N)\right|.$$

Proof. By decomposing A into its simple components and using [Rei03, Theorem 10.5], we can assume that A is simple. Moreover, by replacing K with the centre of A and Z with its integral closure in the centre of A, we may assume that A is a central simple K-algebra. By Lemma 3.3, we may assume that M is annihilated by the power of some maximal ideal $\mathfrak{p}$ of Z. Then by [Wei94, Lemma 3.3.6], the Z-module $\operatorname{Ext}_R^n(M,N)$ is also annihilated by a power of $\mathfrak{p}$, for all $n \in \mathbb{Z}_{\geq 0}$. It follows that for all $n \in \mathbb{Z}_{\geq 0}$, $\operatorname{Ext}_R^n(M,N)$ is naturally a $\widehat{Z}_{\mathfrak{p}}$-module and we have

$$\operatorname{Ext}_R^n(M,N) \cong \widehat{Z}_{\mathfrak{p}} \otimes_Z \operatorname{Ext}_R^n(M,N) \cong \operatorname{Ext}^n_{\widehat{Z}_{\mathfrak{p}} \otimes_Z R}(\widehat{Z}_{\mathfrak{p}} \otimes_Z M, \widehat{Z}_{\mathfrak{p}} \otimes_Z N)$$

as $\widehat{Z}_{\mathfrak{p}}$-modules by Lemma 3.3 and Proposition 2.1. Now letting $K_{\mathfrak{p}}$ denote the fraction field of $\widehat{Z}_{\mathfrak{p}}$, we have that $K_{\mathfrak{p}} \otimes_K A$ is a central simple $K_{\mathfrak{p}}$-algebra and $\widehat{Z}_{\mathfrak{p}} \otimes_Z R$ is a maximal $\widehat{Z}_{\mathfrak{p}}$-order in $K_{\mathfrak{p}} \otimes_K A$. Hence, we are reduced to proving the claim in the case where Z is a complete discrete valuation ring and A is a central simple K-algebra, which we are going to assume in the following.

By Proposition 3.12 we may further assume that $M = R/Rx$ for some $x \in R \cap A^{\times}$. In this case, there is a short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & R \arrow[r, "\cdot x"] & R \arrow[r] & R/Rx \arrow[r] & 0 \end{tikzcd}$$

of R-modules. Applying the functor $\operatorname{Ext}_R(-,N)$ yields an exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \operatorname{Hom}_R(R/Rx,N) \arrow[r] & N \arrow[r] & N \arrow[r] & \operatorname{Ext}_R^1(R/Rx,N) \arrow[r] & 0 \end{tikzcd}$$

of abelian groups. Since N is finite, it follows that $|\operatorname{Hom}_R(R/Rx,N)| = \left|\operatorname{Ext}_R^1(R/Rx,N)\right|$ which finishes the proof. □

Remark 3.33. The statement above is false without the assumption that M be a torsion module: For any $n \in \mathbb{Z}$ we have $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/n) = \mathbb{Z}/n$, but $\mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/n) = 0$. Also, the statement is false without the assumption that N be finite: For any $n \in \mathbb{Z}$ we have $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n, \mathbb{Z}) = 0$, but $\mathrm{Ext}_{\mathbb{Z}}(\mathbb{Z}/n, \mathbb{Z}) = \mathbb{Z}/n$.

For the proof of the final statement below, we follow the proof of [Wei94, Lemma 3.3.1], which is the corresponding statement for Ext groups over $\mathbb{Z}$.

Proposition 3.34. *Let Z be a Dedekind domain with fraction field K, let A be a separable K-algebra and let R be a maximal Z-order in A. Let M and N be R-modules. Then $\mathrm{Ext}^n_R(M, N) = 0$ for all $n \in \mathbb{Z}_{\geq 2}$.*

Proof. Since ${}_R\mathsf{Mod}$ has enough injectives, there is an injective R-module I and an injective R-module homomorphism $N \hookrightarrow I$. By [Rei03, Theorem 21.4], the ring R is hereditary. Hence, by [Lam99, Theorem 3.22], the quotient module I/N is injective. Let $n \in \mathbb{Z}_{\geq 2}$. Applying the functor $\mathrm{Ext}_R(M, -)$ to the short exact sequence

$$0 \longrightarrow N \longrightarrow I \longrightarrow I/N \longrightarrow 0$$

yields an exact sequence

$$\mathrm{Ext}^{n-1}_R(M, I/N) \longrightarrow \mathrm{Ext}^n_R(M, N) \longrightarrow \mathrm{Ext}^n_R(M, I).$$

From injectivity of I and I/N it follows that $\mathrm{Ext}^n_R(M, N) = 0$. □

4 Locally Compact Modules and Pontryagin Duality

Pontryagin duality is an incredibly useful tool when studying locally compact Hausdorff abelian groups. In our later considerations, we will find ourselves placed in two situations, in which we want to apply duality to locally compact groups that also have a module structure that we need to respect:

(1) As we will show, the Arakelov ray class group and related groups that we are interested in are compact topological groups with a continuous $\mathbb{Z}G$-module structure for some finite group G. To avoid having to worry about the topology, we prefer to work with the Pontryagin duals of these modules, which are discrete.

(2) As explained in the introduction, for our heuristic we will consider the good components of the above duals, which are obtained from the latter by tensoring them with a certain $\mathbb{Z}_{(S)}$-order R. In order to be able to relate the discrete R-modules thus obtained to the original compact $\mathbb{Z}G$-modules, we then want to dualise back.

Hence, it is necessary to discuss Pontryagin duality in the framework of locally compact modules over a $\mathbb{Z}_{(S)}$-order. This is the purpose of the present chapter. Since it is no additional work, in the first two subsections we will mostly work in the more general setting of locally compact modules over a locally compact topological ring. In Section 4.1 we review key aspects of the classical duality theory and show that many of its results are naturally compatible with continuous module structures. In Section 4.2 we discuss duality for exact sequences. In the last subsection we specialise to locally compact modules over a $\mathbb{Z}_{(S)}$-order and establish some useful results specific to this context. As a basis for this, we give an explicit description of the Pontryagin dual of $\mathbb{Z}_{(S)}$.

4.1 The Duality Theorem for LCA Modules

This section is mostly based on the classical theory of Pontryagin duality for locally compact Hausdorff abelian groups as for example laid out in [HR79] or [Mor77], and on the paper [Flo79], which discusses key aspects of duality for locally compact modules over a locally compact topological ring. See also the related paper [Lev73], which deals with duality for locally compact modules over a discrete commutative ring.

Let R be a locally compact topological ring. Note that in particular, discrete rings are locally compact.

Proposition 4.1. *Let M and N be topologial groups with N abelian. Then* $\mathrm{Hom}_{\mathrm{cts}}(M, N)$ *is an abelian topological group with respect to the compact-open topology and pointwise addition of maps. Moreover, we have:*

(i) If N is Hausdorff, then so is $\mathrm{Hom}_{\mathrm{cts}}(M, N)$.

(ii) If M is a topological R-module, then $\mathrm{Hom}_{\mathrm{cts}}(M, N)$ is a topological R^{op}-module with multiplication defined by $(r.f)(m) := f(rm)$ for $f \in \mathrm{Hom}_{\mathrm{cts}}(M, N)$, $r \in R^{\mathrm{op}}$ and $m \in M$.

Proof. See [Flo79, Proposition 3]. □

We recall the definition of the Pontryagin dual.

Definition 4.2. Let M be an abelian topological group. Then the *Pontryagin dual of* M is $M^\vee := \mathrm{Hom}_{\mathrm{cts}}(M, \mathbb{R}/\mathbb{Z})$.

By Proposition 4.1, $M^\vee$ is a Hausdorff abelian topological group, and if M is a topological R-module, then $M^\vee$ is a topological R^{op}-module.

Remark 4.3 ([Flo79, Section 4 and Theorem 6])**.** There is also a different perspective on duality for a topological left R-module M with the dual of R as the character module instead of $\mathbb{R}/\mathbb{Z}$. Analogously as in Proposition 4.1, the right R-module structure of R induces a topological left R-module structure on $R^\vee$, allowing to consider the set $\mathrm{Hom}_{R,\mathrm{cts}}(M, R^\vee)$ of continuous left R-module homomorphisms, a Hausdorff abelian topological group. Via the right R-module structure on $R^\vee$, it becomes a topological right R-module, and one can show that there is a natural isomorphism $M^\vee \cong \mathrm{Hom}_{R,\mathrm{cts}}(M, R^\vee)$ of topological right R-modules.

The most powerful statements on duality are obtained for the following class of groups.

Definition 4.4. An *LCA group* is a Hausdorff locally compact abelian topological group. An *LCA R-module* is an LCA group that is a topological R-module.

Note that if R is discrete, then an LCA group M is an LCA R-module if and only if the maps $M \to M,\ m \mapsto rm$ are continuous for all $r \in R$.

We will always write LCA groups and modules additively. Note that LCA groups are the same as LCA $\mathbb{Z}$-modules. Thus, the discussion below of duality for LCA R-modules recovers the classical theory on LCA groups for $R = \mathbb{Z}$.

It is clear that products, closed submodules and quotients by closed submodules of LCA R-modules are again LCA R-modules. LCA R-modules together with continuous R-module homomorphisms form a category which we will denote by ${}_R\mathsf{LCA}$. We simply write LCA for ${}_\mathbb{Z}\mathsf{LCA}$. Note that if M and N are LCA R-modules, then the set $\mathrm{Hom}_{{}_R\mathsf{LCA}}(M, N)$ of continuous R-module homomorphisms from M to N is a subgroup of $\mathrm{Hom}_{\mathrm{cts}}(M, N)$ and therefore a Hausdorff abelian topological group with respect to the subspace topology.

Proposition 4.5. *Let M be an LCA R-module. Then $M^\vee$ is an LCA R^{op}-module.*

Proof. The dual $M^\vee$ is an LCA group by [HR79, Theorem 23.15] and a topological R^{op}-module by Proposition 4.1. □

We give some important examples of Pontryagin duals that will appear frequently.

Example 4.6 ([HR79, Example 23.27])**.** We have the following isomorphisms of LCA groups:

$$\begin{aligned} \mathbb{Z} &\xrightarrow{\sim} (\mathbb{R}/\mathbb{Z})^\vee, \ n \mapsto (\overline{x} \mapsto \overline{nx}), \\ \mathbb{R}/\mathbb{Z} &\xrightarrow{\sim} \mathbb{Z}^\vee, \ \overline{x} \mapsto (n \mapsto \overline{nx}), \\ \mathbb{R} &\xrightarrow{\sim} \mathbb{R}^\vee, \ x \mapsto (y \mapsto \overline{xy}). \end{aligned}$$

Moreover, if M is a finite LCA group, then $M \cong M^\vee$.

We also have a notion of dual for morphisms.

Definition 4.7. Let M and N be LCA R-modules. For $\varphi \in \operatorname{Hom}_{{}_R\mathsf{LCA}}(M, N)$ define

$$\varphi^\vee \colon N^\vee \to M^\vee, \ f \mapsto f \circ \varphi,$$

which is an element of $\operatorname{Hom}_{{}_{R^{\mathrm{op}}}\mathsf{LCA}}(N^\vee, M^\vee)$, see [HR79, Theorem 24.38].

The above definition evidently makes duality a contravariant functor ${}_R\mathsf{LCA} \to {}_{R^{\mathrm{op}}}\mathsf{LCA}$. The main theorem on the duality functor is the following.

Theorem 4.8 (Pontryagin Duality)**.** *Let M be an LCA R-module. Then the map*

$$M \to M^{\vee\vee}, \ m \mapsto (f \mapsto f(m))$$

is an isomorphism of LCA R-modules which is natural in M. In particular, duality

$$\vee \colon {}_R\mathsf{LCA} \to {}_{R^{\mathrm{op}}}\mathsf{LCA}$$

is an involutory anti-equivalence of categories.

Proof. See [HR79, Theorem 24.8] or [Mor77, Theorem 23] for the case $R = \mathbb{Z}$. That the map $M \to M^{\vee\vee}$ is R-linear is immediately verified. □

Corollary 4.9. *Let M and N be LCA R-modules. Then the map*

$$\operatorname{Hom}_{{}_R\mathsf{LCA}}(M, N) \to \operatorname{Hom}_{{}_{R^{\mathrm{op}}}\mathsf{LCA}}(N^\vee, M^\vee), \ \varphi \mapsto \varphi^\vee$$

is an isomorphism of Hausdorff abelian topological groups.

4.1.1 The Compact-Discrete Duality

Proposition 4.10 ([HR79, Theorem 23.17])**.** *Let M be an LCA group. If M is compact, then $M^\vee$ is discrete. If M is discrete, then $M^\vee$ is compact.*

We will later deal with LCA groups whose dual is not only discrete but also finitely generated, and now provide a characterisation of such groups.

Definition 4.11. Let M be an LCA group. We say that M *has no small subgroups* if there exists a neighbourhood of 0 that does not contain any nontrivial subgroup of M.

For a characterisation of groups with no small subgroups see [Mos67, Theorem 2.4].

Proposition 4.12. *Let M be an LCA group. Then the following are equivalent:*

(i) M is compact and has no small subgroups,

(ii) $M^\vee$ is discrete and finitely generated,

(iii) there is an isomorphism of LCA groups $M \cong F \oplus (\mathbb{R}/\mathbb{Z})^n$ for some $n \in \mathbb{Z}_{\geq 0}$ and a finite abelian group F,

(iv) there is an isomorphism of LCA groups $M_0 \cong (\mathbb{R}/\mathbb{Z})^n$ for some $n \in \mathbb{Z}_{\geq 0}$, and the quotient M/M_0 is finite,

(v) M is a compact real abelian Lie group.

Moreover, any continuous group homomorphism between objects of the above type is also a homomorphism of the associated Lie groups.

Proof. The equivalence of (i), (ii) and (iii) is [Mos67, Corollary 2 on page 366].

That (iv) implies (iii) follows from [Mos67, Theorem 3.2]. Suppose that (iii) holds. Then the Lie group structure on $F \oplus (\mathbb{R}/\mathbb{Z})^n$ induces a Lie group structure on M, so (v) holds. Moreover, any continuous group homomorphism between objects of the type in (iii) must map the toral part into the toral part, as it is the connected component of the identity. It follows from Corollary 4.9 and Example 4.6 that the morphism restricted to the toral part is given by an $n \times n$ integer matrix and hence smooth, i.e. a Lie group homomorphism. Hence, also the overall map is a Lie group homomorphism. This proves the additional statement.

Finally, suppose that M is a compact real abelian Lie group. Then M_0 is a compact connected real abelian Lie group and thus by [Bum13, Proposition 15.3] there is an isomorphism $M_0 \cong (\mathbb{R}/\mathbb{Z})^n$ for some $n \in \mathbb{Z}_{\geq 0}$. Moreover, the quotient M/M_0 is both compact and discrete, hence finite. This shows that (v) implies (iv) and finishes the proof. □

4.1.2 Duality for Submodules and Quotient Modules

We collect some results on the duals of the connected component of the identity and of certain torsion submodules. These will be derived from the following general result on the duals of submodules and quotient modules.

Definition 4.13. Let M be an LCA group and let $\varnothing \neq N \subseteq M$. We define

$$N^{\perp} := \left\{ f \in M^{\vee} \,\middle|\, f(n) = 0 \text{ for all } n \in N \right\}$$

and call it the *annihilator of N in $M^{\vee}$*.

The annihilator is a closed subgroup of $M^{\vee}$, cf. [HR79, Remark 23.24]. If M is an LCA R-module and N is a closed submodule, then $N^{\perp}$ is a closed submodule of $M^{\vee}$.

Proposition 4.14. *Let M be an LCA R-module and let $N \leq M$ be a closed submodule. Then there are isomorphisms*

$$(M/N)^{\vee} \xrightarrow{\sim} N^{\perp}, \ f \mapsto f \circ \pi,$$

where $\pi \colon M \to M/N$ is the natural projection, and

$$M^{\vee}/N^{\perp} \xrightarrow{\sim} N^{\vee}, \ \overline{f} \mapsto f\big|_N$$

of LCA R^{op}-modules which are functorial in M.

Proof. [HR79, Theorems 23.25 and 24.11] state that the maps are isomorphisms of LCA groups. Compatibility with the R^{op}-module structure and functoriality are easily checked. □

We derive consequences of the above proposition for some submodules of our interest by computing annihilators.

Proposition 4.15. *The following hold.*

(i) Let M be a compact LCA group. Then $(M_0)^{\perp} = (M^{\vee})_{\mathrm{tors}}$.

(ii) Let M be a discrete LCA group. Then $(M_{\mathrm{tors}})^{\perp} = (M^{\vee})_0$.

Proof. See [HR79, Corollary 24.20]. □

Corollary 4.16. *Let Z be a localisation of $\mathbb{Z}$ and suppose that R is a Z-order in some finite-dimensional $\mathbb{Q}$-algebra. Then the following hold:*

(i) Let M be a compact LCA R-module. Then there are isomorphisms

$$(M/M_0)^\vee \xrightarrow{\sim} (M^\vee)_{\text{tors}}, \ f \mapsto f \circ \pi,$$

where $\pi \colon M \to M/M_0$ is the natural projection, and

$$M^\vee/(M^\vee)_{\text{tors}} \xrightarrow{\sim} (M_0)^\vee, \ \overline{f} \mapsto f\big|_{M_0}$$

of discrete LCA R^{op}-modules which are functorial in M.

(ii) Let M be a discrete LCA R-module. Then there are isomorphisms

$$M^\vee/(M^\vee)_0 \xrightarrow{\sim} (M_{\text{tors}})^\vee, \ \overline{f} \mapsto (m \mapsto f(m))$$

and

$$(M^\vee)_0 \xrightarrow{\sim} (M/M_{\text{tors}})^\vee, \ f \mapsto (\overline{m} \mapsto f(m))$$

of compact LCA R^{op}-modules which are functorial in M.

Proof. Statement (i) is immediate from Propositions 4.14 and 4.15. Statement (ii) follows from (i) using the duality isomorphism. □

Proposition 4.17. *Let M be an LCA R-module and let $r \in R$. Then $(rM)^\perp = M^\vee[r]$ and $M[r]^\perp = \overline{rM^\vee}$, where $\overline{rM^\vee}$ denotes the topological closure of $rM^\vee$.*

Proof. One can do the same proof as in [HR79, Theorem 24.22]. □

Corollary 4.18. *Let Z be a Dedekind domain and suppose that R is a Z-order in some finite-dimensional algebra over the fraction field of Z. Let M be a finite LCA R-module and let $\mathfrak{p} \in \operatorname{Max}(Z)$. Then the map*

$$M^\vee[\mathfrak{p}^\infty] \to M[\mathfrak{p}^\infty]^\vee, \ f \mapsto f\big|_{M[\mathfrak{p}^\infty]}$$

is an isomorphism of finite LCA R^{op}-modules.

Proof. By Example 4.6 we have $M \cong M^\vee$ as abelian groups. Write $|M| = |M^\vee| = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_k^{r_k} \subseteq Z$ with $\mathfrak{p}_i \in \operatorname{Max}(Z)$. Since Z is a Dedekind domain, we can find $z_i \in \prod_{j \neq i} \mathfrak{p}_j^{r_j}$ with $1 = z_1 + \cdots + z_k$. Then $z_i M = M[\mathfrak{p}_i^\infty]$ and $z_i(M^\vee) = M^\vee[\mathfrak{p}_i^\infty]$. The map

$$M^\vee/(M^\vee[z_i]) \to z_i(M^\vee), \ \overline{f} \mapsto z_i f$$

clearly is an R^{op}-module isomorphism. Moreover, Propositions 4.14 and 4.17 give an isomorphism

$$M^\vee/(M^\vee[z_i]) \xrightarrow{\sim} (z_i M)^\vee, \ \overline{f} \mapsto f\big|_{z_i M}.$$

The concatenation

$$M^\vee[\mathfrak{p}_i^\infty] = z_i(M^\vee) \xrightarrow{\sim} M^\vee/(M^\vee[z_i]) \xrightarrow{\sim} (z_i M)^\vee = M[\mathfrak{p}_i^\infty]^\vee$$

is the map from the claim. □

We end this section with a result that shows that duality is compatible with isotypical components.

Lemma 4.19. *Let M be an LCA R-module. Suppose that $R = R_1 \times \cdots \times R_n$ is a product of locally compact topological rings and let $M = M_1 \oplus \cdots \oplus M_n$ be the decomposition into isotypical components.*

Then each M_i is an LCA R_i-module. The natural isomorphism of LCA groups

$$\begin{aligned} &(M_1)^\vee \oplus \cdots \oplus (M_n)^\vee \xrightarrow{\sim} M^\vee, \\ &\qquad\qquad (f_1, \ldots, f_n) \mapsto \big(m_1 + \cdots + m_n \mapsto f_1(m_1) + \cdots + f_n(m_n)\big) \end{aligned}$$

is an R^{op}-homomorphism, and $(M_i)^\vee$ lies in the block R_i^{op}. In particular, we have isomorphisms

$$(M_i)^\vee \cong (M^\vee)_i, \qquad \begin{aligned} f_i &\mapsto \big(m_1 + \cdots + m_n \mapsto f_i(m_i)\big) \\ f\big|_{M_i} &\mapsfrom f \end{aligned}$$

of LCA R^{op}-modules.

Proof. We have that

$$\begin{aligned} M_i &= \{\, m \in M \mid (r_1, \ldots, r_{i-1}, 0, r_{i+1}, \ldots, r_n)m = 0 \text{ for all } r_j \in R_j \,\} \\ &= \{\, m \in M \mid (1, \ldots, 1, 0, 1, \ldots, 1)m = 0 \,\} \end{aligned}$$

is a closed subgroup of M and hence an LCA group. Clearly, multiplication $R_i \times M_i \to M_i$ is continuous, so M_i is an LCA R_i-module. It is easy to check that the isomorphism is an R^{op}-module homomorphism. Since M_i lies in the block R_i, it follows immediately that $(M_i)^\vee$ lies in the block R_i^{op}. □

4.2 Strict Homomorphisms and Extensions

Let again R be a locally compact ring. Related to our previous discussion of extensions of abstract modules in Chapter 2, this section is concerned with extensions of LCA R-modules and their interaction with the duality functor. The material is taken from [Mos67] and [FG71], to which we also refer for further information and statements.

It turns out that in order to have nice behaviour under dualising, we need to restrict to so-called strict homomorphisms.

Definition 4.20. Let M and N be LCA groups and let $\varphi \in \mathrm{Hom}_{\mathrm{cts}}(M, N)$. We say that φ is *strict* if it is an open map onto its image.

This terminology is taken from [HS07]. It stems from a more general notion of strict homomorphisms that can be defined in any additive category with kernels and cokernels [Sch99]. Note that in the case of LCA groups, a strict homomorphism may also be called a *relatively open* homomorphism; we prefer to use the notion strict as it is rooted in homological algebra. Strict homomorphisms are called *proper* in [Mos67] and [FG71]. An important condition that ensures strictness is the following.

Proposition 4.21. *Let M and N be LCA groups and let $\varphi \in \mathrm{Hom}_{\mathrm{cts}}(M, N)$. If $\varphi(M)$ is closed and M is the countable union of compact sets, then φ is strict.*

Proof. This is essentially the so-called open mapping theorem, see [Mos67, page 362]. □

Definition 4.22. A sequence $M \xrightarrow{\varphi} N \xrightarrow{\psi} L$ of LCA R-modules and continuous R-module homomorphisms is called *exact* if $\operatorname{im}\varphi = \ker\psi$. We say that the sequence is *strictly exact* if it is exact and both φ and ψ are strict.

Crucially, strictly exact sequences behave well under dualising.

Proposition 4.23 ([Mos67, Theorem 2.1])**.** *Let M, N and L be LCA R-modules. If $M \xrightarrow{\varphi} N \xrightarrow{\psi} L$ is a strictly exact sequence, then also $L^\vee \xrightarrow{\psi^\vee} N^\vee \xrightarrow{\varphi^\vee} M^\vee$ is strictly exact.*

We now discuss extensions of LCA R-modules. Note that fibre products and pushouts of strict morphisms of LCA R-modules exist, cf. [FG71, Proposition 2.5].

Definition 4.24. Let M and N be LCA R-modules.

(a) An *extension* of M by N is a short strictly exact sequence $0 \to N \to L \to M \to 0$ of LCA R-modules.

(b) We say that two extensions $0 \to N \to L \to M \to 0$ and $0 \to N \to L' \to M \to 0$ of M by N are *equivalent* if there is $\varphi \in \mathrm{Hom}_{{}_R\mathsf{LCA}}(L, L')$ that makes the diagram

$$\begin{tikzcd}
0 \arrow[r] & N \arrow[r] \arrow[d, equal] & L \arrow[r] \arrow[d, "\varphi"] & M \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & N \arrow[r] & L' \arrow[r] & M \arrow[r] & 0
\end{tikzcd}$$

commute. We denote by $E_{{}_R\mathsf{LCA}}(M, N)$ the set of equivalence classes of extensions of M by N.

(c) The *Baer sum* of extensions of M by N is defined as in Definition 2.3.

We remark that the map φ is bijective by the 5-Lemma and is strict by [FG71, Corollary 2.2], so it is necessarily an isomorphism of LCA R-modules.

Proposition 4.25. *Let M and N be LCA R-modules. Then $E_{{}_R\mathsf{LCA}}(M,N)$ forms an abelian group with respect to Baer sum, and we have an additive functor*

$$E_{{}_R\mathsf{LCA}}(-,-)\colon\ {}_R\mathsf{LCA}^{\mathrm{op}} \times {}_R\mathsf{LCA} \to \mathsf{Ab}\,.$$

Moreover, Pontryagin duality induces a natural isomorphism

$$E_{{}_R\mathsf{LCA}}(M,N) \xrightarrow{\sim} E_{{}_{R^{\mathrm{op}}}\mathsf{LCA}}(N^\vee, M^\vee),\ \ \Theta \mapsto \Theta^\vee.$$

Proof. This follows as in [FG71, Section 2]. □

Remark 4.26.

(a) Let M and N be LCA R-modules. If $0 \to N \to L \to M \to 0$ is a short strictly exact sequence in which L is just a topological R-module, then L is automatically locally compact by [HR79, Theorem 5.25]. Moreover, by loc. cit., if M and N are both compact, then so is L. Dually, using Propositions 4.10 and 4.23, if M and N are discrete, then so is L. In particular, if M and N are discrete, then $E_{{}_R\mathsf{LCA}}(M,N) = \mathrm{Ext}^1_R(M,N)$.

(b) In the case $R = \mathbb{Z}$, one can also homologically define Ext functors as derived functors of Hom on a domain which is slightly smaller than $\mathsf{LCA}^{\mathrm{op}} \times \mathsf{LCA}$ and prove an analogue of Proposition 2.5, see [Mos67, Section VI].

4.3 The Pontryagin Dual of $\mathbb{Z}_{(S)}$

Throughout this section, let S be a nonempty subset of the union of $\{0\}$ and the set of rational primes. We consider $\mathbb{Z}_{(S)}$ with the discrete topology. Moreover, if R is a $\mathbb{Z}_{(S)}$-order in some finite-dimensional $\mathbb{Q}$-algebra, then we also consider any R-lattice – being isomorphic to $\mathbb{Z}_{(S)}^n$ as a $\mathbb{Z}_{(S)}$-module for some n – with the discrete topology.

The first two subsections are concerned with determining the Pontryagin dual of $\mathbb{Z}_{(S)}$. On the two ends of the spectrum, the Pontryagin duals are well-known: The Pontryagin dual of $\mathbb{Z}$ is $\mathbb{R}/\mathbb{Z}$ (see Example 4.6), and the Pontryagin dual of $\mathbb{Q}$ is $\mathbb{A}_\mathbb{Q}/\mathbb{Q}$, where $\mathbb{A}_\mathbb{Q}$ denotes the rational adeles (see [CF67, Theorem XV.4.1.4], or [Con] for a more direct proof). It has been observed in [CEW97, Section 3] that the latter isomorphism generalises to $\mathbb{Z}_{(S)}$ for any S in a straight forward manner. Since we will later need the explicit description of the isomorphism between $\mathbb{Z}_{(S)}$ and its dual, and for completeness and the convenience of the reader, we provide a detailed account of the construction with all necessary statements and proofs adapted from the case $S = \{0\}$. The proofs and explicit description of the isomorphism have been omitted in [CEW97], which otherwise contains all the main results from the first two subsections. Our exposition is largely based on [CF67, Chapter XV] and [Con].

In the final two subsections we use the theory about the dual of $\mathbb{Z}_{(S)}$ to establish an isomorphism between certain Ext and Hom groups over a $\mathbb{Z}_{(S)}$-algebra and a result on the tensor product of a lattice over a $\mathbb{Z}_{(S)}$-order with a compact LCA $\mathbb{Z}_{(S)}$-module, both of which will be useful tools later on.

4.3.1 A Generalisation of the Rational Adeles

Definition 4.27. For $x \in \mathbb{Q}_p$ denote by $\{x\}_p$ the *p-adic fractional part of x*. Explicitly, if

$$x = b_{-m}p^{-m} + \cdots + b_{-1}p^{-1} + \sum_{k=0}^{\infty} b_k p^k \qquad \text{with } m \in \mathbb{Z}_{\geq 0} \text{ and } 0 \leq b_i < p,$$

then $\{x\}_p = b_{-m}p^{-m} + \cdots + b_{-1}p^{-1}$.

It has the following properties:

Lemma 4.28. *Let $x, y \in \mathbb{Q}_p$ and let $w \in \mathbb{Q}$. Then:*

(i) $x - \{x\}_p \in \mathbb{Z}_p$,

(ii) $\{x\}_p = 0$ *if and only if* $x \in \mathbb{Z}_p$,

(iii) $\{x\}_p + \{y\}_p - \{x + y\}_p \in \mathbb{Z}$,

(iv) $w - \sum_{p<\infty} \{w\}_p \in \mathbb{Z}$.

Proof. This is easily verified. Details can be found for example in [Con]. □

Definition 4.29. Define

$$\mathbb{A}_{(S)} := \prod_{p \notin S}{}' \mathbb{Q}_p,$$

where p runs over rational primes and ∞, and where the restricted product is taken with respect to the subrings $\mathbb{Z}_p$ for $p < \infty$ and $\mathbb{R}$ for $p = \infty$.

With slightly different notation and S swapped with its complement in the set of rational primes, this definition is a special case of [CEW97, Definition 3.1] for $k = \mathbb{Q}$. Note that if S is the set of all rational primes, then $\mathbb{A}_{(S)} = \mathbb{R}$, and if $S = \{0\}$, then $\mathbb{A}_{(S)} = \mathbb{A}_{\mathbb{Q}}$. So $\mathbb{A}_{(S)}$ can be thought of as a generalisation of the rational adeles. We next show that it has analogous properties.

Lemma 4.30. *It holds that*

$$\mathbb{A}_{(S)} = \mathbb{Z}_{(S)} + \left([0,1) \times \prod_{\substack{p \notin S \\ p < \infty}} \mathbb{Z}_p \right),$$

where the sum is taken inside $\mathbb{A}_{(S)}$. Moreover, the expression of an element of $\mathbb{A}_{(S)}$ as the sum of two elements as given by the right hand side is unique.

Proof. Let $a \in \mathbb{A}_{(S)}$. Let T be the finite set of primes with $a_p \notin \mathbb{Z}_p$ for $p \in T$. Then $r := \sum_{p \in T} \{a_p\}_p \in \mathbb{Z}_{(S)}$ and $a - r \in \mathbb{R} \times \prod_{p \notin S, p<\infty} \mathbb{Z}_p$. It follows that $a - (r + \lfloor a_\infty - r \rfloor) \in [0,1) \times \prod_{p \notin S, p<\infty} \mathbb{Z}_p$ with $r + \lfloor a_\infty - r \rfloor \in \mathbb{Z}_{(S)}$ which proves the decomposition of $\mathbb{A}_{(S)}$. To show uniqueness, let $b \in \mathbb{Z}_{(S)} \cap \Big([0,1) \times \prod_{p \notin S, p<\infty} \mathbb{Z}_p\Big)$. Then $v_p(b) \geq 0$ for all primes p, which gives $b \in \mathbb{Z}$. But then $b \in [0,1)$ forces $b = 0$. □

Proposition 4.31. *$\mathbb{A}_{(S)}$ is a locally compact Hausdorff topological ring. Moreover, $\mathbb{Z}_{(S)}$ is discrete in $\mathbb{A}_{(S)}$ and the quotient $\mathbb{A}_{(S)}/\mathbb{Z}_{(S)}$ is compact.*

Proof. That $\mathbb{A}_{(S)}$ is a locally compact and Hausdorff topological ring follows exactly as for the rational adeles, cf. [CF67, Section II.14]. To show that $\mathbb{Z}_{(S)}$ is discrete in $\mathbb{A}_{(S)}$, consider the open set

$$U := (-1,1) \times \prod_{\substack{p \notin S \\ p<\infty}} \mathbb{Z}_p \subseteq \mathbb{A}_{(S)}.$$

If $a \in U \cap \mathbb{Z}_{(S)}$, then $v_p(a) \geq 0$ for all primes p, so $a \in \mathbb{Z}$. But also $a \in (-1,1)$, whence $a = 0$ and so $U \cap \mathbb{Z}_{(S)} = \{0\}$. Discreteness follows. Finally, Lemma 4.30 shows that $\mathbb{A}_{(S)}/\mathbb{Z}_{(S)}$ is the image of the compact set $[0,1] \times \prod_{p \notin S, p<\infty} \mathbb{Z}_p$ under the projection $\mathbb{A}_{(S)} \to \mathbb{A}_{(S)}/\mathbb{Z}_{(S)}$ and therefore itself compact. □

4.3.2 The Pontryagin Duals of $\mathbb{A}_{(S)}$ and $\mathbb{Z}_{(S)}$

Definition 4.32. For p a rational prime, we define

$$\chi_p \colon \mathbb{Q}_p \to \mathbb{R}/\mathbb{Z},\ x \mapsto \overline{-\{x\}_p},$$

and we further put

$$\chi_\infty \colon \mathbb{R} \to \mathbb{R}/\mathbb{Z},\ x \mapsto \overline{x}.$$

For $a \in \mathbb{A}_{(S)}$ we define

$$\chi_a \colon \mathbb{A}_{(S)} \to \mathbb{R}/\mathbb{Z},\ b \mapsto \sum_{p \notin S} \chi_p(a_p b_p) = \overline{a_\infty b_\infty - \sum_{\substack{p \notin S \\ p<\infty}} \{a_p b_p\}_p}.$$

Theorem 4.33. *The map*

$$\mathbb{A}_{(S)} \to \mathbb{A}_{(S)}^\vee,\ a \mapsto (b \mapsto \chi_a(b))$$

is an isomorphism of LCA $\mathbb{Z}_{(S)}$-modules.

Proof. For $p \leq \infty$, [CF67, Theorem XV.2.1.1] shows that the map

$$\mathbb{Q}_p \to \mathbb{Q}_p^\vee,\ y \mapsto (x \mapsto \chi_p(xy))$$

is an isomorphism. It follows easily from Lemma 4.28 that it maps $\mathbb{Z}_p$ onto $\mathbb{Z}_p^\perp$ for $p < \infty$. Then [CF67, Theorem XV.3.2.1] yields the claim. □

Theorem 4.34. *The map*

$$\mathbb{A}_{(S)}/\mathbb{Z}_{(S)} \to \mathbb{Z}_{(S)}^\vee,\ \overline{a} \mapsto \chi_a\big|_{\mathbb{Z}_{(S)}}$$

is an isomorphism of compact LCA $\mathbb{Z}_{(S)}$-modules. In particular, we have a short strictly exact sequence of LCA $\mathbb{Z}_{(S)}$-modules

$$\begin{tikzcd} 0 \arrow[r] & \mathbb{Z}_{(S)} \arrow[r] & \mathbb{A}_{(S)} \arrow[r] & \mathbb{Z}_{(S)}^\vee \arrow[r] & 0. \end{tikzcd}$$

Proof. Denote by $\alpha\colon \mathbb{A}_{(S)} \to \mathbb{A}_{(S)}^\vee$ the isomorphism from Theorem 4.33. In view of the second isomorphism in Proposition 4.14, it only remains to show that $\alpha(\mathbb{Z}_{(S)}) = \mathbb{Z}_{(S)}^\perp$. Let $a, z \in \mathbb{Z}_{(S)}$. Then by Lemma 4.28 (iv) and (ii) we have

$$\alpha(a)(z) = \chi_a(z) = \overline{az - \sum_{\substack{p \notin S \\ p < \infty}} \{az\}_p} = \overline{\sum_{p \in S} \{az\}_p} = 0$$

which shows $\alpha(\mathbb{Z}_{(S)}) \subseteq \mathbb{Z}_{(S)}^\perp$. For the converse, we first consider the factor group $\alpha^{-1}(\mathbb{Z}_{(S)}^\perp)/\mathbb{Z}_{(S)}$ which is a subgroup of $\mathbb{A}_{(S)}/\mathbb{Z}_{(S)}$. By Proposition 4.31, $\mathbb{A}_{(S)}/\mathbb{Z}_{(S)}$ is compact. Hence, by Propositions 4.14 and 4.10, $\mathbb{Z}_{(S)}^\perp$ is discrete, which implies that also $\alpha^{-1}(\mathbb{Z}_{(S)}^\perp)/\mathbb{Z}_{(S)}$ is discrete. In particular, $\alpha^{-1}(\mathbb{Z}_{(S)}^\perp)/\mathbb{Z}_{(S)}$ is a closed subgroup of the compact group $\mathbb{A}_{(S)}/\mathbb{Z}_{(S)}$ and therefore also compact. Being compact and discrete, $\alpha^{-1}(\mathbb{Z}_{(S)}^\perp)/\mathbb{Z}_{(S)}$ must be finite. Now let $f \in \mathbb{Z}_{(S)}^\perp$. Then there is $n \in \mathbb{Z}$ with $nf \in \alpha(\mathbb{Z}_{(S)})$, so there is $a \in \mathbb{Z}_{(S)}$ with $nf = \alpha(a)$. For $b \in \mathbb{A}_{(S)}$ it holds that

$$f(b) = f\Big(n \cdot \frac{b}{n}\Big) = nf\Big(\frac{b}{n}\Big) = \alpha(a)\Big(\frac{b}{n}\Big) = \chi_a\Big(\frac{b}{n}\Big) = \chi_{\frac{a}{n}}(b) = \alpha\Big(\frac{a}{n}\Big)(b),$$

giving $f = \alpha\left(\frac{a}{n}\right)$. Let $q \in S$ and let $b := \prod_{p \neq q} p^{v_p(n)} \in \mathbb{Z}$. Then using Lemma 4.28 (iv) and (ii) we have

$$0 = f(b) = \chi_{\frac{a}{n}}(b) = \overline{\sum_{p \in S} \left\{\frac{ab}{n}\right\}_p} = \overline{\sum_{p \in S} \left\{\frac{a}{q^{v_q(n)}}\right\}_p} = \overline{\left\{\frac{a}{q^{v_q(n)}}\right\}_q}.$$

Hence, $\left\{\frac{a}{q^{v_q(n)}}\right\}_q \in \mathbb{Z}$ and Lemma 4.28 (i) gives $\frac{a}{q^{v_q(n)}} \in \mathbb{Z}_q$. This means that $v_q(\frac{a}{n}) \geq 0$ and therefore $\frac{a}{n} \in \mathbb{Z}_{(S)}$, which yields $f = \alpha\left(\frac{a}{n}\right) \in \alpha(\mathbb{Z}_{(S)})$, as desired. □

Note that if S is the set of all rational primes, then we recover the isomorphism $\mathbb{R}/\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}^\vee$ from Example 4.6.

Remark 4.35. By adapting the arguments in [Con], one can also give an elementary proof of Theorem 4.34 which does not make use of the Pontryagin duality theorem.

4.3.3 An Isomorphism between Ext and Hom Groups

Let R be a $\mathbb{Z}_{(S)}$-algebra. In this section, we prove that for a finite R-module M and a $\mathbb{Z}_{(S)}$-torsionfree R-module N there is a natural isomorphism of abelian groups $\mathrm{Ext}^1_R(M, N) \cong \mathrm{Hom}_R(M, N \otimes_{\mathbb{Z}_{(S)}} \mathbb{A}_{(S)}/\mathbb{Z}_{(S)})$. This generalises the corresponding result from [BP25, page 13] for the case $R = \mathbb{Z}_{(S)} = \mathbb{Z}$.

We start by specialising to extensions and homomorphisms over $\mathbb{Z}$ and below use the construction from [BP25] to build an isomorphism via group cohomology. By tracing all the maps occurring in the cohomological argument, we will then be able to upgrade this isomorphism to an isomorphism between the respective Ext and Hom groups over R.

Remark 4.36. Let M be a finite abelian group and let N be a torsionfree $\mathbb{Z}_{(S)}$-module. We recall some statements from group cohomology. Denote by $E_c(M, N)$ the set of equivalence classes of central extensions of M by N, that is, of extensions

$$\begin{tikzcd} 0 \arrow[r] & N \arrow[r] & L \arrow[r] & M \arrow[r] & 0 \end{tikzcd}$$

where L is a group (not necessarily abelian) and N is central in L. With slight abuse of notation, we will write L additively; this is justified as later on the group L will always be abelian. Regard N as an M-module with trivial action. It is well-known that there is a bijection $E_c(M, N) \longleftrightarrow H^2(M, N)$, cf. [Bro82, Theorem IV.3.12]. It is given as follows. Suppose that an equivalence class of central extensions is represented by

$$\begin{tikzcd} 0 \arrow[r] & N \arrow[r, "\alpha"] & L \arrow[r, "\beta"] & M \arrow[r] & 0. \end{tikzcd}$$

Pick a set-theoretic map $s\colon M \to L$ with $\beta s = \mathrm{id}_M$ and $s(0) = 0$. Then the map

$$M \times M \to N, \ (a, b) \mapsto \alpha^{-1}(s(a) + s(b) - s(a + b))$$

is a normalised 2-cocycle (that is, a 2-cocycle that maps $(0, 0)$ to 0) and hence represents an element of $H^2(M, N)$. Conversely, any element of $H^2(M, N)$ can be represented by a normalised 2-cocycle $\chi\colon M \times M \to N$. Define $L_\chi := N \times M$, with group operation

$$(x, a) + (y, b) := (x + y + \chi(a, b), a + b)$$

for $x, y \in N$ and $a, b \in M$. Then a representative for the image of the class of χ in $E_c(M, N)$ is given by the central extension

$$\begin{tikzcd} 0 \arrow[r] & N \arrow[r] & L_\chi \arrow[r] & M \arrow[r] & 0 \end{tikzcd}$$

where the left hand map is $x \mapsto (x, 0)$ and the right hand map is $(x, a) \mapsto a$. Moreover, the set $E_c(M, N)$ is an abelian group under Baer sum, and the above bijection is a group isomorphism, cf. [ML63, Exercise IV.4.7].

Construction 4.37. Let M be a finite abelian group and let N be a torsionfree $\mathbb{Z}_{(S)}$-module. It is clear that the map $\operatorname{Ext}^1_{\mathbb{Z}}(M, N) \to E_c(M, N)$ that sends a class of extensions represented by $0 \to N \to L \to M \to 0$ to the class of central extensions represented by $0 \to N \to L \to M \to 0$ is an injective group homomorphism. By [Bro82, Exercise IV.3.8], the commutator pairing gives rise to a group homomorphism $E_c(M, N) \to \operatorname{Hom}_{\mathbb{Z}}(\bigwedge^2 M, N)$, and it is easy to see that the kernel of this homomorphism is the image of $\operatorname{Ext}^1_{\mathbb{Z}}(M, N)$ in $E_c(M, N)$. Moreover, it follows from [Bro82, Exercise V.6.5] that the group homomorphism $E_c(M, N) \to \operatorname{Hom}_{\mathbb{Z}}(\bigwedge^2 M, N)$ is surjective. Thus, there is a short exact sequence

$$0 \longrightarrow \operatorname{Ext}^1_{\mathbb{Z}}(M, N) \longrightarrow E_c(M, N) \longrightarrow \operatorname{Hom}_{\mathbb{Z}}(\textstyle\bigwedge^2 M, N) \longrightarrow 0.$$

Since $\bigwedge^2 M$ is finite and N is torsion-free, the right hand term of the above sequence is zero, so that the left hand map is an isomorphism. This also implies that in every central extension of M by N, the middle group is abelian, and that for all normalised 2-cocycles $\chi \colon M \times M \to N$ we have $\chi(a, b) = \chi(b, a)$ for all $a, b \in M$, which will be used below.

So far we have achieved isomorphisms $\operatorname{Ext}^1_{\mathbb{Z}}(M, N) \cong E_c(M, N) \cong H^2(M, N)$. Now since N is $\mathbb{Z}_{(S)}$-torsionfree, it is a flat $\mathbb{Z}_{(S)}$-module, and so there is a short exact sequence

$$0 \longrightarrow N \xrightarrow{\iota} N \otimes_{\mathbb{Z}_{(S)}} \mathbb{A}_{(S)} \xrightarrow{\pi} N \otimes_{\mathbb{Z}_{(S)}} \mathbb{A}_{(S)}/\mathbb{Z}_{(S)} \longrightarrow 0.$$

Again regarding the modules as trivial M-modules, the long exact cohomology sequence associated to the above exact sequence gives

$$\begin{tikzcd}
\cdots \arrow[r] & H^1(M, N \otimes_{\mathbb{Z}_{(S)}} \mathbb{A}_{(S)}) \arrow[r] & H^1(M, N \otimes_{\mathbb{Z}_{(S)}} \mathbb{A}_{(S)}/\mathbb{Z}_{(S)}) \arrow[dll, rounded corners, "\delta"] \\
H^2(M, N) \arrow[r] & H^2(M, N \otimes_{\mathbb{Z}_{(S)}} \mathbb{A}_{(S)}) \arrow[r] & \cdots .
\end{tikzcd}$$

Since multiplication by $|M|$ is an automorphism of $N \otimes_{\mathbb{Z}_{(S)}} \mathbb{A}_{(S)}$, it follows from [CF67, Corollary 1 on page 105] that $H^q(M, N \otimes_{\mathbb{Z}_{(S)}} \mathbb{A}_{(S)}) = 0$ for all $q \in \mathbb{Z}_{\geq 1}$. Hence, δ is an isomorphism. Finally, since we regard $N \otimes_{\mathbb{Z}_{(S)}} \mathbb{A}_{(S)}/\mathbb{Z}_{(S)}$ as a trivial M-module, we have $H^1(M, N \otimes_{\mathbb{Z}_{(S)}} \mathbb{A}_{(S)}/\mathbb{Z}_{(S)}) = \operatorname{Hom}_{\mathbb{Z}}(M, N \otimes_{\mathbb{Z}_{(S)}} \mathbb{A}_{(S)}/\mathbb{Z}_{(S)})$. In summary, we have established an isomorphism $\operatorname{Ext}^1_{\mathbb{Z}}(M, N) \cong \operatorname{Hom}_{\mathbb{Z}}(M, N \otimes_{\mathbb{Z}_{(S)}} \mathbb{A}_{(S)}/\mathbb{Z}_{(S)})$.

In order to be able to trace all intermediate isomorphisms occurring above for the upgrade to R-extensions and R-homomorphisms, we next give a description of δ and its inverse.

Lemma 4.38. *Use the notation from Construction 4.37.*

(i) The connecting homomorphism $\delta\colon H^1(M, N \otimes_{\mathbb{Z}_{(S)}} \mathbb{A}_{(S)}/\mathbb{Z}_{(S)}) \to H^2(M, N)$ is given as follows: Given a group homomorphism $\varphi\colon M \to N \otimes_{\mathbb{Z}_{(S)}} \mathbb{A}_{(S)}/\mathbb{Z}_{(S)}$, choose a set-theoretic lift $\widetilde{\varphi}\colon M \to N \otimes_{\mathbb{Z}_{(S)}} \mathbb{A}_{(S)}$ with $\widetilde{\varphi}(0) = 0$. Then

$$\chi_\varphi\colon M \times M \to N, \ (a, b) \mapsto \iota^{-1}(\widetilde{\varphi}(a) + \widetilde{\varphi}(b) - \widetilde{\varphi}(a + b))$$

is a normalised 2-cocycle, and $\delta(\varphi)$ is given by the class of χ_φ.

(ii) The map $\delta^{-1}\colon H^2(M, N) \to H^1(M, N \otimes_{\mathbb{Z}_{(S)}} \mathbb{A}_{(S)}/\mathbb{Z}_{(S)})$ is given as follows: Let $\chi\colon M \times M \to N$ be a normalised 2-cocycle. Then

$$\varphi_\chi\colon M \to N \otimes_{\mathbb{Z}_{(S)}} \mathbb{A}_{(S)}/\mathbb{Z}_{(S)}, \ a \mapsto \sum_{k=1}^{|M|-1} \chi(a, ka) \otimes \overline{\frac{1}{|M|}}.$$

is a group homomorphism and the image of the class of χ under δ^{-1} is given by φ_χ.

Proof. Claim (i) is standard, cf. [Wei94, Addendum 1.3.3]. To prove (ii), let $\chi\colon M \times M \to N$ be a normalised 2-cocycle. It is clear that $\varphi_{\chi+\chi'} = \varphi_\chi + \varphi_{\chi'}$. If χ is a normalised 2-coboundary, then there is a (set) map $\theta\colon M \to N$ with $\theta(0) = 0$ such that $\chi(a, b) = \theta(a) + \theta(b) - \theta(a + b)$ for all $a, b \in M$. It follows that

$$\begin{aligned} \varphi_\chi(a) &= \sum_{k=1}^{|M|-1} \theta(a) + \theta(ka) - \theta((k+1)a) \otimes \overline{\frac{1}{|M|}} \\ &= \big(|M|\,\theta(a) - \theta(|M|\,a)\big) \otimes \overline{\frac{1}{|M|}} \\ &= \theta(a) \otimes \overline{1} \\ &= 0 \end{aligned}$$

for any $a \in M$. Hence, $\chi \mapsto \varphi_\chi$ is a well-defined map on $H^2(M, N)$. We next show that φ_χ is a group homomorphism, that is, $\varphi_\chi \in H^1(M, N \otimes_{\mathbb{Z}_{(S)}} \mathbb{A}_{(S)}/\mathbb{Z}_{(S)})$. To this end, let $a, b \in M$. We first investigate the expression

$$D_{\chi,k}(a, b) := \chi(a, ka) + \chi(b, kb) - \chi(a + b, k(a + b))$$

for $k \in \mathbb{Z}_{>0}$. We will rewrite it using the 2-cocycle identity which reads

$$\chi(m_1, m_2) = \chi(m_2, m_3) + \chi(m_1, m_2 + m_3) - \chi(m_1 + m_2, m_3)$$

for $m_1, m_2, m_3 \in M$. Applying it with $m_1 = a$, $m_2 = b$, $m_3 = k(a + b)$ gives

$$\chi(a, b) = \chi(b, k(a + b)) + \chi(a, ka + (k + 1)b) - \chi(a + b, k(a + b)),$$

whence

$$D_{\chi,k}(a,b) = \chi(a,ka) + \chi(b,kb) + \chi(a,b) - \chi(b,k(a+b)) - \chi(a,ka+(k+1)b).$$

The 2-cocycle identity with $m_1 = a$, $m_2 = ka$, $m_3 = (k+1)b$ gives

$$\chi(a,ka) = \chi(ka,(k+1)b) + \chi(a,ka+(k+1)b) - \chi((k+1)a,(k+1)b),$$

whence

$$D_{\chi,k}(a,b) = \chi(ka,(k+1)b) - \chi((k+1)a,(k+1)b) + \chi(b,kb) + \chi(a,b) - \chi(b,k(a+b)).$$

The 2-cocycle identity with $m_1 = ka$, $m_2 = b$, $m_3 = kb$ gives

$$\chi(ka,b) = \chi(b,kb) + \chi(ka,(k+1)b) - \chi(ka+b,kb),$$

whence

$$D_{\chi,k}(a,b) = \chi(ka,b) + \chi(ka+b,kb) - \chi((k+1)a,(k+1)b) + \chi(a,b) - \chi(b,k(a+b)).$$

Finally, the 2-cocycle identity with $m_1 = b$, $m_2 = ka$, $m_3 = kb$ gives

$$\chi(b,ka) = \chi(ka,kb) + \chi(b,k(a+b)) - \chi(ka+b,kb),$$

whence

$$D_{\chi,k}(a,b) = \chi(ka,b) - \chi(b,ka) + \chi(ka,kb) - \chi((k+1)a,(k+1)b) + \chi(a,b).$$

Now as remarked above, we have $\chi(ka,b) - \chi(b,ka) = 0$ which gives

$$D_{\chi,k}(a,b) = \chi(a,b) + \chi(ka,kb) - \chi((k+1)a,(k+1)b). \tag{4.39}$$

It follows that

$$\begin{aligned}
\varphi_\chi(a) + \varphi_\chi(b) - \varphi_\chi(a+b) &= \sum_{k=1}^{|M|-1} D_{\chi,k}(a,b) \otimes \overline{\frac{1}{|M|}} \\
&= \big(|M|\,\chi(a,b) - \chi(|M|\,a,|M|\,b)\big) \otimes \overline{\frac{1}{|M|}} \\
&= \chi(a,b) \otimes \overline{1} \\
&= 0
\end{aligned}$$

which shows that φ_χ is a group homomorphism. Thus we get a well-defined map

$$H^2(M,N) \to H^1(M, N \otimes_{\mathbb{Z}_{(S)}} \mathbb{A}_{(S)}/\mathbb{Z}_{(S)}),\ [\chi] \mapsto \varphi_\chi.$$

We verify that this is precisely δ^{-1}. Starting with a class $[\chi] \in H^2(M,N)$ represented by a normalised 2-cocycle $\chi\colon M \times M \to N$, we have to show that $\delta(\varphi_\chi) = [\chi]$. It is clear that

$$\widetilde{\varphi_\chi}\colon M \to N \otimes_{\mathbb{Z}_{(S)}} \mathbb{A}_{(S)},\ a \mapsto \sum_{k=1}^{|M|-1} \chi(a,ka) \otimes \frac{1}{|M|}$$

is a lift of φ_χ with $\widetilde{\varphi_\chi}(0) = 0$. Using (4.39) again, we have

$$\begin{aligned}
\iota^{-1}(\widetilde{\varphi_\chi}(a) + \widetilde{\varphi_\chi}(b) - \widetilde{\varphi_\chi}(a+b)) &= \iota^{-1}\left(\sum_{k=1}^{|M|-1} D_{\chi,k}(a,b) \otimes \frac{1}{|M|}\right) \\
&= \iota^{-1}\left(\chi(a,b) \otimes 1\right) \\
&= \chi(a,b)
\end{aligned}$$

for $a, b \in M$, whence $\delta(\varphi_\chi) = [\chi]$. Conversely, suppose that $\varphi\colon M \to N \otimes_{\mathbb{Z}_{(S)}} \mathbb{A}_{(S)}/\mathbb{Z}_{(S)}$ is a group homomorphism. Let $\widetilde{\varphi}\colon M \to N \otimes_{\mathbb{Z}_{(S)}} \mathbb{A}_{(S)}$ be a lift of φ with $\widetilde{\varphi}(0) = 0$. Then for $a \in M$ we have

$$\begin{aligned}
\sum_{k=1}^{|M|-1} \chi_\varphi(a, ka) \otimes \overline{\frac{1}{|M|}} &= \iota^{-1}\left(\sum_{k=1}^{|M|-1} \widetilde{\varphi}(a) + \widetilde{\varphi}(ka) - \widetilde{\varphi}((k+1)a)\right) \otimes \overline{\frac{1}{|M|}} \\
&= \iota^{-1}\left(|M|\, \widetilde{\varphi}(a)\right) \otimes \overline{\frac{1}{|M|}}.
\end{aligned}$$

Now it holds that

$$\iota^{-1}\left(|M|\, \widetilde{\varphi}(a)\right) \otimes 1 = \iota\left(\iota^{-1}\left(|M|\, \widetilde{\varphi}(a)\right)\right) = |M|\, \widetilde{\varphi}(a)$$

which means that

$$\widetilde{\varphi}(a) = \iota^{-1}\left(|M|\, \widetilde{\varphi}(a)\right) \otimes \frac{1}{|M|}$$

and therefore

$$\varphi(a) = \iota^{-1}\left(|M|\, \widetilde{\varphi}(a)\right) \otimes \overline{\frac{1}{|M|}} = \sum_{k=1}^{|M|-1} \chi_\varphi(a, ka) \otimes \overline{\frac{1}{|M|}}.$$

We conclude that the map $H^2(M,N) \to H^1(M, N \otimes_{\mathbb{Z}_{(S)}} \mathbb{A}_{(S)}/\mathbb{Z}_{(S)})$ given above is indeed δ^{-1}. □

We now upgrade the isomorphisms from Construction 4.37 to R-extensions and R-homomorphisms.

Construction 4.40. Let R be a $\mathbb{Z}_{(S)}$-algebra. Let M be a finite R-module and let N be an R-module that is $\mathbb{Z}_{(S)}$-torsionfree. We define a map

$$\Psi\colon \operatorname{Ext}^1_R(M,N) \to \operatorname{Hom}_R(M, N \otimes_{\mathbb{Z}_{(S)}} \mathbb{A}_{(S)}/\mathbb{Z}_{(S)})$$

as follows: Let

$$\begin{tikzcd} 0 \arrow[r] & N \arrow[r, "\alpha"] & L \arrow[r, "\beta"] & M \arrow[r] & 0 \end{tikzcd}$$

be an extension of R-modules representing a class $\Theta \in \operatorname{Ext}^1_R(M,N)$. Pick a set-theoretic map $s\colon M \to L$ with $\beta s = \mathrm{id}_M$ and $s(0)=0$. Define

$$\chi\colon M \times M \to N,\ (a,b) \mapsto \alpha^{-1}(s(a)+s(b)-s(a+b))$$

and

$$\varphi\colon M \to N \otimes_{\mathbb{Z}_{(S)}} \mathbb{A}_{(S)}/\mathbb{Z}_{(S)},\ a \mapsto \sum_{k=1}^{|M|-1} \chi(a,ka) \otimes \overline{\frac{1}{|M|}} = \alpha^{-1}(|M|\, s(a)) \otimes \overline{\frac{1}{|M|}}.$$

By Remark 4.36, Construction 4.37 and Lemma 4.38, the map φ is a group homomorphism and depends neither on the choice of section s, nor on the choice of representative for Θ. We show that φ is in fact an R-module homomorphism. To this end, let $a \in M$ and $r \in R$. Then

$$\begin{aligned} \varphi(ra) - r\varphi(a) &= \big(\alpha^{-1}(|M|\, s(ra)) - r\alpha^{-1}(|M|\, s(a))\big) \otimes \overline{\frac{1}{|M|}} \\ &= \alpha^{-1}\left(|M|\, s(ra) - |M|\, rs(a)\right) \otimes \overline{\frac{1}{|M|}} \\ &= \alpha^{-1}\left(s(ra) - rs(a)\right) \otimes \overline{1} \\ &= 0 \end{aligned}$$

where we crucially used that α is an R-module homomorphism and that $s(ra)-rs(a) \in \ker\beta = \operatorname{im}\alpha$. We may thus define $\Psi(\Theta) := \varphi \in \operatorname{Hom}_R(M, N \otimes_{\mathbb{Z}_{(S)}} \mathbb{A}_{(S)}/\mathbb{Z}_{(S)})$.

We furthermore define a map

$$\Psi'\colon \operatorname{Hom}_R(M, N \otimes_{\mathbb{Z}_{(S)}} \mathbb{A}_{(S)}/\mathbb{Z}_{(S)}) \to \operatorname{Ext}^1_R(M,N)$$

as follows: Let $\varphi \in \operatorname{Hom}_R(M, N \otimes_{\mathbb{Z}_{(S)}} \mathbb{A}_{(S)}/\mathbb{Z}_{(S)})$. Choose a set-theoretic lift $\widetilde{\varphi}\colon M \to N \otimes_{\mathbb{Z}_{(S)}} \mathbb{A}_{(S)}$ of φ with $\widetilde{\varphi}(0)=0$. Since N is a flat $\mathbb{Z}_{(S)}$-module, there is an exact sequence

$$\begin{tikzcd} 0 \arrow[r] & N \arrow[r, "\iota"] & N \otimes_{\mathbb{Z}_{(S)}} \mathbb{A}_{(S)} \arrow[r, "\pi"] & N \otimes_{\mathbb{Z}_{(S)}} \mathbb{A}_{(S)}/\mathbb{Z}_{(S)} \arrow[r] & 0 \end{tikzcd}$$

of R-modules. Now define $L_{\widetilde{\varphi}} := N \times M$ with group operation

$$(x,a)+(y,b) := \big(x+y+\iota^{-1}(\widetilde{\varphi}(a)+\widetilde{\varphi}(b)-\widetilde{\varphi}(a+b)), a+b\big)$$

for $x,y \in N$ and $a,b \in M$. Then by Remark 4.36 and Construction 4.37, $(L_{\widetilde{\varphi}},+)$ is an abelian group and we have an extension

$$\Theta_{\widetilde{\varphi}}\colon \qquad \begin{tikzcd} 0 \arrow[r] & N \arrow[r] & L_{\widetilde{\varphi}} \arrow[r] & M \arrow[r] & 0 \end{tikzcd}$$

of abelian groups, where the left hand map is $x \mapsto (x,0)$ and the right hand map is $(x,a) \mapsto a$. We now define an R-module structure on $L_{\widetilde{\varphi}}$. Since π and φ are R-module homomorphisms, we have $r\widetilde{\varphi}(a) - \widetilde{\varphi}(ra) \in \ker \pi = \operatorname{im} \iota$ for all $a \in M$ and $r \in R$. We may thus define

$$r \cdot (x, a) := \big(rx + \iota^{-1}(r\widetilde{\varphi}(a) - \widetilde{\varphi}(ra)), ra\big)$$

for $r \in R$ and $(x, a) \in L_{\widetilde{\varphi}}$. It is easy to check that this defines an R-module structure on $L_{\widetilde{\varphi}}$. The extension $\Theta_{\widetilde{\varphi}}$ hence is an extension of R-modules. Now suppose that $\widehat{\varphi}\colon M \to N \otimes_{\mathbb{Z}_{(S)}} \mathbb{A}_{(S)}$ is another lift of φ with $\widehat{\varphi}(0) = 0$. Then $\widetilde{\varphi}(a) - \widehat{\varphi}(a) \in \ker \pi = \operatorname{im} \iota$ for all $a \in M$. Define a map

$$\eta\colon L_{\widetilde{\varphi}} \to L_{\widehat{\varphi}},\ (x, a) \mapsto \big(x + \iota^{-1}(\widetilde{\varphi}(a) - \widehat{\varphi}(a)), a\big)\,.$$

Then for $(x, a), (y, b) \in L_{\widetilde{\varphi}}$ and $r \in R$ we have

$$\begin{aligned}
\eta\left((x, a) + (y, b)\right) &= \eta\left(x + y + \iota^{-1}\left(\widetilde{\varphi}(a) + \widetilde{\varphi}(b) - \widetilde{\varphi}(a + b)\right), a + b\right) \\
&= \big(x + y + \iota^{-1}(\widetilde{\varphi}(a) + \widetilde{\varphi}(b) - \widehat{\varphi}(a + b)), a + b\big) \\
&= \big(x + \iota^{-1}(\widetilde{\varphi}(a) - \widehat{\varphi}(a)), a\big) + \big(y + \iota^{-1}(\widetilde{\varphi}(b) - \widehat{\varphi}(b)), b\big) \\
&= \eta(x, a) + \eta(y, b)
\end{aligned}$$

as well as

$$\begin{aligned}
\eta\left(r(x, a)\right) &= \eta\left(rx + \iota^{-1}(r\widetilde{\varphi}(a) - \widetilde{\varphi}(ra)), ra\right) \\
&= \big(rx + \iota^{-1}(r\widetilde{\varphi}(a) - \widehat{\varphi}(ra)), ra\big) \\
&= r\left(x + \iota^{-1}(\widetilde{\varphi}(a) - \widehat{\varphi}(a)), a\right) \\
&= r\eta(x, a)
\end{aligned}$$

Hence, η is an R-module homomorphism. Moreover, it is clear that the diagram

$$\begin{tikzcd}
0 \arrow[r] & N \arrow[r] \arrow[d, equal] & L_{\widetilde{\varphi}} \arrow[r] \arrow[d, "\eta"] & M \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & N \arrow[r] & L_{\widehat{\varphi}} \arrow[r] & M \arrow[r] & 0
\end{tikzcd}$$

commutes. This shows that the extensions $\Theta_{\widetilde{\varphi}}$ and $\Theta_{\widehat{\varphi}}$ are equivalent which means that the assignment $\Psi'(\varphi) := \Theta_{\widetilde{\varphi}} \in \operatorname{Ext}^1_R(M, N)$ is well-defined.

Proposition 4.41. *Let R be a $\mathbb{Z}_{(S)}$-algebra. Let M be a finite R-module and let N be an R-module that is $\mathbb{Z}_{(S)}$-torsionfree. Then the maps*

$$\begin{tikzcd}
\operatorname{Ext}^1_R(M, N) \arrow[r, shift left, "\Psi"] & \operatorname{Hom}_R(M, N \otimes_{\mathbb{Z}_{(S)}} \mathbb{A}_{(S)}/\mathbb{Z}_{(S)}) \arrow[l, shift left, "\Psi'"]
\end{tikzcd}$$

from Construction 4.40 are group homomorphisms and inverse to each other. Moreover, Ψ and Ψ' are natural in M and N.

Proof. Note that Ψ is the concatenation of the maps

$$\mathrm{Ext}^1_R(M,N) \to \mathrm{Ext}^1_{\mathbb{Z}}(M,N) \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{Z}}(M, N \otimes_{\mathbb{Z}_{(S)}} \mathbb{A}_{(S)}/\mathbb{Z}_{(S)})$$

where the right hand map is the isomorphism from Construction 4.37. It follows that Ψ is a group homomorphism. Furthermore, Remark 4.36, Construction 4.37 and Lemma 4.38 give that $\Psi \circ \Psi' = \mathrm{id}$.

We now show that $\Psi' \circ \Psi = \mathrm{id}$. Suppose that

$$\Theta\colon \qquad 0 \longrightarrow N \xrightarrow{\alpha} L \xrightarrow{\beta} M \longrightarrow 0$$

is an extension of R-modules. Pick a set-theoretic map $s\colon M \to L$ with $\beta s = \mathrm{id}_M$ and $s(0) = 0$. Define

$$\chi\colon M \times M \to N,\ (a,b) \mapsto \alpha^{-1}(s(a) + s(b) - s(a+b)),$$

so that

$$\begin{aligned} \varphi := \Psi(\Theta)\colon M &\to N \otimes_{\mathbb{Z}_{(S)}} \mathbb{A}_{(S)}/\mathbb{Z}_{(S)}, \\ a &\mapsto \sum_{k=1}^{|M|-1} \chi(a,ka) \otimes \overline{\frac{1}{|M|}} = \alpha^{-1}(|M|\, s(a)) \otimes \overline{\frac{1}{|M|}}. \end{aligned}$$

Then clearly

$$\widetilde{\varphi}\colon M \to N \otimes_{\mathbb{Z}_{(S)}} \mathbb{A}_{(S)},\ a \mapsto \alpha^{-1}(|M|\, s(a)) \otimes \frac{1}{|M|}$$

is a lift of φ with $\widetilde{\varphi}(0) = 0$. Recall the exact sequence

$$0 \longrightarrow N \xrightarrow{\iota} N \otimes_{\mathbb{Z}_{(S)}} \mathbb{A}_{(S)} \xrightarrow{\pi} N \otimes_{\mathbb{Z}_{(S)}} \mathbb{A}_{(S)}/\mathbb{Z}_{(S)} \longrightarrow 0.$$

As we have shown in the proof of Lemma 4.38, it holds that

$$\iota^{-1}(\widetilde{\varphi}(a) + \widetilde{\varphi}(b) - \widetilde{\varphi}(a+b)) = \chi(a,b)$$

for all $a, b \in N$. Moreover, analogously as in Construction 4.40 one sees that

$$r\widetilde{\varphi}(a) - \widetilde{\varphi}(ra) = \alpha^{-1}(rs(a) - s(ra)) \otimes 1.$$

Then by definition, $\Psi'(\Psi(\Theta))$ is given by the extension

$$0 \longrightarrow N \longrightarrow L_{\widetilde{\varphi}} \longrightarrow M \longrightarrow 0$$

where $L_{\widetilde{\varphi}} = N \times M$ is an R-module with respect to the operations

$$\begin{aligned} (x,a) + (y,b) &= (x + y + \chi(a,b), a+b)\,, \\ r(x,a) &= \big(rx + \alpha^{-1}(rs(a) - s(ra)), ra\big)\,, \end{aligned}$$

for $(x,a),(y,b) \in L_{\widetilde{\varphi}}$ and $r \in R$. Now define

$$\eta\colon L_{\widetilde{\varphi}} \to E,\ (x,a) \mapsto \alpha(x) + s(a).$$

It is immediate that η is an R-module homomorphism and that the diagram

$$\begin{tikzcd}
0 \arrow[r] & N \arrow[r] \arrow[d, equal] & L_{\widetilde{\varphi}} \arrow[r] \arrow[d, "\eta"] & M \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & N \arrow[r, "\alpha"'] & E \arrow[r, "\beta"'] & M \arrow[r] & 0
\end{tikzcd}$$

commutes. We conclude that $\Psi'(\Psi(\Theta)) = \Theta$. Finally, it is a straightforward calculation to check naturality of Ψ and Ψ. □

4.3.4 Tensor Products of Lattices with Compact Modules

Inspired by [BJL24, Section 2.1], we establish an isomorphism for the tensor product of a lattice over a $\mathbb{Z}_{(S)}$-order with a compact LCA $\mathbb{Z}_{(S)}$-module. We will frequently apply it to the expression $N \otimes_{\mathbb{Z}_{(S)}} \mathbb{A}_{(S)}/\mathbb{Z}_{(S)}$ from the previous subsection.

Proposition 4.42. *Let R be a $\mathbb{Z}_{(S)}$-order in some finite-dimensional $\mathbb{Q}$-algebra (as usual regarded with the discrete topology). Let M be an R-lattice and let $n = \operatorname{rk}_{\mathbb{Z}_{(S)}} M$. Let C be a compact LCA $\mathbb{Z}_{(S)}$-module. Topologise $M \otimes_{\mathbb{Z}_{(S)}} C$ via an isomorphism $M \otimes_{\mathbb{Z}_{(S)}} C \cong C^n$ obtained by choosing a $\mathbb{Z}_{(S)}$-basis of M.*

Then $M \otimes_{\mathbb{Z}_{(S)}} C$ is a compact LCA R-module and the topology is independent of the chosen isomorphism. Regarding $\operatorname{Hom}_{\mathbb{Z}_{(S)}}(M, C^\vee)$ as a discrete R^{op}-module as in Proposition 4.1, there is an isomorphism of compact LCA R-modules

$$M \otimes_{\mathbb{Z}_{(S)}} C \xrightarrow{\sim} \operatorname{Hom}_{\mathbb{Z}_{(S)}}(M, C^\vee)^\vee,\ m \otimes c \mapsto \big(\varphi \mapsto \varphi(m)(c)\big)$$

which is natural in M. In particular, there is an isomorphism of compact LCA R-modules

$$M \otimes_{\mathbb{Z}_{(S)}} \mathbb{A}_{(S)}/\mathbb{Z}_{(S)} \xrightarrow{\sim} (M^*)^\vee,\ m \otimes \overline{a} \mapsto \big(f \mapsto \chi_a(f(m))\big)$$

which is natural in M.

Proof. Let $m_1, \dots, m_n \in M$ be a $\mathbb{Z}_{(S)}$-basis for M. Then we have an isomorphism of $\mathbb{Z}_{(S)}$-modules

$$\alpha\colon M \otimes_{\mathbb{Z}_{(S)}} C \to C^n, \quad \begin{array}{l} (z_1 m_1 + \dots + z_n m_n) \otimes c \mapsto (z_1 c, \dots, z_n c), \\ (m_1 \otimes c_1) + \dots + (m_n \otimes c_n) \leftarrow\!\shortmid (c_1, \dots, c_n). \end{array}$$

If $(m_1', \dots, m_n')$ is a different basis for M with corresponding isomorphism $\alpha'\colon M \otimes_{\mathbb{Z}_{(S)}} C \to C^n$ and we write $m_i = \sum_j a_{ij} m_j'$ with $a_{ij} \in \mathbb{Z}_{(S)}$ and $A = (a_{ij})$, then

$$\alpha' \circ \alpha^{-1}(c_1, \dots, c_n) = A^T(c_1, \dots, c_n)$$

is a homeomorphism on C^n, so the topology on $M \otimes_{\mathbb{Z}_{(S)}} C$ is independent of the choice of basis. Now let $r \in R$. We need to check that

$$\mu_r \colon M \otimes_{\mathbb{Z}_{(S)}} C \to M \otimes_{\mathbb{Z}_{(S)}} C,\ m \otimes c \mapsto rm \otimes c$$

is continuous. By definition of the topology, this is the case if and only if the map $\alpha\mu_r\alpha^{-1} \colon C^n \to C^n$ is continuous.

$$\begin{tikzcd}
M \otimes_{\mathbb{Z}_{(S)}} C \arrow[r, "\alpha"] \arrow[d, "\mu_r"'] & C^n \arrow[d, "\alpha\mu_r\alpha^{-1}"] \\
M \otimes_{\mathbb{Z}_{(S)}} C \arrow[r, "\alpha"'] & C^n
\end{tikzcd}$$

But writing $rm_i = \sum_{j=1}^n b_{ij}m_j$ for $b_{ij} \in \mathbb{Z}_{(S)}$ and $B = (b_{ij})$, we have

$$\alpha\mu_r\alpha^{-1}(c_1, \dots, c_n) = B^T(c_1, \dots, c_n)$$

which immediately shows that the map is continuous. For the next part, write

$$\beta \colon M \otimes_{\mathbb{Z}_{(S)}} C \to \mathrm{Hom}_{\mathbb{Z}_{(S)}}(M, C^\vee)^\vee,\ m \otimes c \mapsto (\varphi \mapsto \varphi(m)(c)).$$

We have an isomorphism of discrete LCA $\mathbb{Z}_{(S)}$-modules

$$\gamma\colon\ \mathrm{Hom}_{\mathbb{Z}_{(S)}}(M, C^\vee) \to (C^n)^\vee,\ \varphi \mapsto ((c_1, \dots, c_n) \mapsto \varphi(m_1)(c_1) + \cdots + \varphi(m_n)(c_n))$$

whose dual fits into a commutative diagram

$$\begin{tikzcd}
M \otimes_{\mathbb{Z}_{(S)}} C \arrow[r, "\beta"] \arrow[d, "\alpha"'] & \mathrm{Hom}_{\mathbb{Z}_{(S)}}(M, C^\vee)^\vee \\
C^n \arrow[r] & (C^n)^{\vee\vee}, \arrow[u, "\gamma^\vee"']
\end{tikzcd}$$

where the lower map is the duality isomorphism. It follows that β is an isomorphism of compact abelian groups. Furthermore, for $m \in M$, $c \in C$, $r \in R$ and $\varphi \in \mathrm{Hom}_{\mathbb{Z}_{(S)}}(M, C^\vee)$ we have

$$(r.\beta(m \otimes c))(\varphi) = \beta(m \otimes c)(r.\varphi) = (r.\varphi)(m)(c) = \varphi(rm)(c) = \beta(rm \otimes c)(\varphi)$$

which shows that β is an R-homomorphism. If N is another R-lattice and $f \colon M \to N$ is an R-homomorphism, then one easily sees that the diagram

$$\begin{tikzcd}
M \otimes_{\mathbb{Z}_{(S)}} C \arrow[r, "\sim"] \arrow[d, "f \otimes \mathrm{id}_C"'] & \mathrm{Hom}_{\mathbb{Z}_{(S)}}(M, C^\vee)^\vee \arrow[d, "(f^*)^\vee"] \\
N \otimes_{\mathbb{Z}_{(S)}} C \arrow[r, "\sim"] & \mathrm{Hom}_{\mathbb{Z}_{(S)}}(N, C^\vee)^\vee
\end{tikzcd}$$

commutes, which shows naturality. The final claim follows from the above applied to $C = \mathbb{A}_{(S)}/\mathbb{Z}_{(S)}$ together with Theorem 4.34 and the Pontryagin duality isomorphism. □

Remark 4.43. For LCA groups M and N, the *tensor product* $M \otimes_{\mathrm{LCA}} N$ is defined to be the Pontryagin dual of the group of continuous bilinear maps from $M \times N$ to $\mathbb{R}/\mathbb{Z}$, equipped with the compact-open topology, see [Mos67, Section IV]. Under certain mild assumptions on M and N it is again an LCA group. If M and N are discrete abelian groups, then also $M \otimes_{\mathrm{LCA}} N$ is discrete and equals the usual tensor product $M \otimes_{\mathbb{Z}} N$ of abelian groups [Mos67, Theorem 4.4 and Corollary 1 to Theorem 4.7]. Another relation of $\otimes_{\mathrm{LCA}}$ with $\otimes_{\mathbb{Z}}$ is given by the above proposition: For a finitely generated torsionfree discrete abelian group M and a compact abelian group C, it shows that $M \otimes_{\mathbb{Z}} C \cong \mathrm{Hom}_{\mathrm{cts}}(M, C^\vee)^\vee$. On the other hand, [Mos67, Theorem 4.2] gives $M \otimes_{\mathrm{LCA}} C \cong \mathrm{Hom}_{\mathrm{cts}}(M, C^\vee)^\vee$, whence $M \otimes_{\mathrm{LCA}} C \cong M \otimes_{\mathbb{Z}} C$.

5 Commensurability of Automorphism Groups of Chain Complexes

Recall from the introduction that for our main conjecture we wish to define a probability distribution on the space of outcomes for the good part of the Arakelov ray class sequence that weights each sequence in the space of outcomes by the inverse of the size of a certain subgroup of its automorphism group. One here encounters the problem that the latter subgroups are in general not finite. The purpose of the present chapter is to resolve this problem by developing a theory that allows to compare the sizes of certain subgroups of the automorphism groups of short exact sequences, even when those subgroups are infinite. This theory will then allow us to prove Theorem 1.11 and to eventually construct the probability distribution in Theorem 1.12.

We will establish a commensurability theory for automorphism groups of short exact sequences by extending the work of Bartel and Lenstra [BL17], who developed a theory that allows to compare the sizes of possibly infinite automorphism groups of suitable modules. In order to have the notions and tools from an abelian category at our disposal, we will work in the category of chain complexes of modules, which also has the advantage of leading to a more general theory. The results are applicable to short exact sequences by viewing them as chain complexes. Moreover, the theory of [BL17] can be seen as a special case of the results from this chapter by viewing a module as a chain complex concentrated in degree zero.

Roughly speaking, the idea to compare the sizes of the automorphism groups of two chain complexes L and M is to do so via a third object that is 'within a finite distance' of $\operatorname{Aut} L$ and $\operatorname{Aut} M$. Such a third object might not always exist but we will show that if L and M are themselves 'within finite distance', then from any object X within finite distance of both L and M one can construct a natural object $A(X)$ within finite distance of both $\operatorname{Aut} L$ and $\operatorname{Aut} M$. The latter will then be used to define the index of automorphism groups $\operatorname{ia}(L, M)$, which is to be thought of as $|\operatorname{Aut} M : \operatorname{Aut} L|$. The main challenge for this will be to establish independence of the comparing object X.

$$\begin{tikzcd}
 & X \arrow[dl, "\text{fin. dist.}"'] \arrow[dr, "\text{fin. dist.}"] & & & & A(X) \arrow[dl, "\text{fin. dist.}"'] \arrow[dr, "\text{fin. dist.}"] & \\
L & & M & \rightsquigarrow & \operatorname{Aut} L & & \operatorname{Aut} M
\end{tikzcd}$$

Apart from the last subsection, we proceed exactly as in [BL17] and prove the analogues of their results for chain complexes. The proofs generalise without too many complications, and we will usually just explain which steps need to be adapted in order to make them work in the more general context. We have also stuck to Bartel and Lenstra's notation as much as possible. In the last subsection, we take the theory one step further to allow to also compare sizes of suitable subgroups of automorphism groups of chain complexes.

5.1 Categories with Isogenies

Throughout this section, let R be a ring.

The key definition to compare objects of infinite size is the following. It makes precise what we mean by two objects being ‘within finite distance’.

Definition 5.1 ([BL17, page 2])**.** An *isogeny* of groups is a group homomorphism $f\colon L \to M$ with $|\ker f| < \infty$ and $|M : \operatorname{im} f| < \infty$. Its *index* is defined to be $\mathrm{i}(f) := |M : \operatorname{im} f| \,/\, |\ker f|$. Isogenies of rings and isogenies of R-modules are defined to be morphisms in the appropriate category which are group isogenies on the underlying additive groups.

For our applications, we want to generalise the above to chain complexes. We will use the following terminology. If $\mathcal{C}$ is an abelian category, we write $\mathsf{Ch}(\mathcal{C})$ for the category of chain complexes in $\mathcal{C}$. We will usually write an element $L \in \mathsf{Ch}(\mathcal{C})$ as $L = (L_i)_{i\in\mathbb{Z}}$ and denote the boundary maps $L_i \to L_{i-1}$ by ∂_i^L or ∂_i or even just ∂. Thus we can visualise L as

$$\cdots \xrightarrow{\partial_{i+2}} L_{i+1} \xrightarrow{\partial_{i+1}} L_i \xrightarrow{\partial_i} L_{i-1} \xrightarrow{\partial_{i-1}} \cdots .$$

If $f\colon L \to M$ is a chain map, then we write $f = (f_i)_{i\in\mathbb{Z}}$ where $f_i\colon L_i \to M_i$ are the component morphisms. We furthermore denote by $\mathsf{Ch}(\mathcal{C})^b$ the subcategory of $\mathsf{Ch}(\mathcal{C})$ of bounded chain complexes, that is, of chain complexes $L \in \mathcal{C}$ for which there are $l, u \in \mathbb{Z}$ such that $L_i = 0$ for all $i < l$ and all $i > u$.

Remark 5.2. Let $\mathcal{C}$ be an abelian category. Then also $\mathsf{Ch}(\mathcal{C})$ is an abelian category. If $f = (f_i)_i \colon L \to M$ is a morphism of chain complexes, then its kernel is given by $(\ker f_i)_i$ and its cokernel is given by $(\operatorname{cok} f_i)_i$, where the boundary maps are the natural maps induced by the boundary maps of L and M, respectively.

If $g\colon X \to M$ and $h\colon Y \to M$ are two morphisms of chain complexes, then the fibre product $X \times_M Y$ is given by $(X_i \times_{M_i} Y_i)_i$ with boundary maps induced by the universal property of the fibre product in the diagram below:

$$\begin{tikzcd}
X_{i+1} \times_{M_{i+1}} Y_{i+1} \arrow[rd, dashed] \arrow[rrd, bend left, "\partial^Y_{i+1} \circ q_{i+1}"] \arrow[rdd, bend right, "\partial^X_{i+1} \circ p_{i+1}"'] & & \\
& X_i \times_{M_i} Y_i \arrow[r, "q_i"] \arrow[d, "p_i"'] & Y_i \arrow[d, "h_i"] \\
& X_i \arrow[r, "g_i"'] & M_i.
\end{tikzcd}$$

The category $\mathsf{Ch}(\mathcal{C})^b$ is an abelian subcategory of $\mathsf{Ch}(\mathcal{C})$. The explicit descriptions of kernels, cokernels and fibre products above also hold in $\mathsf{Ch}(\mathcal{C})^b$.

We will mainly be interested in bounded chain complexes over the category ${}_R\mathsf{mod}$ of finitely generated R-modules, which we note is abelian if and only if R is noetherian [Wei94, Example 1.6.3]. Some results can also be obtained for chain complexes over ${}_R\mathsf{Mod}$.

To define isogenies, we first need a notion of finiteness.

Definition 5.3.

(a) A bounded chain complex $L \in \mathsf{Ch}({}_R\mathsf{Mod})^b$ is called *finite* if L_i is finite for all i. In this case, we define the *cardinality* of L to be $|L| := \prod_{i\in\mathbb{Z}} |L_i|$. We also write $|L| < \infty$ to indicate that L is a finite chain complex.

(b) An *isogeny* of chain complexes in $\mathsf{Ch}({}_R\mathsf{Mod})^b$ is a chain map $f\colon L \to M$ with $|\ker f| < \infty$ and $|\operatorname{cok} f| < \infty$. Its *index* is defined to be $\mathrm{i}(f) := |\operatorname{cok} f| \,/\, |\ker f|$.

Note that the above definitions reduce to the corresponding definitions for modules when viewing modules as chain complexes concentrated in degree 0. Importantly, finiteness behaves well with respect to short exact sequences.

Proposition 5.4. *Let $0 \to L \to M \to N \to 0$ be a short exact sequence in $\mathsf{Ch}({}_R\mathsf{Mod})^b$. Then M is finite if and only if both L and N are finite. In that case, we have $|M| = |L| \cdot |N|$.*

Proof. This is immediate from [Wei94, Exercise 1.2.4]. □

This in particular implies that subcomplexes and quotient complexes of finite complexes are finite. To unify notation, we make the following definition.

Definition 5.5. Let $\mathcal{C}$ be a category.

(a) We say $\mathcal{C}$ is of *type I* if $\mathcal{C}$ has fibre products and there is a functor $\mathcal{C} \to \mathsf{Grp}$ that preserves fibre products. In this case, an *isogeny* in $\mathcal{C}$ is a morphism in $\mathcal{C}$ that becomes an isogeny in Grp, and the index of an isogeny in $\mathcal{C}$ is defined to be the index of the corresponding group isogeny.

(b) We say $\mathcal{C}$ is of *type II* if $\mathcal{C} = \mathsf{Ch}({}_R\mathsf{Mod})$ for some ring R or if $\mathcal{C} = \mathsf{Ch}({}_R\mathsf{mod})$ for some noetherian ring R.

(c) We say $\mathcal{C}$ *has isogenies* or is a *category with isogenies* if it is of type I or type II.

Categories of type I are those for which the theory in Section 2 of [BL17] is developed. The categories Grp, Ring, ${}_R\mathsf{Mod}$ for any ring R and ${}_R\mathsf{mod}$ for any noetherian ring R are all of type I. As a basis for our extended commensurability theory, we will show in the remainder of this section and in the following section that the statements from Section 2 of [BL17] also hold for categories of type II.

Proposition 5.6 ([ML71, Exercise VIII.4.6])**.** *Let $\mathcal{C}$ be an abelian category and let $f\colon L \to M$ and $g\colon M \to N$ be morphisms in $\mathcal{C}$. Then there is an exact sequence*

$$0 \longrightarrow \ker f \longrightarrow \ker(gf) \longrightarrow \ker g \longrightarrow \operatorname{cok} f \longrightarrow \operatorname{cok}(gf) \longrightarrow \operatorname{cok} g \longrightarrow 0.$$

The final two statements of this section will be crucial for the theory to be developed in the following sections.

Proposition 5.7. *Let $\mathcal{C}$ be a category with isogenies and let $f\colon L \to M$ and $g\colon M \to N$ be morphisms in $\mathcal{C}$. If two of f, g, gf are isogenies, then so is the third. In that case, we have $\mathrm{i}(gf) = \mathrm{i}(g)\mathrm{i}(f)$.*

Proof. If $\mathcal{C}$ is of type I, then this is [BL17, Proposition 2.1]. The proof for $\mathcal{C}$ of type II is analogous – just combine Propositions 5.6 and 5.4. □

Proposition 5.8. *Let $\mathcal{C}$ be a category and let $g\colon X \to M$ and $h\colon Y \to M$ be morphisms in $\mathcal{C}$. Suppose that the fibre product $X \times_M Y$ of g and h exists.*

$$\begin{tikzcd}
X \times_M Y \arrow[r, "\pi_Y"] \arrow[d, "\pi_X"'] & Y \arrow[d, "h"] \\
X \arrow[r, "g"'] & M
\end{tikzcd}$$

(i) Suppose that $\mathcal{C}$ has kernels. Then $\ker \pi_X \cong \ker h$ and $\ker \pi_Y \cong \ker g$.

(ii) Suppose that $\mathcal{C}$ has isognies. If h is an isogeny, then so is π_X. If g is an isogeny, then so is π_Y.

Proof. Suppose that $\mathcal{C}$ has kernels. Using the universal property of the fibre product, it is straightforward to prove that $\ker \pi_X$ together with the morphism $\ker \pi_X \hookrightarrow X \times_M Y \xrightarrow{\pi_Y} Y$ satisfies the universal property of a kernel of h. Then we must have $\ker \pi_X \cong \ker h$. The proof for $\ker \pi_Y \cong \ker g$ is analogous.

Now suppose that $\mathcal{C}$ has isogenies. If $\mathcal{C}$ is of type I, then claim (ii) is in [BL17, Proposition 2.4]. Assume that $\mathcal{C}$ is of type II. Then it is in particular abelian. We show that there is a monomorphism $\operatorname{cok} \pi_X \hookrightarrow \operatorname{cok} h$. For this, by the Freyd–Mitchell Embedding Theorem [Wei94, Theorem 1.6.1] applied to the smallest abelian subcategory of $\mathcal{C}$ containing the objects and morphisms of the fibre product diagram, we can assume to be working in the category of modules over some ring. In that case, it is easy to see that the map

$$X/\operatorname{im} \pi_X \to M/\operatorname{im} h, \ \overline{x} \mapsto \overline{g(x)}$$

is well-defined and injective. Now if h is an isogeny, then $\ker \pi_X$ is finite by part (i), and $\operatorname{cok} \pi_X$ is finite by Proposition 5.4 applied to the monomorphism $\operatorname{cok} \pi_X \hookrightarrow \operatorname{cok} h$. Hence, π_X is an isogeny. The proof of the second claim is again analogous. □

5.2 Calculus of Correspondences

While an isogeny $f\colon L \to M$ does not naturally induce a map between the automorphism groups $\operatorname{Aut} L$ and $\operatorname{Aut} M$, there is a natural object $\mathrm{a}(f)$ associated to f with maps to both $\operatorname{Aut} L$ and $\operatorname{Aut} M$, discussed in a later section. This is why rather than working with isogenies, we will mainly work with the following constructions to compare objects.

Definition 5.9. Let $\mathcal{C}$ be a category and let $L, M \in \mathcal{C}$. A *correspondence* from L to M in $\mathcal{C}$ is a triple $c = (X, f, g)$ where $X \in \mathcal{C}$ and $f\colon X \to L$ and $g\colon X \to M$ are morphisms in $\mathcal{C}$.

$$\begin{tikzcd} & X \arrow[dl, "f"'] \arrow[dr, "g"] & \\ L & & M \end{tikzcd}$$

We will denote such a correspondence by $c\colon L \rightleftharpoons M$.

Definition 5.10. Let $\mathcal{C}$ be a category with isogenies.

(a) A *skew correspondence* in $\mathcal{C}$ is a correspondence $c = (X, f, g)$ in $\mathcal{C}$ in which f is an isogeny.

(b) A *commensurability* in $\mathcal{C}$ is a correspondence $c = (X, f, g)$ in $\mathcal{C}$ for which both f and g are isogenies. The *index* of such a commensurability is defined to be $\mathrm{i}(c) := \mathrm{i}(g)/\mathrm{i}(f)$.

Definition 5.11. Let $\mathcal{C}$ be a category with isogenies. For an isogeny $f\colon L \to M$ in $\mathcal{C}$ we define $c_f := (L, \mathrm{id}_L, f)\colon L \rightleftharpoons M$, which is a commensurability.

There are natural group-like operations for correspondences and commensurabilities that will be essential in the following.

Definition 5.12. Let $\mathcal{C}$ be a category. Let $c = (X, f, g)\colon L \rightleftharpoons M$ and $d = (Y, h, j)\colon M \rightleftharpoons N$ be correspondences in $\mathcal{C}$.

(a) The *inverse* of c is defined to be $c^{-1} := (X, g, f)\colon M \rightleftharpoons L$.

(b) If the fibre product of g and h in $\mathcal{C}$ exists, define the *composition* of c with d to be

$$d \circ c := (X \times_M Y, f \circ \pi_X, j \circ \pi_Y)\colon L \rightleftharpoons N$$

where $\pi_X\colon X \times_M Y \to X$ and $\pi_Y\colon X \times_M Y \to Y$ are the canonical morphisms.

$$\begin{tikzcd} & & X \times_M Y \arrow[dl, "\pi_X"'] \arrow[dr, "\pi_Y"] & & \\ & X \arrow[dl, "f"'] \arrow[dr, "g"] & & Y \arrow[dl, "h"'] \arrow[dr, "j"] & \\ L & & M & & N \end{tikzcd}$$

In order to obtain the expected properties for composition and inverse, one needs to pass to equivalence classes.

Definition 5.13. Let $\mathcal{C}$ be a category with isogenies. Let $c = (X, f, g)\colon L \rightleftharpoons M$ and $d = (Y, h, j)\colon L \rightleftharpoons M$ be two correspondences in $\mathcal{C}$.

(a) We say that c and d are *equivalent* and write $c \sim d$ if there is a commensurability $(W, p, q)\colon X \rightleftharpoons Y$ such that $fp = hq$ and $gp = jq$.

$$\begin{tikzcd}
 & & X \arrow[dl, "f"'] \arrow[dr, "g"] & \\
W \arrow[urr, bend left, "p"] \arrow[drr, bend right, "q"'] & L & & M \\
 & & Y \arrow[ul, "h"] \arrow[ur, "j"'] &
\end{tikzcd}$$

(b) We say that c and d are *isomorphic* and write $c \cong d$ if there is an isomorphism $s\colon X \xrightarrow{\sim} Y$ with $f = hs$ and $g = js$.

$$\begin{tikzcd}
 & X \arrow[dl, "f"'] \arrow[dr, "g"] \arrow[dd, "s"] & \\
L & & M \\
 & Y \arrow[ul, "h"] \arrow[ur, "j"'] &
\end{tikzcd}$$

Clearly, being isomorphic implies being equivalent. Note that if $c \sim d$, then c is a skew correspondence (commensurability) if and only if d is a skew correspondence (commensurability).

We now obtain the analogues of the statements from Section 2 of [BL17]. Close inspection shows that they only hinge on their Propositions 2.1 and 2.4 and the universal property of the fibre product, and therefore easily generalise.

Proposition 5.14. *Let $\mathcal{C}$ be a category with isogenies. Let $c, c'\colon L \rightleftharpoons M$, $d, d'\colon M \rightleftharpoons N$ and $e\colon N \rightleftharpoons P$ be correspondences in $\mathcal{C}$. Then the following hold:*

(i) If $c \sim c'$ and $d \sim d'$, then $d \circ c \sim d' \circ c'$. If $c \cong c'$ and $d \cong d'$, then $d \circ c \cong d' \circ c'$.

(ii) We have $(e \circ d) \circ c \cong e \circ (d \circ c)$.

(iii) We have $c \circ (L, \mathrm{id}_L, \mathrm{id}_L) \cong c$ and $(M, \mathrm{id}_M, \mathrm{id}_M) \circ c \cong c$.

(iv) If c and d are skew correspondences, then so is $d \circ c$.

(v) *If c and d are commensurabilities, then so is $d \circ c$. In this case, we have* $\mathrm{i}(d \circ c) = \mathrm{i}(d)\mathrm{i}(c)$.

(vi) *If $c \sim c'$ are commensurabilities, then* $\mathrm{i}(c) = \mathrm{i}(c')$.

(vii) *If $c \sim c'$, then $c^{-1} \sim (c')^{-1}$. If $c \cong c'$, then $c^{-1} \cong (c')^{-1}$.*

(viii) *We have $(d \circ c)^{-1} \cong c^{-1} \circ d^{-1}$.*

(ix) *If c is a commensurability, then $c^{-1} \circ c \sim (L, \mathrm{id}_L, \mathrm{id}_L)$ and $c \circ c^{-1} \sim (M, \mathrm{id}_M, \mathrm{id}_M)$.*

Proof. For $\mathcal{C}$ of type I see Section 2 of [BL17]. For $\mathcal{C}$ of type II one can do exactly the same proofs, replacing every use of [BL17, Proposition 2.1] by Proposition 5.7 and every use of [BL17, Proposition 2.4] by Proposition 5.8. □

Definition 5.15. Let $\mathcal{C}$ be a category with isogenies.

(a) Define $\mathcal{C}_{\text{skew}}$ to be the category with the same objects as in $\mathcal{C}$ and where for objects $L, M \in \mathcal{C}_{\text{skew}}$, the morphisms from L to M are the equivalence classes of skew correspondences $L \rightleftharpoons M$.

(b) Define $\mathcal{C}_{\text{com}}$ to be the category with the same objects as in $\mathcal{C}$ and where for objects $L, M \in \mathcal{C}_{\text{com}}$, the morphisms from L to M are the equivalence classes of commensurabilities $L \rightleftharpoons M$.

(c) For an object L in $\mathcal{C}$ define $G_L := \mathrm{Hom}_{\mathcal{C}_{\text{com}}}(L, L)$, the group of equivalence classes of commensurabilities $L \rightleftharpoons L$.

By the above we know that $\mathcal{C}_{\text{com}}$ is a groupoid. Even more:

Proposition 5.16. *Let $\mathcal{C}$ be a category with isogenies. Then the category $\mathcal{C}_{\text{com}}$ is the maximal subgroupoid of $\mathcal{C}_{\text{skew}}$.*

Proof. The result for a category of type I is [BL17, Proposition 2.15]. For a category of type II, one can do essentially the same proof. Using notation as in the proof of loc. cit., the only modifications one needs to make are: Use Propositions 5.6 and 5.4 to conclude that $\operatorname{cok} g$ and $\ker p_1'$ are finite; use Proposition 5.8 (i) to conclude that $\ker p_1' \cong \ker g$. □

5.3 Skew Correspondences of Chain Complexes

In this section, we use the notation from [BL17, Notation 6.1]:

Setup 5.17. Let Z be an infinite commutative ring satisfying the equivalent conditions of [BL17, Theorem 4.5], which we recall are the following:

(i) for each $0 \neq z \in Z$, the ring Z/zZ is finite;

(ii) the ring Z is a domain, and each nonzero prime ideal of Z is finitely generated as an ideal and has finite index in Z;

(iii) either Z is a field, or it is a one-dimensional noetherian domain with the property that for every maximal ideal $\mathfrak{p}$ of Z the field $Z/\mathfrak{p}$ is finite.

Denote by Q the field of fractions of Z. Let A be a finite-dimensional Q-algebra and R be a left-noetherian Z-subalgebra of A with the property that $Q \cdot R = A$.

From now on, we specialise to bounded chain complexes of finitely generated R-modules. In this section we will prove that the category $\mathsf{Ch}({}_R\mathsf{mod})^b_{\text{skew}}$ is equivalent to the category of bounded chain complexes of finitely generated A-modules. This will be a key ingredient in the proof of our main commensurability theorem. The results in this section are the analogues of the results from Section 6 of [BL17], and as before, the proofs mainly generalise in a straightforward manner.

Lemma 5.18. *Let $L \in \mathsf{Ch}({}_R\mathsf{mod})^b$.*

(i) The Z-torsion submodules of the L_i constitute a finite chain complex $L_{\text{tors}} \in \mathsf{Ch}({}_R\mathsf{mod})^b$. There is a natural monomorphism $L_{\text{tors}} \hookrightarrow L$ and a natural epimorphism $L \twoheadrightarrow L/L_{\text{tors}}$.

(ii) L is finite if and only if $L = L_{\text{tors}}$ and if and only if there is $0 \neq z \in Z$ such that $zL = 0$, where zL denotes the chain complex $(zL_i)_i$.

(iii) Let $0 \neq z \in Z$. Then multiplication by z defines an isogeny $L \to L$.

(iv) Tensoring with Q over Z gives a chain complex $Q \otimes_Z L$ of finitely generated A-modules. The kernel of the natural map $L \to Q \otimes_Z L$ is L_{tors}. Moreover, $Q \otimes_Z L = 0$ if and only if L is finite.

Proof. All statements follow easily from [BL17, Lemmas 4.1 and 6.2]. For part (iv) cf. also Lemma 3.1. □

Proposition 5.19. *Let $L, M \in \mathsf{Ch}({}_R\mathsf{mod})^b$. Then the following are equivalent:*

(i) There exists an isogeny $L \to M$,

(ii) there exists a commensurability $L \rightleftharpoons M$,

(iii) there exists an isomorphism $Q \otimes_Z L \cong Q \otimes_Z M$ of chain complexes of A-modules.

Proof. Bearing in mind the properties from Lemma 5.18, one can do essentially the same proof as in [BL17, Theorem 6.3]. With notation as in loc. cit., the only things to note are: Since we are dealing with bounded chain complexes, there are "global" elements $0 \neq m_1, m_2, m_3 \in Z$ such that $m_1\phi(\overline{L}) \hookrightarrow \overline{M}$, $m_2\overline{M} \hookrightarrow \phi(\overline{L})$ and $m_3 M_{\mathrm{tors}} = 0$; replace the use of [BL17, Proposition 2.1] by Proposition 5.7. □

Lemma 5.20. *Let $L, M \in \mathsf{Ch}({}_R\mathsf{mod})^b$. Suppose that $(X, f, g), (Y, h, j) \colon L \rightleftharpoons M$ are equivalent skew correspondences. Then*

$$(Q \otimes_Z g) \circ (Q \otimes_Z f)^{-1} = (Q \otimes_Z j) \circ (Q \otimes_Z h)^{-1}.$$

Proof. The proof of [BL17, Lemma 6.4] immediately generalises, taking again Lemma 5.18 into account. □

The previous lemma allows us to define a functor

$$\mathcal{F} \colon \mathsf{Ch}({}_R\mathsf{mod})^b_{\mathrm{skew}} \to \mathsf{Ch}({}_A\mathsf{mod})^b$$

which sends a bounded chain complex L of finitely generated R-modules to $Q \otimes_Z L$ and an equivalence class of skew correspondences represented by $(X, f, g) \colon L \rightleftharpoons M$ to the chain map $(Q \otimes_Z g) \circ (Q \otimes_Z f)^{-1}$. It is easy to check that this indeed defines a functor.

We are now going to show that $\mathcal{F}$ is an equivalence of categories.

Lemma 5.21. *Any element of $\mathsf{Ch}({}_A\mathsf{mod})^b$ is isomorphic to $\mathcal{F}(L)$ for some element $L \in \mathsf{Ch}({}_R\mathsf{mod})^b_{\mathrm{skew}}$.*

Proof. Let $V = (V_i, \partial_i)_i \in \mathsf{Ch}({}_A\mathsf{mod})^b$. Without loss of generality, there is $m \in \mathbb{Z}_{>0}$ such that $V_i = 0$ for $i > m$ and $i < 0$.

$$\begin{tikzcd} \cdots \arrow[r] & 0 \arrow[r] & V_m \arrow[r, "\partial_m"] & V_{m-1} \arrow[r, "\partial_{m-1}"] & \cdots \arrow[r, "\partial_1"] & V_0 \arrow[r] & 0 \arrow[r] & \cdots \end{tikzcd}$$

We now inductively choose A-generating systems $(v_1^i, \ldots, v_{n_i}^i)$ of V_i, $i = 0, \ldots, m$, such that $\partial_i(v_k^i)$ is contained in the R-span of $(v_1^{i-1}, \ldots, v_{n_{i-1}}^{i-1})$ for all k. For $i = 0$ we may choose any A-generating system of V_0. For $i > 0$ start by choosing any A-generating system $(w_1^i, \ldots, w_{n_i}^i)$ of V_i. Since $A = Q \cdot R$, we can find $0 \neq z \in Z$ such that $z\partial_i(w_k^i)$ is contained in the R-span of $(v_1^{i-1}, \ldots, v_{n_{i-1}}^{i-1})$ for all k. We then put $v_k^i := zw_k^i$.

Define L_i to be the R-span of $(v_1^i, \ldots, v_{n_i}^i)$ for $i = 0, \ldots, m$, and to be 0 otherwise. Then $\partial_i(L_i) \subseteq L_{i-1}$ for all $i \in \mathbb{Z}$, so $L := (L_i, \partial_i) \in \mathsf{Ch}({}_R\mathsf{mod})^b_{\mathrm{skew}}$. It is easy to see that the map $f = (f_i)_i \colon Q \otimes_Z L \to V$ with

$$f_i \colon Q \otimes_Z L_i \to V_i, \ q \otimes x \mapsto qx$$

is an isomorphism of chain complexes of A-modules. □

Lemma 5.22. *Let $L, M \in \mathsf{Ch}({}_R\mathsf{mod})^b_{\text{skew}}$ and let $\phi\colon \mathcal{F}(L) \to \mathcal{F}(M)$ be a chain map. Then there exists a skew correspondence $c\colon L \rightleftharpoons M$ such that $\mathcal{F}(c) = \phi$.*

Proof. Bearing in mind the properties from Lemma 5.18, one can do essentially the same proof as in [BL17, Lemma 6.7]. With notation as in loc. cit., the only things to note are: Since we are dealing with bounded chain complexes, there is a "global" element $0 \neq m \in Z$ such that $m\phi(\overline{L}) \hookrightarrow \overline{M}$; one can check that $\mathcal{F}(c) = \phi$ componentwise. □

Lemma 5.23. *Let $L, M \in \mathsf{Ch}({}_R\mathsf{mod})^b_{\text{skew}}$ and suppose that $c, d\colon L \rightleftharpoons M$ are skew correspondences with $\mathcal{F}(c) = \mathcal{F}(d)$. Then c and d are equivalent.*

We give a simplified version of the proof of [BL17, Lemma 6.8] without case distinction and correct it slightly, noting that in its second paragraph it only follows that f and h are injective and that $X \times_{L\oplus M} Y \to X \times_L Y$ is an injective isogeny rather than an isomorphism.

Proof. Write $c = (X, f, g)$ and $d = (Y, h, j)$. It suffices to show that in the fibre product

$$\begin{tikzcd}
X \times_{L\oplus M} Y \arrow[r, "\pi_Y"] \arrow[d, "\pi_X"'] & Y \arrow[d, "{(h,j)}"] \\
X \arrow[r, "{(f,g)}"'] & L \oplus M
\end{tikzcd}$$

both π_X and π_Y are isogenies. Now by the universal property of the fibre product there is a unique morphism $\psi\colon X \times_{L\oplus M} Y \to X \times_L Y$ such that $\pi_X = \pi'_X\psi$ and $\pi_Y = \pi'_Y\psi$ where π'_X and π'_Y are the canonical morphisms as given in the diagram below.

$$\begin{tikzcd}
X \times_{L\oplus M} Y \arrow[rd, dashed, "\psi"] \arrow[rrd, bend left, "\pi_Y"] \arrow[rdd, bend right, "\pi_X"'] & & \\
& X \times_L Y \arrow[r, "\pi'_Y"] \arrow[d, "\pi'_X"'] & Y \arrow[d, "h"] \\
& X \arrow[r, "f"'] & L
\end{tikzcd}$$

We show that ψ is an isogeny. By Remark 5.2, the components of ψ are the unique R-module homomorphisms $\psi_i\colon X_i \times_{L_i\oplus M_i} Y_i \to X_i \times_{L_i} Y_i$ such that $(\pi_X)_i = (\pi'_X)_i\psi_i$ and $(\pi_Y)_i = (\pi'_Y)_i\psi_i$, thus sending $(x_i, y_i) \in X_i \times_{L_i\oplus M_i} Y_i$ to (x_i, y_i). It is clear that these maps are injective. Let $i \in \mathbb{Z}$ and let $(x_i, y_i) \in X_i \times_{L_i} Y_i$. By Lemma 5.18 (i) and (ii) there is $0 \neq z \in Z$ such that $zM_{\text{tors}} = 0$. The condition $\mathcal{F}(c) = \mathcal{F}(d)$ implies that

$$\begin{aligned}
1 \otimes g_i(x_i) &= (Q \otimes_Z g_i) \circ (Q \otimes_Z f_i)^{-1}(1 \otimes f_i(x_i)) \\
&= (Q \otimes_Z j_i) \circ (Q \otimes_Z h_i)^{-1}(1 \otimes h_i(y_i)) \\
&= 1 \otimes j_i(y_i),
\end{aligned}$$

and Lemma 5.18 (iv) then yields $zg_i(x_i) = zj_i(y_i)$. Consequently, $z(X_i \times_{L_i} Y_i) \subseteq \operatorname{im}\psi_i$. We conclude from Lemma 5.18 (iii) that ψ_i is an isogeny and then from Remark 5.2 that ψ is an isogeny.

As c and d are skew correspondences, Proposition 5.8 shows that both π'_X and π'_Y are isogenies. Hence, also π_X and π_Y are isogenies by Proposition 5.7. □

Proposition 5.24. *The functor* $\mathcal{F}\colon \mathsf{Ch}({}_R\mathsf{mod})^b_{\text{skew}} \to \mathsf{Ch}({}_A\mathsf{mod})^b$ *is an equivalence of categories.*

Proof. The functor $\mathcal{F}$ is essentially surjective by Lemma 5.21, is full by Lemma 5.22 and is faithful by Lemma 5.23. Hence it is an equivalence of categories. □

As in [BL17], one obtains the following crucial statement from Propositions 5.24 and 5.16:

Corollary 5.25. *Let* $L \in \mathsf{Ch}({}_R\mathsf{mod})^b$. *Then the map*

$$G_L \to \operatorname{Aut}(Q \otimes_Z L),\ (X, f, g) \mapsto (Q \otimes_Z g) \circ (Q \otimes_Z f)^{-1}$$

is a group isomorphism.

For an explicit description of the inverse isomorphism, see the proof of Proposition 5.28 below.

5.4 From Commensurabilities of Chain Complexes to Commensurabilities of Automorphism Groups

Keep using Setup 5.17. We now pass from correspondences of chain complexes to correspondences of their endomorphism rings and automorphism groups.

Definition 5.26. Let $c = (X, f, g)\colon L \rightleftharpoons M$ be a correspondence in $\mathsf{Ch}({}_R\mathsf{mod})^b$.

(a) Define the *endomorphism ring* of c to be

$$\operatorname{End} c := \{\, (\lambda, \xi, \mu) \in (\operatorname{End} L) \times (\operatorname{End} X) \times (\operatorname{End} M) \mid \lambda f = f\xi, \mu g = g\xi \,\}\,.$$

Write $\mathrm{e}(c)\colon \operatorname{End} L \rightleftharpoons \operatorname{End} M$ for the correspondence that consists of the canonical projections $\operatorname{End} c \to \operatorname{End} L$ and $\operatorname{End} c \to \operatorname{End} M$.

$$\begin{tikzcd}
 & X \arrow[dl, "f"'] \arrow[dr, "g"] \arrow[ddd, "\xi"] & \\
L \arrow[d, "\lambda"] & & M \arrow[d, "\mu"] \\
L & & M \\
 & X \arrow[ul, "f"] \arrow[ur, "g"'] &
\end{tikzcd}$$

(b) Define the *automorphism group* of c to be $\operatorname{Aut} c := (\operatorname{End} c)^\times$. Write $\mathrm{a}(c)\colon \operatorname{Aut} L \rightleftharpoons \operatorname{Aut} M$ for the correspondence that consists of the canonical projections $\operatorname{Aut} c \to \operatorname{Aut} L$ and $\operatorname{Aut} c \to \operatorname{Aut} M$.

Proposition 5.27. *Let $L, M, N \in \mathsf{Ch}({}_R\mathsf{mod})^b$. Let $c, c'\colon L \rightleftharpoons M$ and $d\colon M \rightleftharpoons N$ be commensurabilities. Then the following hold:*

(i) The correspondence $\mathrm{e}(c)\colon \operatorname{End} L \rightleftharpoons \operatorname{End} M$ is a ring commensurability and the correspondence $\mathrm{a}(c)\colon \operatorname{Aut} L \rightleftharpoons \operatorname{Aut} M$ is a group commensurability.

(ii) We have $\mathrm{e}(d \circ c) \sim \mathrm{e}(d) \circ \mathrm{e}(c)$ and $\mathrm{a}(d \circ c) \sim \mathrm{a}(d) \circ \mathrm{a}(c)$.

(iii) If $c \cong c'$, then $\mathrm{e}(c) \cong \mathrm{e}(c')$ and $\mathrm{a}(c) \cong \mathrm{a}(c')$. If $c \sim c'$, then $\mathrm{e}(c) \sim \mathrm{e}(c')$ and $\mathrm{a}(c) \sim \mathrm{a}(c')$.

Proof. The proofs are essentially the same as for the statements 7.1 through 7.4 of [BL17]. One first proves the analogue statement of [BL17, Lemma 7.1] for chain complexes. The proof is exactly the same, replacing [BL17, Lemma 6.2] by Lemma 5.18. To be able to apply [BL17, Lemma 4.1] to $\operatorname{End} L$ one needs that $\operatorname{End} L$ is finitely generated Z-module. This follows by embedding it into $\bigoplus_i \operatorname{End} L_i$ and using [Rei03, Theorem 2.34] and the fact that Z is noetherian.

One then concludes statement (i) as in the proof of [BL17, Theorem 7.2].

Part (ii) is proved exactly as [BL17, Theorem 7.3], replacing [BL17, Propositions 2.6 and 2.1] by Proposition 5.14 (v) and Proposition 5.7, respectively. That the map $\operatorname{End} c \times_{\operatorname{End} M} \operatorname{End} d \to \operatorname{End}(d \circ c)$ is well-defined, needs to be checked componentwise, using Remark 5.2.

Finally, part (iii) is proved exactly as [BL17, Proposition 7.4], replacing [BL17, Propositions 2.13 and 2.11] by Proposition 5.14 (viii) and (i). The canonical isomorphisms appearing also hold for chain complexes, using again Remark 5.2. □

By the above proposition and Proposition 5.14 (v) and (vi), we have two functors of groupoids

$$\mathsf{Ch}({}_R\mathsf{mod})^b_{\mathrm{com}} \to \mathbb{Q}_{>0},\ c \mapsto \mathrm{i}(\mathrm{e}(c)),$$
$$\mathsf{Ch}({}_R\mathsf{mod})^b_{\mathrm{com}} \to \mathbb{Q}_{>0},\ c \mapsto \mathrm{i}(\mathrm{a}(c)),$$

where we regard $\mathbb{Q}_{>0}$ as a groupoid with one object. For any $L \in \mathsf{Ch}({}_R\mathsf{mod})^b$ we in particular get group homomorphisms

$$\mathrm{i} \circ \mathrm{e}, \mathrm{i} \circ \mathrm{a} \colon G_L = \mathrm{Hom}_{\mathsf{Ch}({}_R\mathsf{mod})^b_{\mathrm{com}}}(L, L) \to \mathbb{Q}_{>0}.$$

Now recall that $G_L \cong \mathrm{Aut}(Q \otimes_Z L)$ by Corollary 5.25. The above two group homomorphisms have the following crucial property:

Proposition 5.28. *Let $L \in \mathsf{Ch}({}_R\mathsf{mod})^b$. Suppose that $c \in G_L$ corresponds to an element $\alpha \in \mathfrak{Z}(\mathrm{End}(Q \otimes_Z L))^\times \subseteq \mathrm{Aut}(Q \otimes_Z L)$. Then $\mathrm{e}(c) \sim (\mathrm{End}\, L, \mathrm{id}, \mathrm{id})$. In particular, we have $\mathrm{i}(\mathrm{e}(c)) = \mathrm{i}(\mathrm{a}(c)) = 1$.*

Proof. We closely follow the proof of [BL17, Proposition 7.8]. By Lemma 5.18, the natural morphism $f \colon L \twoheadrightarrow L/L_{\mathrm{tors}}$ is an isogeny and hence induces an isomorphism

$$\mathrm{End}(Q \otimes_Z L) \xrightarrow{\sim} \mathrm{End}(Q \otimes L/L_{\mathrm{tors}}),\ \beta \mapsto (Q \otimes_Z f) \circ \beta \circ (Q \otimes_Z f)^{-1}.$$

The commensurability $c_f \colon L \rightleftharpoons L/L_{\mathrm{tors}}$ further gives an isomorphism

$$G_L \xrightarrow{\sim} G_{L/L_{\mathrm{tors}}},\ d \mapsto c_f \circ d \circ c_f^{-1}$$

which fits into a commutative diagram

$$\begin{tikzcd}
G_L \arrow[r, "\sim"] \arrow[d, "\wr"] & G_{L/L_{\mathrm{tors}}} \arrow[d, "\wr"] \\
\mathrm{Aut}(Q \otimes_Z L) \arrow[r, "\sim"] & \mathrm{Aut}(Q \otimes L/L_{\mathrm{tors}}).
\end{tikzcd}$$

This diagram together with Proposition 5.27 (iii) shows that we may assume that $L_{\mathrm{tors}} = 0$. Then by Lemma 5.18 we have monomorphisms $L \hookrightarrow Q \otimes_Z L$ and $\mathrm{End}\, L \hookrightarrow \mathrm{End}(Q \otimes_Z L)$. In the following we will tacitly regard L as a subcomplex of $Q \otimes_Z L$ and $\mathrm{End}\, L$ as a subring of $\mathrm{End}(Q \otimes_Z L)$ via these maps.

It follows from the proof of [BL17, Proposition 7.8] applied componentwise that c is equivalent to the commensurability $(L \cap \alpha^{-1} L, i, \alpha i) \colon L \rightleftharpoons L$ where $i \colon L \cap \alpha^{-1} L \hookrightarrow L$ is the natural morphism and the intersection takes place componentwise in the components of $Q \otimes_Z L$ to form the complex $L \cap \alpha^{-1} L$. Thus we have

$$\mathrm{End}\, c = \left\{ (\lambda, \xi, \mu) \in (\mathrm{End}\, L) \times \mathrm{End}(L \cap \alpha^{-1} L) \times (\mathrm{End}\, L) \,\middle|\, \lambda i = i\xi, \mu\alpha i = \alpha i \xi \right\}.$$

Let $(\lambda, \xi, \mu) \in \operatorname{End} c$. Then the above conditions immediately imply that $\alpha\lambda i = \mu\alpha i$. We show that in fact $\alpha\lambda = \mu\alpha$. It is enough to check this componentwise, so let $j \in \mathbb{Z}$. Since L_j is finitely generated, there is $0 \neq z \in Z$ such that $z\alpha_j(L_j) \subseteq L_j$ which gives $zL_j \subseteq L_j \cap \alpha_j^{-1} L_j$. Hence, $\alpha_j\lambda_j$ and $\mu_j\alpha_j$ agree on zL_j. But the latter generates $Q \otimes_Z L_j$ over Q, so we must have $\alpha_j\lambda_j = \mu_j\alpha_j$. In summary, we have shown that $\lambda = \alpha^{-1}\mu\alpha$ which implies $\lambda = \mu$ as $\alpha \in \mathfrak{Z}(\operatorname{End}(Q \otimes_Z L))^\times$.

By the above, we have $\mathrm{e}(c) = (\operatorname{End} c, p_0, p_0)\colon \operatorname{End} L \rightleftharpoons \operatorname{End} L$, with p_0 an isogeny by Proposition 5.27 (i). Hence, the commensurability $c_{p_0}\colon \operatorname{End} c \rightleftharpoons \operatorname{End} L$ defines an equivalence between $\mathrm{e}(c)$ and $(\operatorname{End} L, \mathrm{id}, \mathrm{id})$. □

5.5 The Index of Automorphism Groups of Chain Complexes

Again keep using Setup 5.17. We are finally ready to define the index of automorphism groups of suitable chain complexes, generalising the results from Section 8 of [BL17].

Proposition 5.29. *Let $L, M \in \mathsf{Ch}({}_R\mathsf{mod})^b$. Then the following hold:*

(i) There is a commensurability $L \rightleftharpoons M$ if and only if the chain complexes of A-modules $Q \otimes_Z L$ and $Q \otimes_Z M$ are isomorphic.

(ii) If $c\colon L \rightleftharpoons M$ is a commensurability, then $\mathrm{e}(c)\colon \operatorname{End} L \rightleftharpoons \operatorname{End} M$ is a ring commensurability and $\mathrm{a}(c)\colon \operatorname{Aut} L \rightleftharpoons \operatorname{Aut} M$ is a group commensurability.

(iii) Suppose that $c, c'\colon L \rightleftharpoons M$ are commensurabilities. Assume that $\operatorname{End}(Q \otimes_Z L) \cong \operatorname{End}(Q \otimes_Z M)$ is a semisimple ring. Then

$$\mathrm{i}(\mathrm{e}(c)) = \mathrm{i}(\mathrm{e}(c')), \qquad \mathrm{i}(\mathrm{a}(c)) = \mathrm{i}(\mathrm{a}(c')).$$

Proof. We argue as in the proof of [BL17, Theorem 8.1]. Part (i) is Proposition 5.19 and part (ii) is Proposition 5.27. By Proposition 5.27 (iii) and Proposition 5.14 (v), claim (iii) is equivalent to the statement

$$\mathrm{i}(\mathrm{e}(c^{-1} \circ c')) = \mathrm{i}(\mathrm{a}(c^{-1} \circ c')) = 1.$$

Hence, to conclude it suffices to show that the two group homomorphisms

$$\mathrm{i} \circ \mathrm{e}, \mathrm{i} \circ \mathrm{a}\colon G_L = \operatorname{Hom}_{\mathsf{Ch}({}_R\mathsf{mod})^b_{\mathrm{com}}}(L, L) \to \mathbb{Q}_{>0}$$

are trivial. Let $B := \operatorname{End}(Q \otimes_Z L)$. Then $B^\times \cong G_L$ by Corollary 5.25, and $\mathrm{i} \circ \mathrm{e}$ and $\mathrm{i} \circ \mathrm{a}$ factor through $B^\times / \mathfrak{Z}(B)^\times$ by Proposition 5.28. Since $\mathbb{Q}_{>0}$ is abelian, they also factor through $B^\times / [B^\times, B^\times]$. So $\mathrm{i} \circ \mathrm{e}$ and $\mathrm{i} \circ \mathrm{a}$ factor through $B^\times / (\mathfrak{Z}(B)^\times [B^\times, B^\times])$.

By assumption, B is semisimple. We show that B is finitely generated over its centre. For this first note that $\mathfrak{Z}(A) \subseteq \mathfrak{Z}(B)$ and that the natural map

$$B = \operatorname{End}(Q \otimes_Z L) \hookrightarrow \prod_i \operatorname{End}_A(Q \otimes_Z L_i), \; f \mapsto (f_i)_i$$

is a $\mathfrak{Z}(A)$-algebra homomorphism. The fact that A is a finite-dimensional Q-algebra implies that $\mathfrak{Z}(A)$ is a noetherian ring and that A is a finitely generated $\mathfrak{Z}(A)$-module. Hence, it follows from [Rei03, Theorem 2.34] that $\operatorname{End}_A(Q \otimes_Z L_i)$ is a finitely generated $\mathfrak{Z}(A)$-module for all i. But then also $B = \operatorname{End}(Q \otimes_Z L)$ is a finitely generated $\mathfrak{Z}(A)$-module, since $\mathfrak{Z}(A)$ is noetherian. In particular, B is finitely generated over $\mathfrak{Z}(B)$. This allows us to apply [BL17, Theorem 5.6] which shows that $B^\times/(\mathfrak{Z}(B)^\times[B^\times, B^\times])$ is an abelian group of finite exponent. Hence, any homomorphism $B^\times/(\mathfrak{Z}(B)^\times[B^\times, B^\times]) \to \mathbb{Q}_{>0}$ is trivial and the claim follows. □

The following example shows that the semisimplicity assumption in part (iii) is necessary.

Example 5.30. In the above proposition we consider the case $Z = \mathbb{Z}$, $Q = \mathbb{Q}$, $A = Q = \mathbb{Q}$, $R = Z = \mathbb{Z}$. Let L be the exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \mathbb{Z} \arrow[r] & \mathbb{Z}^2 \arrow[r] & \mathbb{Z} \arrow[r] & 0 \end{tikzcd}$$

where $\mathbb{Z} \to \mathbb{Z}^2$ sends x to $(x, 0)$ and $\mathbb{Z}^2 \to \mathbb{Z}$ sends (x, y) to y. It is easy to see that there is an isomorphism $\operatorname{End} L \xrightarrow{\sim} \left(\begin{smallmatrix} \mathbb{Z} & \mathbb{Z} \\ 0 & \mathbb{Z} \end{smallmatrix}\right)$ given by sending an endomorphism $L \to L$ to its middle map $\mathbb{Z}^2 \to \mathbb{Z}^2$. In the same way, one has $\operatorname{End}(\mathbb{Q} \otimes_{\mathbb{Z}} L) \cong \left(\begin{smallmatrix} \mathbb{Q} & \mathbb{Q} \\ 0 & \mathbb{Q} \end{smallmatrix}\right)$. In particular, $\operatorname{End}(\mathbb{Q} \otimes_{\mathbb{Z}} L)$ is not semisimple.

We now give examples of commensurabilities $c, c' \colon L \rightleftharpoons L$ for which $\mathrm{i}(\mathrm{e}(c)) \neq \mathrm{i}(\mathrm{e}(c'))$ and $\mathrm{i}(\mathrm{a}(c)) \neq \mathrm{i}(\mathrm{a}(c'))$. In fact, it will turn out that these values can be arbitrarily far apart. To this end, let $0 \neq n, m \in \mathbb{Z}$ with $\gcd(n, m) = 1$. The map $f_{n,m} \colon L \to L$ given by

$$\begin{tikzcd} 0 \arrow[r] & \mathbb{Z} \arrow[r] \arrow[d, "\cdot n"] & \mathbb{Z}^2 \arrow[r] \arrow[d, "\left(\begin{smallmatrix} n & 0 \\ 0 & m \end{smallmatrix}\right)"] & \mathbb{Z} \arrow[r] \arrow[d, "\cdot m"] & 0 \\ 0 \arrow[r] & \mathbb{Z} \arrow[r] & \mathbb{Z}^2 \arrow[r] & \mathbb{Z} \arrow[r] & 0 \end{tikzcd}$$

is clearly an isogeny. Hence, we get a commensurability $c_{n,m} := (L, \mathrm{id}, f_{n,m}) \colon L \rightleftharpoons L$. Under the isomorphism $\operatorname{End} L \cong \left(\begin{smallmatrix} \mathbb{Z} & \mathbb{Z} \\ 0 & \mathbb{Z} \end{smallmatrix}\right)$, the endomorphism ring $\operatorname{End} c_{n,m}$ corresponds to

$$\begin{aligned} E := & \left\{ (\lambda, \lambda, \mu) \in \begin{pmatrix} \mathbb{Z} & \mathbb{Z} \\ 0 & \mathbb{Z} \end{pmatrix}^3 \;\middle|\; \mu \begin{pmatrix} n & 0 \\ 0 & m \end{pmatrix} = \begin{pmatrix} n & 0 \\ 0 & m \end{pmatrix} \lambda \right\} \\ = & \left\{ (\lambda, \lambda, \mu) \in \begin{pmatrix} \mathbb{Z} & \mathbb{Z} \\ 0 & \mathbb{Z} \end{pmatrix}^3 \;\middle|\; \lambda_{11} = \mu_{11},\ \lambda_{22} = \mu_{22},\ n\lambda_{21} = m\mu_{21} \right\}. \end{aligned}$$

The projection $p_0 \colon E \to \left(\begin{smallmatrix} \mathbb{Z} & \mathbb{Z} \\ 0 & \mathbb{Z} \end{smallmatrix}\right)$, $(\lambda, \lambda, \mu) \mapsto \lambda$ is clearly injective and by the condition $\gcd(n, m) = 1$ has image $\left(\begin{smallmatrix} \mathbb{Z} & m\mathbb{Z} \\ 0 & \mathbb{Z} \end{smallmatrix}\right)$. Analogously, $p_1 \colon E \to \left(\begin{smallmatrix} \mathbb{Z} & \mathbb{Z} \\ 0 & \mathbb{Z} \end{smallmatrix}\right)$, $(\lambda, \lambda, \mu) \mapsto \mu$ is injective and has image $\left(\begin{smallmatrix} \mathbb{Z} & n\mathbb{Z} \\ 0 & \mathbb{Z} \end{smallmatrix}\right)$. Hence, $\mathrm{i}(\mathrm{e}(c_{n,m})) = \frac{\mathrm{i}(p_1)}{\mathrm{i}(p_0)} = \frac{n}{m}$.

For the commensurability of automorphism groups, we get that under the isomorphism $\operatorname{End} L \cong \left(\begin{smallmatrix} \mathbb{Z} & \mathbb{Z} \\ 0 & \mathbb{Z} \end{smallmatrix}\right)$, the automorphism group $\operatorname{Aut} c_{n,m}$ corresponds to

$$E^\times = \left\{ (\lambda, \lambda, \mu) \in \begin{pmatrix} \pm 1 & \mathbb{Z} \\ 0 & \pm 1 \end{pmatrix}^3 \,\middle|\, \lambda_{11} = \mu_{11},\ \lambda_{22} = \mu_{22},\ n\lambda_{21} = m\mu_{21} \right\}.$$

Hence, $p_0 \colon E^\times \to \left(\begin{smallmatrix} \pm 1 & \mathbb{Z} \\ 0 & \pm 1 \end{smallmatrix}\right)$, $(\lambda, \lambda, \mu) \mapsto \lambda$ is injective and has image $\left(\begin{smallmatrix} \pm 1 & m\mathbb{Z} \\ 0 & \pm 1 \end{smallmatrix}\right)$, and $p_1 \colon E^\times \to \left(\begin{smallmatrix} \pm 1 & \mathbb{Z} \\ 0 & \pm 1 \end{smallmatrix}\right)$, $(\lambda, \lambda, \mu) \mapsto \mu$ is injective and has image $\left(\begin{smallmatrix} \pm 1 & n\mathbb{Z} \\ 0 & \pm 1 \end{smallmatrix}\right)$. Now it is easy to see that $\left|\left(\begin{smallmatrix} \pm 1 & \mathbb{Z} \\ 0 & \pm 1 \end{smallmatrix}\right) : \left(\begin{smallmatrix} 1 & \mathbb{Z} \\ 0 & 1 \end{smallmatrix}\right)\right| = 4$ and $\left|\left(\begin{smallmatrix} \pm 1 & m\mathbb{Z} \\ 0 & \pm 1 \end{smallmatrix}\right) : \left(\begin{smallmatrix} 1 & m\mathbb{Z} \\ 0 & 1 \end{smallmatrix}\right)\right| = 4$. Moreover, using that $\left(\begin{smallmatrix} 1 & \mathbb{Z} \\ 0 & 1 \end{smallmatrix}\right) \cong \mathbb{Z}$, one finds that $\left|\left(\begin{smallmatrix} 1 & \mathbb{Z} \\ 0 & 1 \end{smallmatrix}\right) : \left(\begin{smallmatrix} 1 & m\mathbb{Z} \\ 0 & 1 \end{smallmatrix}\right)\right| = m$. It follows that $\mathrm{i}(p_0) = m$ and $\mathrm{i}(p_1) = n$. Then by definition, $\mathrm{i}(\mathrm{a}(c_{n,m})) = \frac{n}{m}$.

The above proposition allows us to define the index of automorphism groups of chain complexes which become isomorphic over A with semisimple endomorphism ring as the index of the automorphism correspondence of any commensurability between the chain complexes, independently of that chosen commensurability.

Theorem 5.31. *Let $V \in \mathsf{Ch}({}_A\mathsf{mod})^b$ such that $\operatorname{End}(V)$ is a semisimple ring. Define*

$$\mathcal{S} := \mathcal{S}_V := \left\{ L \in \mathsf{Ch}({}_R\mathsf{mod})^b \,\middle|\, Q \otimes_Z L \cong V \right\}.$$

Then there is a unique function $\mathrm{ia} \colon \mathcal{S} \times \mathcal{S} \to \mathbb{Q}_{>0}$ such that:

(i) If $L, L', M, M' \in \mathcal{S}$ and $L \cong L'$ and $M \cong M'$, then $\mathrm{ia}(L, M) = \mathrm{ia}(L', M')$.

(ii) If $L, M, N \in \mathcal{S}$, then $\mathrm{ia}(L, M) \cdot \mathrm{ia}(M, N) = \mathrm{ia}(L, N)$.

(iii) If $L, M \in \mathcal{S}$ and there is a monomorphism $L \hookrightarrow M$ with finite cokernel, then with

$$H := \{ \mu \in \operatorname{Aut} M \mid \mu L = L \} := \{ \mu \in \operatorname{Aut} M \mid \mu_i L_i = L_i \textit{ for all } i \}$$

and

$$\rho \colon H \to \operatorname{Aut} L,\ \mu = (\mu_i) \mapsto \mu\big|_L := \left(\mu_i\big|_{L_i}\right)_i$$

one has

$$\mathrm{ia}(L, M) = \frac{|\operatorname{Aut} M : H| \cdot |\ker \rho|}{|\operatorname{Aut} L : \operatorname{im} \rho|}.$$

Proof. If $L, M \in \mathcal{S}$, then by Proposition 5.29 there is a commensurability $c \colon L \rightleftharpoons M$, and we may define $\mathrm{ia}(L, M) := \mathrm{i}(\mathrm{a}(c))$, independently of c. That this function uniquely satisfies properties (i), (ii) and (iii) is proved exactly as in [BL17, Theorem 8.3], making use of Lemma 5.18. □

Properties (i), (ii) and (iii) make precise the statement that one should think of $\mathrm{ia}(L, M)$ as $|\operatorname{Aut} M : \operatorname{Aut} L|$. Note that in contrast to [BL17, Section 8], we do not require A to be semisimple but instead $\operatorname{End}(V)$ to be semisimple (and R to be left-noetherian, which previously was implied by semisimplicity of A). This is because, unlike for modules, semisimplicity of A does not imply semisimplicity of the endomorphism ring of a bounded chain complex of finitely generated A-modules, cf. Example 5.30.

5.6 The Index of Subgroups of Automorphism Groups of Chain Complexes

Again keep using Setup 5.17.

Let $L, M \in \mathsf{Ch}({}_R\mathsf{mod})^b$ be commensurable. We aim to generalise the results obtained above such that we may also define an index of certain subgroups $\Gamma_L \leq \operatorname{Aut} L$ and $\Gamma_M \leq \operatorname{Aut} M$ of the automorphism groups of L and M.

Definition 5.32. Let $L, M \in \mathsf{Ch}({}_R\mathsf{mod})^b$ and let $\Gamma_L \leq \operatorname{Aut} L$ and $\Gamma_M \leq \operatorname{Aut} M$. Let $c = (X, f, g) \colon L \rightleftharpoons M$ be a correspondence in $\mathsf{Ch}({}_R\mathsf{mod})^b$. We define

$$\operatorname{Aut}(c)|_{\Gamma_L,\Gamma_M} := \{ (\lambda, \xi, \mu) \in \Gamma_L \times (\operatorname{Aut} X) \times \Gamma_M \mid \lambda f = f\xi, \mu g = g\xi \}$$

and write $\mathrm{a}(c)|_{\Gamma_L,\Gamma_M} \colon \Gamma_L \rightleftharpoons \Gamma_M$ for the correspondence that consist of the canonical projections $\operatorname{Aut}(c)|_{\Gamma_L,\Gamma_M} \to \Gamma_L$ and $\operatorname{Aut}(c)|_{\Gamma_L,\Gamma_M} \to \Gamma_M$. We call $\mathrm{a}(c)|_{\Gamma_L,\Gamma_M}$ the *automorphism correspondence of c restricted to Γ_L and Γ_M.*

5.6.1 Basic Properties of Restricted Automorphism Correspondences

The restricted and unrestricted automorphism correspondences are related as follows.

Proposition 5.33. *Let $L, M \in \mathsf{Ch}({}_R\mathsf{mod})^b$ and let $\Gamma_L \leq \operatorname{Aut} L$ and $\Gamma_M \leq \operatorname{Aut} M$. Let $c \colon L \rightleftharpoons M$ be a correspondence. Denote by $i_L \colon \Gamma_L \hookrightarrow \operatorname{Aut} L$ and $i_M \colon \Gamma_M \hookrightarrow \operatorname{Aut} M$ the inclusions. Then*

$$\mathrm{a}(c)|_{\Gamma_L,\Gamma_M} \cong c_{i_M}^{-1} \circ \mathrm{a}(c) \circ c_{i_L}.$$

Proof. One easily checks that

$$\alpha \colon \operatorname{Aut}(c)|_{\Gamma_L,\Gamma_M} \to \Gamma_L \times_{\operatorname{Aut} L} \operatorname{Aut}(c) \times_{\operatorname{Aut} M} \Gamma_M,\ (\lambda, \xi, \mu) \mapsto (\lambda, (\lambda, \xi, \mu), \mu)$$

is an isomorphism between $\mathrm{a}(c)|_{\Gamma_L,\Gamma_M}$ and $c_{i_M}^{-1} \circ \mathrm{a}(c) \circ c_{i_L}$. □

Lemma 5.34. *Let $L, M \in \mathsf{Ch}({}_R\mathsf{mod})^b$ and let $\Gamma_L \leq \operatorname{Aut} L$ and $\Gamma_M \leq \operatorname{Aut} M$. Let $c \colon L \rightleftharpoons M$ be a correspondence. Then*

$$\mathrm{a}(c^{-1})|_{\Gamma_M,\Gamma_L} \cong (\mathrm{a}(c)|_{\Gamma_L,\Gamma_M})^{-1}.$$

Proof. This is readily verified. □

We aim to show that the restricted correspondences $\mathrm{a}(c)|_{\Gamma_L,\Gamma_M}$ inherit some of the properties from $\mathrm{a}(c)$. For this, the following proposition is crucial.

Proposition 5.35. *Let $L, M, N \in \mathsf{Ch}({}_R\mathsf{mod})^b$ and let $\Gamma_L \leq \operatorname{Aut} L$, $\Gamma_M \leq \operatorname{Aut} M$ and $\Gamma_N \leq \operatorname{Aut} N$. Let $c\colon L \rightleftharpoons M$, $d\colon M \rightleftharpoons N$ and $e\colon L \rightleftharpoons N$ be correspondences. If $\mathrm{a}(d) \circ \mathrm{a}(c) \sim \mathrm{a}(e)$, then $\mathrm{a}(d)|_{\Gamma_M,\Gamma_N} \circ \mathrm{a}(c)|_{\Gamma_L,\Gamma_M} \sim \mathrm{a}(e)|_{\Gamma_L,\Gamma_N}$.*

Proof. Write $\mathrm{a}(c) = (\operatorname{Aut} c, p_c, q_c)$, and similarly for $\mathrm{a}(d)$ and $\mathrm{a}(e)$. Then we have $\mathrm{a}(c)|_{\Gamma_L,\Gamma_M} = (\operatorname{Aut}(c)|_{\Gamma_L,\Gamma_M}, p'_c, q'_c)$, where the dashes signify restriction, and analogously for $\mathrm{a}(d)|_{\Gamma_M,\Gamma_N}$ and $\mathrm{a}(e)|_{\Gamma_L,\Gamma_N}$. Let $(W, k, l)\colon \operatorname{Aut} c \times_{\operatorname{Aut} M} \operatorname{Aut} d \rightleftharpoons \operatorname{Aut} e$ be an equivalence between $\mathrm{a}(d) \circ \mathrm{a}(c)$ and $\mathrm{a}(e)$, so that we have the following commutative diagram:

$$\begin{tikzcd}
 & & & \operatorname{Aut} c \times_{\operatorname{Aut} M} \operatorname{Aut} d \arrow[dl] \arrow[drr] & & & \\
 & & \operatorname{Aut} c \arrow[dl, "p_c"'] \arrow[dr, "q_c"] & & & \operatorname{Aut} d \arrow[dll, "p_d"'] \arrow[dr, "q_d"] & \\
W \arrow[uurrr, bend left, "k"] \arrow[drrr, bend right, "l"'] & \operatorname{Aut} L & & \operatorname{Aut} M & & & \operatorname{Aut} N \\
 & & & \operatorname{Aut} e. \arrow[ull, "p_e"] \arrow[urrr, "q_e"'] & & &
\end{tikzcd}$$

Define

$$W' := k^{-1}\big(\operatorname{Aut}(c)|_{\Gamma_L,\Gamma_M} \times_{\Gamma_M} \operatorname{Aut}(d)|_{\Gamma_M,\Gamma_N}\big) \,\cap\, l^{-1}\big(\operatorname{Aut}(e)|_{\Gamma_L,\Gamma_N}\big)$$

and let $k'\colon W' \to \operatorname{Aut}(c)|_{\Gamma_L,\Gamma_M} \times_{\Gamma_M} \operatorname{Aut}(d)|_{\Gamma_M,\Gamma_N}$ and $l'\colon W' \to \operatorname{Aut}(e)|_{\Gamma_L,\Gamma_N}$ be the restrictions of k and l, respectively. We show that k' is an isogeny; in the same way one sees that l' is an isogeny. This will then prove the claim. Since k is an isogeny, it is clear that $\ker k'$ is finite. Moreover, it follows that

$$\frac{\operatorname{Aut}(c)|_{\Gamma_L,\Gamma_M} \times_{\Gamma_M} \operatorname{Aut}(d)|_{\Gamma_M,\Gamma_N}}{(\operatorname{Aut}(c)|_{\Gamma_L,\Gamma_M} \times_{\Gamma_M} \operatorname{Aut}(d)|_{\Gamma_M,\Gamma_N}) \cap k(W)}$$

is finite. Let $\sigma_1, \ldots, \sigma_n \in \operatorname{Aut}(c)|_{\Gamma_L,\Gamma_M} \times_{\Gamma_M} \operatorname{Aut}(d)|_{\Gamma_M,\Gamma_N}$ be a system of representatives for the classes in this quotient. Let $\sigma \in \operatorname{Aut}(c)|_{\Gamma_L,\Gamma_M} \times_{\Gamma_M} \operatorname{Aut}(d)|_{\Gamma_M,\Gamma_N}$. Then there is $i \in \{1, \ldots, n\}$ such that $\sigma\sigma_i^{-1} \in k(W)$. So there is $w \in W$ with $\sigma\sigma_i^{-1} = k(w)$. This means $w \in k^{-1}(\operatorname{Aut}(c)|_{\Gamma_L,\Gamma_M} \times_{\Gamma_M} \operatorname{Aut}(d)|_{\Gamma_M,\Gamma_N})$. By commutativity of the diagram above, it follows that also $w \in l^{-1}(\operatorname{Aut}(e)|_{\Gamma_L,\Gamma_N})$, so in fact $w \in W'$. Hence, $\sigma \equiv \sigma_i \mod k'(W')$. It follows that $\Big|\operatorname{Aut}(c)|_{\Gamma_L,\Gamma_M} \times_{\Gamma_M} \operatorname{Aut}(d)|_{\Gamma_M,\Gamma_N} : k'(W')\Big| < \infty$, so k' is an isogeny. □

Corollary 5.36. *Let $L, M, N \in \mathsf{Ch}({}_R\mathsf{mod})^b$. Let $\Gamma_L \leq \operatorname{Aut} L$, $\Gamma_M \leq \operatorname{Aut} M$ and $\Gamma_N \leq \operatorname{Aut} N$. Let $c, c'\colon L \rightleftharpoons M$ and $d\colon M \rightleftharpoons N$ be commensurabilities. Then the following hold:*

(i) *If* $c \sim c'$, *then* $\mathrm{a}(c)|_{\Gamma_L,\Gamma_M} \sim \mathrm{a}(c')|_{\Gamma_L,\Gamma_M}$.

(ii) *We have* $\mathrm{a}(d \circ c)|_{\Gamma_L,\Gamma_N} \sim \mathrm{a}(d)|_{\Gamma_M,\Gamma_N} \circ \mathrm{a}(c)|_{\Gamma_L,\Gamma_M}$.

Proof. This is immediate from Propositions 5.27 and 5.35. □

Corollary 5.37. *Let* $L \in \mathsf{Ch}({}_R\mathsf{mod})^b$ *and let* $\Gamma_L \leq \operatorname{Aut} L$. *Suppose that* $c \in G_L$ *corresponds to an element* $\alpha \in \mathfrak{Z}(\operatorname{End}(Q \otimes_Z L))^\times \subseteq \operatorname{Aut}(Q \otimes_Z L)$. *Then* $\mathrm{a}(c)|_{\Gamma_L,\Gamma_L} \sim (\Gamma_L, \mathrm{id}_{\Gamma_L}, \mathrm{id}_{\Gamma_L})$. *In particular, we have* $\mathrm{i}(\mathrm{a}(c)|_{\Gamma_L,\Gamma_L}) = 1$.

Proof. This follows from Propositions 5.28 and 5.35. □

5.6.2 Admissible Subgroups

Unlike when considering the full automorphism group, it is not guaranteed for any choice of $\Gamma_L \leq \operatorname{Aut} L$ and $\Gamma_M \leq \operatorname{Aut} M$ that if $c\colon L \rightleftharpoons M$ is a commensurability, then also $\mathrm{a}(c)|_{\Gamma_L,\Gamma_M}$ is a commensurability. One way to see this is to note that necessarily, Γ_L and Γ_M need to be commensurable as groups. Consider the case where $\operatorname{Aut} L$ and $\operatorname{Aut} M$ are both infinite. Choosing $\Gamma_L = \operatorname{Aut} L$ and $\Gamma_M = 1$, we have that for every commensurability $c\colon L \rightleftharpoons M$, the restricted correspondence $\mathrm{a}(c)|_{\Gamma_L,\Gamma_M}$ is *not* a commensurability. Thus, we need to restrict ourselves to suitable subgroups of the automorphism groups, for which we can feasibly define an index.

Definition 5.38. Let $L, M \in \mathsf{Ch}({}_R\mathsf{mod})^b$ be commensurable and let $\Gamma_L \leq \operatorname{Aut} L$ and $\Gamma_M \leq \operatorname{Aut} M$. We say that the pair (Γ_L, Γ_M) is *admissible* for (L, M) if for every commensurability $c\colon L \rightleftharpoons M$ we have that $\mathrm{a}(c)|_{\Gamma_L,\Gamma_M}\colon \Gamma_L \rightleftharpoons \Gamma_M$ is a group commensurability.

Proposition 5.39. *Let* $L, M, N \in \mathsf{Ch}({}_R\mathsf{mod})^b$ *be commensurable and let* $\Gamma_L \leq \operatorname{Aut} L$, $\Gamma_M \leq \operatorname{Aut} M$ *and* $\Gamma_N \leq \operatorname{Aut} N$.

(i) *If* (Γ_L, Γ_M) *is admissible for* (L, M), *then* (Γ_M, Γ_L) *is admissible for* (M, L).

(ii) *If* (Γ_L, Γ_M) *and* (Γ_M, Γ_N) *are admissible for* (L, M) *and* (M, N), *respectively, then* (Γ_L, Γ_N) *is admissible for* (L, N).

Proof. Statement (i) follows from Lemma 5.34. To prove (ii), suppose that (Γ_L, Γ_M) and (Γ_M, Γ_N) are admissible for (L, M) and (M, N), respectively. Let $e\colon L \rightleftharpoons N$ be a commensurability. Choose any commensurability $c\colon L \rightleftharpoons M$. Then $e \circ c^{-1}\colon M \rightleftharpoons N$ is a commensurability by Proposition 5.14 (v). From the assumption and Proposition 5.14 and Corollary 5.36, it follows that

$$\mathrm{a}(e)|_{\Gamma_L,\Gamma_N} \sim \mathrm{a}(e \circ c^{-1} \circ c)|_{\Gamma_L,\Gamma_N} \sim \mathrm{a}(e \circ c^{-1})|_{\Gamma_M,\Gamma_N} \circ \mathrm{a}(c)|_{\Gamma_L,\Gamma_M}$$

is a commensurability. □

Proposition 5.40. *Let $L, M \in \mathsf{Ch}({}_R\mathsf{mod})^b$ be commensurable and let $\Gamma_L \leq \operatorname{Aut} L$ and $\Gamma_M \leq \operatorname{Aut} M$.*

(i) If Γ_L and Γ_M are finite, then (Γ_L, Γ_M) is admissible for (L, M) and moreover we have the following: If $c\colon L \rightleftharpoons M$ is a commensurability, then

$$\mathrm{i}(\mathrm{a}(c)|_{\Gamma_L,\Gamma_M}) = \frac{|\Gamma_M|}{|\Gamma_L|}.$$

(ii) If Γ_L and Γ_M have finite index in $\operatorname{Aut} L$ and $\operatorname{Aut} M$, respectively, then (Γ_L, Γ_M) is admissible for (L, M) and we moreover have the following: If $c\colon L \rightleftharpoons M$ is a commensurability, then

$$\mathrm{i}(\mathrm{a}(c)|_{\Gamma_L,\Gamma_M}) = \frac{|\operatorname{Aut} L : \Gamma_L|}{|\operatorname{Aut} M : \Gamma_M|} \cdot \mathrm{i}(\mathrm{a}(c)).$$

Proof. Using Proposition 5.27 (i), statement (i) is immediate. Statement (ii) follows from Propositions 5.33 and 5.14. □

5.6.3 The Index of Admissible Subgroups

We finally obtain a generalisation of Theorem 5.31 that allows us to define the index of admissible subgroups of the automorphism groups of suitable chain complexes.

Proposition 5.41. *Let $L, M \in \mathsf{Ch}({}_R\mathsf{mod})^b$ be commensurable. Let $\Gamma_L \leq \operatorname{Aut} L$ and $\Gamma_M \leq \operatorname{Aut} M$ be such that (Γ_L, Γ_M) is admissible for (L, M). Suppose that $c, c'\colon L \rightleftharpoons M$ are commensurabilities. Assume that $\operatorname{End}(Q \otimes_Z L) \cong \operatorname{End}(Q \otimes_Z M)$ is a semisimple ring. Then $\mathrm{i}(\mathrm{a}(c)|_{\Gamma_L,\Gamma_M}) = \mathrm{i}(\mathrm{a}(c')|_{\Gamma_L,\Gamma_M})$.*

Proof. The proof is analogous to that of [BL17, Theorem 8.1] and Proposition 5.29 (iii). By Proposition 5.14, Lemma 5.34 and Corollary 5.36, the claim is equivalent to the statement $\mathrm{i}(\mathrm{a}(c^{-1} \circ c')|_{\Gamma_L,\Gamma_L}) = 1$. Since (Γ_L, Γ_M) is admissible for (L, M), it follows from Proposition 5.39 that (Γ_L, Γ_L) is admissible for (L, L). Hence,

$$\mathrm{i} \circ \mathrm{a}|_{\Gamma_L,\Gamma_L} \colon G_L = \operatorname{Hom}_{\mathsf{Ch}({}_R\mathsf{mod})^b_{\mathrm{com}}}(L, L) \to \mathbb{Q}_{>0}$$

is well-defined, and the claim follows if we can show that this homomorphism is trivial. Let $B := \operatorname{End}(Q \otimes_Z L)$. Then $B^\times \cong G_L$ by Corollary 5.25, and $\mathrm{i} \circ \mathrm{a}|_{\Gamma_L,\Gamma_L}$ factors through $B^\times/\mathfrak{Z}(B)^\times$ by Corollary 5.37. Since $\mathbb{Q}_{>0}$ is abelian, it also factors through $B^\times/[B^\times, B^\times]$. Thus, $\mathrm{i} \circ \mathrm{a}|_{\Gamma_L,\Gamma_L}$ factors through $B^\times/(\mathfrak{Z}(B)^\times[B^\times, B^\times])$. It now follows as in the proof of Proposition 5.29 that $\mathrm{i} \circ \mathrm{a}|_{\Gamma_L,\Gamma_L}$ is trivial. □

The main result to be used later on in Section 8.2 is the following.

Theorem 5.42. *Let Z be an infinite commutative ring such that for all $0 \neq z \in Z$, the ring Z/zZ is finite. Denote by Q the field of fractions of Z. Let A be a finite dimensional Q-algebra and R be a left-noetherian Z-subalgebra of A with the property that $Q \cdot R = A$. Let $V \in \mathsf{Ch}({}_A\mathsf{mod})^b$ such that $\operatorname{End}(V)$ is a semisimple ring. Define*

$$\mathcal{S} := \mathcal{S}_V := \left\{ L \in \mathsf{Ch}({}_R\mathsf{mod})^b \,\middle|\, Q \otimes_Z L \cong V \right\}$$

and

$$\mathcal{T} := \{ (L, M, \Gamma_L, \Gamma_M) \mid L, M \in \mathcal{S}, (\Gamma_L, \Gamma_M) \text{ admissible for } (L, M) \}.$$

Then there is a unique function

$$\mathrm{ia}| : \mathcal{T} \to \mathbb{Q}_{>0},\ (L, M, \Gamma_L, \Gamma_M) \mapsto \mathrm{ia}(L, M)|_{\Gamma_L, \Gamma_M}$$

with the following properties:

(i) If $(L, M, \Gamma_L, \Gamma_M) \in \mathcal{T}$ and $L', M' \in \mathcal{S}$ and there are isomorphisms $\varphi\colon L \xrightarrow{\sim} L'$ and $\psi\colon M \xrightarrow{\sim} M'$, then $(L', M', \varphi\Gamma_L\varphi^{-1}, \psi\Gamma_M\psi^{-1}) \in \mathcal{T}$ and

$$\mathrm{ia}(L, M)|_{\Gamma_L, \Gamma_M} = \mathrm{ia}(L', M')|_{\varphi\Gamma_L\varphi^{-1}, \psi\Gamma_M\psi^{-1}}.$$

(ii) If $(L, M, \Gamma_L, \Gamma_M), (M, N, \Gamma_M, \Gamma_N) \in \mathcal{T}$, then $(L, N, \Gamma_L, \Gamma_N) \in \mathcal{T}$ and

$$\mathrm{ia}(L, M)|_{\Gamma_L, \Gamma_M} \cdot \mathrm{ia}(M, N)|_{\Gamma_M, \Gamma_N} = \mathrm{ia}(L, N)|_{\Gamma_L, \Gamma_N}.$$

(iii) If $(L, M, \Gamma_L, \Gamma_M) \in \mathcal{T}$ and there is a monomorphism $L \hookrightarrow M$ with finite cokernel, then with

$$H := \left\{ \mu \in \Gamma_M \,\middle|\, \mu L = L, \exists\, \tau \in \Gamma_L : \mu\big|_L = \tau \right\}$$

and $\rho\colon H \to \Gamma_L, \mu \mapsto \mu|_L$ one has

$$\mathrm{ia}(L, M)|_{\Gamma_L, \Gamma_M} = \frac{|\Gamma_M : H| \cdot |\ker \rho|}{|\Gamma_L : \operatorname{im} \rho|}.$$

Moreover, it has the following additional properties:

(iv) If $L, M \in \mathcal{S}$, then $\mathrm{ia}(L, M)|_{\operatorname{Aut} L, \operatorname{Aut} M} = \mathrm{ia}(L, M)$.

(v) If $L, M \in \mathcal{S}$ and $\Gamma_L \leq \operatorname{Aut} L$ and $\Gamma_M \leq \operatorname{Aut} M$ have finite index, then

$$\mathrm{ia}(L, M)|_{\Gamma_L, \Gamma_M} = \frac{|\operatorname{Aut} L : \Gamma_L|}{|\operatorname{Aut} M : \Gamma_M|} \cdot \mathrm{ia}(L, M).$$

Proof. Let $(L, M, \Gamma_L, \Gamma_M) \in \mathcal{T}$. Then by Proposition 5.29, there is a commensurability $c\colon L \rightleftharpoons M$. We define

$$\mathrm{ia}(L, M)|_{\Gamma_L, \Gamma_M} := \mathrm{i}(\mathrm{a}(c)|_{\Gamma_L, \Gamma_M}),$$

which is independent of c by Proposition 5.41.

To prove (i), let $(L, M, \Gamma_L, \Gamma_M) \in \mathcal{T}$, let $L', M' \in \mathcal{S}$, and suppose that there are isomorphisms $\varphi\colon L \xrightarrow{\sim} L'$ and $\psi\colon M \xrightarrow{\sim} M'$. Let $c' = (X', f', g')\colon L' \rightleftharpoons M'$ be a commensurability. Then clearly, $c := (X', \varphi^{-1} \circ f', \psi^{-1} \circ g')\colon L \rightleftharpoons M$ is a commensurability, so $\mathrm{a}(c)|_{\Gamma_L, \Gamma_M}$ is a commensurability. It is immediate that the map

$$\operatorname{Aut}(c)|_{\Gamma_L,\Gamma_M} \to \operatorname{Aut}(c')|_{\varphi\Gamma_L\varphi^{-1},\psi\Gamma_M\psi^{-1}},\ (\lambda, \xi, \mu) \mapsto (\varphi\lambda\varphi^{-1}, \xi, \psi\mu\psi^{-1})$$

is an isomorphism. It fits into a commutative diagram

$$\begin{tikzcd}
& \operatorname{Aut}(c)|_{\Gamma_L,\Gamma_M} \arrow[dl] \arrow[dr] \arrow[ddd] & \\
\Gamma_L \arrow[d] & & \Gamma_M \arrow[d] \\
\varphi\Gamma_L\varphi^{-1} & & \psi\Gamma_M\psi^{-1} \\
& \operatorname{Aut}(c')|_{\varphi\Gamma_L\varphi^{-1},\psi\Gamma_M\psi^{-1}} \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

from which claim (i) follows. Statement (ii) is immediate from Proposition 5.39 (ii) and Corollary 5.36 (ii). For (iii) suppose that $(L, M, \Gamma_L, \Gamma_M) \in \mathcal{T}$ and that there is a monomorphism $i\colon L \hookrightarrow M$ with finite cokernel. It induces a commensurability $c_i\colon L \rightleftharpoons M$, and the isomorphism

$$\operatorname{Aut}(c_i)|_{\Gamma_L,\Gamma_M} \xrightarrow{\sim} H,\ (\lambda, \lambda, \mu) \mapsto \mu$$

defines an isomorphism between $\mathrm{a}(c_i)|_{\Gamma_L,\Gamma_M}$ and (H, ρ, j), where $j\colon H \hookrightarrow \Gamma_M$ is the inclusion. The claim follows.

We next prove uniqueness. Suppose $t\colon \mathcal{T} \to \mathbb{Q}_{>0}$ is a function satisfying (i), (ii) and (iii). Let $(L, M, \Gamma_L, \Gamma_M) \in \mathcal{T}$. By Lemma 5.18, there are $m_1, m_2 \in Z \setminus \{0\}$ such that $m_1 L_{\mathrm{tors}} = m_2 M_{\mathrm{tors}} = 0$. Let $i\colon m_1 L \hookrightarrow L$ be the natural map, which is an isogeny by loc. cit. Then $i^{-1}\Gamma_L i \leq \operatorname{Aut} m_1 L$, and we now show that $(i^{-1}\Gamma_L i, \Gamma_M)$ is admissible for $(m_1 L, M)$. First we investigate the map

$$\alpha\colon \Gamma_L \to i^{-1}\Gamma_L i,\ \lambda \mapsto i^{-1}\lambda i,$$

which is clearly surjective. Let

$$\Theta_L\colon \qquad 0 \longrightarrow L_{\mathrm{tors}} \longrightarrow L \longrightarrow L/L_{\mathrm{tors}} \longrightarrow 0,$$

a short exact sequence of chain complexes. There is a natural injection

$$\operatorname{Aut} L \hookrightarrow \operatorname{Aut} \Theta_L,\ \lambda \mapsto (\lambda', \lambda, \overline{\lambda}),$$

where λ' and $\overline{\lambda}$ are the automorphisms of L_{tors} and L/L_{tors}, respectively, that are induced by λ. Moreover, it follows from the proof of Proposition 2.12 applied componentwise that the natural map

$$\operatorname{Aut}\Theta_L \to \operatorname{Aut}L_{\mathrm{tors}} \times \operatorname{Aut}L/L_{\mathrm{tors}}$$

has kernel isomorphic to $\operatorname{Hom}(L/L_{\mathrm{tors}}, L_{\mathrm{tors}})$. Now if $\lambda \in \ker\alpha$, then $\overline{\lambda}$ is the identity. Hence, the concatenation

$$\ker\alpha \hookrightarrow \operatorname{Aut}\Theta_L \to \operatorname{Aut}L_{\mathrm{tors}} \times \operatorname{Aut}L/L_{\mathrm{tors}}$$

has finite image and finite kernel. This shows that $\ker\alpha$ is finite and therefore that α is an isogeny. Now let $c = (X, f, g)\colon m_1L \rightleftharpoons M$ be a commensurability. Then also $c' := (X, if, g)\colon L \rightleftharpoons M$ is a commensurability, so $\mathrm{a}(c')|_{\Gamma_L,\Gamma_M}$ is a commensurability. Define

$$\operatorname{Aut}(c')|_{\Gamma_L,\Gamma_M} \to \operatorname{Aut}(c)|_{i^{-1}\Gamma_L i,\Gamma_M},\ (\lambda, \xi, \mu) \mapsto (i^{-1}\lambda i, \xi, \mu).$$

This map is surjective and has finite kernel, as α does, so it is an isogeny. It fits into a commutative diagram

$$\begin{tikzcd}
 & & \operatorname{Aut}(c')|_{\Gamma_L,\Gamma_M} \arrow[dl] \arrow[dr] & \\
\operatorname{Aut}(c')|_{\Gamma_L,\Gamma_M} \arrow[urr, bend left, "\mathrm{id}"] \arrow[ddrr, bend right] & \Gamma_L \arrow[d, "\alpha"] & & \Gamma_M \arrow[d, "\mathrm{id}"] \\
 & i^{-1}\Gamma_L i & & \Gamma_M \\
 & & \operatorname{Aut}(c)|_{i^{-1}\Gamma_L i,\Gamma_M}, \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

which together with Proposition 5.7 shows that $\mathrm{a}(c)|_{i^{-1}\Gamma_L i,\Gamma_M}$ is a commensurability. Thus, $(i^{-1}\Gamma_L i, \Gamma_M)$ is admissible for (m_1L, M). In the same manner, when letting $j\colon m_2M \hookrightarrow M$ denote the natural map, one sees that $(\Gamma_L, j^{-1}\Gamma_M j)$ is admissible for (L, m_2M) and that $(i^{-1}\Gamma_L i, j^{-1}\Gamma_M j)$ is admissible for (m_1L, m_2M). Then by property (ii) we have

$$t(L, M, \Gamma_L, \Gamma_M) = \frac{t(m_1L, m_2M, i^{-1}\Gamma_L i, j^{-1}\Gamma_M j) \cdot t(m_2M, M, j^{-1}\Gamma_M j, \Gamma_M)}{t(m_1L, L, i^{-1}\Gamma_L i, \Gamma_L)}.$$

The values of all three factors on the right hand side are determined by property (iii), so t must equal ia.

Finally, property (iv) is clearly satisfied, and property (v) follow from Proposition 5.40. □

6 Arakelov Ray Class Groups

In this chapter, we introduce the central object of the thesis, the Arakelov ray class group $\operatorname{Pic}_K^0(\mathfrak{m})$. It is an 'Arakelov version' of the ray class group and has first appeared in [BP25]. Here, we recall its definition and the properties established in [BP25]. As $\operatorname{Pic}_K^0(\mathfrak{m})$ is the main object of our interest, we give a detailed construction and provide proofs of the relevant statements. First, in Sections 6.1 and 6.2 we review ray class groups and relevant aspects of Minkowski theory. The Arakelov ray class group and its associated short exact sequence $\mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})$ are then constructed in Section 6.3. In the final subsection we discuss some of the information that is carried by the sequence $\mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})$.

Throughout this chapter, let K be a number field. For an infinite prime $\mathfrak{p} \mid \infty$ of K we denote by $\sigma_{\mathfrak{p}} \colon K \hookrightarrow \mathbb{C}$ a representative of the class of embeddings corresponding to $\mathfrak{p}$. We denote by Id_K the group of fractional ideals of K and by Prin_K the group of principal fractional ideals. We write $\operatorname{Cl}_K = \operatorname{Id}_K / \operatorname{Prin}_K$ for the ideal class group.

Note that $\operatorname{Aut}(K)$ operates on the infinite primes of K. If $\tau \in \operatorname{Aut}(K)$ and $\mathfrak{p} \mid \infty$, then a representative for the class of embeddings associated to $\tau(\mathfrak{p})$ is by definition given by $\sigma_{\tau(\mathfrak{p})} = \sigma_{\mathfrak{p}} \circ \tau^{-1}$. Moreover, there is a natural action of $\operatorname{Aut}(K)$ on Id_K, Prin_K and Cl_K.

Definition 6.1. A *modulus* in K is a pair $\mathfrak{m} = (\mathfrak{m}_0, \mathfrak{m}_\infty)$ where $\mathfrak{m}_0$ is a nonzero integral ideal of $\mathcal{O}_K$ and $\mathfrak{m}_\infty$ is a set of real places of K. If $H \leq \operatorname{Aut}(K)$, then we say that $\mathfrak{m}$ is *H-stable* if $\tau(\mathfrak{m}_0) = \mathfrak{m}_0$ and $\tau(\mathfrak{m}_\infty) = \mathfrak{m}_\infty$ for all $\tau \in H$.

For the remainder of this chapter, let $\mathfrak{m} = (\mathfrak{m}_0, \mathfrak{m}_\infty)$ be a modulus in K.

6.1 Ray Class Groups

We recall the definition and basic properties of the ray class group. We follow [Coh00, Section 3.2], but use the notation from [BP25, Section 1.1].

Definition 6.2. We say that a fractional ideal $I \in \operatorname{Id}_K$ is *coprime to* $\mathfrak{m}$ if $v_{\mathfrak{p}}(I) = 0$ for all $\mathfrak{p} \mid \mathfrak{m}_0$, and we denote by $\operatorname{Id}_K(\mathfrak{m})$ the group of all such ideals. We define

$$K^1(\mathfrak{m}) := \left\{ a \in K^\times \,\middle|\, v_{\mathfrak{p}}(a-1) \geq v_{\mathfrak{p}}(\mathfrak{m}_0) \text{ for all } \mathfrak{p} \mid \mathfrak{m}_0,\ \sigma_{\mathfrak{p}}(a) > 0 \text{ for all } \mathfrak{p} \in \mathfrak{m}_\infty \right\}$$

and put $\mathcal{O}_K^1(\mathfrak{m}) := K^1(\mathfrak{m}) \cap \mathcal{O}_K^\times$. Finally, we let $\operatorname{Prin}_K(\mathfrak{m}) := \left\{ a\mathcal{O}_K \,\middle|\, a \in K^1(\mathfrak{m}) \right\}$ and define the *ray class group of K with modulus* $\mathfrak{m}$ to be $\operatorname{Cl}_K(\mathfrak{m}) := \operatorname{Id}_K(\mathfrak{m}) / \operatorname{Prin}_K(\mathfrak{m})$.

Note that we recover the ideal class group as $\operatorname{Cl}_K = \operatorname{Cl}_K(\mathcal{O}_K, \varnothing)$.

Definition 6.3. We say that an element $a \in K^\times$ is *coprime to* $\mathfrak{m}$ if $a\mathcal{O}_K$ is. If $a \in K^\times$ is coprime to $\mathfrak{m}$, then we can write $a = \frac{b}{c}$ with $b, c \in \mathcal{O}_K$ coprime to $\mathfrak{m}$. We have $\overline{b}, \overline{c} \in (\mathcal{O}_K/\mathfrak{m}_0)^\times$ and define $\overline{a} := \overline{b} \cdot \overline{c}^{-1} \in (\mathcal{O}_K/\mathfrak{m}_0)^\times$, which is independent of the choice of b and c. We define a group homomorphism

$$\begin{aligned}\rho := \rho_K(\mathfrak{m})\colon \left\{ a \in K^\times \,\middle|\, a \text{ coprime to } \mathfrak{m} \right\} &\to (\mathcal{O}_K/\mathfrak{m}_0)^\times \times \{\pm 1\}^{\mathfrak{m}_\infty}, \\ a &\mapsto (\overline{a}, (\operatorname{sign} \sigma_{\mathfrak{p}}(a))_{\mathfrak{p}}),\end{aligned}$$

which is surjective by strong approximation.

Note that when restricted to $\mathcal{O}_K^\times$, the first component of ρ is just the map induced by the reduction map $\mathcal{O}_K \to \mathcal{O}_K/\mathfrak{m}_0$.

Remark 6.4. Let $H \leq \operatorname{Aut}(K)$ and suppose that $\mathfrak{m}$ is H-stable. Then it is easy to see that the objects $\operatorname{Id}_K(\mathfrak{m})$, $K^1(\mathfrak{m})$, $\mathcal{O}_K^1(\mathfrak{m})$, $\operatorname{Prin}_K(\mathfrak{m})$, $\operatorname{Cl}_K(\mathfrak{m})$, $\{ a \in K^\times \mid a \text{ coprime to } \mathfrak{m} \}$, $\mathcal{O}_K/\mathfrak{m}_0$, $\{\pm 1\}^{\mathfrak{m}_\infty}$ discussed above are H-modules. The action on $\{\pm 1\}^{\mathfrak{m}_\infty}$ is given by $\tau.(a_{\mathfrak{p}})_{\mathfrak{p} \in \mathfrak{m}_\infty} = (a_{\tau^{-1}(\mathfrak{p})})_{\mathfrak{p} \in \mathfrak{m}_\infty}$ for $a_{\mathfrak{p}} \in \{\pm 1\}$ and $\tau \in H$.

We always have a natural map $\operatorname{Cl}_K(\mathfrak{m}) \to \operatorname{Cl}_K$ from the ray class group to the class group. Its kernel can be described by the following exact sequence.

Proposition 6.5 ([Coh00, Proposition 3.2.3])**.** *Suppose that $\mathfrak{m}$ is H-stable for $H \leq \operatorname{Aut}(K)$. There is an exact sequence of H-modules*

$$0 \longrightarrow \mathcal{O}_K^1(\mathfrak{m}) \longrightarrow \mathcal{O}_K^\times \xrightarrow{\rho} (\mathcal{O}_K/\mathfrak{m}_0)^\times \times \{\pm 1\}^{\mathfrak{m}_\infty} \xrightarrow{\psi} \operatorname{Cl}_K(\mathfrak{m}) \longrightarrow \operatorname{Cl}_K \longrightarrow 0$$

where the left hand map is inclusion, the right hand map is the natural map, and ψ maps $\rho(a)$, where $a \in K^\times$ is coprime to $\mathfrak{m}$, to the class of $a\mathcal{O}_K$. In particular, $\left|\mathcal{O}_K^\times : \mathcal{O}_K^1(\mathfrak{m})\right| < \infty$.

Definition 6.6. We write

$$\mathrm{S}_K^{\mathrm{fin}}(\mathfrak{m})\colon \qquad 0 \longrightarrow \frac{(\mathcal{O}_K/\mathfrak{m}_0)^\times \times \{\pm 1\}^{\mathfrak{m}_\infty}}{\rho(\mathcal{O}_K^\times)} \xrightarrow{\psi} \operatorname{Cl}_K(\mathfrak{m}) \longrightarrow \operatorname{Cl}_K \longrightarrow 0.$$

for the short exact sequence coming from Proposition 6.5 and call it the *ray class group sequence.*

6.2 Minkowski Theory

We review some notions from Minkowski theory and set up some notation that will be used later. The material can be found for example in [Neu99, Section I.5]. A central role in Minkowski theory is played by the finite etale $\mathbb{R}$-algebra $K_{\mathbb{R}} := K \otimes_{\mathbb{Q}} \mathbb{R}$ which offers a way of embedding K into a finite-dimensional real vector space and making use of the theory of lattices. There is an isomorphism of finite etale $\mathbb{R}$-algebras

$$K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\sim} \prod_{\mathfrak{p}|\infty} K_{\mathfrak{p}},\ a \otimes x \mapsto (ax, \dots, ax),$$

and we will generally prefer to work with the right hand description of $K_{\mathbb{R}}$. For each infinite prime $\mathfrak{p} \mid \infty$ we denote by $\|\cdot\|_{\mathfrak{p}} : K_{\mathfrak{p}} \to \mathbb{R}_{\geq 0}$ the associated normalised absolute value. Thus, if $\mathfrak{p}$ is real, then after identifying $K_{\mathfrak{p}}$ with $\mathbb{R}$ we have $\|\cdot\|_{\mathfrak{p}} = |\cdot|$, and if $\mathfrak{p}$ is complex, then after identifying $K_{\mathfrak{p}}$ with $\mathbb{C}$ we have $\|\cdot\|_{\mathfrak{p}} = |\cdot|^2$.

We denote the norm map of the finite etale $\mathbb{R}$-algebra $\prod_{\mathfrak{p}|\infty} K_{\mathfrak{p}}$ by $\mathrm{N}\colon \prod_{\mathfrak{p}|\infty} K_{\mathfrak{p}} \to \mathbb{R}$. Explicitly, it is given by $\mathrm{N}((a_{\mathfrak{p}})_{\mathfrak{p}}) = \prod_{\mathfrak{p}|\infty} \|a_{\mathfrak{p}}\|_{\mathfrak{p}}$. On the unit group $K_{\mathbb{R}}^{\times} \cong \prod_{\mathfrak{p}|\infty} K_{\mathfrak{p}}^{\times}$ we further define a map

$$\mathrm{Log}\colon \prod_{\mathfrak{p}|\infty} K_{\mathfrak{p}}^{\times} \to \prod_{\mathfrak{p}|\infty} \mathbb{R},\ (a_{\mathfrak{p}})_{\mathfrak{p}} \mapsto (\log \|a_{\mathfrak{p}}\|_{\mathfrak{p}})_{\mathfrak{p}}.$$

Note that we have a decomposition

$$\prod_{\mathfrak{p}|\infty} K_{\mathfrak{p}}^{\times} \cong \prod_{\mathfrak{p}|\infty} c(K_{\mathfrak{p}}^{\times}) \times \mathbb{R}_{>0}$$

where $c(K_{\mathfrak{p}}^{\times})$ denotes the maximal compact subgroup of $K_{\mathfrak{p}}^{\times}$. Explicitly, if $\mathfrak{p}$ is real, then $c(K_{\mathfrak{p}}^{\times}) = \{\pm 1\}$ and we have an isomorphism $\mathbb{R}^{\times} \xrightarrow{\sim} \{\pm 1\} \times \mathbb{R}_{>0},\ x \mapsto (\frac{x}{|x|}, |x|)$, and if $\mathfrak{p}$ is complex, then $c(K_{\mathfrak{p}}^{\times}) = S^1$ and we have an isomorphism $\mathbb{C}^{\times} \xrightarrow{\sim} S^1 \times \mathbb{R}_{>0},\ z \mapsto (\frac{z}{|z|}, |z|)$. The above decomposition induces an isomorphism

$$\prod_{\mathfrak{p}|\infty} K_{\mathfrak{p}}^{\times} \Big/ c\Big(\prod_{\mathfrak{p}|\infty} K_{\mathfrak{p}}^{\times}\Big) \xrightarrow{\sim} \prod_{\mathfrak{p}|\infty} \mathbb{R}_{>0}.$$

Since N is trivial on $\prod_{\mathfrak{p}|\infty} c(K_{\mathfrak{p}}^{\times})$, it descends to $\prod_{\mathfrak{p}|\infty} \mathbb{R}_{>0}$, where it is given by

$$\mathrm{N}\colon \prod_{\mathfrak{p}|\infty} \mathbb{R}_{>0} \to \mathbb{R}_{>0},\ (x_{\mathfrak{p}})_{\mathfrak{p}} \mapsto \prod_{\mathfrak{p}|\infty} x_{\mathfrak{p}}^{|K_{\mathfrak{p}}:\mathbb{R}|}. \tag{6.7}$$

Similarly, Log descends to $\prod_{\mathfrak{p}|\infty} \mathbb{R}_{>0}$, where it is given by

$$\overline{\mathrm{Log}}\colon \prod_{\mathfrak{p}|\infty} \mathbb{R}_{>0} \to \prod_{\mathfrak{p}|\infty} \mathbb{R}, (x_{\mathfrak{p}})_{\mathfrak{p}} \mapsto (\log x_{\mathfrak{p}}^{|K_{\mathfrak{p}}:\mathbb{R}|})_{\mathfrak{p}} = (|K_{\mathfrak{p}} : \mathbb{R}| \cdot \log x_{\mathfrak{p}})_{\mathfrak{p}}$$

and defines an isomorphism. Finally, we have the trace map

$$\mathrm{Tr}\colon \prod_{\mathfrak{p}|\infty} \mathbb{R} \to \mathbb{R},\ (x_\mathfrak{p})_\mathfrak{p} \mapsto \sum_{\mathfrak{p}|\infty} x_\mathfrak{p}.$$

The above maps fit into the commutative diagram

$$\begin{tikzcd}
K^\times \arrow[r, hook] \arrow[d, "|\mathrm{N}_{K/\mathbb{Q}}|"'] & \prod_{\mathfrak{p}|\infty} K_\mathfrak{p}^\times \arrow[r, "\mathrm{Log}"] \arrow[d, "\mathrm{N}"] & \prod_{\mathfrak{p}|\infty} \mathbb{R} \arrow[d, "\mathrm{Tr}"] \\
\mathbb{Q}_{>0} \arrow[r, hook] & \mathbb{R}_{>0} \arrow[r, "\log"'] & \mathbb{R}.
\end{tikzcd}$$

We write $(\prod_{\mathfrak{p}|\infty} \mathbb{R})^0$ for the set of $x \in \prod_{\mathfrak{p}|\infty} \mathbb{R}$ for which $\mathrm{Tr}(x) = 0$. Then commutativity of the diagram gives that $\mathrm{Log}(\mathcal{O}_K^\times) \subseteq (\prod_{\mathfrak{p}|\infty} \mathbb{R})^0$. We have the following generalised version of Dirichlet's unit theorem.

Theorem 6.8. *There is a split exact sequence of abelian groups*

$$0 \longrightarrow \mu(K) \cap \mathcal{O}_K^1(\mathfrak{m}) \longrightarrow \mathcal{O}_K^1(\mathfrak{m}) \xrightarrow{\mathrm{Log}} \mathrm{Log}(\mathcal{O}_K^1(\mathfrak{m})) \longrightarrow 0$$

and $\mathrm{Log}(\mathcal{O}_K^1(\mathfrak{m}))$ *is a complete lattice in* $(\prod_{\mathfrak{p}|\infty} \mathbb{R})^0$.

Proof. The statement for $\mathfrak{m} = (\mathcal{O}_K, \varnothing)$ is the classical unit theorem and is proven in [Neu99, Section I.7]. It immediately implies the claim on the exact sequence. Since $|\mathcal{O}_K^\times : \mathcal{O}_K^1(\mathfrak{m})| < \infty$ by Proposition 6.5 and $\mathrm{Log}(\mathcal{O}_K^\times)$ is a complete lattice in $(\prod_{\mathfrak{p}|\infty} \mathbb{R})^0$, it follows that also $\mathrm{Log}(\mathcal{O}_K^1(\mathfrak{m}))$ is a complete lattice in $(\prod_{\mathfrak{p}|\infty} \mathbb{R})^0$. □

6.3 Construction of the Arakelov Ray Class Group and Sequence

In this section, we define the Arakelov ray class group $\mathrm{Pic}_K^0(\mathfrak{m})$ and establish the natural short exact sequence $\mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})$ associated to it, as well as a short exact sequence $\mathrm{D}_K(\mathfrak{m})$ of short exact sequences of which $\mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})$ is the middle term. The construction of $\mathrm{Pic}_K^0(\mathfrak{m})$ is analogous to that of the Arakelov class group as a version of the ideal class group that also incorporates the infinite primes. We review and detail its definition from [BP25], using a slightly different but equivalent approach in the style of Neukirch's construction of the Arakelov class group in [Neu99, Section III.1]. In doing so, we roughly follow the exposition from [Neu99] and generalise it by taking the modulus $\mathfrak{m}$ into account. We give a multiplicative definition here, but one can also define $\mathrm{Pic}_K^0(\mathfrak{m})$ additively, using divisors, just as for Pic_K^0.

Definition 6.9. We define

$$\overline{\mathrm{Id}_K(\mathfrak{m})} := \mathrm{Id}_K(\mathfrak{m}) \times \prod_{\mathfrak{p}|\infty} \mathbb{R}_{>0}$$

and regard it as an LCA group with the discrete topology on $\mathrm{Id}_K(\mathfrak{m})$ and the standard topology on $\prod_{\mathfrak{p}|\infty} \mathbb{R}_{>0}$. For $a \in K^1(\mathfrak{m})$ we define

$$((a)) := \big(a\mathcal{O}_K,\ (|\sigma_{\mathfrak{p}}(a)|^{-1})_{\mathfrak{p}|\infty}\big) \in \overline{\mathrm{Id}_K(\mathfrak{m})}$$

and let $\overline{\mathrm{Prin}_K(\mathfrak{m})} := \{\, ((a)) \,|\, a \in K^1(\mathfrak{m}) \,\}$.

Note that clearly $((a)) \cdot ((b)) = ((ab))$ for $a, b \in K^1(\mathfrak{m})$, so $\overline{\mathrm{Prin}_K(\mathfrak{m})}$ is a subgroup of $\overline{\mathrm{Id}_K(\mathfrak{m})}$. Even more:

Proposition 6.10. *The kernel of $K^1(\mathfrak{m}) \to \overline{\mathrm{Id}_K(\mathfrak{m})}$, $a \mapsto ((a))$ is $\mu(K) \cap \mathcal{O}_K^1(\mathfrak{m})$. Its image $\overline{\mathrm{Prin}_K(\mathfrak{m})}$ is a discrete subgroup of $\overline{\mathrm{Id}_K(\mathfrak{m})}$ and thus in particular closed.*

Proof. We imitate the proof of [Neu99, Proposition III.1.9], with respect to our notation. The composition of maps

$$K^1(\mathfrak{m}) \to \overline{\mathrm{Id}_K(\mathfrak{m})} \to \prod_{\mathfrak{p}|\infty} \mathbb{R}_{>0} \xrightarrow{\overline{\mathrm{Log}}} \prod_{\mathfrak{p}|\infty} \mathbb{R},$$

where the middle map is the projection, is just $-\mathrm{Log}|_{K^1(\mathfrak{m})}$. It follows from this and Theorem 6.8 that the kernel of $K^1(\mathfrak{m}) \to \overline{\mathrm{Id}_K(\mathfrak{m})}$ is $\mu(K) \cap \mathcal{O}_K^1(\mathfrak{m})$.

For the second claim we again make us of Theorem 6.8 which gives in particular that $\mathrm{Log}(\mathcal{O}_K^1(\mathfrak{m}))$ is a discrete subgroup of $(\prod_{\mathfrak{p}|\infty} \mathbb{R})^0$. Hence, there is an open set $U \subseteq \prod_{\mathfrak{p}|\infty} \mathbb{R}$ such that $U \cap \mathrm{Log}(\mathcal{O}_K^1(\mathfrak{m})) = \{0\}$. Consider $V := \{\mathcal{O}_K\} \times \overline{\mathrm{Log}}^{-1}(U) \subseteq \overline{\mathrm{Id}_K(\mathfrak{m})}$, which is an open set containing $1 \in \overline{\mathrm{Id}_K(\mathfrak{m})}$. We claim that $V \cap \overline{\mathrm{Prin}_K(\mathfrak{m})} = \{1\}$. If $a \in K^1(\mathfrak{m})$ is such that $((a)) \in V$, then $a \in \mathcal{O}_K^1(\mathfrak{m})$ and $-\mathrm{Log}(a) = \mathrm{Log}(a^{-1}) \in U$ by our considerations from the first part of the proof. It follows that $\mathrm{Log}(a) = 0$, so $a \in \mu(K) \cap \mathcal{O}_K^1(\mathfrak{m})$ and therefore $((a)) = 1$. This shows that $\overline{\mathrm{Prin}_K(\mathfrak{m})}$ is discrete in $\overline{\mathrm{Id}_K(\mathfrak{m})}$. □

Definition 6.11. We define $\mathrm{Pic}_K(\mathfrak{m}) := \overline{\mathrm{Id}_K(\mathfrak{m})} / \overline{\mathrm{Prin}_K(\mathfrak{m})}$, which is an LCA group.

In analogy to the fact that $\mathrm{Log}(\mathcal{O}_K^1(\mathfrak{m}))$ is contained in the trace-0-hypersurface of $\prod_{\mathfrak{p}|\infty} \mathbb{R}$ with compact quotient, it is more natural to consider a slightly smaller group than $\mathrm{Pic}_K(\mathfrak{m})$ by restricting to certain elements of $\overline{\mathrm{Id}_K(\mathfrak{m})}$. This will again yield a compact object.

Definition 6.12. The absolute norm $\mathrm{N}\colon \mathrm{Id}_K \to \mathbb{Q}_{>0}$ on fractional ideals and the norm map $\mathrm{N}\colon \prod_{\mathfrak{p}\mid\infty} \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ from (6.7) give rise to yet another *norm* map

$$\overline{\mathrm{N}}\colon \overline{\mathrm{Id}_K(\mathfrak{m})} \to \mathbb{R}_{>0},\ (I, (x_\mathfrak{p})_\mathfrak{p}) \mapsto \mathrm{N}(I) \cdot \prod_{\mathfrak{p}\mid\infty} x_\mathfrak{p}^{|K_\mathfrak{p}:\mathbb{R}|}$$

which is a continuous surjective group homomorphism.

Note that for $a \in K^1(\mathfrak{m})$ we have

$$\overline{\mathrm{N}}\big(((a))\big) = \mathrm{N}(a\mathcal{O}_K) \cdot \prod_{\mathfrak{p}\mid\infty} |\sigma_\mathfrak{p}(a)|^{-|K_\mathfrak{p}:\mathbb{R}|} = \prod_{\mathfrak{p}\nmid\infty} \|a\|_\mathfrak{p}^{-1} \cdot \prod_{\mathfrak{p}\mid\infty} \|a\|_\mathfrak{p}^{-1} = 1$$

by the product formula. Thus the norm map descends to $\mathrm{Pic}_K(\mathfrak{m})$.

Definition 6.13. We put

$$\overline{\mathrm{Id}_K(\mathfrak{m})}^0 := \left\{ X \in \overline{\mathrm{Id}_K(\mathfrak{m})} \,\middle|\, \overline{\mathrm{N}}(X) = 1 \right\}.$$

The LCA group

$$\mathrm{Pic}^0_K(\mathfrak{m}) := \overline{\mathrm{Id}_K(\mathfrak{m})}^0 / \overline{\mathrm{Prin}_K(\mathfrak{m})} = \ker(\overline{N}\colon\ \mathrm{Pic}_K(\mathfrak{m}) \to \mathbb{R}_{>0})$$

is called the *Arakelov ray class group of* K *with modulus* $\mathfrak{m}$. We call $\mathrm{Pic}^0_K := \mathrm{Pic}^0_K(\mathcal{O}_K, \varnothing)$ the *Arakelov class group of* K.

The 0 on top is taken from the additive definition of these objects in the language of divisors; see [Sch08, Section 2] or [Neu99, Section III.1] for the corresponding construction of the Arakelov class group.

Remark 6.14. The action of $\mathrm{Aut}(K)$ on $\{\mathfrak{p} \mid \infty\}$ induces an action on $\prod_{\mathfrak{p}\mid\infty} \mathbb{R}$, which for $\tau \in \mathrm{Aut}(K)$ and $(x_\mathfrak{p})_\mathfrak{p} \in \prod_{\mathfrak{p}\mid\infty} \mathbb{R}$ is given by $\tau.(x_\mathfrak{p})_\mathfrak{p} = (x_{\tau^{-1}(\mathfrak{p})})_\mathfrak{p}$. The analogous statement holds for $\prod_{\mathfrak{p}\mid\infty} \mathbb{R}_{>0}$.

Let $H \leq \mathrm{Aut}(K)$ and suppose that $\mathfrak{m}$ is H-stable. Then in addition to the objects mentioned in Remark 6.4, we have that $\overline{\mathrm{Id}_K(\mathfrak{m})}$, $\overline{\mathrm{Prin}_K(\mathfrak{m})}$, $\mathrm{Pic}_K(\mathfrak{m})$, $\overline{\mathrm{Id}_K(\mathfrak{m})}^0$ and $\mathrm{Pic}^0_K(\mathfrak{m})$ are LCA H-modules, and the maps $K^1(\mathfrak{m}) \to \overline{\mathrm{Id}_K(\mathfrak{m})}$ and $\overline{N}$ are continuous H-homomorphisms.

The next statement generalises the fact that the Arakelov class group surjects onto the ideal class group with kernel a compact real torus ([Neu99, Proposition III.1.11]; [Sch08, Proposition 2.2]).

Proposition 6.15. *Suppose that $\mathfrak{m}$ is H-stable for $H \leq \operatorname{Aut}(K)$. There is a short strictly exact sequence of compact LCA H-modules*

$$0 \longrightarrow \mathcal{O}_K^1(\mathfrak{m}) \otimes_{\mathbb{Z}} \mathbb{R}/\mathbb{Z} \longrightarrow \operatorname{Pic}_K^0(\mathfrak{m}) \longrightarrow \operatorname{Cl}_K(\mathfrak{m}) \longrightarrow 0$$

where the right hand map is the natural one and the left hand map is given by $u \otimes \overline{x} \mapsto [(1, (|\sigma_{\mathfrak{p}}(u)|^{-x})_{\mathfrak{p}})]$ for $u \in \mathcal{O}_K^1(\mathfrak{m})$ and $x \in \mathbb{R}$.

In particular, $\mathcal{O}_K^1(\mathfrak{m}) \otimes_{\mathbb{Z}} \mathbb{R}/\mathbb{Z}$ is the connected component of the identity of $\operatorname{Pic}_K^0(\mathfrak{m})$. Moreover, $\operatorname{Pic}_K^0(\mathfrak{m})$ is a compact real abelian Lie group of dimension $|\{\mathfrak{p} \mid \infty\}| - 1$, and the above short exact sequence is an exact sequence of compact real abelian Lie groups.

Proof. We need to investigate the kernel of the natural surjection $\operatorname{Pic}_K^0(\mathfrak{m}) \to \operatorname{Cl}_K(\mathfrak{m})$ and start by imitating the proof of [Neu99, Proposition III.1.11]. We consider the map

$$s \colon \mathcal{O}_K^1(\mathfrak{m}) \to \prod_{\mathfrak{p}|\infty} \mathbb{R}_{>0}, \; u \mapsto (|\sigma_{\mathfrak{p}}(u)|^{-1})_{\mathfrak{p}},$$

a multiplicative analogue of the Log map which embeds units in trace-0-space. Note that it is just the concatenation of the natural map $\mathcal{O}_K^1(\mathfrak{m}) \to \overline{\operatorname{Prin}_K(\mathfrak{m})}$ with the projection $\overline{\operatorname{Id}_K(\mathfrak{m})} \to \prod_{\mathfrak{p}|\infty} \mathbb{R}_{>0}$. Thus Proposition 6.10 shows that $\ker(s) = \mathcal{O}_K^1(\mathfrak{m}) \cap \mu(K)$ and that s has discrete image. We denote by $(\prod_{\mathfrak{p}|\infty} \mathbb{R}_{>0})^0$ the set of $x \in \prod_{\mathfrak{p}|\infty} \mathbb{R}_{>0}$ with $\mathrm{N}(x) = 1$, where N is the map from (6.7). Then $\operatorname{im}(s) \subseteq (\prod_{\mathfrak{p}|\infty} \mathbb{R}_{>0})^0$ by the product formula, and there is a natural commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \frac{\mathcal{O}_K^1(\mathfrak{m})}{\mathcal{O}_K^1(\mathfrak{m}) \cap \mu(K)} \arrow[r] \arrow[d, hook, "s"] & \overline{\operatorname{Prin}_K(\mathfrak{m})} \arrow[r] \arrow[d, hook] & \operatorname{Prin}_K(\mathfrak{m}) \arrow[r] \arrow[d, hook] & 0 \\
0 \arrow[r] & (\prod_{\mathfrak{p}|\infty} \mathbb{R}_{>0})^0 \arrow[r] & \overline{\operatorname{Id}_K(\mathfrak{m})}^0 \arrow[r] & \operatorname{Id}_K(\mathfrak{m}) \arrow[r] & 0
\end{tikzcd}$$

with exact rows. The snake lemma gives us a short exact sequence of LCA groups

$$0 \longrightarrow \frac{(\prod_{\mathfrak{p}|\infty} \mathbb{R}_{>0})^0}{s(\mathcal{O}_K^1(\mathfrak{m}))} \longrightarrow \operatorname{Pic}_K^0(\mathfrak{m}) \longrightarrow \operatorname{Cl}_K(\mathfrak{m}) \longrightarrow 0.$$

We now provide a different description of the left hand term. In a first step, we connect it to the objects from Minkowski theory. For $u \in \mathcal{O}_K^1(\mathfrak{m})$ it holds that $\overline{\operatorname{Log}}(s(u)) = \operatorname{Log}(u^{-1})$, so that we have a commutative diagram

$$\begin{tikzcd}
s(\mathcal{O}_K^1(\mathfrak{m})) \arrow[r, hook] \arrow[d, "\overline{\operatorname{Log}}"'] & (\prod_{\mathfrak{p}|\infty} \mathbb{R}_{>0})^0 \arrow[d, "\overline{\operatorname{Log}}"] \\
\operatorname{Log}(\mathcal{O}_K^1(\mathfrak{m})) \arrow[r, hook] & (\prod_{\mathfrak{p}|\infty} \mathbb{R})^0
\end{tikzcd}$$

in which the vertical maps are isomorphisms. It follows that $\overline{\mathrm{Log}}$ induces an isomorphism

$$\overline{\mathrm{Log}}\colon \frac{(\prod_{\mathfrak{p}|\infty}\mathbb{R}_{>0})^0}{s(\mathcal{O}_K^1(\mathfrak{m}))} \xrightarrow{\sim} \frac{(\prod_{\mathfrak{p}|\infty}\mathbb{R})^0}{\mathrm{Log}(\mathcal{O}_K^1(\mathfrak{m}))}$$

of LCA groups. Next we define a map

$$\mathcal{O}_K^1(\mathfrak{m})\otimes_{\mathbb{Z}}\mathbb{R}/\mathbb{Z} \to \frac{(\prod_{\mathfrak{p}|\infty}\mathbb{R})^0}{\mathrm{Log}(\mathcal{O}_K^1(\mathfrak{m}))},\ u\otimes\overline{x}\mapsto\overline{x\cdot\mathrm{Log}(u^{-1})}.$$

This is clearly well-defined, and it is continuous, using the topology from Proposition 4.42 on $\mathcal{O}_K^1(\mathfrak{m})\otimes_{\mathbb{Z}}\mathbb{R}/\mathbb{Z}$. By Theorem 6.8, $\mathrm{Log}(\mathcal{O}_K^1(\mathfrak{m}))$ is a complete lattice in $(\prod_{\mathfrak{p}|\infty}\mathbb{R})^0$ which shows that the map is surjective. Moreover, we may pick $u_1,\dots,u_n\in\mathcal{O}_K^1(\mathfrak{m})$ such that $\mathrm{Log}(u_1),\dots,\mathrm{Log}(u_n)$ are a $\mathbb{Z}$-basis of $\mathrm{Log}(\mathcal{O}_K^1(\mathfrak{m}))$ and an $\mathbb{R}$-basis of $(\prod_{\mathfrak{p}|\infty}\mathbb{R})^0$. Then every element of $\mathcal{O}_K^1(\mathfrak{m})\otimes_{\mathbb{Z}}\mathbb{R}/\mathbb{Z}$ can be written as $\sum_{i=1}^n u_i\otimes\overline{x_i}$ for some $x_i\in\mathbb{R}$. If such an element is contained in the kernel of the above map, then $\sum_{i=1}^n -x_i\,\mathrm{Log}(u_i)\in\mathrm{Log}(\mathcal{O}_K^1(\mathfrak{m}))$ and $\mathbb{R}$-linear independence gives $x_i\in\mathbb{Z}$ for all i, so $\sum_{i=1}^n u_i\otimes\overline{x_i}=0$. Hence, the above map is injective and therefore an isomorphism of LCA groups. By tracing the given isomorphisms, one obtains the claimed short exact sequence, which is strictly exact by Proposition 4.21. Being the finite union of compact sets, $\mathrm{Pic}_K^0(\mathfrak{m})$ is compact. Note that all maps appearing above are in fact H-homomorphisms.

Since $\mathrm{Cl}_K(\mathfrak{m})$ is finite, $\mathcal{O}_K^1(\mathfrak{m})\otimes_{\mathbb{Z}}\mathbb{R}/\mathbb{Z}$ is a closed subgroup of $\mathrm{Pic}_K^0(\mathfrak{m})$ of finite index, hence an open subgroup. It then follows from [HR79, Theorem 7.8] that $\mathcal{O}_K^1(\mathfrak{m})\otimes_{\mathbb{Z}}\mathbb{R}/\mathbb{Z}$ is the connected component of the identity of $\mathrm{Pic}_K^0(\mathfrak{m})$. The final claim is immediate from Proposition 4.12. □

As an analogue of Proposition 6.5 we obtain:

Proposition 6.16. *Suppose that $\mathfrak{m}$ is H-stable for $H\le\mathrm{Aut}(K)$. There is an exact sequence of compact real abelian Lie groups with an action of H by continuous group automorphisms*

$$0\longrightarrow\mu(K)\cap\mathcal{O}_K^1(\mathfrak{m})\longrightarrow\mu(K)\xrightarrow{\rho}(\mathcal{O}_K/\mathfrak{m}_0)^\times\times\{\pm1\}^{\mathfrak{m}_\infty}\xrightarrow{\psi}\mathrm{Pic}_K^0(\mathfrak{m})\longrightarrow\mathrm{Pic}_K^0\longrightarrow 0$$

where the left hand map is inclusion, the right hand map is the natural map, and ψ maps $\rho(a)$, where $a\in K^\times$ is coprime to $\mathfrak{m}$, to the class of $(a\mathcal{O}_K,(|\sigma_{\mathfrak{p}}(a)|^{-1})_{\mathfrak{p}})$.

Proof. The proof of [Coh00, Proposition 3.2.3] immediately generalises. □

Definition 6.17. We write

$$\mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})\colon\qquad 0\longrightarrow\frac{(\mathcal{O}_K/\mathfrak{m}_0)^\times\times\{\pm1\}^{\mathfrak{m}_\infty}}{\rho(\mu(K))}\xrightarrow{\psi}\mathrm{Pic}_K^0(\mathfrak{m})\longrightarrow\mathrm{Pic}_K^0\longrightarrow 0$$

for the short exact sequence coming from Proposition 6.16 and refer to it as the *Arakelov ray class group sequence.*

The exact sequence $\mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})$ and the sequence from Proposition 6.15 fit together in a big commutative diagram which summarises much of the content of this section.

Theorem 6.18. *Suppose that $\mathfrak{m}$ is H-stable for $H \leq \mathrm{Aut}(K)$. There is a commutative diagram of compact real abelian Lie groups with an action of H by continuous group automorphisms*

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & \frac{\rho(\mathcal{O}_K^\times)}{\rho(\mu(K))} \arrow[r] \arrow[d] & \mathcal{O}_K^1(\mathfrak{m}) \otimes_{\mathbb{Z}} \mathbb{R}/\mathbb{Z} \arrow[r] \arrow[d] & \mathcal{O}_K^\times \otimes_{\mathbb{Z}} \mathbb{R}/\mathbb{Z} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \frac{(\mathcal{O}_K/\mathfrak{m}_0)^\times \times \{\pm 1\}^{\mathfrak{m}_\infty}}{\rho(\mu(K))} \arrow[r] \arrow[d] & \mathrm{Pic}_K^0(\mathfrak{m}) \arrow[r] \arrow[d] & \mathrm{Pic}_K^0 \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \frac{(\mathcal{O}_K/\mathfrak{m}_0)^\times \times \{\pm 1\}^{\mathfrak{m}_\infty}}{\rho(\mathcal{O}_K^\times)} \arrow[r] \arrow[d] & \mathrm{Cl}_K(\mathfrak{m}) \arrow[r] \arrow[d] & \mathrm{Cl}_K \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

with exact rows and columns, where: ρ is the map from Definition 6.3; the middle row is $\mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})$; the bottom row is $\mathrm{S}_K^{\mathrm{fin}}(\mathfrak{m})$; the middle and right hand columns are the sequences from Proposition 6.15; the left hand map in the top row maps the class of $\rho(u)$ to $u^t \otimes \overline{\frac{1}{t}}$, where $u \in \mathcal{O}_K^\times$ and $t = \left|\mathcal{O}_K^\times : \mathcal{O}_K^1(\mathfrak{m})\right|$.

Proof. Commutativity of all four squares of the diagram is immediate from the definition of the respective maps. All of the exactness is clear except for the top row. Exactness of the latter follows from the snake lemma. □

Denoting the top row in the diagram above by $\mathrm{S}_K^{\mathrm{tori}}(\mathfrak{m})$, we can write the diagram as a short exact sequence

$$\mathrm{D}_K(\mathfrak{m})\colon \qquad 0 \longrightarrow \mathrm{S}_K^{\mathrm{tori}}(\mathfrak{m}) \longrightarrow \mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m}) \longrightarrow \mathrm{S}_K^{\mathrm{fin}}(\mathfrak{m}) \longrightarrow 0$$

of short exact sequences of compact real abelian Lie groups.

6.4 Information Carried by the Arakelov Ray Class Sequence

In this section, we show that the Arakelov ray class sequence $\mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})$ 'knows about' both the diagram $\mathrm{D}_K(\mathfrak{m})$ and the reduction map $\rho_K(\mathfrak{m})$ in the sense that the latter two can be obtained from the former by certain general constructions performed on short exact sequences. This is taken from [BP25, Section 3].

6.4.1 Recovering the Diagram $\mathrm{D}_K(\mathfrak{m})$

We recall the construction from [BP25, page 11] that shows that the diagram $\mathrm{D}_K(\mathfrak{m})$ can be recovered from just the short exact sequence $\mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})$. We use the slightly more general setting of LCA modules over a locally compact ring.

Construction 6.19. Let R be locally compact topological ring. Let

$$\Gamma\colon \qquad 0 \longrightarrow Y \xrightarrow{\gamma} W \xrightarrow{\delta} X \longrightarrow 0$$

be a short exact sequence of compact LCA R-modules. Note that it is automatically strictly exact by Proposition 4.21. We show that Γ naturally induces a short exact sequence of short exact sequences of which it is the middle term.

Since W is compact, so are W_0 and $\delta(W_0)$. Strictness of δ and [HR79, Theorem 7.12] imply that $\delta(W_0) = X_0$. It follows from this and Proposition 4.21 that there is a short strictly exact sequence of compact LCA R-modules

$$\Gamma_0\colon \qquad 0 \longrightarrow \ker(\delta|_{W_0}) \longrightarrow W_0 \xrightarrow{\delta|_{W_0}} X_0 \longrightarrow 0.$$

We also get a short strictlyexact sequence of compact LCA R-modules

$$\overline{\Gamma}\colon \qquad 0 \longrightarrow \ker(\overline{\delta}) \longrightarrow W/W_0 \xrightarrow{\overline{\delta}} X/X_0 \longrightarrow 0$$

where $\overline{\delta}$ is the natural map induced by δ. Now define a morphism

$$\gamma'\colon Y \to \ker(\overline{\delta}),\ y \mapsto \overline{\gamma(y)}.$$

It is then easy to see that

$$0 \longrightarrow \ker(\delta|_{W_0}) \xrightarrow{\gamma^{-1}} Y \xrightarrow{\gamma'} \ker(\overline{\delta}) \longrightarrow 0$$

is a short strictly exact sequence of compact LCA R-modules. Moreover, we have a commutative diagram of compact LCA R-modules with strictly exact rows and columns

$$\begin{tikzcd}
 & & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
\Gamma_0\colon & 0 \arrow[r] & \ker(\delta|_{W_0}) \arrow[r] \arrow[d, "\gamma^{-1}"] & W_0 \arrow[r, "\delta|_{W_0}"] \arrow[d] & X_0 \arrow[r] \arrow[d] & 0 \\
\Gamma\colon & 0 \arrow[r] & Y \arrow[r, "\gamma"] \arrow[d, "\gamma'"] & W \arrow[r, "\delta"] \arrow[d] & X \arrow[r] \arrow[d] & 0 \\
\overline{\Gamma}\colon & 0 \arrow[r] & \ker(\overline{\delta}) \arrow[r] \arrow[d] & W/W_0 \arrow[r, "\overline{\delta}"] \arrow[d] & X/X_0 \arrow[r] \arrow[d] & 0 \\
 & & 0 & 0 & 0. &
\end{tikzcd}$$

That is to say, there is a short exact sequence

$$\mathrm{D}_{\mathrm{c}}(\Gamma)\colon \qquad 0 \longrightarrow \Gamma_0 \longrightarrow \Gamma \longrightarrow \overline{\Gamma} \longrightarrow 0$$

of short strictly exact sequences of compact LCA R-modules.

Proposition 6.20. *It holds that* $\mathrm{D}_{\mathrm{c}}(\mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})) = \mathrm{D}_K(\mathfrak{m})$.

Proof. This is immediate from Theorem 6.18. □

6.4.2 Recovering the Reduction Map $\rho_K(\mathfrak{m})$

Recall the natural reduction map

$$\rho := \rho_K(\mathfrak{m})\colon \mathcal{O}_K^\times \to (\mathcal{O}_K/\mathfrak{m}_0)^\times \times \{\pm 1\}^{\mathfrak{m}_\infty}, \; u \mapsto (\overline{u}, (\operatorname{sign}\sigma_{\mathfrak{p}}(u))_{\mathfrak{p}})$$

from Definition 6.3. Denote by

$$\overline{\rho} := \overline{\rho_K(\mathfrak{m})}\colon \frac{\mathcal{O}_K^\times}{\mu(K)} \to \frac{(\mathcal{O}_K/\mathfrak{m}_0)^\times \times \{\pm 1\}^{\mathfrak{m}_\infty}}{\rho(\mu(K))}$$

the map induced by ρ. We discuss the construction from [BP25, page 13] that allows to recover $\overline{\rho}$ from $\mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})$. We work in the slightly more general setting that takes into account group actions.

Construction 6.21. Let G be a finite group. Let X be a compact real abelian Lie group with an action of G by continuous group automorphisms. Let Y be a finite $\mathbb{Z}G$-module. We construct a map

$$\omega_{\mathrm{c}} := \omega_{\mathrm{c}}^{X,Y} : E_{\mathbb{Z}G}\mathsf{LCA}(X,Y) \to \operatorname{Hom}_{\mathbb{Z}G}((X^\vee/(X^\vee)_{\mathrm{tors}})^*, Y),$$

where we recall that $(X^\vee/(X^\vee)_{\mathrm{tors}})^* = \operatorname{Hom}_{\mathbb{Z}}(X^\vee/(X^\vee)_{\mathrm{tors}}, \mathbb{Z})$ is the dual lattice from Definition 3.6 (here, $Z = \mathbb{Z}$ and $R = \mathbb{Z}G$). Let $\Gamma \in E_{\mathbb{Z}G}\mathsf{LCA}(X,Y)$ and suppose that it is given by the short strictly exact sequence

$$0 \longrightarrow Y \xrightarrow{\gamma} W \xrightarrow{\delta} X \longrightarrow 0$$

of LCA $\mathbb{Z}G$-modules. Note that W is compact by Remark 4.26 (a). By Pontryagin duality and Corollary 4.16 (ii) we have a natural isomorphism

$$X_0 \xrightarrow{\sim} (X^\vee/(X^\vee)_{\mathrm{tors}})^\vee, \; x \mapsto (\overline{f} \mapsto f(x))$$

of compact LCA $\mathbb{Z}G$-modules and by Propositions 4.42 and 3.7 there is a natural isomorphism

$$(X^\vee/(X^\vee)_{\mathrm{tors}})^* \otimes_{\mathbb{Z}} \mathbb{R}/\mathbb{Z} \xrightarrow{\sim} (X^\vee/(X^\vee)_{\mathrm{tors}})^\vee, \; h \otimes \overline{t} \mapsto (\overline{f} \mapsto \overline{h(\overline{f}) \cdot t})$$

of compact LCA $\mathbb{Z}G$-modules, and analogously with X replaced by W. We moreover have a short exact sequence

$$0 \longrightarrow X^\vee/(X^\vee)_{\mathrm{tors}} \xrightarrow{\overline{\delta^\vee}} W^\vee/(W^\vee)_{\mathrm{tors}} \longrightarrow Y^\vee/\gamma^\vee((W^\vee)_{\mathrm{tors}}) \longrightarrow 0$$

of discrete $(\mathbb{Z}G)^{\mathrm{op}}$-modules. Since Y is finite, this shows that $(\overline{\delta^\vee})^*$ is injective with finite cokernel. Hence, $(\overline{\delta^\vee})^* \otimes \mathrm{id}_{\mathbb{R}}$ is an isomorphism of real vector spaces and G-modules. Now consider the commutative diagram

$$\begin{tikzcd}
 & & & (X^\vee/(X^\vee)_{\mathrm{tors}})^* \arrow[d, phantom, sloped, "\subseteq"] \arrow[dddd, dashed, rounded corners, to path={-- ([yshift=-3ex]\tikztostart.south |- \tikztotarget.north)}, draw=none] \arrow[ddddll, dashed, bend right] & \\
 & & (W^\vee/(W^\vee)_{\mathrm{tors}})^* \otimes_{\mathbb{Z}} \mathbb{R} \arrow[r, "(\overline{\delta^\vee})^* \otimes \mathrm{id}_{\mathbb{R}}", "\sim"'] \arrow[d] & (X^\vee/(X^\vee)_{\mathrm{tors}})^* \otimes_{\mathbb{Z}} \mathbb{R} \arrow[d] & \\
 & & (W^\vee/(W^\vee)_{\mathrm{tors}})^* \otimes_{\mathbb{Z}} \mathbb{R}/\mathbb{Z} \arrow[r] \arrow[d, phantom, sloped, "\cong"] & (X^\vee/(X^\vee)_{\mathrm{tors}})^* \otimes_{\mathbb{Z}} \mathbb{R}/\mathbb{Z} \arrow[d, phantom, sloped, "\cong"] & \\
0 \arrow[r] & \ker \delta|_{W_0} \arrow[r] \arrow[d, "\gamma^{-1}"] & W_0 \arrow[r, "\delta|_{W_0}"] \arrow[d] & X_0 \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & Y \arrow[r, "\gamma"] & W \arrow[r, "\delta"] & X \arrow[r] & 0.
\end{tikzcd}$$

By commutativity, the image of $(X^\vee/(X^\vee)_{\mathrm{tors}})^*$ in W_0 is contained in $\ker \delta|_{W_0}$, so we may apply γ^{-1} to it to land in Y. This gives a map $\omega_{\mathrm{c}}(\Gamma) \in \mathrm{Hom}_{\mathbb{Z}G}((X^\vee/(X^\vee)_{\mathrm{tors}})^*, Y)$, depicted in green above. One checks that it is independent of the chosen representative for Γ.

For $\varphi \in (X^\vee/(X^\vee)_{\mathrm{tors}})^*$ we can explicitly give the image of $\gamma(\omega_{\mathrm{c}}(\Gamma)(\varphi)) \in W$ under any element of $W^\vee$, by tracing the isomorphisms above: Let $g \in W^\vee$. Then there is a unique $\overline{h} \in X^\vee/(X^\vee)_{\mathrm{tors}}$ such that $|Y|\,\overline{g} = \overline{\delta^\vee}(\overline{h})$ and it holds that

$$g\big(\gamma(\omega_{\mathrm{c}}(\Gamma)(\varphi))\big) = \overline{\varphi(\overline{h}) \cdot \frac{1}{|Y|}}.$$

The construction above is related to Construction 6.19 in the following way.

Proposition 6.22. *Let G be a finite group. Let X be a compact real abelian Lie group with an action of G by continuous group automorphisms. Let Y be a finite $\mathbb{Z}G$-module. Suppose that $\Gamma \in E_{\mathbb{Z}G}\mathsf{LCA}(X, Y)$ is given by the short strictly exact sequence*

$$0 \longrightarrow Y \xrightarrow{\gamma} W \xrightarrow{\delta} X \longrightarrow 0$$

of compact LCA $\mathbb{Z}G$-modules. Then there is a surjective $\mathbb{Z}G$-module homomorphism $\sigma\colon (X^\vee/(X^\vee)_{\mathrm{tors}})^* \twoheadrightarrow \ker \delta|_{W_0}$ with $\omega_{\mathrm{c}}(\Gamma) = \gamma^{-1} \circ \sigma$.

Proof. By Construction 6.21 we can write $\omega_{\mathrm{c}}(\Gamma) = \gamma^{-1} \circ \gamma \circ \omega_{\mathrm{c}}(\Gamma)$, where $\gamma \circ \omega_{\mathrm{c}}(\Gamma)$ is a homomorphism from $(X^\vee/(X^\vee)_{\mathrm{tors}})^*$ to $\ker \delta|_{W_0}$. It follows from the commutative diagram in Construction 6.21 that $\gamma \circ \omega_{\mathrm{c}}(\Gamma)$ is surjective. □

Construction 6.23. Let $\mathfrak{n}$ be a modulus in K that is H-stable for $H \leq \mathrm{Aut}(K)$. The short exact sequence from Proposition 6.15 induces an isomorphism

$$\mathrm{Pic}^0_K(\mathfrak{n})^\vee/(\mathrm{Pic}^0_K(\mathfrak{n})^\vee)_{\mathrm{tors}} \xrightarrow{\sim} (\mathcal{O}^1_K(\mathfrak{n}) \otimes_{\mathbb{Z}} \mathbb{R}/\mathbb{Z})^\vee.$$

Now by Pontryagin duality and Proposition 4.42, there are natural isomorphisms

$$\mathcal{O}^1_K(\mathfrak{n})^* \xrightarrow{\sim} (\mathcal{O}^1_K(\mathfrak{n})^*)^{\vee\vee} \xrightarrow{\sim} (\mathcal{O}^1_K(\mathfrak{n}) \otimes_{\mathbb{Z}} \mathbb{R}/\mathbb{Z})^\vee,$$

and using further Proposition 3.7 we have natural isomorphisms

$$((\mathcal{O}^1_K(\mathfrak{n}) \otimes_{\mathbb{Z}} \mathbb{R}/\mathbb{Z})^\vee)^* \xrightarrow{\sim} \mathcal{O}^1_K(\mathfrak{n})^{**} \xleftarrow{\sim} \mathcal{O}^1_K(\mathfrak{n})/(\mu(K) \cap \mathcal{O}^1_K(\mathfrak{n})).$$

Overall, we obtain a natural isomorphism

$$(\mathrm{Pic}^0_K(\mathfrak{n})^\vee/(\mathrm{Pic}^0_K(\mathfrak{n})^\vee)_{\mathrm{tors}})^* \cong \mathcal{O}^1_K(\mathfrak{n})/(\mu(K) \cap \mathcal{O}^1_K(\mathfrak{n}))$$

of H-modules.

Proposition 6.24. *Suppose that $\mathfrak{m}$ is H-stable for $H \leq \mathrm{Aut}(K)$. Then under the isomorphism*

$$((\mathrm{Pic}^0_K)^\vee/((\mathrm{Pic}^0_K)^\vee)_{\mathrm{tors}})^* \cong \mathcal{O}^\times_K/\mu(K)$$

from Construction 6.23 and when considering $\mathrm{S}^{\mathrm{Ara}}_K(\mathfrak{m})$ as a short exact sequence of compact LCA H-modules, we have $\omega_{\mathrm{c}}(\mathrm{S}^{\mathrm{Ara}}_K(\mathfrak{m})) = \overline{\rho_K(\mathfrak{m})}$.

Proof. One checks that for any modulus $\mathfrak{n}$ in K, the isomorphism from Construction 6.23 tensored with $\mathrm{id}_{\mathbb{R}}$ fits into a commutative diagram

$$\begin{tikzcd}
(\mathrm{Pic}^0_K(\mathfrak{n})^\vee/(\mathrm{Pic}^0_K(\mathfrak{n})^\vee)_{\mathrm{tors}})^* \otimes_{\mathbb{Z}} \mathbb{R} \arrow[d] \arrow[r, phantom, "\cong"] & \mathcal{O}^1_K(\mathfrak{n})/(\mu(K) \cap \mathcal{O}^1_K(\mathfrak{n})) \otimes_{\mathbb{Z}} \mathbb{R} \arrow[dd] \\
(\mathrm{Pic}^0_K(\mathfrak{n})^\vee/(\mathrm{Pic}^0_K(\mathfrak{n})^\vee)_{\mathrm{tors}})^* \otimes_{\mathbb{Z}} \mathbb{R}/\mathbb{Z} \arrow[d, phantom, sloped, "\cong"] & \\
\mathrm{Pic}^0_K(\mathfrak{n})_0 & \mathcal{O}^1_K(\mathfrak{n}) \otimes_{\mathbb{Z}} \mathbb{R}/\mathbb{Z} \arrow[l, "\sim"']
\end{tikzcd}$$

where the isomorphism on the left hand side is the one from Construction 6.21 and the bottom map is the map from Proposition 6.15. Now by Proposition 6.5, the inclusion $\mathcal{O}^1_K(\mathfrak{m}) \hookrightarrow \mathcal{O}^\times_K$ induces an isomorphism

$$\mathcal{O}^1_K(\mathfrak{m})/(\mu(K) \cap \mathcal{O}^1_K(\mathfrak{m})) \otimes_{\mathbb{Z}} \mathbb{R} \xrightarrow{\sim} \mathcal{O}^\times_K/\mu(K) \otimes_{\mathbb{Z}} \mathbb{R}$$

whose inverse sends $u \otimes x$ to $u^t \otimes \frac{1}{t}$, where $t = \left|\mathcal{O}_K^\times : \mathcal{O}_K^1(\mathfrak{m})\right|$. By the above commutative diagram, in order to prove the claim, we have to show that the concatenation

$$\begin{aligned} \mathcal{O}_K^\times/\mu(K) &\hookrightarrow \mathcal{O}_K^\times/\mu(K) \otimes_\mathbb{Z} \mathbb{R} \\ &\xrightarrow{\sim} \mathcal{O}_K^1(\mathfrak{m})/(\mu(K) \cap \mathcal{O}_K^1(\mathfrak{m})) \otimes_\mathbb{Z} \mathbb{R} \\ &\to \mathcal{O}_K^1(\mathfrak{m}) \otimes_\mathbb{Z} \mathbb{R}/\mathbb{Z} \\ &\xrightarrow{\sim} \operatorname{Pic}_K^0(\mathfrak{m})_0 \end{aligned}$$

equals $\psi \circ \overline{\rho_K(\mathfrak{m})}$, where ψ is the map from Proposition 6.16. But this is immediate from the definitions of the respective maps. □

7 Picking out Good Components

As explained in the introduction, our main conjecture is concerned with the good part of the Arakelov ray class sequence, which is obtained from $\mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})$ by tensoring its dual with a suitable ring R. In the present chapter, we investigate this process of picking out good components and establish some fundamental properties of the corresponding ring R. We use the notion of good primes from [BL20]:

Definition 7.1 ([BL20, page 930])**.** Let G be a finite group and let $A = \mathbb{Q}G/I$ for some two-sided ideal I. We call a rational prime p *good for* A if there is a direct product decomposition as rings $\mathbb{Z}_{(p)}G \cong J \times J'$, where J is a maximal $\mathbb{Z}_{(p)}$-order in A, and the quotient map $\mathbb{Z}_{(p)}G \to A$ equals the projection $\mathbb{Z}_{(p)}G \to J$ composed with the inclusion $J \hookrightarrow A$.

If p is good for A, there is thus a commutative diagram

$$\begin{tikzcd}
J \times J' \arrow[r, phantom, "\cong"] \arrow[d] & \mathbb{Z}_{(p)}G \arrow[d] \\
J \arrow[r, hook] & A,
\end{tikzcd}$$

and it holds that $J = \mathrm{im}(\mathbb{Z}_{(p)}G \to A)$. Most importantly, the good primes include those coprime to the order of G:

Lemma 7.2. *Primes not dividing $|G|$ are good for A.*

Proof. This is immediate from [Rei03, Theorems 41.1 and 10.5]. □

For the most part, we will use the following notation.

Setup 7.3. Let G be a finite group and let $A = \mathbb{Q}G/I$ for some two-sided ideal I. Let S be a nonempty set of good primes for A and let $R := \mathrm{im}(\mathbb{Z}_{(S)}G \to A)$. We denote the localisation of the $\mathbb{Z}_{(S)}$-algebra R at $p\mathbb{Z}_{(S)}$ by R_p.

Suppose that $e_0, \dots, e_t$ are the primitive central idempotents of $\mathbb{Q}G$, that I is generated by $e_0, \dots, e_s$ for some $-1 \leq s \leq t$ (where we mean $I = 0$ if $s = -1$) and that S consists of rational primes not dividing $|G|$. Then by [Rei03, Theorems 41.1 and 10.5] we have $R \cong \mathbb{Z}_{(S)}G/(e_0\mathbb{Z}_{(S)}G \oplus \cdots \oplus e_s\mathbb{Z}_{(S)}G)$, and if M is a finite $\mathbb{Z}G$-module, it holds that

$$R \otimes_{\mathbb{Z}G} M \cong M[S^\infty]/(e_0M[S^\infty] \oplus \cdots \oplus e_sM[S^\infty]).$$

So by tensoring with R, one picks out the components of the good part $M[S^\infty]$ that belong to the blocks of $\mathbb{Q}G$ not contained in I.

7.1 Basic Properties of R and its Localisations

Use Setup 7.3. We prove some basic properties of R that will be used later.

In many situations, we will deal with Pontryagin duals or lattice duals of certain $\mathbb{Z}G$-modules or R-modules. These duals are a priori modules over the opposite rings. A convenient property of the specific rings we are working with is that they are self-opposite which allows to naturally regard modules over their opposite as modules over the original ring.

Construction 7.4. Let T be a ring and suppose that T admits an antiautomorphism $\tau\colon T \to T$. Then τ induces a ring isomorphism $T \xrightarrow{\sim} T^{\mathrm{op}}$. Hence, if M is a left T^{op}-module with action $T^{\mathrm{op}} \times M \to M$, $(t, m) \mapsto t * m$, then we may regard M as a left T-module via $t.m := \tau(t) * m$. This way any homomorphism $\varphi\colon M \to N$ of left T^{op}-modules is also a homomorphism of left T-modules. Analogously, if M is a right T^{op}-module with action given by $m * t$, then we may regard M as a right T-module via $m.t := m * \tau(t)$.

Convention 7.5. In the case of $\mathbb{Q}G$, we have the canonical involutory antiautomorphism

$$\tau\colon \mathbb{Q}G \to \mathbb{Q}G,\ g \mapsto g^{-1}.$$

If $Z \subseteq \mathbb{Q}$ is a subring, then τ restricts to an antiautomorphism of ZG. Moreover, if $e \in \mathbb{Q}G$ is one of the pairwise orthogonal primitive central idempotents, then we have $\tau(e) = e$ by [Lam91, Proposition 8.15] and [Isa76, Theorem 9.21 (c)]. In particular, $\tau(I) = I$, and τ induces an antiautomorphism $\overline{\tau}\colon A \to A$ that restricts to antiautomorphisms of R and R_p for $p \in S$. We will always use the antiautomorphisms τ and $\overline{\tau}$ to regard left resp. right modules over the opposite ring of any of the rings mentioned in this paragraph as left resp. right modules over the ring itself.

A key feature of R is that its localisations at the $p \in S$ allow us to make use of the properties of good primes.

Lemma 7.6. *Let $p \in S$ and let $\rho\colon J \times J' \xrightarrow{\sim} \mathbb{Z}_{(p)}G$ be a ring isomorphism, where J is a maximal $\mathbb{Z}_{(p)}$-order in A, and the quotient map $\mathbb{Z}_{(p)}G \to A$ equals the projection $\mathbb{Z}_{(p)}G \to J$ composed with the inclusion $J \hookrightarrow A$. Then $J = R_p$ and we have a commutative diagram*

$$\begin{tikzcd} R_p \times J' \arrow[r, "\rho"] \arrow[d] & \mathbb{Z}_{(p)}G \arrow[d] \\ R_p \arrow[r, hook] & A. \end{tikzcd} \tag{7.7}$$

Write $e := \rho(1, 0) \in \mathbb{Z}_{(p)}G$. The following hold:

(i) $(I \cap \mathbb{Z}_{(p)}G) \cdot e = 0$.

(ii) *For all $x \in \mathbb{Z}_{(p)}G$ and $w \in R_p$ we have $\rho(xw, 0) = x \cdot \rho(w, 0)$ and $\rho(wx, 0) = \rho(w, 0) \cdot x$. In particular, ρ induces an isomorphism $R_p \xrightarrow{\sim} \mathbb{Z}_{(p)}G \cdot e$ of left and right $\mathbb{Z}_{(p)}G$-algebras.*

(iii) *$\tau(e) = e$.*

(iv) *For all $w \in R_p$ we have $\tau(\rho(w, 0)) = \rho(\overline{\tau}(w), 0)$.*

Moreover, if $\widetilde{\rho}\colon R_p \times \widetilde{J}' \xrightarrow{\sim} \mathbb{Z}_{(p)}G$ is another ring homomorphism for which the analogue of (7.7) commutes, and $\widetilde{e} := \widetilde{\rho}(1, 0)$, then $e = \widetilde{e}$ and $\rho|_{R_p} = \widetilde{\rho}|_{R_p}$ as maps $R_p \to \mathbb{Z}_{(p)}G \cdot e$.

Proof. We have $R_p = (\mathbb{Z}_{(S)} \setminus p\mathbb{Z}_{(S)})^{-1}R = \operatorname{im}(\mathbb{Z}_{(p)}G \to A)$, so $R_p = J$.

Let $x \in (I \cap \mathbb{Z}_{(p)}G) \cdot e \subseteq \mathbb{Z}_{(p)}G \cdot e$. Then there is $w \in R_p$ with $x = \rho(w, 0)$. Using commutativity of (7.7) and the fact that $x \in I$, it follows that $w = 0$. So $x = 0$ and (i) is proved.

Note that e is a central idempotent of $\mathbb{Z}_{(p)}G$. As such, it commutes with all $g \in G$ which implies that it is also a central idempotent of $\mathbb{Q}G$. Hence, e is a sum of certain of the pairwise orthogonal primitive central idempotents of $\mathbb{Q}G$. But then it follows as in Convention 7.5 that $\tau(e) = e$, proving (iii).

For (iv) let $w \in R_p$. Commutativity of (7.7) implies that

$$\overline{\tau(\rho(w, 0)) - \rho(\overline{\tau}(w), 0)} = \overline{\tau}(w) - \overline{\tau}(w) = 0$$

which shows $\tau(\rho(w, 0)) - \rho(\overline{\tau}(w), 0) \in I \cap \mathbb{Z}_{(p)}G$. Moreover, by (iii) we have

$$\tau(\rho(w, 0)) = \tau(\rho(1, 0) \cdot \rho(w, 0)) = \tau(\rho(w, 0)) \cdot \tau(e) = \tau(\rho(w, 0)) \cdot e,$$

so that

$$\tau(\rho(w, 0)) - \rho(\overline{\tau}(w), 0) \in (I \cap \mathbb{Z}_{(p)}G) \cdot e.$$

Claim (iv) now follows from (i).

The identities in (ii) are proved analogously as for (iv): reduce modulo I and use (i).

Finally, suppose that $\widetilde{\rho}\colon R_p \times \widetilde{J}' \xrightarrow{\sim} \mathbb{Z}_{(p)}G$ is another ring homomorphism for which the analogue of (7.7) commutes. Then by (ii) we have $\mathbb{Z}_{(p)}G \cdot e \cong \mathbb{Z}_{(p)}G \cdot \widetilde{e}$ as $\mathbb{Z}_{(p)}G$-algebras. It thus follows from [Lam91, Exercise 22.2] that $e = \widetilde{e}$. Furthermore, if $w = \overline{x} \in R_p = \operatorname{im}(\mathbb{Z}_{(p)}G \to A)$, where $x \in \mathbb{Z}_{(p)}G$, then

$$\rho(w, 0) = \rho(x \cdot 1, 0) = xe = x\widetilde{e} = \widetilde{\rho}(x \cdot 1, 0) = \widetilde{\rho}(w, 0)$$

by part (ii). □

In the following, we discuss some more ring theoretic properties of R. When these are local properties, one can often prove them by either using properties of the maximal order $R_p = \operatorname{im}(\mathbb{Z}_{(p)}G \to A)$, or by obtaining the statement for $\mathbb{Z}_{(p)}G$ and then transferring it to R_p using a decomposition $\mathbb{Z}_{(p)}G \cong R_p \times J'_p$.

Proposition 7.8. *R is a maximal $\mathbb{Z}_{(S)}$-order in A.*

Proof. By [Rei03, Corollary 11.2], R is a maximal $\mathbb{Z}_{(S)}$-order in A if and only if R_p is a maximal $\mathbb{Z}_{(p)}$-order in A for all $p \in S$. But the latter holds by Lemma 7.6. □

This allows us to use all the statements on maximal orders we proved in the earlier chapters.

Proposition 7.9. *Let V be a finitely generated A-module. Then $V \cong V^*$ as A-modules.*

Proof. By [CR81, Exercise 9.13 and page 246], every finitely generated $\mathbb{Q}G$-module is isomorphic to its dual. This implies the claim as $A = \mathbb{Q}G/I$. □

Corollary 7.10. *Suppose that S is finite. Let M be an R-lattice. Then $M \cong M^*$ (noncanonically) as R-modules.*

Proof. By Propositions 7.9 and 2.1, there are isomorphisms of A-modules

$$A \otimes_R M \cong (A \otimes_R M)^* = (\mathbb{Q} \otimes_{\mathbb{Z}_{(S)}} M)^* \cong \mathbb{Q} \otimes_{\mathbb{Z}_{(S)}} M^* = A \otimes_R M^*.$$

Since M^* is an R-lattice by Proposition 3.7, an application of Proposition 3.10 yields $M \cong M^*$. □

Note that the statement is clearly false if M is not assumed to be a lattice: If M is any finite nontrivial R-module, then $M^* = 0$ while $M \neq 0$.

Notation 7.11. For $p \in S$, if M is a $\mathbb{Z}_{(p)}G$-module, then we denote by M_{R_p} the R_p-isotypical component of M, coming from a ring isomorphism $R_p \times J' \xrightarrow{\sim} \mathbb{Z}_{(p)}G$ for which (7.7) commutes. Moreover, for $w \in R_p$ we denote the element of $\mathbb{Z}_{(p)}G$ corresponding to $(w, 0)$ also simply by $(w, 0)$, or by $(w, 0)_p$ if p is not clear from the context. These notations are justified as by Lemma 7.6 they are independent of the chosen isomorphism in the definition of a good prime.

Taking these isotypical components interacts well with the antiautomorphisms from Convention 7.5.

Lemma 7.12. *Let $p \in S$. Let M be a left $(\mathbb{Z}_{(p)}G)^{\mathrm{op}}$-module. Then the R_p^{op}-isotypical component $M_{R_p^{\mathrm{op}}}$ is a left R_p^{op}-module. Regard it as a left R_p-module as in Convention 7.5 and denote the action by $w \bullet m$ for $w \in R_p$ and $m \in M_{R_p^{\mathrm{op}}}$.*

Regarding M as a left $\mathbb{Z}_{(p)}G$-module, the R_p-isotypical component M_{R_p} is a left R_p-module and we denote the action by $w \circ m$ for $w \in R_p$ and $m \in M_{R_p}$.

Then it holds that $M_{R_p^{\mathrm{op}}} = M_{R_p}$ and $w \bullet m = w \circ m$ for all $w \in R_p$ and $m \in M_{R_p}$, i.e. the identity

$$\mathrm{id}\colon (M_{R_p}, \circ) \to (M_{R_p^{\mathrm{op}}}, \bullet)$$

is an isomorphism of R_p-modules.

Proof. Denote the action of $\mathbb{Z}_{(p)}G^{\mathrm{op}}$ on M by $x * m$ for $x \in \mathbb{Z}_{(p)}G^{\mathrm{op}}$ and $m \in M$. Then by Lemma 7.6 (iii) we have

$$M_{R_p^{\mathrm{op}}} = (1,0) * M = \tau(1,0) * M = M_{R_p}.$$

Moreover, for $w \in R_p$ and $m \in M_{R_p}$, Lemma 7.6 (iv) gives

$$w \bullet m = (\overline{\tau}(w), 0) * m = \tau(w,0) * m = w \circ m,$$

as claimed. □

7.2 Tensoring with R over $\mathbb{Z}G$

Keep using Setup 7.3. As explained at the beginning of this chapter, the reason to consider the ring R is because tensoring a $\mathbb{Z}G$-module M with it picks out good components of M. In this subsection, we investigate the process of forming this tensor product in some more detail and prove several compatibility results of it with other constructions. We start with the crucial property of flatness.

Proposition 7.13. *R is a flat left and right $\mathbb{Z}G$-module.*

Proof. Let $0 \to N \to L \to M \to 0$ be an exact sequence of left $\mathbb{Z}G$-modules. We need to show that then also

$$0 \longrightarrow R \otimes_{\mathbb{Z}G} N \longrightarrow R \otimes_{\mathbb{Z}G} L \longrightarrow R \otimes_{\mathbb{Z}G} M \longrightarrow 0$$

is exact. Treating the sequence as a sequence of $\mathbb{Z}_{(S)}$-modules, by [Rei03, Corollary 3.16] this is equivalent to the statement that

$$0 \longrightarrow R_p \otimes_{\mathbb{Z}G} N \longrightarrow R_p \otimes_{\mathbb{Z}G} L \longrightarrow R_p \otimes_{\mathbb{Z}G} M \longrightarrow 0 \tag{7.14}$$

is exact for all $p \in S$. So let $p \in S$. Since $\mathbb{Z}_{(p)}$ is flat over $\mathbb{Z}$ and $\mathbb{Z}_{(p)}G \cong \mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} \mathbb{Z}G$, it follows that $\mathbb{Z}_{(p)}G$ is a flat left and right $\mathbb{Z}G$-module. Hence,

$$0 \longrightarrow \mathbb{Z}_{(p)}G \otimes_{\mathbb{Z}G} N \longrightarrow \mathbb{Z}_{(p)}G \otimes_{\mathbb{Z}G} L \longrightarrow \mathbb{Z}_{(p)}G \otimes_{\mathbb{Z}G} M \longrightarrow 0$$

is exact. Passing to isotypical components and noting Lemma 7.6 (ii), it follows that (7.14) is exact. So R is a flat right $\mathbb{Z}G$-module. The same proof works for R as a left $\mathbb{Z}G$-module. □

Lemma 7.15. *Let M be a $\mathbb{Z}G$-module. Then the following hold:*

(i) We have $(R \otimes_{\mathbb{Z}G} M)_{\mathrm{tors}} = R \otimes_{\mathbb{Z}G} M_{\mathrm{tors}}$ and the natural map

$$(R \otimes_{\mathbb{Z}G} M)/(R \otimes_{\mathbb{Z}G} M)_{\mathrm{tors}} \to R \otimes_{\mathbb{Z}G} M/M_{\mathrm{tors}}$$

is an isomorphism of R-modules. In particular, if M is a $\mathbb{Z}G$-lattice, then $R \otimes_{\mathbb{Z}G} M$ is an R-lattice.

(ii) Let $n \in \mathbb{Z}$. Then $(R \otimes_{\mathbb{Z}G} M)[n] = R \otimes_{\mathbb{Z}G} M[n]$ and the natural map

$$(R \otimes_{\mathbb{Z}G} M)/n(R \otimes_{\mathbb{Z}G} M) \to R \otimes_{\mathbb{Z}G} M/nM$$

is an isomorphism of R-modules.

(iii) If M is finite, then so is $R \otimes_{\mathbb{Z}G} M$. Moreover, we then have $(R \otimes_{\mathbb{Z}G} M)[p^\infty] = R \otimes_{\mathbb{Z}G} M[p^\infty]$ for any prime p.

Proof. We first show that if M is $\mathbb{Z}$-torsionfree, then $R \otimes_{\mathbb{Z}G} M$ is $\mathbb{Z}_{(S)}$-torsionfree. By [Sta25, Tag 0AUT], the latter is equivalent to the statement that $R_p \otimes_{\mathbb{Z}G} M$ is $\mathbb{Z}_{(p)}$-torsionfree for all $p \in S$. Now by loc. cit., for $p \in S$, the module $\mathbb{Z}_{(p)}G \otimes_{\mathbb{Z}G} M \cong \mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} M$ is $\mathbb{Z}_{(p)}$-torsionfree. As $R_p \otimes_{\mathbb{Z}G} M$ is a direct summand of this module, it is also $\mathbb{Z}_{(p)}$-torsionfree. This proves the claim.

Flatness of R gives an exact sequence of R-modules

$$0 \longrightarrow R \otimes_{\mathbb{Z}G} M_{\mathrm{tors}} \longrightarrow R \otimes_{\mathbb{Z}G} M \longrightarrow R \otimes_{\mathbb{Z}G} M/M_{\mathrm{tors}} \longrightarrow 0,$$

where $R \otimes_{\mathbb{Z}G} M/M_{\mathrm{tors}}$ is $\mathbb{Z}_{(S)}$-torsionfree by what we have proved above. Claim (i) follows. For (ii) simply apply the exact functor $R \otimes_{\mathbb{Z}G} -$ to the exact sequence

$$0 \longrightarrow M[n] \longrightarrow M \xrightarrow{\cdot n} M \longrightarrow M/nM \longrightarrow 0.$$

Finally, suppose that M is finite. Then by (i), $R \otimes_{\mathbb{Z}G} M$ is a finitely generated torsion $\mathbb{Z}_{(S)}$-module, hence finite. If p is a prime, then clearly $R \otimes_{\mathbb{Z}G} M[p^\infty] \subseteq (R \otimes_{\mathbb{Z}G} M)[p^\infty]$. On the other hand, the decomposition $M = \bigoplus_q M[q^\infty]$ gives $R \otimes_{\mathbb{Z}G} M = \bigoplus_q R \otimes_{\mathbb{Z}G} M[q^\infty]$. It follows that $R \otimes_{\mathbb{Z}G} M[p^\infty] = (R \otimes_{\mathbb{Z}G} M)[p^\infty]$. □

Tensoring with R behaves well with taking isotypical components with respect to the localisations of R.

Lemma 7.16. *Let M be a finite $\mathbb{Z}G$-module. Let $r \in R$ and $m \in M$. Then*

$$r \otimes m = \sum_{p \in S} 1 \otimes (r, 0)_p m_p \in R \otimes_{\mathbb{Z}G} M,$$

where m_p denotes the $M[p^\infty]$-component of m.

Proof. Write $r = \overline{x}$ for $x \in \mathbb{Z}_{(S)}G$. Then $r \otimes m = \sum_{p \in S} r \otimes m_p = \sum_{p \in S} 1 \otimes xm_p$, using that for $p \in S$, $M[p^\infty]$ has the structure of a $\mathbb{Z}_{(S)}G$-module. Now let $p \in S$ and let $\rho\colon R_p \times J' \xrightarrow{\sim} \mathbb{Z}_{(p)}G$ be a ring isomorphism for which (7.7) commutes. Then $1 = (1,0)_p + \rho(0,1) \in \mathbb{Z}_{(p)}G$ and

$$xm_p = x(1,0)_p m_p + x\rho(0,1)m_p = (r,0)_p m_p + x\rho(0,1)m_p.$$

By commutativity of (7.7) we have $\rho(0,1) \in \mathbb{Z}_{(p)}G \cap I$, so there is $b \in \mathbb{Z} \setminus p\mathbb{Z}$ with $b\rho(0,1) \in \mathbb{Z}G \cap I$. It follows that

$$1 \otimes x\rho(0,1)m_p = \overline{b\rho(0,1)} \otimes x\frac{1}{b}m_p = 0 \in R \otimes_{\mathbb{Z}G} M[p^\infty].$$

Hence, $1 \otimes xm_p = 1 \otimes (r,0)_p m_p$, and the claim follows. □

We now prove compatibility of $R \otimes_{\mathbb{Z}G} -$ with Pontryagin duality for finite modules.

Proposition 7.17. *Let M be a finite $\mathbb{Z}G$-module. For $\varphi \in (R \otimes_{\mathbb{Z}G} M)^\vee$ define*

$$\widetilde{\varphi}\colon M \to \mathbb{R}/\mathbb{Z},\ m \mapsto \varphi(1 \otimes m).$$

Then the map

$$\delta := \delta_M\colon (R \otimes_{\mathbb{Z}G} M)^\vee \to R \otimes_{\mathbb{Z}G} M^\vee,\ \varphi \mapsto 1 \otimes \widetilde{\varphi}$$

is an R-module isomorphism, where we regard $M^\vee$ as a $\mathbb{Z}G$-module and $(R \otimes_{\mathbb{Z}G} M)^\vee$ as an R-module as in Convention 7.5. Moreover, this isomorphism is natural in M: If N is another finite $\mathbb{Z}G$-module and $\alpha\colon M \to N$ is a $\mathbb{Z}G$-homomorphism, then the diagram

$$\begin{tikzcd}
(R \otimes_{\mathbb{Z}G} N)^\vee \arrow[r, "\delta_N"] \arrow[d, "(\mathrm{id}_R \otimes \alpha)^\vee"'] & R \otimes_{\mathbb{Z}G} N^\vee \arrow[d, "\mathrm{id}_R \otimes \alpha^\vee"] \\
(R \otimes_{\mathbb{Z}G} M)^\vee \arrow[r, "\delta_M"'] & R \otimes_{\mathbb{Z}G} M^\vee
\end{tikzcd}$$

commutes.

Proof. It is clear that δ is $\mathbb{Z}$-linear. We prove that it is an R-module isomorphism by constructing its inverse. For a prime p, there are isomorphisms of $\mathbb{Z}_{(p)}G$-modules

$$\begin{aligned}
\mathbb{Z}_{(p)}G \otimes_{\mathbb{Z}G} M^\vee &\cong \mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} M^\vee && (\mathbb{Z}_{(p)}G \cong \mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} \mathbb{Z}G) \\
&\cong M^\vee[p^\infty] && (\text{Lemma } 3.3) \\
&\cong M[p^\infty]^\vee && (\text{Corollary } 4.18) \\
&\cong (\mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} M)^\vee && (\text{Lemma } 3.3) \\
&\cong (\mathbb{Z}_{(p)}G \otimes_{\mathbb{Z}G} M)^\vee. && (\mathbb{Z}_{(p)}G \cong \mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} \mathbb{Z}G)
\end{aligned}$$

The overall isomorphism is given by

$$\begin{aligned}\mathbb{Z}_{(p)}G \otimes_{\mathbb{Z}G} M^\vee &\to (\mathbb{Z}_{(p)}G \otimes_{\mathbb{Z}G} M)^\vee,\\ x \otimes f &\mapsto \big((y \otimes m) \mapsto f(\tau(x) y m_p)\big),\end{aligned}$$

where m_p denotes the $M[p^\infty]$-component of m. Now let $p \in S$. Then there are isomorphisms of R_p-modules

$$\begin{aligned}(R \otimes_{\mathbb{Z}G} M^\vee)[p^\infty] &\cong R_p \otimes_{\mathbb{Z}G} M^\vee && \text{(Lemma 3.3)}\\ &\cong (\mathbb{Z}_{(p)}G \otimes_{\mathbb{Z}G} M^\vee)_{R_p} && \text{(Lemma 7.6 (ii))}\\ &\cong \big((\mathbb{Z}_{(p)}G \otimes_{\mathbb{Z}G} M)^\vee\big)_{R_p} && \text{(above)}\\ &\cong \big((\mathbb{Z}_{(p)}G \otimes_{\mathbb{Z}G} M)^\vee\big)_{R_p^{\mathrm{op}}} && \text{(Lemma 7.12)}\\ &\cong \big((\mathbb{Z}_{(p)}G \otimes_{\mathbb{Z}G} M)_{R_p}\big)^\vee && \text{(Lemma 4.19)}\\ &\cong (R_p \otimes_{\mathbb{Z}G} M)^\vee && \text{(Lemma 7.6 (ii))}\\ &\cong (R \otimes_{\mathbb{Z}G} M)[p^\infty]^\vee && \text{(Lemma 3.3)}\\ &\cong (R \otimes_{\mathbb{Z}G} M)^\vee[p^\infty], && \text{(Corollary 4.18)}\end{aligned}$$

where in the appropriate places we again regard the Pontryagin duals as modules over the respective ring rather than its opposite, as per Convention 7.5. Note also that $R \otimes_{\mathbb{Z}G} M$ is finite by Lemma 7.15 (iii), and we regard it with its natural discrete topology to form the Pontryagin dual. The overall isomorphism above is given by

$$\begin{aligned}\gamma_p \colon (R \otimes_{\mathbb{Z}G} M^\vee)[p^\infty] &\to (R \otimes_{\mathbb{Z}G} M)^\vee[p^\infty],\\ r \otimes f &\mapsto \big(s \otimes m \mapsto f((\overline{\tau}(r)s, 0)_p m_p)\big).\end{aligned}$$

The isomorphisms γ_p glue together to an R-module isomorphism

$$\gamma \colon R \otimes_{\mathbb{Z}G} M^\vee \xrightarrow{\sim} (R \otimes_{\mathbb{Z}G} M)^\vee.$$

We show that γ is the inverse of δ.

Let $\varphi \in (R \otimes_{\mathbb{Z}G} M)^\vee$ and let $r \in R$ and $m \in M$. Then using Lemma 7.16 we have

$$\begin{aligned}(\gamma \circ \delta)(\varphi)\ (r \otimes m) &= \sum_{p \in S} \gamma_p(1 \otimes \widetilde{\varphi}_p)\ (r \otimes m)\\ &= \sum_{p \in S} \widetilde{\varphi}_p((r, 0)_p m_p)\\ &= \sum_{p \in S} \varphi(1 \otimes (r, 0)_p m_p)\\ &= \varphi(r \otimes m),\end{aligned}$$

so $(\gamma \circ \delta)(\varphi) = \varphi$. Conversely, let $r \in R$ and $f \in M^\vee$. Then

$$\begin{aligned}(\delta \circ \gamma)(r \otimes f) &= \sum_{p \in S} \delta(\gamma_p(r \otimes f_p)) \\ &= \sum_{p \in S} 1 \otimes \gamma_p \widetilde{(r \otimes f_p)}.\end{aligned}$$

Here, for $m \in M$ we have

$$\begin{aligned}\gamma_p \widetilde{(r \otimes f_p)}(m) &= \gamma_p(r \otimes f_p)(1 \otimes m) \\ &= f_p((\overline{\tau}(r), 0)_p m_p) \\ &= f_p(\tau((r, 0)_p) m_p) \\ &= ((r, 0)_p f_p)(m)\end{aligned}$$

where we have used Lemma 7.6 (iv). It follows from this and Lemma 7.16 that

$$(\delta \circ \gamma)(r \otimes f) = \sum_{p \in S} 1 \otimes (r, 0)_p f_p = r \otimes f.$$

Hence, γ is the inverse of δ which shows that δ is an R-module isomorphism. It is straightforward to verify naturality of δ. □

Ending this section, we show that $R \otimes_{\mathbb{Z}G} -$ is compatible with duality for lattices.

Proposition 7.18. *Suppose that S is finite. Let M be a $\mathbb{Z}G$-lattice. Define a map*

$$d := d_M \colon (R \otimes_{\mathbb{Z}G} M)^* \to R \otimes_{\mathbb{Z}G} M^*, \ \varphi \mapsto \frac{1}{b} \otimes \varphi_b$$

where $b \in \mathbb{Z} \setminus \bigcup_{p \in S} p\mathbb{Z}$ is chosen such that $b \cdot \varphi(1 \otimes M) \subseteq \mathbb{Z}$ and where

$$\varphi_b \colon M \to \mathbb{Z}, \ m \mapsto b \cdot \varphi(1 \otimes m).$$

Then the element $\frac{1}{b} \otimes \varphi_b \in R \otimes_{\mathbb{Z}G} M^*$ is independent of the choice of b and the map d_M is an R-module isomorphism. Moreover, it is natural in M: If N is another $\mathbb{Z}G$-lattice and $\alpha \colon M \to N$ is a $\mathbb{Z}G$-homomorphism, then the diagram

$$\begin{tikzcd}(R \otimes_{\mathbb{Z}G} N)^* \arrow[r, "d_N"] \arrow[d, "(\mathrm{id}_R \otimes \alpha)^*"'] & R \otimes_{\mathbb{Z}G} N^* \arrow[d, "\mathrm{id}_R \otimes \alpha^*"] \\ (R \otimes_{\mathbb{Z}G} M)^* \arrow[r, "d_M"'] & R \otimes_{\mathbb{Z}G} M^*\end{tikzcd}$$

commutes.

Note that by $(R \otimes_{\mathbb{Z}G} M)^*$ we mean $\mathrm{Hom}_{\mathbb{Z}_{(S)}}(R \otimes_{\mathbb{Z}G} M, \mathbb{Z}_{(S)})$ and by M^* we mean $\mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Z})$.

Proof. Independence of b is checked immediately. We first show that d is R-linear. Let $\varphi, \psi \in (R \otimes_{\mathbb{Z}G} M)^*$. Let $b \in \mathbb{Z} \setminus \bigcup_{p \in S} p\mathbb{Z}$ such that $b \cdot \varphi(1 \otimes M) \subseteq \mathbb{Z}$ and $b \cdot \psi(1 \otimes M) \subseteq \mathbb{Z}$. Then

$$d(\varphi + \psi) = \frac{1}{b} \otimes (\varphi + \psi)_b = \frac{1}{b} \otimes \varphi_b + \frac{1}{b} \otimes \psi_b = d(\varphi) + d(\psi).$$

Now let $r \in R$ and suppose that this time $b \in \mathbb{Z} \setminus \bigcup_{p \in S} p\mathbb{Z}$ is such that $b \cdot \varphi(1 \otimes M) \subseteq \mathbb{Z}$ and $b \cdot (r\varphi)(1 \otimes M) \subseteq \mathbb{Z}$. Write $r = \overline{u \cdot w}$ with $u \in \mathbb{Z}_{(S)}$ and $w \in \mathbb{Z}G$. For $m \in M$ we have

$$(r\varphi)_b(m) = b \cdot (r\varphi)(1 \otimes m) = b\varphi(\overline{\tau}(r) \otimes m) = ub\varphi(\overline{\tau(w)} \otimes m).$$

Now put $\widetilde{\varphi}(m) := \varphi(\overline{\tau(w)} \otimes m)$. Without loss of generality, b is such that $b\widetilde{\varphi} \in M^*$. Then

$$d(r\varphi) = \frac{1}{b} \otimes (r\varphi)_b = \frac{1}{b} \otimes ub\widetilde{\varphi} = \frac{1}{b}\overline{u} \otimes b\widetilde{\varphi}.$$

On the other hand,

$$rd(\varphi) = r\frac{1}{b} \otimes \varphi_b = \frac{1}{b}\overline{u} \otimes w\varphi_b,$$

where for $m \in M$,

$$w\varphi_b(m) = \varphi_b(\tau(w)m) = b \cdot \varphi(1 \otimes \tau(w)m) = b \cdot \varphi(\overline{\tau(w)} \otimes m) = b\widetilde{\varphi}(m),$$

whence $rd(\varphi) = d(r\varphi)$.

We now construct a map $R \otimes_{\mathbb{Z}G} M^* \to (R \otimes_{\mathbb{Z}G} M)^*$ that will give rise to the inverse of d. First, for a prime p, there are isomorphisms of $\mathbb{Z}_{(p)}G$-modules

$$\begin{aligned} \mathbb{Z}_{(p)}G \otimes_{\mathbb{Z}G} M^* &\cong \mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} M^* && (\mathbb{Z}_{(p)}G \cong \mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} \mathbb{Z}G) \\ &\cong (\mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} M)^* && (\text{Proposition 2.1}) \\ &\cong (\mathbb{Z}_{(p)}G \otimes_{\mathbb{Z}G} M)^*. && (\mathbb{Z}_{(p)}G \cong \mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} \mathbb{Z}G) \end{aligned}$$

The overall isomorphism is given by

$$\begin{aligned} \alpha_p \colon \mathbb{Z}_{(p)}G \otimes_{\mathbb{Z}G} M^* &\to (\mathbb{Z}_{(p)}G \otimes_{\mathbb{Z}G} M)^*, \\ g \otimes f &\mapsto \big(h \otimes m \mapsto f(\tau(g)hm)\big) \end{aligned}$$

where $g, h \in G$, $f \in M^*$ and $m \in M$. Next, let $p \in S$. Then there are isomorphisms of

R_p-modules

$$\begin{aligned}
\mathbb{Z}_{(p)} \otimes_{\mathbb{Z}_S} R \otimes_{\mathbb{Z}G} M^* &\cong R_p \otimes_{\mathbb{Z}G} M^* \\
&= (\mathbb{Z}_{(p)}G \otimes_{\mathbb{Z}G} M^*)_{R_p} \\
&\cong (\mathbb{Z}_{(p)}G \otimes_{\mathbb{Z}G} M)^*_{R_p} && \text{(above)} \\
&= (\mathbb{Z}_{(p)}G \otimes_{\mathbb{Z}G} M)^*_{R_p^{\mathrm{op}}} && \text{(Lemma 7.12)} \\
&\cong ((\mathbb{Z}_{(p)}G \otimes_{\mathbb{Z}G} M)_{R_p})^* && \text{(Lemma 3.8)} \\
&= (R_p \otimes_{\mathbb{Z}G} M)^* \\
&\cong (\mathbb{Z}_{(p)} \otimes_{\mathbb{Z}_{(S)}} R \otimes_{\mathbb{Z}G} M)^* \\
&\cong \mathbb{Z}_{(p)} \otimes_{\mathbb{Z}_{(S)}} (R \otimes_{\mathbb{Z}G} M)^*. && \text{(Proposition 2.1)}
\end{aligned}$$

We denote the overall isomorphism by

$$\gamma_p \colon \mathbb{Z}_{(p)} \otimes_{\mathbb{Z}_{(S)}} R \otimes_{\mathbb{Z}G} M^* \to \mathbb{Z}_{(p)} \otimes_{\mathbb{Z}_{(S)}} (R \otimes_{\mathbb{Z}G} M)^*.$$

It factors through the isomorphism

$$\begin{aligned}
\beta_p \colon \mathbb{Z}_{(p)} \otimes_{\mathbb{Z}_{(S)}} R \otimes_{\mathbb{Z}G} M^* &\to (\mathbb{Z}_{(p)} \otimes_{\mathbb{Z}_{(S)}} R \otimes_{\mathbb{Z}G} M)^*, \\
a \otimes r \otimes f &\mapsto \big(b \otimes s \otimes m \mapsto \alpha_p((ar,0)_p \otimes f)\,((bs,0)_p \otimes m)\big).
\end{aligned}$$

Explicitly, if we denote by

$$\varepsilon_p \colon \mathbb{Z}_{(p)} \otimes_{\mathbb{Z}_{(S)}} (R \otimes_{\mathbb{Z}G} M)^* \xrightarrow{\sim} (\mathbb{Z}_{(p)} \otimes_{\mathbb{Z}_{(S)}} R \otimes_{\mathbb{Z}G} M)^*$$

the isomorphism from Proposition 2.1, then $\gamma_p = (\varepsilon_p)^{-1} \circ \beta_p$.

Now for $p \in S$ choose $\widetilde{c_p} \in \mathbb{Z}$ with $\widetilde{c_p} \equiv 1 \mod p$, $\widetilde{c_p} \equiv 0 \mod q$ for all $q \in S \setminus \{p\}$ and $\widetilde{c_p}(1,0)_p \in \mathbb{Z}G$. Let $c_p := \widetilde{c_p}^2$. For $r \in R$ and $f \in M^*$ define

$$h_p(r,f) \colon R \otimes_{\mathbb{Z}G} M \to \mathbb{Z}_{(S)},\ s \otimes m \mapsto \alpha_p(\widetilde{c_p}(r,0)_p \otimes f)\,(\widetilde{c_p}(s,0)_p \otimes m).$$

It holds that

$$\varepsilon_p(1 \otimes h_p(r,f)) = c_p \beta_p(1 \otimes r \otimes f),$$

which shows that $c_p\gamma_p(1 \otimes r \otimes f) = 1 \otimes h_p(r,f)$ and therefore that $c_p\gamma_p$ maps $R \otimes_{\mathbb{Z}G} M^*$ into $(R \otimes_{\mathbb{Z}G} M)^*$ (we may regard them as submodules of $\mathbb{Z}_{(p)} \otimes_{\mathbb{Z}_{(S)}} R \otimes_{\mathbb{Z}G} M^*$ and $\mathbb{Z}_{(p)} \otimes_{\mathbb{Z}_{(S)}} (R \otimes_{\mathbb{Z}G} M)^*$, respectively, by Lemma 3.1). Then by [Rei03, Exercise 18.3], the map

$$\gamma := \sum_{p \in S} c_p^2 \gamma_p \colon R \otimes_{\mathbb{Z}G} M^* \to (R \otimes_{\mathbb{Z}G} M)^*$$

is an R-module isomorphism.

We compute $\gamma \circ d$ and $d \circ \gamma$. For the former, let $\varphi \in (R \otimes_{\mathbb{Z}G} M)^*$ and let $b \in \mathbb{Z} \setminus \bigcup_{p\in S} p\mathbb{Z}$ be such that $b \cdot \varphi(1 \otimes M) \subseteq \mathbb{Z}$. Let $r \in R$ and $m \in M$. Write $r = \overline{u \cdot w}$ with $u \in \mathbb{Z}_{(S)}$ and $w \in \mathbb{Z}G$. It follows as in the proof of Lemma 7.16 that

$$1 \otimes c_p m = 1 \otimes c_p(1,0)_p m \in R \otimes_{\mathbb{Z}G} M.$$

Using this, Lemma 7.6 (iii) and the fact that $(1,0)_p$ is a central idempotent, we obtain

$$\begin{aligned}(\gamma \circ d)(\varphi)\,(r \otimes m) &= \sum_{p \in S} c_p \alpha_p(\widetilde{c_p}(1/b,0)_p \otimes \varphi_b)\,(\widetilde{c_p}(r,0)_p \otimes m)\\ &= \sum_{p \in S} c_p \frac{1}{b} u \alpha_p(\widetilde{c_p}(1,0)_p \otimes \varphi_b)\,(\widetilde{c_p} w(1,0)_p \otimes m)\\ &= \sum_{p \in S} c_p \frac{1}{b} u \varphi_b(\tau(\widetilde{c_p}(1,0)_p)\widetilde{c_p} w(1,0)_p m)\\ &= \sum_{p \in S} c_p u \varphi(\overline{w} \otimes c_p(1,0)_p m)\\ &= \sum_{p \in S} c_p \varphi(r \otimes c_p m)\\ &= \left(\sum_{p \in S} c_p^2\right) \varphi(r \otimes m).\end{aligned}$$

Now let $f \in M^*$. Let $b \in \mathbb{Z} \setminus \bigcup_{p \in S} p\mathbb{Z}$ be such that $b \cdot \gamma(1 \otimes f)(1 \otimes M) \subseteq \mathbb{Z}$. For $m \in M$ we have by Lemma 7.6 (iii) and as $(1,0)_p$ is a central idempotent that

$$\begin{aligned}\gamma(1 \otimes f)_b(m) &= b \cdot \gamma(1 \otimes f)(1 \otimes m)\\ &= b \sum_{p \in S} c_p \alpha_p(\widetilde{c_p}(1,0)_p \otimes f)\,(\widetilde{c_p}(1,0)_p \otimes m)\\ &= b \sum_{p \in S} c_p f(\tau(\widetilde{c_p}(1,0)_p)\widetilde{c_p}(1,0)_p m)\\ &= b \sum_{p \in S} c_p f(c_p(1,0)_p m)\\ &= b \sum_{p \in S} c_p\,(c_p(1,0)_p)\,.f(m).\end{aligned}$$

One again shows as in the proof of Lemma 7.16 that

$$1 \otimes c_p f = 1 \otimes c_p(1,0)_p f \in R \otimes_{\mathbb{Z}G} M^*.$$

It follows from this and the above that

$$(d \circ \gamma)(1 \otimes f) = \frac{1}{b} \otimes \gamma(1 \otimes f)_b = \sum_{p \in S} c_p(1 \otimes c_p f) = \left(\sum_{p \in S} c_p^2\right)(1 \otimes f).$$

By R-linearity of d we then have $d \circ \gamma = \left(\sum_{p \in S} c_p^2\right)$ id, as well as the previously shown $\gamma \circ d = \left(\sum_{p \in S} c_p^2\right)$ id. Since $\sum_{p \in S} c_p^2 \in \mathbb{Z}_{(S)}^\times$ by choice of the c_p, we infer that d is an isomorphism. It is straightforward to verify naturality of d. □

7.3 Information Carried by the Good Part of a Short Exact Sequence

In Section 6.4 we discussed two constructions on certain short exact sequences of compact modules and showed that when applied to the Arakelov ray class sequence, they allow to recover the diagram from Theorem 6.18 and the natural reduction map on the unit group, respectively. Since our main conjecture will be concerned with $R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee$, the question arises whether one can obtain analogue statements for the latter sequence. In what follows, we show that the constructions mentioned above are indeed compatible with duality and the functor $R \otimes_{\mathbb{Z}G} -$, in the sense that from the good part $R \otimes_{\mathbb{Z}G} \Gamma^\vee$ of a short exact sequence of compact modules Γ one can obtain the good part of the output of the corresponding construction applied to Γ. To this end, we first establish the 'duals' of the constructions from Section 6.4 and then show that these behave well with respect to extending scalars from $\mathbb{Z}G$ to R. The dual constructions have already appeared in [BP25, Section 3] for $\mathbb{Z}$- and $\mathbb{Z}C_2$-modules; below we discuss them in a more general setting. The results on compatibility with extension of scalars are new.

7.3.1 Recovering the Good Part of the Diagram

We first consider Construction 6.19. In view of Corollary 4.16, its analogue on the dual side of sequences of discrete modules is the following.

Construction 7.19. Let Z be an integral domain and let R be a Z-order in some finite-dimensional algebra over the fraction field of Z. Let

$$\Delta\colon \qquad 0 \longrightarrow N \xrightarrow{\alpha} L \xrightarrow{\beta} M \longrightarrow 0$$

be a short exact sequence of R-modules. Then there are natural short exact sequences of R-modules

$$\Delta_{\mathrm{tors}}\colon \qquad 0 \longrightarrow N_{\mathrm{tors}} \xrightarrow{\alpha|_{N_{\mathrm{tors}}}} L_{\mathrm{tors}} \longrightarrow \mathrm{cok}(\alpha|_{N_{\mathrm{tors}}}) \longrightarrow 0$$

and

$$\Delta_{\mathrm{torsfree}}\colon \qquad 0 \longrightarrow N/N_{\mathrm{tors}} \xrightarrow{\overline{\alpha}} L/L_{\mathrm{tors}} \longrightarrow \mathrm{cok}(\overline{\alpha}) \longrightarrow 0.$$

By the snake lemma applied to the two left hand columns below, there is a commutative diagram of R-modules

$$\begin{tikzcd}
 & & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
\Delta_{\mathrm{tors}}\colon & 0 \arrow[r] & N_{\mathrm{tors}} \arrow[r, "\alpha|_{N_{\mathrm{tors}}}"] \arrow[d] & L_{\mathrm{tors}} \arrow[r] \arrow[d] & \operatorname{cok}(\alpha|_{N_{\mathrm{tors}}}) \arrow[r] \arrow[d, "\beta'"] & 0 \\
\Delta\colon & 0 \arrow[r] & N \arrow[r, "\alpha"] \arrow[d] & L \arrow[r, "\beta"] \arrow[d] & M \arrow[r] \arrow[d, "\widetilde{\beta}"] & 0 \\
\Delta_{\mathrm{torsfree}}\colon & 0 \arrow[r] & N/N_{\mathrm{tors}} \arrow[r, "\overline{\alpha}"] \arrow[d] & L/L_{\mathrm{tors}} \arrow[r] \arrow[d] & \operatorname{cok}(\overline{\alpha}) \arrow[r] \arrow[d] & 0 \\
 & & 0 & 0 & 0 &
\end{tikzcd}$$

with exact rows and columns, where

$$\beta'\colon\ \operatorname{cok}(\alpha\big|_{N_{\mathrm{tors}}}) = L_{\mathrm{tors}}/\alpha(N_{\mathrm{tors}}) \to M,\ \bar{l} \mapsto \beta(l)$$

and where $\widetilde{\beta}\colon M \to \operatorname{cok}(\overline{\alpha})$ is defined as follows: Given $m \in M$, choose a preimage $l_m \in L$ of m under β. Then $\widetilde{\beta}(m)$ is the class of $\overline{l_m} \in L/L_{\mathrm{tors}}$ in $\operatorname{cok}(\overline{\alpha})$. This means that there is a short exact sequence

$$\mathrm{D_d}(\Delta)\colon \qquad 0 \longrightarrow \Delta_{\mathrm{tors}} \longrightarrow \Delta \longrightarrow \Delta_{\mathrm{torsfree}} \longrightarrow 0$$

of short exact sequences of R-modules.

Proposition 7.20. *Let Z be a localisation of $\mathbb{Z}$ and suppose that R is a Z-order in some finite-dimensional $\mathbb{Q}$-algebra.*

(i) Let Γ be a short exact sequence of compact LCA R-modules. Then there is a canonical isomorphism $\mathrm{D_c}(\Gamma)^\vee \cong \mathrm{D_d}(\Gamma^\vee)$ of short exact sequences of short exact sequences of R^{op}-modules.

(ii) Let Δ be a short exact sequence of discrete R-modules. Then there is a canonical isomorphism $\mathrm{D_d}(\Delta)^\vee \cong \mathrm{D_c}(\Delta^\vee)$ of short exact sequences of short strictly exact sequences of compact LCA R^{op}-modules.

Note that by Propositions 4.21, 4.23 and 4.10, $\Gamma^\vee$ is a short exact sequence of discrete R^{op}-modules and $\Delta^\vee$ is a short exact sequence of compact LCA R^{op}-modules, so the statements make sense.

Proof. This follows easily from Corollary 4.16. □

The construction $\mathrm{D_d}(-)$ is compatible with flat base change that respects torsion. In particular, we obtain:

Proposition 7.21. *Use Setup 7.3. Let Δ be a short exact sequence of $\mathbb{Z}G$-modules. Then there is a canonical isomorphism $\mathrm{D_d}(R \otimes_{\mathbb{Z}G} \Delta) \cong R \otimes_{\mathbb{Z}G} \mathrm{D_d}(\Delta)$ of short exact sequences of short exact sequences of R-modules.*

Proof. This follows immediately from Lemma 7.15 (i). □

7.3.2 Recovering the Good Part of the Reduction Map

We finally establish the dual of Construction 6.21. We generalise the construction from [BP25, page 14] by making use of Propositions 4.41 and 4.42.

Construction 7.22. Let S be a nonempty subset of the union of $\{0\}$ and the set of rational primes. Let R be a $\mathbb{Z}_{(S)}$-order in some finite-dimensional $\mathbb{Q}$-algebra. Let M be a finite R-module and let N be a finitely generated R-module. Then we have maps

$$\begin{aligned} \mathrm{Ext}^1_R(M,N) &\to \mathrm{Ext}^1_R(M, N/N_{\mathrm{tors}}) && \text{(By functoriality)} \\ &\xrightarrow{\sim} \mathrm{Hom}_R(M, N/N_{\mathrm{tors}} \otimes_{\mathbb{Z}_{(S)}} \mathbb{A}_{(S)}/\mathbb{Z}_{(S)}) && \text{(Proposition 4.41)} \\ &\xrightarrow{\sim} \mathrm{Hom}_R(M, ((N/N_{\mathrm{tors}})^*)^\vee). && \text{(Proposition 4.42)} \end{aligned}$$

We denote the resulting map by

$$\omega_{\mathrm{d}} := \omega_{\mathrm{d},R} := \omega_{\mathrm{d},R}^{M,N} \colon \mathrm{Ext}^1_R(M,N) \to \mathrm{Hom}_R(M, ((N/N_{\mathrm{tors}})^*)^\vee).$$

Explicitly, it is given as follows: Let

$$\begin{tikzcd} \Delta\colon & 0 \arrow[r] & N \arrow[r, "\alpha"] & L \arrow[r, "\beta"] & M \arrow[r] & 0 \end{tikzcd}$$

be a short exact sequence of R-modules. Choose a map $s\colon M \to L$ with $s(0) = 0$ and $\beta s = \mathrm{id}_M$. If $l \in L$, then $|M|l \in \ker\beta = \operatorname{im}\alpha$, so there is a unique $n_l \in N$ with $\alpha(n_l) = |M|l$. For $m \in M$ we then have

$$\omega_{\mathrm{d}}(\Delta)(m)\colon (N/N_{\mathrm{tors}})^* \to \mathbb{R}/\mathbb{Z},\ f \mapsto \chi_{1/|M|}(f(\overline{n_{s(m)}})).$$

Note that we may replace $|M|$ by any positive integer that annihilates M.

Proposition 7.23. *Let S be a nonempty subset of the union of $\{0\}$ and the set of rational primes. Let R be a $\mathbb{Z}_{(S)}$-order in some finite-dimensional $\mathbb{Q}$-algebra A. Let M be a finite R-module and let N be a finitely generated R-module. Then*

$$\omega_{\mathrm{d}}\colon \mathrm{Ext}^1_R(M,N) \to \mathrm{Hom}_R(M, ((N/N_{\mathrm{tors}})^*)^\vee)$$

is a group homomorphism which is natural in M and N and whose kernel is the image of the natural injection $\mathrm{Ext}^1_R(M, N_{\mathrm{tors}}) \hookrightarrow \mathrm{Ext}^1_R(M,N)$.

If A is a separable $\mathbb{Q}$-algebra and R is a maximal $\mathbb{Z}_{(S)}$-order in A, then ω_{d} is surjective.

Proof. Naturality follows from functoriality of Ext and Propositions 4.41 and 4.42. The natural map $\operatorname{Ext}^1_R(M, N_{\mathrm{tors}}) \to \operatorname{Ext}^1_R(M, N)$ is injective as M is finite and N/N_{tors} is torsionfree, so that $\operatorname{Hom}_R(M, N/N_{\mathrm{tors}}) = 0$. It is clear that its image is the kernel of ω_{d}. The claim on surjectivity follows from Proposition 3.34. □

Dually to Proposition 6.22 we have:

Proposition 7.24. *Let S be a nonempty subset of the union of $\{0\}$ and the set of rational primes. Let R be a $\mathbb{Z}_{(S)}$-order in some finite-dimensional $\mathbb{Q}$-algebra. Let M be a finite R-module and let N be a finitely generated R-module. Let*

$$\Delta\colon \qquad 0 \longrightarrow N \xrightarrow{\alpha} L \xrightarrow{\beta} M \longrightarrow 0$$

be a short exact sequence of R-modules. Then there is an injective R-module homomorphism $\iota\colon \operatorname{cok}\overline{\alpha} \hookrightarrow ((N/N_{\mathrm{tors}})^*)^\vee$ such that $\omega_{\mathrm{d}}(\Delta) = \iota \circ \widetilde{\beta}$, where $\overline{\alpha}$ and $\widetilde{\beta}$ are defined as in Construction 7.19.

Proof. We use the notation from Construction 7.22. We first define

$$\iota'\colon \operatorname{cok}\overline{\alpha} \to N/N_{\mathrm{tors}} \otimes_{\mathbb{Z}_{(S)}} \mathbb{A}_{(S)}/\mathbb{Z}_{(S)},\ \bar{l} + \overline{\alpha}(N/N_{\mathrm{tors}}) \mapsto \overline{n_l} \otimes \overline{\frac{1}{|M|}}.$$

One readily checks that this is well-defined and an R-module homomorphism. Now suppose that $l \in L$ is such that $\overline{n_l} \otimes \overline{\frac{1}{|M|}} = 0$. Then there is $n \in N$ with

$$\overline{n_l} \otimes \frac{1}{|M|} = \overline{n} \otimes 1 = |M|\,\overline{n} \otimes \frac{1}{|M|} \in N/N_{\mathrm{tors}} \otimes_{\mathbb{Z}_{(S)}} \mathbb{A}_{(S)}.$$

It follows that $\overline{n_l} - |M|\,\overline{n} = 0$, so there is $n_0 \in N_{\mathrm{tors}}$ with $n_l = |M|\,n + n_0$. This implies $|M|\,\bar{l} = \overline{\alpha}(\overline{n_l}) = \overline{\alpha}(|M|\,\overline{n})$. Working in $L/L_{\mathrm{tors}} \otimes_{\mathbb{Z}_{(S)}} \mathbb{A}_{(S)} \supseteq L/L_{\mathrm{tors}}$, it follows that $\bar{l} = \overline{\alpha}(\overline{n})$, which shows that ι' is injective. We then define

$$\iota\colon \operatorname{cok}\overline{\alpha} \hookrightarrow ((N/N_{\mathrm{tors}})^*)^\vee,\ \bar{l} + \overline{\alpha}(N/N_{\mathrm{tors}}) \mapsto \big(f \mapsto \chi_{1/|M|}(f(\overline{n_l}))\big)$$

to be the concatenation of ι' with the isomorphism from Proposition 4.42. For $m \in M$ we have by definition of $\widetilde{\beta}$ that $\widetilde{\beta}(m) = \overline{s(m)} + \overline{\alpha}(N/N_{\mathrm{tors}})$. It follows that $(\iota \circ \widetilde{\beta})(m) = \omega_{\mathrm{d}}(\Delta)(m)$. □

Proposition 7.25. *Let G be a finite group.*

(i) Let X be a compact real abelian Lie group with an action of G by continuous group automorphisms and let Y be a finite $\mathbb{Z}G$-module. Then there is a commutative diagram

$$\begin{tikzcd}
E_{\mathbb{Z}G}\mathsf{LCA}(X, Y) \arrow[rr, "\omega_{\mathrm{c}}"] \arrow[d, "\vee"', "4.25"] & & \operatorname{Hom}_{\mathbb{Z}G}((X^\vee/(X^\vee)_{\mathrm{tors}})^*, Y) \arrow[d, "4.9"', "\vee"] \\
\operatorname{Ext}^1_{(\mathbb{Z}G)^{\mathrm{op}}}(Y^\vee, X^\vee) \arrow[rr, "\omega_{\mathrm{d}}"'] & & \operatorname{Hom}_{(\mathbb{Z}G)^{\mathrm{op}}}(Y^\vee, ((X^\vee/(X^\vee)_{\mathrm{tors}})^*)^\vee).
\end{tikzcd}$$

In particular, ω_{c} is a group homomorphism.

(ii) Let M be a finite $\mathbb{Z}G$-module and let N be a finitely generated $\mathbb{Z}G$-module. Then there is a commutative diagram

$$\begin{tikzcd}
\operatorname{Ext}^1_{\mathbb{Z}G}(M,N) \arrow[r, "\omega_{\mathrm{d}}"] \arrow[d, equal, "4.26"] & \operatorname{Hom}_{\mathbb{Z}G}(M,((N/N_{\mathrm{tors}})^*)^\vee) \arrow[d, "\vee", "4.9"'] \\
E_{\mathbb{Z}G\mathsf{LCA}}(M,N) \arrow[dd, "\vee"', "4.25"] & \operatorname{Hom}_{(\mathbb{Z}G)^{\mathrm{op}}}((((N/N_{\mathrm{tors}})^*)^{\vee\vee},M^\vee) \arrow[d, "\wr"] \\
 & \operatorname{Hom}_{(\mathbb{Z}G)^{\mathrm{op}}}((N/N_{\mathrm{tors}})^*,M^\vee) \arrow[d, "\wr"] \\
E_{(\mathbb{Z}G)^{\mathrm{op}}\mathsf{LCA}}(N^\vee,M^\vee) \arrow[r, "\omega_{\mathrm{c}}"'] & \operatorname{Hom}_{(\mathbb{Z}G)^{\mathrm{op}}}((N^{\vee\vee}/(N^{\vee\vee})_{\mathrm{tors}})^*,M^\vee)
\end{tikzcd}$$

where the unlabelled isomorphisms on the right hand side are induced by the Pontryagin duality isomorphism.

Proof. This is a lengthy but straightforward calculation. □

Finally, we show that for an input Γ of Construction 6.21 and R as in Setup 7.3 we have $\omega_{\mathrm{d}}(R\otimes_{\mathbb{Z}G}\Gamma^\vee)=(R\otimes_{\mathbb{Z}G}\omega_{\mathrm{c}}(\Gamma))^\vee$ up to natural isomorphism.

Proposition 7.26. *Use Setup 7.3. Let X be a compact real abelian Lie group with an action of G by continuous group automorphisms and let Y be a finite $\mathbb{Z}G$-module. Then there is a commutative diagram*

$$\begin{tikzcd}
E_{\mathbb{Z}G\mathsf{LCA}}(X,Y) \arrow[r, "\omega_{\mathrm{c}}"] \arrow[dd, "\vee"', "4.25"] & \operatorname{Hom}_{\mathbb{Z}G}((X^\vee/(X^\vee)_{\mathrm{tors}})^*,Y) \arrow[d, "R\otimes_{\mathbb{Z}G}-"] \\
 & \operatorname{Hom}_R(R\otimes_{\mathbb{Z}G}(X^\vee/(X^\vee)_{\mathrm{tors}})^*,R\otimes_{\mathbb{Z}G}Y) \arrow[d, "7.18"', "(d_{X^\vee/(X^\vee)_{\mathrm{tors}}})^*"] \\
\operatorname{Ext}^1_{\mathbb{Z}G}(Y^\vee,X^\vee) \arrow[dd, "R\otimes_{\mathbb{Z}G}-"', "2.8"] & \operatorname{Hom}_R((R\otimes_{\mathbb{Z}G}X^\vee/(X^\vee)_{\mathrm{tors}})^*,R\otimes_{\mathbb{Z}G}Y) \arrow[d, "4.9"', "\vee"] \\
 & \operatorname{Hom}_R((R\otimes_{\mathbb{Z}G}Y)^\vee,((R\otimes_{\mathbb{Z}G}X^\vee/(X^\vee)_{\mathrm{tors}})^*)^\vee) \\
\operatorname{Ext}^1_R(R\otimes_{\mathbb{Z}G}Y^\vee,R\otimes_{\mathbb{Z}G}X^\vee) \arrow[r, "\omega_{\mathrm{d}}"'] & \operatorname{Hom}_R(R\otimes_{\mathbb{Z}G}Y^\vee,((R\otimes_{\mathbb{Z}G}X^\vee/(X^\vee)_{\mathrm{tors}})^*)^\vee). \arrow[u, "7.17", "(\delta_Y)^*"']
\end{tikzcd}$$

Proof. Let $\Gamma \in E_{\mathbb{Z}G\mathsf{LCA}}(X, Y)$ and suppose that it is given by the short strictly exact sequence

$$0 \longrightarrow Y \xrightarrow{\gamma} W \xrightarrow{\delta} X \longrightarrow 0$$

of compact LCA $\mathbb{Z}G$-modules. We check that when plugging in Γ and going right and down to $\mathrm{Hom}_R((R \otimes_{\mathbb{Z}G} Y)^\vee, ((R \otimes_{\mathbb{Z}G} X^\vee/(X^\vee)_{\mathrm{tors}})^*)^\vee)$ we get the same element as when going down, right and up. To this end, further let $\varphi \in (R \otimes_{\mathbb{Z}G} Y)^\vee$ and let $\psi \in (R \otimes_{\mathbb{Z}G} X^\vee/(X^\vee)_{\mathrm{tors}})^*$.

Plugging in Γ, going right and down and plugging in φ and then ψ, we obtain the element

$$\begin{aligned}
\big((d_{X^\vee/(X^\vee)_{\mathrm{tors}}})^*(\mathrm{id}_R \otimes \omega_{\mathrm{c}}(\Gamma))\big)^\vee (\varphi)\ (\psi) \\
&= \varphi\big((\mathrm{id}_R \otimes \omega_{\mathrm{c}}(\Gamma))\ (d_{X^\vee/(X^\vee)_{\mathrm{tors}}}\psi)\big) \\
&= \varphi\Big(\frac{1}{b} \otimes \omega_{\mathrm{c}}(\Gamma)(\psi_b)\Big)
\end{aligned}$$

where $b \in \mathbb{Z} \setminus \bigcup_{p\in S} p\mathbb{Z}$ is such that $b \cdot \psi(1 \otimes X^\vee/(X^\vee)_{\mathrm{tors}}) \subseteq \mathbb{Z}$. By Lemma 3.3 we have a decomposition $Y = \bigoplus_{p\in S} Y[p^\infty] \oplus \bigoplus_{p\notin S} Y[p^\infty]$ into $\mathbb{Z}G$-submodules, and since R is a $\mathbb{Z}_{(S)}$-algebra it holds that

$$R \otimes_{\mathbb{Z}G} Y = \bigoplus_{p\in S} R \otimes_{\mathbb{Z}G} Y[p^\infty].$$

For $p \mid |Y|$ let $c_p \in \mathbb{Z}$ with $c_p \equiv 0 \mod q^{v_q(|Y|)}$ for $q \mid |Y|$ with $q \neq p$ and such that $1 = \sum_{p||Y|} c_p$. For a prime p with $p \nmid |Y|$ we further put $c_p := 0$. Moreover, for $p \in S$ let $k_p \in \mathbb{Z}$ with $k_p \equiv \frac{1}{b} \mod p^{v_p(|Y|)}\mathbb{Z}_{(p)}$. Then

$$\frac{1}{b} \otimes \omega_{\mathrm{c}}(\Gamma)(\psi_b) = \sum_{p\in S} \frac{1}{b} \otimes c_p\omega_{\mathrm{c}}(\Gamma)(\psi_b) = \sum_{p\in S} 1 \otimes k_p c_p \omega_{\mathrm{c}}(\Gamma)(\psi_b).$$

We have $\widetilde{\varphi} \in Y^\vee$, so there is $g \in W^\vee$ with $\gamma^\vee(g) = \widetilde{\varphi}$. Further let $h \in X^\vee$ with $\delta^\vee(h) = |Y|\, g$. Then by the above and Construction 6.21 we have

$$\begin{aligned}
\varphi\Big(\frac{1}{b} \otimes \omega_{\mathrm{c}}(\Gamma)(\psi_b)\Big) &= \sum_{p\in S} \varphi\big(1 \otimes k_p c_p \omega_{\mathrm{c}}(\Gamma)(\psi_b)\big) \\
&= \sum_{p\in S} k_p c_p \widetilde{\varphi}\big(\omega_{\mathrm{c}}(\Gamma)(\psi_b)\big) \\
&= \sum_{p\in S} k_p c_p g\big(\gamma(\omega_{\mathrm{c}}(\Gamma)(\psi_b))\big) \\
&= \sum_{p\in S} \overline{k_p c_p b \psi(1 \otimes \overline{h}) \frac{1}{|Y|}} \quad \in \mathbb{R}/\mathbb{Z}.
\end{aligned}$$

Plugging in Γ in the top left of the diagram, going down, right and up, and plugging in φ and then ψ, we obtain the element

$$(\delta_Y)^*\big(\omega_{\mathrm{d}}(R \otimes_{\mathbb{Z}G} \Gamma^\vee)\big)(\varphi)\ (\psi) = \omega_{\mathrm{d}}(R \otimes_{\mathbb{Z}G} \Gamma^\vee)(1 \otimes \widetilde{\varphi})\ (\psi).$$

Let $s\colon R \otimes_{\mathbb{Z}G} Y^{\vee} \to R \otimes_{\mathbb{Z}G} W^{\vee}$ be a map with $s(0) = 0$ and $(\mathrm{id}_R \otimes \gamma^{\vee})s = \mathrm{id}_{R \otimes_{\mathbb{Z}G} Y^{\vee}}$. We may assume that $s(1 \otimes \widetilde{\varphi}) = 1 \otimes g$. Then

$$|Y|\, s(1 \otimes \widetilde{\varphi}) = 1 \otimes |Y|\, g = (\mathrm{id}_R \otimes \delta^{\vee})(1 \otimes h),$$

so by Construction 7.22 and Lemma 4.28 (iv) we have

$$\omega_{\mathrm{d}}(R \otimes_{\mathbb{Z}G} \Gamma^{\vee})(1 \otimes \widetilde{\varphi})\ (\psi) = \chi_{1/|Y|}\big(\psi(1 \otimes \overline{h})\big) = \sum_{p \in S} \overline{\Big\{\psi(1 \otimes \overline{h})\frac{1}{|Y|}\Big\}_p}.$$

Since $b\psi(1 \otimes \overline{h}) \in \mathbb{Z}$, Lemma 4.28 (iii) gives

$$\overline{\Big\{\psi(1 \otimes \overline{h})\frac{1}{|Y|}\Big\}_p} = \overline{b\psi(1 \otimes \overline{h})\Big\{\frac{1}{b\,|Y|}\Big\}_p}.$$

We now analyse $\overline{\big\{\frac{1}{b|Y|}\big\}_p}$ for $p \in S$. We have

$$\frac{1}{b\,|Y|} = c_p \frac{1}{b\,|Y|} + \sum_{q \neq p} c_q \frac{1}{b\,|Y|}.$$

Here, by choice of b and the c_q, the right hand summand is contained in $\mathbb{Z}_p$, so Lemma 4.28 gives $\overline{\big\{\frac{1}{b|Y|}\big\}_p} = \overline{\big\{c_p\frac{1}{b|Y|}\big\}_p}$. Now let $w \in \mathbb{Z}_{(p)}$ with $\frac{1}{b} = k_p + p^{v_p(|Y|)}w$. Then

$$c_p \frac{1}{b\,|Y|} = c_p k_p \frac{1}{|Y|} + c_p p^{v_p(|Y|)} w \frac{1}{|Y|},$$

where $c_p p^{v_p(|Y|)} w \frac{1}{|Y|} \in \mathbb{Z}_{(p)}$ and $\overline{\big\{c_p k_p \frac{1}{|Y|}\big\}_p} = \overline{k_p\big\{c_p\frac{1}{|Y|}\big\}_p} = \overline{k_p c_p \frac{1}{|Y|}}$, both by choice of c_p. It follows that $\overline{\big\{\frac{1}{b|Y|}\big\}_p} = \overline{k_p c_p \frac{1}{|Y|}}$ and therefore that

$$(\delta_Y)^*\big(\omega_{\mathrm{d}}(R \otimes_{\mathbb{Z}G} \Gamma^{\vee})\big)(\varphi)\ (\psi) = \sum_{p \in S} \overline{b\psi(1 \otimes \overline{h}) k_p c_p \frac{1}{|Y|}}.$$

Hence, both paths in the diagram yield the same element. □

8 The Main Conjecture

In this chapter, we formulate our main conjecture on the distribution of ray class groups. More explicitly, we make a conjecture regarding the distribution of the good part of $\mathrm{Cl}_K(\mathfrak{m})$ for K running over a natural family of Galois extensions of a fixed base number field F and fixed modulus $\mathfrak{m}$ given by an integral ideal of $\mathcal{O}_F$. It has already been stated as Conjecture 1.13 in the introduction; here, we provide a detailed account that adds some more motivation and explanations and fills in all the details and proofs previously left out.

As explained in the introduction, when investigating the distribution of an object attached to a number field, there are several things to take care of in order to obtain meaningful statements:

- which family of number fields to run over,
- how to order the number fields in the family,
- which objects exactly to consider,
- what space of outcomes for the objects to consider.

Note that some or all of these aspects may be interdependent. Providing this setup for our conjecture is the content of Section 8.1. Recall that to make a reasonable conjecture about the distribution of the good part of $\mathrm{Cl}_K(\mathfrak{m})$, we take the approach outlined in Section 1.1.1 to package all its structure into one object and then propose that this object is distributed randomly in the sense of Principle 1.1. As part of the setup, we argue that the desired object is obtained by picking out good components – in the way outlined in Chapter 7 – from the Arakelov ray class sequence $\mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})$. We set up our family of number fields and space of outcomes in a natural way that then also allows us to construct a probability distribution on the space of outcomes that weighs an object proportional to the inverse of the size of its automorphism group. The latter will be achieved using the tools from Chapter 5 and is dealt with in Section 8.2. Finally, in Section 8.3, we state our main conjecture.

8.1 Setup for the Conjecture

We establish all the setup necessary in order to turn the ideas outlined above into a precise conjecture.

8.1.1 G-Extensions

Let G be a finite group and let F be a field. The following definition allows to make precise the notion of a family of Galois extensions of F with Galois group G. It is taken from [Woo10].

Definition 8.1. A *G-extension* of F is a Galois extension K/F together with an isomorphism $\iota\colon G \to \mathrm{Gal}(K/F)$. We regard K as a G-module via $g.x := \iota(g)(x)$ for $g \in G$, $x \in K$. An *isomorphism* of G-extensions is an F-algebra isomorphism that is G-equivariant. Denote by $E_G(F)$ a full set of representatives for the isomorphism classes of G-extensions of F.

We will sometimes suppress ι from the notation. In our family, we will later work with G-extensions inside some fixed algebraic closure. To be able to use results on G-extensions considered as elements of $E_G(F)$, we next prove a statement that links the two approaches. Fix an algebraic closure $\overline{F}$ of F.

Lemma 8.2. *Let (L, ι_L) be a G-extension of F. Then the set*

$$\left\{\, (K, \iota_K) \text{ G-extension of } F \,\middle|\, K \subseteq \overline{F}, (K, \iota_K) \cong (L, \iota_L) \,\right\}$$

has cardinality $\left|\mathrm{Hom}_F(L, \overline{F})/\sim\right|$ where

$$\psi \sim \psi' \quad :\Longleftrightarrow \quad \psi^{-1} \circ \psi' \in \mathfrak{Z}(\mathrm{Gal}(L/F)).$$

In particular, if G is abelian, then the cardinality is 1.

Note that $\psi(L) = \psi'(L)$ since L/F is normal, so $\psi^{-1} \circ \psi' \in \mathrm{Gal}(L/F)$.

Proof. Denote by E the set whose cardinality we have to determine. If $\psi \in \mathrm{Hom}_F(L, \overline{F})$, then $F \subseteq \psi(L) \subseteq \overline{F}$ and $\psi(L)/F$ is Galois. Define

$$\iota_{\psi(L)}\colon G \to \mathrm{Gal}(\psi(L)/F),\ g \mapsto \psi \circ \iota_L(g) \circ \psi^{-1}$$

which is clearly an isomorphism. Hence, $(\psi(L), \iota_{\psi(L)})$ is a G-extension. Moreover, $\psi\colon L \to \psi(L)$ is an F-isomorphism which is easily seen to be compatible with the G-actions. So $(\psi(L), \iota_{\psi(L)}) \cong (L, \iota_L)$ and we can define

$$\mathrm{Hom}_F(L, \overline{F}) \to E,\ \psi \mapsto (\psi(L), \iota_{\psi(L)}).$$

If $(K, \iota_K) \in E$, then there is a G-equivariant F-algebra isomorphism $\chi\colon L \xrightarrow{\sim} K$ and it follows that $\chi \in \mathrm{Hom}_F(L, \overline{F})$ and $(\chi(L), \iota_{\chi(L)}) = (K, \iota_K)$. Hence, the map above is surjective. It remains to show that for $\psi, \psi' \in \mathrm{Hom}_F(L, \overline{F})$ we have $\psi \sim \psi'$ if and only if $(\psi(L), \iota_{\psi(L)}) = (\psi'(L), \iota_{\psi'(L)})$, that is, if and only if $\iota_{\psi(L)} = \iota_{\psi'(L)}$. But for $g \in G$ it holds by definition that $\iota_{\psi(L)}(g) = \iota_{\psi'(L)}(g)$ if and only if $(\psi^{-1} \circ \psi') \circ \iota_L(g) = \iota_L(g) \circ (\psi^{-1} \circ \psi')$. The claim follows. □

Proposition 8.3. *Assume that G is abelian. Let P be a property of G-extensions of F such that if (K, ι_K) and (L, ι_L) are isomorphic G-extensions of F, then (K, ι_K) has property P if and only if (L, ι_L) does. Suppose that there are only finitely many $(L, \iota_L) \in E_G(F)$ with property P. Then*

$$\begin{aligned} &\left|\left\{\, (K, \iota_K) \text{ G-extension of } F \,\middle|\, K \subseteq \overline{F}, (K, \iota_K) \text{ has property P} \,\right\}\right| \\ &\qquad = \left|\left\{\, (L, \iota_L) \in E_G(F) \,\middle|\, (L, \iota_L) \text{ has property P} \,\right\}\right|. \end{aligned}$$

Proof. Note that we can write the first cardinality above as

$$\sum_{\substack{(L,\iota_L)\in E_G(F)\\ (L,\iota_L)\text{ has property P}}} \left|\left\{\, (K,\iota_K)\ G\text{-extension of } F \,\middle|\, K\subseteq \overline{F}, (K,\iota_K)\cong(L,\iota_L)\,\right\}\right|.$$

The claim then follows from Lemma 8.2. □

8.1.2 G-Structured Algebras

In this section, let again G be a finite group and let F be a field. To define the family of number fields for our conjecture, we will need to be able to fix the local behaviour of the fields at certain primes. For this, we will make use of the following algebraic structure, which was introduced in [Woo10, page 105] for abelian G.

Definition 8.4. A *G-structured F-algebra* is an etale F-algebra K of degree $|G|$ with an inclusion $G \hookrightarrow \operatorname{Aut}_F(K)$ such that G acts transitively on the set of primitive central idempotents of K. An *isomorphism* of two G-structured F-algebras K and K' is an F-algebra isomorphism $K \to K'$ that is G-equivariant. Denote by $A_G(F)$ a full set of representatives for the isomorphism classes of G-structured F-algebras.

Note that the notion of isomorphism above agrees with the one given in [Woo10]. Clearly, a G-extension is a G-structured algebra. In the remainder of this subsection, we collect some useful results on G-structured algebras, all of which appear at least implicit in [Woo10, Sections 1.1 and 2.3].

Construction 8.5. Let $H \le G$ and let L be an H-extension of F. We equip the induced representation

$$\operatorname{Ind}_H^G L = FG \otimes_{FH} L = \bigoplus_{y\in G/H} y\otimes L$$

with an algebra structure via the natural isomorphism

$$\bigoplus_{y\in G/H} y\otimes L \cong \prod_{y\in G/H} L$$

of F-vector spaces. Clearly, $\dim_F \operatorname{Ind}_H^G L = |G|$. Let $y_1,\dots,y_r \in G$ be a system of representatives for the left cosets of H in G. The primitive central idempotents of $\operatorname{Ind}_H^G L$ are $e_i = y_i \otimes 1$, $i = 1,\dots,r$. Each $g \in G$ defines a permutation of $\{1,\dots,r\}$ denoted by the same letter which is defined by the fact that for each $i \in \{1,\dots,r\}$ there are unique $g(i) \in \{1,\dots,r\}$ and $h_i \in H$ with $gy_i = y_{g(i)}h_i$. Then for $x \in L$ we have $g(y_i \otimes x) = y_{g(i)} \otimes h_i x$ and in particular $ge_i = e_{g(i)}$.

The G-action on $\operatorname{Ind}_H^G L$ induces a natural map $G \to \operatorname{Aut}_F(\operatorname{Ind}_H^G L)$ into the F-vector space automorphisms. One checks that the map is injective and that its image is in fact contained in the F-algebra automorphisms. As G acts transitively on G/H, it acts transitively on the primitive idempotents of Ind_H^G. Hence, Ind_H^G is a G-structured F-algebra.

For a subgroup H of G, $h \in H$ and $a \in G$ use the notations ${}^a h := aha^{-1}$ and ${}^a H := aHa^{-1}$. We have the following analogue of [CR81, Lemma 10.12 (ii)].

Lemma 8.6. *Let $H \leq G$ and let L be an H-extension of F. Let $a \in G$. Let ${}^a L$ be the ${}^a H$-extension consisting of the field L regarded as a ${}^a H$-module via ${}^a h.x = h.x$ for $x \in {}^a L$ and $h \in H$. Then $\mathrm{Ind}_H^G L \cong \mathrm{Ind}_{{}^a H}^G {}^a L$ as G-structured F-algebras.*

Proof. One checks that the map

$$FG \otimes_{F\,{}^a H} {}^a L \to FG \otimes_{FH} L, \; g \otimes x \mapsto ga \otimes x$$

is an isomorphism of G-structured F-algebras. □

Construction 8.7. Let $K = K_1 \times \cdots \times K_r$ be a G-structured F-algebra, where each K_i is a finite separable extension of F. Since G operates transitively on the set of primitive central idempotents of K, the stabilisers

$$\mathrm{Stab}(e_i) = \{\, g \in G \,|\, g(e_i) = e_i \,\}$$

have index r in G and are all conjugate. Here, e_i denotes the tuple $(0, \ldots, 0, 1, 0, \ldots, 0)$ with 1 in position i. If G is abelian, then

$$H := \mathrm{Stab}(e_1) = \cdots = \mathrm{Stab}(e_r)$$

and it follows as in the proof of [Woo10, Lemma 2.6] that for each i, the natural map $H = \mathrm{Stab}(e_i) \to \mathrm{Aut}_F(K_i)$ is an isomorphism. Hence, each K_i is an H-extension of F, and one easily sees that all K_i are isomorphic as H-extensions.

We have the following variant of [Woo10, Lemma 2.6].

Proposition 8.8. *Assume that G is abelian. Then the maps*

$$\bigsqcup_{H \leq G} E_H(F) \longleftrightarrow A_G(F), \qquad \begin{array}{r} (H, L) \mapsto \mathrm{Ind}_H^G L, \\ (\mathrm{Stab}(e_1), K_1) \leftarrow\!\shortmid K. \end{array}$$

are inverse to each other.

For us, the following G-structured algebras arising from extensions of number fields will be important.

Proposition 8.9. *Let F be a number field and let K/F be a G-extension. Let v be a place of F. Then $K \otimes_F F_v$ is a G-structured F_v-algebra with G acting on the left factor. If w is a place of K with $w \mid v$, then $K \otimes_F F_v \cong \operatorname{Ind}_{D_w}^G K_w$ as G-structured F_v-algebras.*

Proof. For a place w of K denote by $\iota_w \colon (K, |\cdot|_w) \hookrightarrow K_w$ the continuous embedding of $(K, |\cdot|_w)$ into its completion. Suppose that $\sigma \in \operatorname{Gal}(K/F)$ and let $w, w' \mid v$ with $\sigma.w = w'$. By the universal property of completion, there is a unique continuous field homomorphism $\widehat{\sigma}^{(w,w')} \colon K_w \to K_{w'}$ that makes the diagram

$$\begin{tikzcd}
K_w \arrow[r, "\widehat{\sigma}^{(w,w')}"] & K_{w'} \\
K \arrow[u, hook, "\iota_w"] \arrow[r, "\sigma"'] & K \arrow[u, hook, "\iota_{w'}"']
\end{tikzcd}$$

commute. Since F is dense in F_v, $\widehat{\sigma}^{(w,w')}$ is an F_v-algebra homomorphism. Note that if $\tau \in \operatorname{Gal}(K/F)$ with $\tau.w' = w''$, then $(\widehat{\tau \circ \sigma})^{(w,w'')} = \widehat{\tau}^{(w',w'')} \circ \widehat{\sigma}^{(w,w')}$.

The F_v-algebra isomorphism

$$K \otimes_F F_v \xrightarrow{\sim} \prod_{w|v} K_w,\ x \otimes a \mapsto (\iota_w(x)a)_{w|v}$$

is G-equivariant with natural action of G on the right hand side given by $\sigma.(x_w)_{w|v} = (\widehat{\sigma}^{(\sigma^{-1}w,w)}(x_{\sigma^{-1}w}))_{w|v}$. The map $G \to \operatorname{Aut}_{F_v}(K \otimes_F F_v)$, $\sigma \mapsto \sigma \otimes \operatorname{id}_{F_v}$ is injective as $K \to K \otimes_F F_v$ is injective. Since G operates transitively on $\{w \mid v\}$, the above isomorphism shows that G operates transitively on the primitive central idempotents of $K \otimes_F F_v$. So $K \otimes_F F_v$ is a G-structured F_v-algebra.

For the second claim let $w \mid v$ and let $\tau_1, \dots, \tau_r$ be a system of representatives for G/D_w. Define

$$\varphi\colon \operatorname{Ind}_{D_w}^K K_w \cong \prod_{i=1}^r K_w \to \prod_{i=1}^r K_{\tau_i w} \cong K \otimes_F F_v,\ (x_i)_i \mapsto (\widehat{\tau}_i^{(w,\tau_i w)}(x_i))_i.$$

which is clearly an F_v-algebra isomorphism. One verifies that φ is G-equivariant. □

8.1.3 Fair Counting Functions

Let G be a finite abelian group and let F be a number field. We recall the following way of obtaining 'good' functions to order G-extensions of F.

Definition 8.10 ([Woo10, Section 2.1])**.** Let $c_G \colon G \to \mathbb{Z}_{\geq 0}$ be a function such that for any $g \in G$ we have $c_G(g) = 0$ if and only if $g = 1$, and $c_G(g) = c_G(g^e)$ for any $e \in \mathbb{Z}$ coprime to the order of g. For any place v of F with $v \mid |G|\infty$ let further $c_v \colon A_G(F_v) \to \mathbb{Z}_{\geq 0}$ be a function. Extend this to all places of F in the following way.

Let $v \nmid |G|\,\infty$. For $H \leq G$ and L/F_v an H-extension put $c_v(\operatorname{Ind}_H^G L) := c_G(y_v)$, where y_v is any generator of tame inertia in $\operatorname{Gal}(L/F_v) \hookrightarrow G$. Note that by Proposition 8.8, any G-structured F_v-algebra is isomorphic to a unique algebra of the form $\operatorname{Ind}_H^G L$ with H and L as above. Define

$$C\colon E_G(F) \to \mathbb{Z}_{\geq 0},\ K \mapsto \prod_{\mathfrak{p} \trianglelefteq \mathcal{O}_F} N_{F/\mathbb{Q}}(\mathfrak{p})^{c_{\mathfrak{p}}(K \otimes_F F_{\mathfrak{p}})}$$

and call it the *counting function* on $E_G(F)$ given by c_G and c_v. We write $G_r := \{\, g \in G \mid g^r = 1 \,\}$ for $r \in \mathbb{Z}_{\geq 0}$ and $m_C := \min_{g \in G \setminus \{1\}} c_G(g)$, and call C *fair* if $c_G^{-1}(m_C) \cap G_r$ generates G_r for all $r \in \mathbb{Z}_{\geq 0}$.

Note that if C is a counting function on $E_G(F)$, then for any $B \in \mathbb{R}_{>0}$ there are only finitely many $K \in E_G(F)$ with $C(K) < B$, since such a K must be unramified at all primes $\mathfrak{p} \trianglelefteq \mathcal{O}_F$ lying over a rational prime larger than $|G|\,B$. The three counting functions we are mainly interested in are the following.

Example 8.11.

(a) Let

$$c_G\colon G \to \mathbb{Z}_{\geq 0},\ g \mapsto \begin{cases} 0, & g = 1, \\ 1, & \text{else}, \end{cases}$$

and, for $v \mid |G|\,\infty$,

$$c_v(\operatorname{Ind}_H^G M) = \begin{cases} 1, & e(M/F_v) > 1, \\ 0, & \text{else}, \end{cases}$$

where $H \leq G$ and M/F_v is an H-extension. Then the resulting counting function C is given by

$$C(K) = N_{F/\mathbb{Q}}\Bigg(\prod_{\substack{\mathfrak{p} \trianglelefteq \mathcal{O}_F \\ \text{ramified in } K}} \mathfrak{p} \Bigg)$$

for $K \in E_G(F)$. Here, $m_C = 1$, so C is fair.

(b) Let

$$c_G\colon G \to \mathbb{Z}_{\geq 0},\ g \mapsto \begin{cases} 0, & g = 1, \\ 1, & \text{else}, \end{cases}$$

and, for $v \mid |G|\,\infty$, $c_v(\operatorname{Ind}_H^G M) = \mathfrak{f}(M/F_v)$ where $H \leq G$ and M/F_v is an H-extension. Here, $\mathfrak{f}$ denotes the conductor. Then the resulting counting function C is given by $C(K) = N_{F/\mathbb{Q}}(\mathfrak{f}(K/F))$ for $K \in E_G(F)$. Again, $m_C = 1$, so C is fair.

(c) Let

$$c_G\colon G \to \mathbb{Z}_{\geq 0},\ g \mapsto |G| \left(1 - \frac{1}{|g|}\right),$$

where $|g|$ denotes the order of g. Moreover, for $v \mid |G| \infty$, let

$$c_v(\operatorname{Ind}_H^G M) = \begin{cases} |G:H| \cdot v_{\widehat{\mathfrak{p}}}(\operatorname{disc}(M/F_v)), & v \mid |G|, \\ 0, & v \mid \infty, \end{cases}$$

where $H \leq G$, M/F_v is an H-extension and $\widehat{\mathfrak{p}}$ is the maximal ideal of F_v. Then the resulting counting function C is given by $C(K) = N_{F/\mathbb{Q}}(\operatorname{disc}(K/F))$ for $K \in E_G(F)$. The function C is not fair unless G has prime exponent [Woo10, page 108].

We collect two results on the densities of certain families of G-extensions when those are ordered by a fair counting function.

Proposition 8.12. *Let C be a fair counting function on $E_G(F)$. Let P be a finite set of places of F. For each $v \in P$ let T_v be a G-structured F_v-algebra and write $T = (T_v)_{v \in P}$. Then the limit*

$$\Pr_C(T) := \lim_{B \to \infty} \frac{|\{ K \in E_G(F) \mid K \otimes_F F_v \cong T_v \text{ for all } v \in P, C(K) \leq B \}|}{|\{ K \in E_G(F) \mid C(K) \leq B \}|}$$

exists.

Proof. See [Woo10, Theorem 2.1]. □

Note that by Proposition 8.3, we get the same limit as in the proposition above if we instead consider G-extensions contained in an algebraic closure of F in the respective sets occurring in the definition of $\Pr_C(T)$. The paper [Woo10] also proves an independence statement on the local probabilities $\Pr_C(T)$, and in fact provides a way to explicitly calculate $\Pr_C(T)$, which is what we will do later on in Section 10.1.1 for the case $G = C_q$, q prime.

An important property of fair counting functions for Cohen–Lenstra type conjectures (cf. [BL20, Sections 1 and 6]) is that when using them to order G-extensions, fixed nontrivial subfields occur with density zero:

Proposition 8.13. *Let C be a fair counting function on $E_G(F)$. Let P be a set of infinite places of F (possibly empty). For each $v \in P$ let T_v be a G-structured F_v-algebra. Fix an algebraic closure $\overline{F}$ of F and let L be a field with $F \subsetneq L \subseteq \overline{F}$. Denote by $\widetilde{\mathcal{K}}_{C \leq B}$ the set of G-extensions (K, ι) of F with $K \subseteq \overline{F}$, $C(K) \leq B$ and $K \otimes_F F_v \cong T_v$ as G-structured F_v-algebras for all $v \in P$. Then*

$$\lim_{B \to \infty} \frac{\left| \left\{ (K, \iota) \in \widetilde{\mathcal{K}}_{C \leq B} \,\middle|\, L \subseteq K \right\} \right|}{\left| \widetilde{\mathcal{K}}_{C \leq B} \right|} = 0.$$

Proof. This follows as in [BL20, Proposition 6.6]. □

8.1.4 Families of Galois Extensions

Based on [BL20] and [BJL24], we now formalise what we mean by a natural family of Galois extensions of a fixed base number field.

We will investigate the distribution of $\mathrm{Cl}_K(\mathfrak{m})$ in the following setup.

Setup 8.14. Let F be a number field and fix an algebraic closure $\overline{F}$ of F. Let $0 \neq \mathfrak{m}_F \trianglelefteq \mathcal{O}_F$. Let G be a finite group. Let W be a finitely generated $\mathbb{Q}G$-module. Let I be a two-sided ideal of $\mathbb{Q}G$ with $\sum_{g\in G} g \in I$ and let $A = \mathbb{Q}G/I$. Let S be a finite set of primes that are good for A. If G is abelian, let $C = C_F$ be a fair counting function defined on $E_G(F)$. If G is nonabelian, let $C = C_F$ be the function on $E_G(F)$ that assigns to K the ideal norm of the product of the prime ideals of $\mathcal{O}_F$ that ramify in K. Let

$$\begin{aligned}\mathcal{K} := \big\{(K,\iota) \mid (K,\iota) &\text{ is a } G\text{-extension of } F \text{ with } K \subseteq \overline{F},\\ &K \text{ contains no primitive } p\text{-th root of unity for any } p \in S,\\ &\mathbb{Q}\otimes_{\mathbb{Z}} \mathcal{O}_K^\times \cong W \text{ as } \mathbb{Q}G\text{-modules}\big\}\end{aligned}$$

and, for $B \in \mathbb{R}_{>0}$,

$$\mathcal{K}_{C\leq B} := \{\, (K,\iota) \in \mathcal{K} \,|\, C(K) \leq B \,\}\,.$$

Assume that $\mathcal{K}$ is infinite. For $(K,\iota) \in \mathcal{K}$ we use the notation $\mathfrak{m} := (\mathfrak{m}_F, \varnothing)$, a modulus in K, regarding $\mathfrak{m}_F$ as an ideal of $\mathcal{O}_K$.

The family $\mathcal{K}$ is the same as the family of number fields occurring in [BJL24] and differs from the family in [BL20] only in that their condition $A \otimes_{\mathbb{Z}G} \mathcal{O}_K^\times \cong V$ is replaced by the more general $\mathbb{Q}\otimes_{\mathbb{Z}} \mathcal{O}_K^\times \cong W$. In both these sources, fields are always ordered by the function we use in the nonabelian case. We have allowed more general orderings in the abelian case since [Woo10] indicates that these orderings are all well-behaved.

Note that for $(K,\iota) \in \mathcal{K}$, the modulus $\mathfrak{m}$ is G-stable, so that all objects appearing in Theorem 6.18 are compact LCA G-modules. We will later consider only the good part of $\mathrm{Cl}_K(\mathfrak{m})$. The good primes S are contained in the above setup already in order to remove the relevant roots of unity from the fields we consider. We do this in order to avoid complications arising from the roots of unity (cf. [Mal08], [SW23] and the introduction).

The condition $\mathbb{Q}\otimes_{\mathbb{Z}} \mathcal{O}_K^\times \cong W$ is to fix the behaviour of K at the infinite places. There are several different ways to phrase it, as given by the below proposition. For a finite G-set X denote by $\mathbb{Q}[X]$ the permutation module over $\mathbb{Q}$ associated to X. For a number field K denote by Ω_K^∞ its set of infinite places.

Proposition 8.15. *Let K and K' be G-extensions of F. Then the following are equivalent:*

(i) $\mathbb{Q}\otimes_{\mathbb{Z}} \mathcal{O}_K^\times \cong \mathbb{Q}\otimes_{\mathbb{Z}} \mathcal{O}_{K'}^\times$ *as $\mathbb{Q}G$-modules,*

(ii) $\mathbb{Q}[\Omega_K^\infty] \cong \mathbb{Q}[\Omega_{K'}^\infty]$ *as* $\mathbb{Q}G$*-modules,*

(iii) for every $v \in \Omega_F^\infty$ *and* $w \in \Omega_K^\infty$*,* $w' \in \Omega_{K'}^\infty$ *with* $w, w' \mid v$*, the conjugacy classes of* D_w *and* $D_{w'}$ *are equal,*

(iv) $K \otimes_F F_v \cong K' \otimes_F F_v$ *as* G*-structured* F_v*-algebras for all* $v \in \Omega_F^\infty$*.*

Proof. By splitting up Ω_K^∞ into G-orbits and using the orbit-stabiliser theorem it holds that

$$\begin{aligned} \mathbb{Q}[\Omega_K^\infty] &= \bigoplus_{v \in \Omega_F^\infty} \mathbb{Q}[\{\, w \in \Omega_K^\infty \mid w \mid v \,\}] \\ &\cong \bigoplus_{v \in \Omega_F^\infty} \mathbb{Q}[G/D_v] \\ &\cong \bigoplus_{v \in \Omega_F^\infty} \operatorname{Ind}_{D_v}^G 1_{D_v} \end{aligned} \tag{8.16}$$

as $\mathbb{Q}G$-modules, where D_v denotes the decomposition group of any $w \in \Omega_K^\infty$ with $w \mid v$. Then [CM90, Theorem 6.7] yields that $(\mathbb{Q} \otimes_\mathbb{Z} \mathcal{O}_K^\times) \oplus \mathbb{Q} \cong \mathbb{Q}[\Omega_K^\infty]$ as $\mathbb{Q}G$-modules. This immediately shows that (i) implies (ii). The converse follows from the isomorphism $(\mathbb{Q} \otimes_\mathbb{Z} \mathcal{O}_K^\times) \oplus \mathbb{Q} \cong \mathbb{Q}[\Omega_K^\infty]$ and [CR81, Corollary 6.15].

The isomorphism (8.16) also shows that (iii) implies (ii). The converse follows from (8.16) and Artin's Induction Theorem.

That (iii) implies (iv) follows from Lemma 8.6 and Proposition 8.9. For the converse, use again the isomorphism from Proposition 8.9 and consider the stabiliser of one of the primitive central idempotents. □

8.1.5 The Good Part of the Arakelov Ray Class Sequence

Use Setup 8.14. After having established the family of number fields we want to work with, we now specify the exact object to be considered in the conjecture we aim to make.

We are interested in the distribution of the good part $\mathrm{Cl}_K(\mathfrak{m})[S^\infty]$ of the ray class group with modulus $\mathfrak{m}$ as K runs over $\mathcal{K}$. Recall that our strategy towards a reasonable conjecture is to either remove or incorporate into one object all known obstructions to randomness of $\mathrm{Cl}_K(\mathfrak{m})[S^\infty]$ and then conjecture that the resulting object behaves randomly according to Principle 1.1. For these structural considerations, we base our reasoning on the previous work on the distribution of ray class groups of quadratic fields [PS17, BP25] and the paper [BL20] on the distribution of class groups, the latter having to be the special case of our prediction for the trivial modulus.

From the case of class groups, we know that in order for a conjecture as above to hold, we have to consider the Arakelov ray class group instead of the ray class group (cf. the introduction). Next, following [PS17], [BP25] and our guiding principle, we have to take into account the natural short exact sequence $\mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})$, which imposes restrictions on the structure of $\mathrm{Pic}_K^0(\mathfrak{m})$. As in [PS17] and [BP25], we do so by considering the whole sequence $\mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})$ in the conjecture to be made. It contains the term Pic_K^0 of which we know a structural restriction: Its torsion submodule is Cl_K, and at a prime p with $p \nmid |G|$ we have that $\mathrm{Cl}_K[p^\infty]^G = \mathrm{Cl}_F[p^\infty]$ is determined by F. We remove this obstruction to randomness as in [BL20], which deals with the distribution of the good part of Pic_K^0: First, by Pontryagin duality, instead of $\mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})$ we may equivalently consider $\mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee$, which allows us to work with discrete modules rather than compact ones and therefore not having to worry about the topology. Note that by the results of Chapter 4, $\mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee$ is a short exact sequence of $(\mathbb{Z}G)^{\mathrm{op}}$-modules. As usual, we regard it as a short exact sequence of $\mathbb{Z}G$-modules via Convention 7.5. We then pick out good and structurally unobstructed components from $\mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee$ via the method from Chapter 7.

Setup 8.17. Use Setup 8.14. Additionally we fix the following notation. Let $R := \mathrm{im}(\mathbb{Z}_{(S)}G \to A)$ and let $V := A \otimes_{\mathbb{Q}G} W$. Let $\mathcal{M}$ be a full set of representatives for the isomorphism classes of finite R-modules. Let $\mathcal{M}_V$ be a full set of representatives for the isomorphism classes of finitely generated R-modules M with the property that $A \otimes_R M \cong V$.

Note that all of the results from Chapter 7 apply to R. In particular, R is a maximal $\mathbb{Z}_{(S)}$-order in A (Proposition 7.8) and a flat left and right $\mathbb{Z}G$-module (Proposition 7.13). Continuing our discussion from above, we are led to consider the short exact sequence of R-modules $R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee$, which is given by

$$0 \longrightarrow R \otimes_{\mathbb{Z}G} (\mathrm{Pic}_K^0)^\vee \longrightarrow R \otimes_{\mathbb{Z}G} \mathrm{Pic}_K^0(\mathfrak{m})^\vee \longrightarrow R \otimes_{\mathbb{Z}G} ((\mathcal{O}_K/\mathfrak{m}_F)^\times)^\vee \longrightarrow 0.$$

Note that despite dualising, tensoring with R has indeed had the desired effect regarding the class group by Proposition 7.17.

Note also that the exact sequence $R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee$ still restricts the structure of its middle term $R \otimes_{\mathbb{Z}G} \mathrm{Pic}_K^0(\mathfrak{m})^\vee$, as it is generally nonsplit: Any splitting $s\colon R \otimes_{\mathbb{Z}G} \mathrm{Pic}_K^0(\mathfrak{m})^\vee \to R \otimes_{\mathbb{Z}G} (\mathrm{Pic}_K^0)^\vee$ induces a splitting of the torsionfree part of $R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee$ which is only possible if $R \otimes_{\mathbb{Z}G} \left(\frac{\rho(\mathcal{O}_K^\times)}{\rho(\mu(K))}\right)^\vee = 0$. Hence it is not enough to just consider $R \otimes_{\mathbb{Z}G} \mathrm{Pic}_K^0(\mathfrak{m})^\vee$.

Note further that the diagram $R \otimes_{\mathbb{Z}G} \mathrm{D}_K(\mathfrak{m})^\vee$, of which $R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee$ is part of, does in turn not restrict the structure of $R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee$: By Propositions 7.21, 7.20 and 6.20 we may recover it from the latter as $\mathrm{D}_{\mathrm{d}}(R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee)$.

We add one more comment on the nature of $R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee$. We first recall the following lemma from [BL20] that gives a relation between $\mathcal{M}_V$ and $\mathcal{M}$ and will often be useful when dealing with elements of $\mathcal{M}_V$.

Lemma 8.18 ([BL20, Lemma 3.5])**.** *There is a unique (up to isomorphism) finitely generated projective R-module P_V with $A \otimes_R P_V \cong V$. If M is a finitely generated R-module with $A \otimes_R M \cong V$, then there is a unique $M_0 \in \mathcal{M}$ with $M \cong P_V \oplus M_0$.*

We record the following statement found in [BL20] for the trivial modulus.

Lemma 8.19. *Let K be a G-extension of F with $\mathbb{Q} \otimes_{\mathbb{Z}} \mathcal{O}_K^\times \cong W$. Let $\mathfrak{m} := (\mathfrak{m}_F, \varnothing)$. Then*

$$R \otimes_{\mathbb{Z}G} \operatorname{Pic}_K^0(\mathfrak{m})^\vee \cong P_V \oplus (R \otimes_{\mathbb{Z}G} \operatorname{Cl}_K(\mathfrak{m})^\vee).$$

In particular, $R \otimes_{\mathbb{Z}G} \operatorname{Pic}_K^0(\mathfrak{m})^\vee$ is isomorphic to a unique element of $\mathcal{M}_V$.

Proof. By Proposition 3.9, $R \otimes_{\mathbb{Z}G} \operatorname{Pic}_K^0(\mathfrak{m})^\vee$ is a direct sum of its torsion part and torsionfree quotient. Propositions 6.15 and 4.42 and Lemma 7.15 show that $R \otimes_{\mathbb{Z}G} \operatorname{Cl}_K(\mathfrak{m})^\vee$ is the torsion part of $R \otimes_{\mathbb{Z}G} \operatorname{Pic}_K^0(\mathfrak{m})^\vee$ and that the torsionfree quotient is isomorphic to

$$R \otimes_{\mathbb{Z}G} (\mathcal{O}_K^1(\mathfrak{m}) \otimes \mathbb{R}/\mathbb{Z})^\vee \cong R \otimes_{\mathbb{Z}G} \mathcal{O}_K^1(\mathfrak{m})^*.$$

Now we have isomorphisms of $\mathbb{Q}G$-modules

$$\begin{aligned}
\mathbb{Q}G \otimes_{\mathbb{Z}G} \mathcal{O}_K^1(\mathfrak{m})^* &\cong \mathbb{Q} \otimes_{\mathbb{Z}} \mathcal{O}_K^1(\mathfrak{m})^* \\
&\cong (\mathbb{Q} \otimes_{\mathbb{Z}} \mathcal{O}_K^1(\mathfrak{m}))^* && \text{(Proposition 2.1)} \\
&\cong (\mathbb{Q} \otimes_{\mathbb{Z}} \mathcal{O}_K^\times)^* && \text{(Proposition 6.5)} \\
&\cong W^* && \text{(Assumption)} \\
&\cong W && \text{(Proposition 7.9)}
\end{aligned}$$

which give

$$A \otimes_{\mathbb{Z}G} \mathcal{O}_K^1(\mathfrak{m})^* = A \otimes_{\mathbb{Q}G} \mathbb{Q}G \otimes_{\mathbb{Z}G} \mathcal{O}_K^1(\mathfrak{m})^* \cong A \otimes_{\mathbb{Q}G} W = V.$$

Then Lemma 8.18 yields $R \otimes_{\mathbb{Z}G} \mathcal{O}_K^1(\mathfrak{m})^* \cong P_V$. □

By the above lemma, Proposition 7.17 and Pontryagin duality we have that for $(K, \iota) \in \mathcal{K}$, $R \otimes_{\mathbb{Z}G} \operatorname{Pic}_K^0(\mathfrak{m})^\vee$ carries the same information as $R \otimes_{\mathbb{Z}G} \operatorname{Cl}_K(\mathfrak{m})$ and $R \otimes_{\mathbb{Z}G} (\operatorname{Pic}_K^0)^\vee$ carries the same information as $R \otimes_{\mathbb{Z}G} \operatorname{Cl}_K$.

All of the above taken together suggest that on the family $\mathcal{K}$, the sequence $R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee$ incorporates all structure of the good part of the ray class group, that it itself has no structural restrictions and that the natural conjecture we have set out to make therefore is that $R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee$ behaves like a random sequence in the sense of Principle 1.1.

8.1.6 Families of Galois Extensions with Fixed Splitting Behaviour

In this section, we establish a space of outcomes for the sequences $R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee$ for (K, ι) belonging to the family of Galois extensions $\mathcal{K}$. Lemma 8.19 above already provides us with a space for the left hand module of $R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee$. As in [PS17] and [BP25] we next partition $\mathcal{K}$ into finitely many natural subfamilies such that in each subfamily, the right hand module of $R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee$ is constant, allowing to set up a space of outcomes over each subfamily in a simple way. We do this by fixing the local behaviour of the fields in $\mathcal{K}$ at the primes of F dividing $\mathfrak{m}_F$.

We use the following terminology which has been introduced in [Woo10] for abelian G.

Definition 8.20. Let G be a finite group and let F be a number field. Let P be a finite set of places of F and suppose that for each $v \in P$ we have a G-structured F_v-algebra T_v. We say that the collection $T = (T_v)_{v \in P}$ is *viable* for G and F if there exists a G-extension K/F with $K \otimes_F F_v \cong T_v$ for all $v \in P$.

For the remainder of this subsection, we use the following setup.

Setup 8.21. Use Setup 8.17. Further, for each prime $\mathfrak{p}$ of F dividing $\mathfrak{m}_F$ let $T_\mathfrak{p}$ be a G-structured $F_\mathfrak{p}$-algebra such that the collection $T = (T_\mathfrak{p})_{\mathfrak{p} | \mathfrak{m}_F}$ is viable. Let

$$\mathcal{K}^T := \{\, (K, \iota) \in \mathcal{K} \,|\, K \otimes_F F_\mathfrak{p} \cong T_\mathfrak{p} \text{ for all } \mathfrak{p} \mid \mathfrak{m}_F \,\},$$

where the isomorphism is as G-structured $F_\mathfrak{p}$-algebras, and, for $B \in \mathbb{R}_{>0}$,

$$\mathcal{K}^T_{C \le B} := \left\{\, (K, \iota) \in \mathcal{K}^T \,\middle|\, C(K) \le B \,\right\}.$$

In the following, when writing $\mathfrak{p} \mid \mathfrak{m}_F$ we always mean that $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_F$.

Note that since $F_\mathfrak{p}$ is a local field of characteristic 0, there are only finitely many G-structured $F_\mathfrak{p}$-algebras up to isomorphism, as there are only finitely many isomorphism classes of H-extensions of $F_\mathfrak{p}$ for any $H \le G$ [Lan94, Proposition II.14]. Hence, there are only finitely many viable collections $T = (T_\mathfrak{p})_{\mathfrak{p}|\mathfrak{m}_F}$ and corresponding subfamilies $\mathcal{K}^T$ of $\mathcal{K}$.

In suitable contexts, one can obtain a statement on the whole family $\mathcal{K}$ from statements on the subfamilies $\mathcal{K}^T$ for all T, given the existence of the densities of the individual subfamilies in $\mathcal{K}$. Since $\mathcal{K}$ only differs from the type of families with known densities considered in Proposition 8.12 in that certain roots of unity are not allowed to appear, the existence of the densities of $\mathcal{K}^T$ of $\mathcal{K}$ can be ensured for abelian G by virtue of Proposition 8.13:

Proposition 8.22. *Suppose that G is abelian. Then*

$$\lim_{B\to\infty} \frac{\left|\mathcal{K}^T_{C\leq B}\right|}{\left|\mathcal{K}_{C\leq B}\right|} = \mathrm{Pr}_C(T).$$

Proof. Denote by $\widetilde{\mathcal{K}}$ the set of G-extensions (K,ι) of F with $K \subseteq \overline{F}$ and $\mathbb{Q}\otimes_{\mathbb{Z}} \mathcal{O}_K^\times \cong W$ and denote by $\widetilde{\mathcal{K}}^S$ the set of such G-extensions which additionally satisfy $\mu_p \subseteq K$ for some $p \in S$. Denote by $\widetilde{K}^T$ and $\widetilde{K}^{S,T}$ the respective sets of G-extensions as above but with the added condition that $K \otimes_F F_{\mathfrak{p}} \cong T_{\mathfrak{p}}$ for all $\mathfrak{p} \mid \mathfrak{m}_F$. Then $\mathcal{K} = \widetilde{\mathcal{K}} \setminus \widetilde{\mathcal{K}}^S$ and $\mathcal{K}^T = \widetilde{\mathcal{K}}^T \setminus \widetilde{\mathcal{K}}^{S,T}$ and thus

$$\frac{\left|\mathcal{K}^T_{C\leq B}\right|}{\left|\mathcal{K}_{C\leq B}\right|} = \frac{\left|\widetilde{\mathcal{K}}^T_{C\leq B}\right| - \left|\widetilde{\mathcal{K}}^{S,T}_{C\leq B}\right|}{\left|\widetilde{\mathcal{K}}_{C\leq B}\right| - \left|\widetilde{\mathcal{K}}^S_{C\leq B}\right|} = \frac{\frac{\left|\widetilde{\mathcal{K}}^T_{C\leq B}\right|}{\left|\widetilde{\mathcal{K}}_{C\leq B}\right|} - \frac{\left|\widetilde{\mathcal{K}}^{S,T}_{C\leq B}\right|}{\left|\widetilde{\mathcal{K}}_{C\leq B}\right|}}{1 - \frac{\left|\widetilde{\mathcal{K}}^S_{C\leq B}\right|}{\left|\widetilde{\mathcal{K}}_{C\leq B}\right|}}.$$

By Propositions 8.13 and 8.15, both $\frac{\left|\widetilde{\mathcal{K}}^S_{C\leq B}\right|}{\left|\widetilde{\mathcal{K}}_{C\leq B}\right|}$ and $\frac{\left|\widetilde{\mathcal{K}}^{S,T}_{C\leq B}\right|}{\left|\widetilde{\mathcal{K}}_{C\leq B}\right|}$ converge to zero as $B \to \infty$. Moreover, using Propositions 8.3 and 8.15, [Woo10, Corollary 2.4] shows that $\frac{\left|\widetilde{\mathcal{K}}^T_{C\leq B}\right|}{\left|\widetilde{\mathcal{K}}_{C\leq B}\right|}$ converges to $\mathrm{Pr}_C(T)$ as $B \to \infty$. The claim follows. □

We now show that the right hand side of $R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee$ is constant for $(K,\iota) \in \mathcal{K}^T$.

Lemma 8.23. *Suppose that $\mathfrak{p} \mid \mathfrak{m}_F$. Then $T_{\mathfrak{p}}$ has a unique maximal $\mathcal{O}_{F_{\mathfrak{p}}}$-order $\mathcal{O}_{T_{\mathfrak{p}}}$, the integral closure of $\mathcal{O}_{F_{\mathfrak{p}}}$ in $T_{\mathfrak{p}}$. It is invariant under the G-action of $T_{\mathfrak{p}}$, so that G acts by $\mathcal{O}_{F_{\mathfrak{p}}}$-algebra automorphisms on $\mathcal{O}_{T_{\mathfrak{p}}}$.*

Proof. The first claim is immediate from [Rei03, Theorems 8.6 and 10.5]. If $g \in G$, then $g.\mathcal{O}_{T_{\mathfrak{p}}}$ is another maximal $\mathcal{O}_{F_{\mathfrak{p}}}$-order in $T_{\mathfrak{p}}$, so $g.\mathcal{O}_{T_{\mathfrak{p}}} = \mathcal{O}_{T_{\mathfrak{p}}}$, so $\mathcal{O}_{T_{\mathfrak{p}}}$ is a G-module. □

Definition 8.24. We define

$$\mathcal{O}_T := \prod_{\mathfrak{p}\mid\mathfrak{m}_F} \mathcal{O}_{T_{\mathfrak{p}}},$$

which is the integral closure of $\prod_{\mathfrak{p}\mid\mathfrak{m}_F} \mathcal{O}_{F_{\mathfrak{p}}}$ in $\prod_{\mathfrak{p}\mid\mathfrak{m}_F} T_{\mathfrak{p}}$, as well as

$$U_T := (\mathcal{O}_T/\mathfrak{m}_F)^\times = \prod_{\mathfrak{p}\mid\mathfrak{m}_F} (\mathcal{O}_{T_{\mathfrak{p}}}/\mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{m}_F)})^\times,$$

$$U_{T,R} := R \otimes_{\mathbb{Z}G} U_T = R \otimes_{\mathbb{Z}G} \prod_{\mathfrak{p}\mid\mathfrak{m}_F} (\mathcal{O}_{T_{\mathfrak{p}}}/\mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{m}_F)})^\times.$$

Proposition 8.25. *Let K be a G-extension of F with $K \otimes_F F_\mathfrak{p} \cong T_\mathfrak{p}$ as G-structured $F_\mathfrak{p}$-algebras for all $\mathfrak{p} \mid \mathfrak{m}_F$. Then there is a G-equivariant $\mathcal{O}_F$-algebra isomorphism*

$$\mathcal{O}_K/\mathfrak{m}_F \cong \prod_{\mathfrak{p}|\mathfrak{m}_F} \mathcal{O}_{T_\mathfrak{p}}/\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{m}_F)} = \mathcal{O}_T/\mathfrak{m}_F.$$

If $\mu_{p^\infty}(K) = \mu_{p^\infty}(F)$ for all $p \in S$, then the above isomorphism induces an isomorphism

$$R \otimes_{\mathbb{Z}G} \frac{(\mathcal{O}_K/\mathfrak{m}_F)^\times}{\rho(\mu(K))} \cong R \otimes_{\mathbb{Z}G} \frac{(\mathcal{O}_T/\mathfrak{m}_F)^\times}{\mu_S(F)}$$

of R-modules, where $\mu_S(F)$ denotes the set of roots of unity in F whose order is a product of primes in S.

Proof. By the Chinese remainder theorem we have G-equivariant $\mathcal{O}_F$-algebra isomorphisms

$$\mathcal{O}_K/\mathfrak{m}_F \cong \prod_{\mathfrak{p}|\mathfrak{m}_F} \mathcal{O}_K/\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{m}_F)} \cong \prod_{\mathfrak{p}|\mathfrak{m}_F} \prod_{\substack{\mathfrak{q}|\mathfrak{p} \\ \text{in } K}} \mathcal{O}_K/\mathfrak{q}^{v_\mathfrak{p}(\mathfrak{m}_F)v_\mathfrak{q}(\mathfrak{p})}.$$

The inclusions $K \hookrightarrow K_\mathfrak{q}$ for $\mathfrak{q} \mid \mathfrak{p}$ give rise to an isomorphism of $\mathcal{O}_F$-algebras

$$\begin{aligned} \prod_{\substack{\mathfrak{q}|\mathfrak{p} \\ \text{in } K}} \mathcal{O}_K/\mathfrak{q}^{v_\mathfrak{p}(\mathfrak{m}_F)v_\mathfrak{q}(\mathfrak{p})} &\xrightarrow{\sim} \prod_{\substack{\mathfrak{q}|\mathfrak{p} \\ \text{in } K}} \mathcal{O}_{K_\mathfrak{q}}/\mathfrak{q}^{v_\mathfrak{p}(\mathfrak{m}_F)v_\mathfrak{q}(\mathfrak{p})} \\ &= \prod_{\substack{\mathfrak{q}|\mathfrak{p} \\ \text{in } K}} \mathcal{O}_{K_\mathfrak{q}}/\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{m}_F)} \\ &= \Big(\prod_{\substack{\mathfrak{q}|\mathfrak{p} \\ \text{in } K}} \mathcal{O}_{K_\mathfrak{q}}\Big)\Big/\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{m}_F)}. \end{aligned} \tag{8.26}$$

Note that the inclusions $K \hookrightarrow K_\mathfrak{q}$ also give rise to an isomorphism of etale $F_\mathfrak{p}$-algebras $K \otimes_F F_\mathfrak{p} \xrightarrow{\sim} \prod_{\mathfrak{q}|\mathfrak{p}} K_\mathfrak{q}$, which is G-equivariant with respect to the natural actions on both sides (cf. the proof of Proposition 8.9). Hence also (8.26) is G-equivariant. By assumption and Lemma 8.23 we have that $\prod_{\mathfrak{q}|\mathfrak{p}} \mathcal{O}_{K_\mathfrak{q}} \cong \mathcal{O}_{T_\mathfrak{p}}$ as $\mathcal{O}_{F_\mathfrak{p}}$-algebras and as G-modules, which establishes the desired isomorphism.

Finally, suppose that $\mu_{p^\infty}(K) = \mu_{p^\infty}(F)$ for all $p \in S$. We have $\mu(K) = \mu_S(K) \cdot \mu_{S'}(K)$ where $\mu_{S'}(K)$ is the set of roots of unity in K whose order is coprime to all $p \in S$. Since R is a $\mathbb{Z}_{(S)}$-algebra, the exact sequence

$$0 \longrightarrow \rho(\mu_{S'}(K)) \longrightarrow \frac{(\mathcal{O}_K/\mathfrak{m}_F)^\times}{\rho(\mu_S(K))} \longrightarrow \frac{(\mathcal{O}_K/\mathfrak{m}_F)^\times}{\rho(\mu(K))} \longrightarrow 0$$

yields

$$R \otimes_{\mathbb{Z}G} \frac{(\mathcal{O}_K/\mathfrak{m}_F)^\times}{\rho(\mu(K))} \cong R \otimes_{\mathbb{Z}G} \frac{(\mathcal{O}_K/\mathfrak{m}_F)^\times}{\rho(\mu_S(K))} = R \otimes_{\mathbb{Z}G} \frac{(\mathcal{O}_K/\mathfrak{m}_F)^\times}{\rho(\mu_S(F))}.$$

The claim follows from the isomorphism established above. □

Note that if $(K,\iota) \in \mathcal{K}^T$, then $\mu_S(F) = \mu_S(K) = 1$. Hence, the above proposition shows that the right hand side of $R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee$ is indeed constant as (K,ι) runs over $\mathcal{K}^T$.

Definition 8.27. We write $\mathrm{Aut}_{G\text{-eq. alg.}}(\mathcal{O}_T/\mathfrak{m}_F)$ for the set of G-equivariant $\mathcal{O}_F$-algebra automorphisms of $\mathcal{O}_T/\mathfrak{m}_F$ and define

$$\begin{aligned}\mathrm{Aut}_{G\text{-eq. alg.}}(U_{T,R}) &:= \left\{ \mathrm{id}_R \otimes \varphi^\times \,\middle|\, \varphi \in \mathrm{Aut}_{G\text{-eq. alg.}}(\mathcal{O}_T/\mathfrak{m}_F) \right\},\\ \mathrm{Aut}_{G\text{-eq. alg.}}(U_{T,R}^\vee) &:= \left\{ (\mathrm{id}_R \otimes \varphi^\times)^\vee \,\middle|\, \varphi \in \mathrm{Aut}_{G\text{-eq. alg.}}(\mathcal{O}_T/\mathfrak{m}_F) \right\},\end{aligned}$$

which are subgroups of $\mathrm{Aut}_R(U_{T,R})$ and $\mathrm{Aut}_R(U_{T,R}^\vee)$, respectively.

Construction 8.28. Let $(K,\iota) \in \mathcal{K}^T$. By Lemma 8.19, there is a unique $M \in \mathcal{M}_V$ with $R \otimes_{\mathbb{Z}G} (\mathrm{Pic}_K^0)^\vee \cong M$ as R-modules. Moreover, the natural isomorphism from Proposition 7.17 together with any G-equivariant $\mathcal{O}_F$-algebra isomorphism from Proposition 8.25 give an isomorphism

$$R \otimes_{\mathbb{Z}G} \left(\frac{(\mathcal{O}_K/\mathfrak{m}_F)^\times}{\rho(\mu(K))} \right)^\vee \xrightarrow{\sim} \left(R \otimes_{\mathbb{Z}G} \frac{(\mathcal{O}_K/\mathfrak{m}_F)^\times}{\rho(\mu(K))} \right)^\vee \cong U_{T,R}^\vee.$$

Using the above isomorphisms, we can identify $R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee$ with an element of $\mathrm{Ext}_R^1(U_{T,R}^\vee, M)$. When choosing different isomorphisms at all stages where there is no natural choice, we end up with an element of $\mathrm{Ext}_R^1(U_{T,R}^\vee, M)$ that is $(\mathrm{Aut}_{G\text{-eq. alg.}}(U_{T,R}^\vee) \times \mathrm{Aut}\, N)$-isomorphic to the previous one. Thus, via the method described above, we may uniquely identify $R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee$ with an element of

$$\bigsqcup_{N \in \mathcal{M}_V} \mathrm{Ext}_R^1(U_{T,R}^\vee, N) / \mathrm{Aut}_{G\text{-eq. alg.}}(U_{T,R}^\vee) \times \mathrm{Aut}\, N,$$

independently of the choices of all noncanonical isomorphisms.

Definition 8.29. For $N \in \mathcal{M}_V$, we let $\mathcal{E}(U_{T,R}^\vee, N)$ be a system of representatives for the $(\mathrm{Aut}_{G\text{-eq. alg.}}(U_{T,R}^\vee) \times \mathrm{Aut}\, N)$-isomorphism classes in $\mathrm{Ext}_R^1(U_{T,R}^\vee, N)$. Define

$$\mathcal{E}(U_{T,R}^\vee, \mathcal{M}_V) := \bigsqcup_{N \in \mathcal{M}_V} \mathcal{E}(U_{T,R}^\vee, N).$$

As described in Construction 8.28, for $(K,\iota) \in \mathcal{K}^T$ we can uniquely identify $R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee$ with an element of $\mathcal{E}(U_{T,R}^\vee, \mathcal{M}_V)$, and we will denote that element by $[R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee]$. Finally, for $N \in \mathcal{M}_V$ and $\Theta \in \mathrm{Ext}_R^1(U_{T,R}^\vee, N)$ we write

$$[\Theta]_{G\text{-eq. alg.}} := [\Theta]_{\mathrm{Aut}_{G\text{-eq. alg.}}(U_{T,R}^\vee) \times \mathrm{Aut}\, N}$$

and

$$\mathrm{Aut}_{G\text{-eq. alg.}}(\Theta) := \mathrm{Aut}_{\mathrm{Aut}_{G\text{-eq. alg.}}(U_{T,R}^\vee) \times \mathrm{Aut}\, N}(\Theta).$$

The set $\mathcal{E}(U_{T,R}^\vee, \mathcal{M}_V)$ thus acts as a set of outcomes for the sequences $R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee$ for $(K,\iota) \in \mathcal{K}^T$. Note that since $\mathrm{Ext}_R^1(U_{T,R}^\vee, N)$ is finite for $N \in \mathcal{M}_V$ by Lemma 3.31 and since $\mathcal{M}_V$ is countable, the set $\mathcal{E}(U_{T,R}^\vee, \mathcal{M}_V)$ is countable. We also note that all of the statements to follow below do not depend on the choice of system of representatives.

8.2 The Distribution of Random Sequences

Use Setup 8.21. In this section, we construct a probability distribution on $\mathcal{E}(U_{T,R}^{\vee}, \mathcal{M}_V)$ that weighs an element Θ by the inverse of the size of $\operatorname{Aut}_{G\text{-eq. alg.}}(\Theta)$. Since the latter is generally not finite, we will employ the commensurability theory from Section 5.6 for this. This is the analogous procedure as in [BL20], where, when faced with the same sort of problem, Bartel–Lenstra used their commensurability theory from [BL17] to construct on $\mathcal{M}_V$ the probability distribution $\mathbb{P}^{\mathrm{BL}}$ from the introduction.

We set up some more notation that will be used in this section.

Denote by $\underline{V}$ the short exact sequence

$$0 \longrightarrow V \xrightarrow{\mathrm{id}} V \longrightarrow 0 \longrightarrow 0.$$

Then $\operatorname{End} \underline{V} \cong \operatorname{End} V$ is semisimple (see the proof of [BL17, Theorem 8.1]) and for any $\Theta \in \mathcal{E}(U_{T,R}^{\vee}, \mathcal{M}_V)$ it holds that $\mathbb{Q} \otimes_{\mathbb{Z}} \Theta \cong \underline{V}$. Moreover, since $U_{T,R}$ is finite, we have $|\operatorname{Aut} \Theta : \operatorname{Aut}_{G\text{-eq. alg.}}(\Theta)| < \infty$ by Corollary 2.13. Hence, Proposition 5.40 and Theorem 5.42 give us a well-defined function

$$\mathcal{E}(U_{T,R}^{\vee}, \mathcal{M}_V) \times \mathcal{E}(U_{T,R}^{\vee}, \mathcal{M}_V) \to \mathbb{Q}_{>0}, \ (\Theta, \Theta') \mapsto \operatorname{ia}(\Theta, \Theta')|_{\operatorname{Aut}_{G\text{-eq. alg.}}(\Theta), \operatorname{Aut}_{G\text{-eq. alg.}}(\Theta')}$$

whose output can be thought of as the index of $\operatorname{Aut}_{G\text{-eq. alg.}}(\Theta)$ in $\operatorname{Aut}_{G\text{-eq. alg.}}(\Theta')$. In the following, we will use the shorthand notation

$$\operatorname{ia}_{G\text{-eq. alg.}}(\Theta, \Theta') := \operatorname{ia}(\Theta, \Theta')|_{\operatorname{Aut}_{G\text{-eq. alg.}}(\Theta), \operatorname{Aut}_{G\text{-eq. alg.}}(\Theta')}$$

for $\Theta, \Theta' \in \mathcal{E}(U_{T,R}^{\vee}, \mathcal{M}_V)$. Note also that by Theorem 5.31 there is a function

$$\operatorname{ia}\colon \mathcal{E}(U_{T,R}^{\vee}, \mathcal{M}_V) \times \mathcal{E}(U_{T,R}^{\vee}, \mathcal{M}_V) \to \mathbb{Q}_{>0}, \ (\Theta, \Theta') \mapsto \operatorname{ia}(\Theta, \Theta')$$

whose output can be thought of as the index of $\operatorname{Aut} \Theta$ in $\operatorname{Aut} \Theta'$ and which is related to the previous function as described in Theorem 5.42 (v).

The key in constructing the desired probability distribution is to ensure convergence of $\sum_{\Delta \in \mathcal{E}(U_{T,R}^{\vee}, \mathcal{M}_V)} \operatorname{ia}_{G\text{-eq. alg.}}(\Delta, \Pi)$ for some Π. For the latter, we will need to compute the index $\operatorname{ia}_{G\text{-eq. alg.}}(\Delta, \Pi)$ in some way. This is achieved by the following two lemmas.

Lemma 8.30. *Let Θ be a short exact sequence of finitely generated R-modules with $A \otimes_R \Theta \cong \underline{V}$. Then Θ is isomorphic to a short exact sequence*

$$0 \longrightarrow P_V \oplus N_0 \longrightarrow P_V \oplus L_0 \longrightarrow M_0 \longrightarrow 0$$

for unique $N_0, L_0, M_0 \in \mathcal{M}$.

Proof. This is immediate from Lemma 8.18. □

Lemma 8.31. *Let $N_0, L_0, M_0 \in \mathcal{M}$ and suppose that*

$$\Theta\colon \qquad 0 \longrightarrow P_V \oplus N_0 \xrightarrow{\alpha} P_V \oplus L_0 \longrightarrow M_0 \longrightarrow 0$$

is a short exact sequence of R-modules. Further let

$$\underline{P_V}\colon \qquad 0 \longrightarrow P_V \xrightarrow{\mathrm{id}} P_V \longrightarrow 0 \longrightarrow 0.$$

Then we have

$$\mathrm{ia}(\Theta, \underline{P_V}) = \frac{|[\Theta]|}{|\mathrm{Hom}(P_V, N_0)| \cdot |\mathrm{Aut}\, N_0| \cdot |\mathrm{Hom}(M_0, N_0)| \cdot |\mathrm{Aut}\, M_0|},$$

where as usual $[\Theta]$ denotes the isomorphism class of $\Theta \in \mathrm{Ext}^1_R(M_0, P_V \oplus N_0)$.

Note that $[\Theta]$ is finite by Lemma 3.31.

Proof. Let $\pi\colon P_V \oplus L_0 \to P_V$ be the projection onto the first coordinate. Using Proposition 5.7, we then have that $f := (\pi \circ \alpha, \alpha, 0)\colon \Theta \to \underline{P_V}$ is an isogeny.

$$\begin{tikzcd}
\Theta\colon \arrow[d, "f"] & 0 \arrow[r] & P_V \oplus N_0 \arrow[r, "\alpha"] \arrow[d, "\pi\circ\alpha"] & P_V \oplus L_0 \arrow[r] \arrow[d, "\pi"] & M_0 \arrow[r] \arrow[d] & 0 \\
\underline{P_V}\colon & 0 \arrow[r] & P_V \arrow[r, "\mathrm{id}"] & P_V \arrow[r] & 0 \arrow[r] & 0
\end{tikzcd}$$

Hence, $c_f = (\Theta, \mathrm{id}, f)\colon \Theta \rightleftharpoons \underline{P_V}$ is a commensurability and we have $\mathrm{ia}(\Theta, \underline{P_V}) = \mathrm{i}(\mathrm{a}(c_f))$. Write $\mathrm{a}(c_f) = (\mathrm{Aut}\, c_f, p_0, p_1)\colon \mathrm{Aut}\,\Theta \rightleftharpoons \mathrm{Aut}\,\underline{P_V}$ and recall that

$$\mathrm{Aut}\, c_f = \left\{ (\theta, \theta, \psi) \in \mathrm{Aut}\,\Theta \times \mathrm{Aut}\,\Theta \times \mathrm{Aut}\,\underline{P_V} \,\middle|\, \psi f = f\theta \right\}.$$

To prove the claim, we calculate $\mathrm{i}(\mathrm{a}(c_f)) = \mathrm{i}(p_1)/\mathrm{i}(p_0)$. We first show that

$$p_0\colon \mathrm{Aut}\, c_f \to \mathrm{Aut}\,\Theta,\ (\theta, \theta, \psi) \mapsto \theta$$

is an isomorphism. Injectivity is clear by the description of $\mathrm{Aut}\, c_f$. For surjectivity let $\theta \in \mathrm{Aut}\,\Theta$ and write $\theta = (\nu, \lambda, \mu)$ with $\nu \in \mathrm{Aut}(P_V \oplus N_0)$, $\lambda \in \mathrm{Aut}(P_V \oplus L_0)$ and $\mu \in \mathrm{Aut}\, M_0$. Since L_0 is finite and P_V is $\mathbb{Z}_{(S)}$-torsionfree, we have $\mathrm{Hom}(L_0, P_V) = 0$ from which it follows that λ has the form

$$\lambda = \begin{pmatrix} \lambda_{11} & \\ \lambda_{21} & \lambda_{22} \end{pmatrix} \in \begin{pmatrix} \mathrm{Aut}\, P_V & \\ \mathrm{Hom}(P_V, L_0) & \mathrm{Aut}\, L_0 \end{pmatrix} = \mathrm{Aut}(P_V \oplus L_0).$$

It is then clear that $\lambda_{11} \in \mathrm{Aut}\, P_V = \mathrm{Aut}\,\underline{P_V}$ satisfies $\lambda_{11}\pi = \pi\lambda$. Moreover, this implies $\lambda_{11}\pi\alpha = \pi\lambda\alpha = \pi\alpha\nu$ which shows $(\theta, \theta, \lambda_{11}) \in \mathrm{Aut}\, c_f$. Hence, p_0 is an isomorphism.

Under the isomorphism p_0, the second projection p_1 corresponds to the map

$$\mathrm{Aut}\,\Theta \to \mathrm{Aut}\, P_V,\ \theta = (\nu, \lambda, \mu) \mapsto \lambda_{11},$$

which factors as the composition

$$\operatorname{Aut}\Theta \xrightarrow{q} \operatorname{Aut}(P_V \oplus L_0) \to \operatorname{Aut} P_V$$

of two canonical projections, both of which are isogenies. By Proposition 5.7 we then have

$$\mathrm{ia}(\Theta, \underline{P_V}) = \mathrm{i}(p_1) = \mathrm{i}(q) \cdot \frac{1}{|\operatorname{Hom}(P_V, L_0)| \cdot |\operatorname{Aut} L_0|}. \tag{8.32}$$

It remains to compute $\mathrm{i}(q)$, which we will do by employing the commensurability $c_\alpha = (P_V \oplus N_0, \mathrm{id}, \alpha)\colon P_V \oplus N_0 \rightleftharpoons P_V \oplus L_0$. It yields a commensurability

$$\mathrm{a}(c_\alpha) = (\operatorname{Aut} c_\alpha, p'_0, p'_1)\colon \operatorname{Aut}(P_V \oplus N_0) \rightleftharpoons \operatorname{Aut}(P_V \oplus L_0),$$

where by definition,

$$\operatorname{Aut} c_\alpha = \{\, (\nu, \nu, \lambda) \in \operatorname{Aut}(P_V \oplus N_0) \times \operatorname{Aut}(P_V \oplus N_0) \times \operatorname{Aut}(P_V \oplus L_0) \mid \lambda\alpha = \alpha\nu \,\}.$$

There is an isomorphism

$$\operatorname{Aut}\Theta \xrightarrow{\sim} \operatorname{Aut} c_\alpha, \;\; \theta = (\nu, \lambda, \mu) \mapsto (\nu, \nu, \lambda)$$

under which q corresponds to p'_1, so in particular $\mathrm{i}(q) = \mathrm{i}(p'_1)$. By definition of ia, we have

$$\mathrm{i}(p'_1) = \mathrm{i}(\mathrm{a}(c_\alpha)) \cdot \mathrm{i}(p'_0) = \mathrm{ia}(P_V \oplus N_0, P_V \oplus L_0) \cdot \mathrm{i}(p'_0). \tag{8.33}$$

Under the isomorphism $\operatorname{Aut}\Theta \cong \operatorname{Aut} c_\alpha$ from above, p'_0 factors as the composition

$$\operatorname{Aut}\Theta \xrightarrow{\rho} \operatorname{Aut}(P_V \oplus N_0) \times \operatorname{Aut} M_0 \to \operatorname{Aut}(P_V \oplus N_0)$$

of two canonical projections, which gives $\mathrm{i}(p'_0) = \mathrm{i}(\rho)/\,|\operatorname{Aut} M_0|$. Now by Proposition 2.12 we have

$$\mathrm{i}(\rho) = \frac{|(\operatorname{Aut}(P_V \oplus N_0) \times \operatorname{Aut} M_0) : \operatorname{Stab}(\Theta)|}{|\operatorname{Hom}(M_0, P_V \oplus N_0)|} = \frac{|[\Theta]|}{|\operatorname{Hom}(M_0, N_0)|},$$

whence

$$\mathrm{i}(p'_0) = \frac{|[\Theta]|}{|\operatorname{Hom}(M_0, N_0)| \cdot |\operatorname{Aut} M_0|}.$$

Plugging this and the expression for $\mathrm{ia}(P_V \oplus N_0, P_V \oplus L_0)$ from [BL20, Proposition 3.4] into (8.33) yields

$$\mathrm{i}(q) = \mathrm{i}(p'_1) = \frac{|\operatorname{Hom}(P_V, L_0)| \cdot |\operatorname{Aut} L_0| \cdot |[\Theta]|}{|\operatorname{Hom}(P_V, N_0)| \cdot |\operatorname{Aut} N_0| \cdot |\operatorname{Hom}(M_0, N_0)| \cdot |\operatorname{Aut} M_0|}$$

The claim now follows by plugging this expression into (8.32). □

Note that the expression for $\mathrm{ia}(\Theta, \underline{P_V})$ from the above lemma is precisely what one gets when 'calculating' $|\mathrm{Aut}\,\Theta|$ using Proposition 2.12 (ii), and 'cancelling' $|\mathrm{Aut}\,P_V|$ in the 'fraction' $\frac{|\mathrm{Aut}\,\underline{P_V}|}{|\mathrm{Aut}\,\Theta|}$. This shows that our theory of commensurability works as expected.

We are finally ready to construct the probability distribution and thereby prove Theorem 1.12.

Theorem 8.34. *There is a unique discrete probability distribution $\mathbb{P}_T$ on $\mathcal{E}(U_{T,R}^\vee, \mathcal{M}_V)$ with the property that for all $\Theta, \Theta' \in \mathcal{E}(U_{T,R}^\vee, \mathcal{M}_V)$ we have*

$$\frac{\mathbb{P}_T(\Theta)}{\mathbb{P}_T(\Theta')} = \mathrm{ia}_{G\text{-eq. alg.}}(\Theta, \Theta').$$

This distribution also has the following properties:

(i) If $\Theta, \Theta' \in \mathcal{E}(U_{T,R}^\vee, \mathcal{M}_V)$ and Φ is a short exact sequence of R-modules that is finite in the sense of Chapter 5 with $\Theta \oplus \Phi \cong \Theta'$, then

$$\mathbb{P}_T(\Theta) = \left|\mathrm{Aut}_{G\text{-eq. alg.}}(\Theta') : \mathrm{Aut}_{G\text{-eq. alg.}}(\Theta)\right| \cdot \mathbb{P}_T(\Theta')$$

where the inclusion $\mathrm{Aut}_{G\text{-eq. alg.}}(\Theta) \hookrightarrow \mathrm{Aut}_{G\text{-eq. alg.}}(\Theta')$ is given by $f \mapsto f \oplus \mathrm{id}_\Phi$.

(ii) If $\Theta \in \mathcal{E}(U_{T,R}^\vee, \mathcal{M}_V)$ is given by

$$0 \longrightarrow N \longrightarrow L \longrightarrow U_{T,R}^\vee \longrightarrow 0,$$

then we have

$$\mathbb{P}_T(\Theta) = \mathbb{P}^{\mathrm{BL}}(N) \cdot \frac{|[\Theta]_{G\text{-eq. alg.}}|}{\left|\mathrm{Ext}^1_R(U_{T,R}^\vee, N)\right|}.$$

In particular, if $\sigma \colon \mathcal{E}(U_{T,R}^\vee, \mathcal{M}_V) \to \mathcal{M}_V$ is the map sending Θ to the unique element of $\mathcal{M}_V$ that is isomorphic to N, then $\sigma_* \mathbb{P}_T = \mathbb{P}^{\mathrm{BL}}$.

Proof. Uniqueness of the distribution is clear. Let $\Pi \in \mathcal{E}(U_{T,R}^\vee, \mathcal{M}_V)$. We show that $\sum_{\Delta \in \mathcal{E}(U_{T,R}^\vee, \mathcal{M}_V)} \mathrm{ia}_{G\text{-eq. alg.}}(\Delta, \Pi)$ converges. For $\Delta \in \mathcal{E}(U_{T,R}^\vee, \mathcal{M}_V)$ it holds by Theorem 5.42 that

$$\mathrm{ia}_{G\text{-eq. alg.}}(\Delta, \Pi) = \frac{|\mathrm{Aut}\,\Delta : \mathrm{Aut}_{G\text{-eq. alg.}}(\Delta)| \cdot \mathrm{ia}(\Delta, \underline{P_V})}{|\mathrm{Aut}\,\Pi : \mathrm{Aut}_{G\text{-eq. alg.}}(\Pi)| \cdot \mathrm{ia}(\Pi, \underline{P_V})}$$

which leads us to investigate

$$c := \sum_{\Delta \in \mathcal{E}(U_{T,R}^\vee, \mathcal{M}_V)} |\mathrm{Aut}\,\Delta : \mathrm{Aut}_{G\text{-eq. alg.}}(\Delta)| \cdot \mathrm{ia}(\Delta, \underline{P_V}),$$

whose convergence we aim to prove. By Lemma 8.18 we can write

$$c = \sum_{N_0 \in \mathcal{M}} \sum_{\Delta \in \mathcal{E}(U_{T,R}^\vee, P_V \oplus N_0)} |\mathrm{Aut}\,\Delta : \mathrm{Aut}_{G\text{-eq. alg.}}(\Delta)| \cdot \mathrm{ia}(\Delta, \underline{P_V}).$$

We next rewrite the summands. Let $\Delta \in \mathrm{Ext}^1_R(U^\vee_{T,R}, P_V \oplus N_0)$. Then Lemmas 8.30 and 8.31 give

$$\begin{aligned} s(\Delta) &:= |\mathrm{Aut}\,\Delta : \mathrm{Aut}_{G\text{-eq. alg.}}(\Delta)| \cdot \mathrm{ia}(\Delta, \underline{P_V}) \\ &= \frac{|\mathrm{Aut}\,\Delta : \mathrm{Aut}_{G\text{-eq. alg.}}(\Delta)| \cdot |[\Delta]|}{|\mathrm{Hom}(P_V, N_0)| \cdot |\mathrm{Aut}\,N_0| \cdot \left|\mathrm{Hom}(U^\vee_{T,R}, N_0)\right| \cdot \left|\mathrm{Aut}\,U^\vee_{T,R}\right|}. \end{aligned}$$

Using Proposition 3.32 we have

$$\begin{aligned} \left|\mathrm{Ext}^1_R(U^\vee_{T,R}, P_V \oplus N_0)\right| &= \left|\mathrm{Ext}^1_R(U^\vee_{T,R}, P_V)\right| \cdot \left|\mathrm{Ext}^1_R(U^\vee_{T,R}, N_0)\right| \\ &= \left|\mathrm{Ext}^1_R(U^\vee_{T,R}, P_V)\right| \cdot \left|\mathrm{Hom}(U^\vee_{T,R}, N_0)\right|. \end{aligned}$$

This together with Corollary 2.13 yields

$$s(\Delta) = \frac{\left|\mathrm{Ext}^1_R(U^\vee_{T,R}, P_V)\right|}{\left|\mathrm{Aut}_{G\text{-eq. alg.}}(U^\vee_{T,R})\right|} \cdot \frac{|[\Delta]_{G\text{-eq. alg.}}|}{|\mathrm{Hom}(P_V, N_0)| \cdot |\mathrm{Aut}\,N_0| \cdot \left|\mathrm{Ext}^1_R(U^\vee_{T,R}, P_V \oplus N_0)\right|}.$$

It follows that

$$c = \sum_{N_0 \in \mathcal{M}} \sum_{\Delta \in \mathcal{E}(U^\vee_{T,R}, P_V \oplus N_0)} s(\Delta) = \frac{\left|\mathrm{Ext}^1_R(U^\vee_{T,R}, P_V)\right|}{\left|\mathrm{Aut}_{G\text{-eq. alg.}}(U^\vee_{T,R})\right|} \sum_{N_0 \in \mathcal{M}} \frac{1}{|\mathrm{Hom}(P_V, N_0)| \cdot |\mathrm{Aut}\,N_0|}.$$

Since S is finite, [CM90, Theorem 3.6] shows that

$$\widetilde{c} := \sum_{N_0 \in \mathcal{M}} \frac{1}{|\mathrm{Hom}(P_V, N_0)| \cdot |\mathrm{Aut}\,N_0|} < \infty$$

and therefore also that $c < \infty$. Thus, for $\Theta \in \mathcal{E}(U^\vee_{T,R}, \mathcal{M}_V)$ we may define

$$\mathbb{P}_T(\Theta) := \frac{\mathrm{ia}_{G\text{-eq. alg.}}(\Theta, \Pi)}{\sum_{\Delta \in \mathcal{E}(U^\vee_{T,R}, \mathcal{M}_V)} \mathrm{ia}_{G\text{-eq. alg.}}(\Delta, \Pi)},$$

which by Theorem 5.42 (ii) is independent of Π and moreover satisfies $\mathbb{P}_T(\Theta)/\mathbb{P}_T(\Theta') = \mathrm{ia}_{G\text{-eq. alg.}}(\Theta, \Theta')$. It is clear that this defines a discrete probability distribution on $\mathcal{E}(U^\vee_{T,R}, \mathcal{M}_V)$. Statement (i) follows easily from Theorem 5.42 (iii).

Finally, for (ii), let $\Theta \in \mathcal{E}(U^\vee_{T,R}, \mathcal{M}_V)$. By Lemma 8.30, Θ is isomorphic to a short exact sequence

$$0 \longrightarrow P_V \oplus N_0 \longrightarrow P_V \oplus L_0 \longrightarrow U^\vee_{T,R} \longrightarrow 0$$

with $N_0, L_0 \in \mathcal{M}$. By the above calculations, we have

$$\begin{aligned} \mathbb{P}_T(\Theta) &= s(\Theta) \cdot c^{-1} \\ &= \frac{|[\Theta]_{G\text{-eq. alg.}}|}{|\mathrm{Hom}(P_V, N_0)| \cdot |\mathrm{Aut}\,N_0| \cdot \left|\mathrm{Ext}^1_R(U^\vee_{T,R}, P_V \oplus N_0)\right|} \cdot \widetilde{c}^{-1}. \end{aligned}$$

Now by [BL20, Proposition 3.4] it holds that

$$\frac{1}{|\mathrm{Hom}(P_V, N_0)| \cdot |\mathrm{Aut}\, N_0|} \cdot \widetilde{c}^{-1} = \frac{\mathrm{ia}(P_V \oplus N_0, P_V)}{\sum_{M_0 \in \mathcal{M}} \mathrm{ia}(P_V \oplus M_0, P_V)}.$$

The latter expression equals $\mathbb{P}^{\mathrm{BL}}(P_V \oplus N_0)$ by the proof of [BL20, Proposition 3.6]. □

Remark 8.35. Part (ii) of the above theorem gives a different way of understanding the distribution $\mathbb{P}_T$, namely in terms of the subspaces $\mathcal{E}(U_{T,R}^\vee, N)$ of $\mathcal{E}(U_{T,R}^\vee, \mathcal{M}_V)$: It implies that for $\Theta \in \mathcal{E}(U_{T,R}^\vee, \mathcal{M}_V)$, $N \in \mathcal{M}_V$ and $\Delta \in \mathcal{E}(U_{T,R}^\vee, N)$ we have

$$\mathbb{P}_T(\Theta \in \mathcal{E}(U_{T,R}^\vee, N)) = \mathbb{P}^{\mathrm{BL}}(N)$$

and

$$\mathbb{P}_T(\Theta = \Delta \mid \Theta \in \mathcal{E}(U_{T,R}^\vee, N)) = \frac{|[\Delta]_{G\text{-eq. alg.}}|}{\left|\mathrm{Ext}^1_R(U_{T,R}^\vee, N)\right|}.$$

Definition 8.36. For $f\colon \mathcal{E}(U_{T,R}^\vee, \mathcal{M}_V) \to \mathbb{C}$ define its *expected value* to be

$$\mathbb{E}(f) := \sum_{\Theta \in \mathcal{E}(U_{T,R}^\vee, \mathcal{M}_V)} f(\Theta) \cdot \mathbb{P}_T(\Theta)$$

if the sum converges absolutely.

8.3 The Conjecture for the Distribution of Arakelov Ray Class Sequences

We recall the setup that has been established in the previous sections.

Setup 8.37. Let F be a number field and fix an algebraic closure $\overline{F}$ of F. Let $0 \neq \mathfrak{m}_F \trianglelefteq \mathcal{O}_F$. Let G be a finite group. Let W be a finitely generated $\mathbb{Q}G$-module. Let I be a two-sided ideal of $\mathbb{Q}G$ with $\sum_{g \in G} g \in I$ and let $A = \mathbb{Q}G/I$. Let S be a finite set of primes that are good for A. If G is abelian, let $C = C_F$ be a fair counting function defined on $E_G(F)$. If G is nonabelian, let $C = C_F$ be the function on $E_G(F)$ that assigns to K the ideal norm of the product of the prime ideals of $\mathcal{O}_F$ that ramify in K. Let

$$\begin{aligned} \mathcal{K} := \big\{(K, \iota) \mid (K, \iota) &\text{ is a } G\text{-extension of } F \text{ with } K \subseteq \overline{F}, \\ &K \text{ contains no primitive } p\text{-th root of unity for any } p \in S, \\ &\mathbb{Q} \otimes_{\mathbb{Z}} \mathcal{O}_K^\times \cong W \text{ as } \mathbb{Q}G\text{-modules}\big\} \end{aligned}$$

and, for $B \in \mathbb{R}_{>0}$,

$$\mathcal{K}_{C \le B} := \{\, (K, \iota) \in \mathcal{K} \mid C(K) \le B \,\}.$$

Assume that $\mathcal{K}$ is infinite. For $(K, \iota) \in \mathcal{K}$ we use the notation $\mathfrak{m} := (\mathfrak{m}_F, \varnothing)$, regarding $\mathfrak{m}_F$ as an ideal of $\mathcal{O}_K$. Let $R := \mathrm{im}(\mathbb{Z}_{(S)}G \to A)$ and let $V := A \otimes_{\mathbb{Q}G} W$. Let $\mathcal{M}$ be a set of representatives for the isomorphism classes of finite R-modules. Let $\mathcal{M}_V$ be a set of representatives for the isomorphism classes of finitely generated R-modules M with the property that $A \otimes_R M \cong V$. For each prime $\mathfrak{p}$ of F dividing $\mathfrak{m}_F$ let $T_\mathfrak{p}$ be a G-structured $F_\mathfrak{p}$-algebra such that the collection $T = (T_\mathfrak{p})_{\mathfrak{p} \mid \mathfrak{m}_F}$ is viable. Let

$$\mathcal{K}^T := \{\, (K, \iota) \in \mathcal{K} \mid K \otimes_F F_\mathfrak{p} \cong T_\mathfrak{p} \text{ for all } \mathfrak{p} \mid \mathfrak{m}_F \,\},$$

where the isomorphism is as G-structured $F_\mathfrak{p}$-algebras, and, for $B \in \mathbb{R}_{>0}$,

$$\mathcal{K}^T_{C \leq B} := \left\{ (K, \iota) \in \mathcal{K}^T \,\middle|\, C(K) \leq B \right\}.$$

We principally regard all this notation as fixed, except for possibly T, which in some instances we allow to vary in order to obtain statements on the full family $\mathcal{K}$ from the subfamilies $\mathcal{K}^T$. This is indicated by the use of a subscript or superscript T. Our main conjecture now is the following.

Conjecture 8.38. *Use Setup 8.37. Let $f \colon \mathcal{E}(U^\vee_{T,R}, \mathcal{M}_V) \to \mathbb{C}$ be 'reasonable'. Then the limit*

$$\operatorname{Av}(f) := \lim_{B \to \infty} \frac{\sum_{(K,\iota) \in \mathcal{K}^T_{C \leq B}} f([R \otimes_{\mathbb{Z}G} \mathrm{S}^{\mathrm{Ara}}_K(\mathfrak{m})^\vee])}{\left| \mathcal{K}^T_{C \leq B} \right|}$$

exists and equals $\mathbb{E}(f)$.

Here, for a function f to be called 'reasonable', we require the necessary condition that $\mathbb{E}(f)$ exists. Further than that, we do make precise what we mean by a 'reasonable' function and refer the reader to the discussion in [BL20, Section 7]. We refer to $\operatorname{Av}(f)$ as the *average* of f. Taking f to be the indicator function of $\Theta \in \mathcal{E}(U^\vee_{T,R}, \mathcal{M}_V)$, we obtain:

Corollary 8.39. *Assume that Conjecture 8.38 holds. Let $\Theta \in \mathcal{E}(U^\vee_{T,R}, \mathcal{M}_V)$. Then*

$$\lim_{B \to \infty} \frac{\left| \left\{ (K, \iota) \in \mathcal{K}^T_{C \leq B} \,\middle|\, [R \otimes_{\mathbb{Z}G} \mathrm{S}^{\mathrm{Ara}}_K(\mathfrak{m})^\vee] = \Theta \right\} \right|}{\left| \mathcal{K}^T_{C \leq B} \right|} = \mathbb{P}_T(\Theta).$$

Thus, by definition of $\mathbb{P}_T$, the conjecture should be understood as saying that for (K, ι) running over $\mathcal{K}^T$, the sequence $R \otimes_{\mathbb{Z}G} \mathrm{S}^{\mathrm{Ara}}_K(\mathfrak{m})^\vee$ behaves randomly in the sense of Principle 1.1.

9 Implications of the Main Conjecture

The aim of this chapter is to derive implications of Conjecture 8.38 for objects attached to a number field other than $R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee$. This is possible whenever the following three steps are performable. Say we are interested in the statistical behaviour of object X_K attached to $(K, \iota) \in \mathcal{K}^T$.

(1) Find a set $\mathcal{X}$ only depending on $\mathcal{K}^T$ such that for $(K, \iota) \in \mathcal{K}^T$, the object X_K can be identified with a unique element $[X_K] \in \mathcal{X}$. This 'constant' space of outcomes makes it possible to formulate statements about the distribution of the objects X_K which a priori may live in entirely different spaces.

(2) Construct a function $\xi\colon \mathcal{E}(U_{T,R}^\vee, \mathcal{M}_V) \to \mathcal{X}$ with $\xi([R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee]) = [X_K]$.

(3) For a 'reasonable' function $h\colon \mathcal{X} \to \mathbb{C}$, compute $\mathbb{E}(h \circ \xi)$.

If all this is possible, then Conjecture 8.38 applied to $f := h \circ \xi$ provides the statement

$$\lim_{B\to\infty} \frac{\sum_{(K,\iota)\in\mathcal{K}^T_{C\le B}} h([X_K])}{\left|\mathcal{K}^T_{C\le B}\right|} = \sum_{\Theta\in\mathcal{E}(U_{T,R}^\vee,\mathcal{M}_V)} (h\circ\xi)(\Theta)\cdot\mathbb{P}_T(\Theta) \tag{9.1}$$

on the distribution of the objects X_K. If $\mathcal{X}$ is countable, then we regard it as a discrete measurable space and we have

$$\begin{aligned}\sum_{\Theta\in\mathcal{E}(U_{T,R}^\vee,\mathcal{M}_V)} (h\circ\xi)(\Theta)\cdot\mathbb{P}_T(\Theta) &= \sum_{x\in\mathcal{X}}\sum_{\Theta\in\xi^{-1}(x)} h(x)\cdot\mathbb{P}_T(\Theta)\\ &= \sum_{x\in\mathcal{X}} h(x)\cdot\xi_*\mathbb{P}_T(x),\end{aligned}$$

so (9.1) becomes

$$\lim_{B\to\infty} \frac{\sum_{(K,\iota)\in\mathcal{K}^T_{C\le B}} h([X_K])}{\left|\mathcal{K}^T_{C\le B}\right|} = \sum_{x\in\mathcal{X}} h(x)\cdot\xi_*\mathbb{P}_T(x).$$

This means that the distribution of the objects X_K is governed by the pushforward distribution $\xi_*\mathbb{P}_T$.

In the subsections of this chapter, we will obtain the following items as consequences of Conjecture 8.38.

- Section 9.1: The distribution of $R \otimes_{\mathbb{Z}G} (\mathrm{Pic}_K^0)^\vee$ for (K,ι) running over $\mathcal{K}^T$ and $\mathcal{K}$.
- Section 9.2: The distribution of the sequence $R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee$ for $(K,\iota) \in \mathcal{K}^T$ for which the left hand term $R \otimes_{\mathbb{Z}G} (\mathrm{Pic}_K^0)^\vee$ is isomorphic to a fixed module $N \in \mathcal{M}_V$.
- Section 9.3: The distribution of $R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{fin}}(\mathfrak{m})^\vee$ for $(K,\iota) \in \mathcal{K}^T$ and for (K,ι) in certain finer subfamilies.

- Section 9.4: The distribution of the reduction map $\mathrm{id}_R \otimes \overline{\rho_K(\mathfrak{m})}$ for $(K, \iota) \in \mathcal{K}^T$ and for $(K, \iota) \in \mathcal{K}^T$ such that $R \otimes_{\mathbb{Z}G} (\mathrm{Pic}^0_K)^\vee$ is isomorphic to a fixed module $N \in \mathcal{M}_V$.
- Section 9.5: The average ℓ-torsion of $\mathrm{Cl}_K(\mathfrak{m})$ for G abelian, ℓ a prime with $\ell \nmid |G| \cdot |\mathrm{Cl}_F|$, and (K, ι) running over $\mathcal{K}^T$ and $\mathcal{K}$ defined using $S = \{\ell\}$.

Unless otherwise stated, we work with Setup 8.37.

9.1 Ideal Class Groups

We consider the case where $\mathfrak{m}_F = \mathcal{O}_F$ is the trivial modulus. Then there are no $\mathfrak{p} \mid \mathfrak{m}_F$, so $\mathcal{K}^T = \mathcal{K}$. Being an empty product, $\mathcal{O}_T$ is the zero ring, and so U_T and $U_{T,R}$ are trivial modules. It follows that for any $N \in \mathcal{M}_V$, $\mathrm{Ext}^1_R(U^\vee_{T,R}, N)$ is trivial. Hence, there is a canonical bijection between $\mathcal{M}_V$ and $\mathcal{E}(U^\vee_{T,R}, \mathcal{M}_V)$ which without loss of generality we can assume to be given by

$$\mathcal{M}_V \xrightarrow{\sim} \mathcal{E}(U^\vee_{T,R}, \mathcal{M}_V), \ M \mapsto \underline{M}\colon \ 0 \to M \xrightarrow{\mathrm{id}} M \to 0 \to 0.$$

By Theorem 8.34 we then have that $\mathbb{P}_T(\underline{M}) = \mathbb{P}^{\mathrm{BL}}(M)$ for $M \in \mathcal{M}_V$. Moreover, if $f\colon \mathcal{M}_V \to \mathbb{C}$ is a 'reasonable' function, then we obtain a corresponding 'reasonable' function $\underline{f}\colon \mathcal{E}(U^\vee_{T,R}, \mathcal{M}_V) \to \mathbb{C}$ with $\underline{f}(\underline{M}) = f(M)$ for $M \in \mathcal{M}_V$. This shows that our main conjecture implies the Cohen–Lenstra–Martinet Heuristics as phrased in [BL20, Conjecture 1.5]:

Corollary 9.2. *Conjecture 8.38 implies Conjecture 1.7.*

In fact, we do get a stronger statement under slightly stronger assumptions. For $(K, \iota) \in \mathcal{K}$ denote by $[R \otimes_{\mathbb{Z}G} (\mathrm{Pic}^0_K)^\vee]$ the unique element of $\mathcal{M}_V$ that is isomorphic to $R \otimes_{\mathbb{Z}G} (\mathrm{Pic}^0_K)^\vee$.

Corollary 9.3. *Let $f\colon \mathcal{M}_V \to \mathbb{C}$ be 'reasonable'. Let P be a finite set of primes of F and let $T = (T_\mathfrak{p})_{\mathfrak{p} \in P}$ be a viable collection of G-structured $F_\mathfrak{p}$-algebras. Assume that Conjecture 8.38 holds for the modulus $\prod_{\mathfrak{p} \in P} \mathfrak{p}$, the collection T and the function $f \circ \sigma$, where $\sigma\colon \mathcal{E}(U^\vee_{T,R}, \mathcal{M}_V) \to \mathcal{M}_V$ is the function from Theorem 8.34 for the modulus $\prod_{\mathfrak{p} \in P} \mathfrak{p}$. Then*

$$\lim_{B \to \infty} \frac{\sum_{(K,\iota) \in \mathcal{K}^T_{C \le B}} f([R \otimes_{\mathbb{Z}G} (\mathrm{Pic}^0_K)^\vee])}{\left|\mathcal{K}^T_{C \le B}\right|} = \sum_{N \in \mathcal{M}_V} f(N) \cdot \mathbb{P}^{\mathrm{BL}}(N).$$

Proof. Apply Conjecture 8.38 to $f \circ \sigma$ and use Theorem 8.34 to obtain the expression above on the right hand side for $\mathbb{E}(f \circ \sigma)$. □

9.2 Sequences with Fixed Left Hand Side

In our model, we have defined the family $\mathcal{K}^T$ in such a way that for $(K,\iota) \in \mathcal{K}^T$, the right hand term of $R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee$ is constant, always being isomorphic via a G-equivariant $\mathcal{O}_F$-algebra isomorphism to $U_{T,R}^\vee$, cf. Proposition 8.25. In this section, we investigate the situation in which we additionally fix the left hand module in $R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee$.

Definition 9.4. Let $N \in \mathcal{M}_V$. We define $\mathcal{K}^T(N)$ to be the set of $(K,\iota) \in \mathcal{K}^T$ with $R \otimes_{\mathbb{Z}G} (\mathrm{Pic}_K^0)^\vee \cong N$.

Note that we have

$$(K,\iota) \in \mathcal{K}^T(N) \qquad \Longleftrightarrow \qquad [R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee] \in \mathcal{E}(U_{T,R}^\vee, N)$$

which means that when modelling $R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee$, the subfamily $\mathcal{K}^T(N)$ of $\mathcal{K}^T$ corresponds to the subspace $\mathcal{E}(U_{T,R}^\vee, N)$ of $\mathcal{E}(U_{T,R}^\vee, \mathcal{M}_V)$. This observation allows us to derive a statement about the distribution of $R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee$ when (K,ι) ranges over $\mathcal{K}^T(N)$ from our conjecture and the knowledge about the probability distribution induced by $\mathbb{P}_T$ on $\mathcal{E}(U_{T,R}^\vee, N)$.

Proposition 9.5. *Let $N \in \mathcal{M}_V$. Then the restriction and renormalisation $\mathbb{P}_{T,N}$ of $\mathbb{P}_T$ to $\mathcal{E}(U_{T,R}^\vee, N)$ is given by*

$$\mathbb{P}_{T,N}(\Theta) = \frac{|[\Theta]_{G\text{-eq. alg.}}|}{\left|\mathrm{Ext}_R^1(U_{T,R}^\vee, N)\right|}$$

for $\Theta \in \mathcal{E}(U_{T,R}^\vee, N)$.

Proof. This is immediate from Remark 8.35. □

Corollary 9.6. *Let $N \in \mathcal{M}_V$ and let $f\colon \mathcal{E}(U_{T,R}^\vee, N) \to \mathbb{C}$ be 'reasonable'. Assume that Conjecture 8.38 holds for $\mathbb{1}_{\mathcal{E}(U_{T,R}^\vee, N)}$ and the function $\widetilde{f}\colon \mathcal{E}(U_{T,R}^\vee, \mathcal{M}_V) \to \mathbb{C}$ that extends f by zero. Then*

$$\lim_{B\to\infty} \frac{\sum_{(K,\iota)\in\mathcal{K}^T_{C\le B}(N)} f([R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee])}{\left|\mathcal{K}^T_{C\le B}(N)\right|} = \sum_{\Theta\in\mathcal{E}(U_{T,R}^\vee, N)} f(\Theta)\cdot \mathbb{P}_{T,N}(\Theta).$$

Proof. We have

$$\mathbb{E}(\widetilde{f}) = \sum_{\Theta\in\mathcal{E}(U_{T,R}^\vee, N)} f(\Theta)\cdot\mathbb{P}_T(\Theta) = \mathbb{P}^{\mathrm{BL}}(N)\cdot \sum_{\Theta\in\mathcal{E}(U_{T,R}^\vee, N)} f(\Theta)\cdot\mathbb{P}_{T,N}(\Theta),$$

while

$$\mathrm{Av}(\widetilde{f}) = \lim_{B\to\infty} \frac{\sum_{(K,\iota)\in\mathcal{K}^T_{C\le B}(N)} f([R\otimes_{\mathbb{Z}G}\mathrm{S}^{\mathrm{Ara}}_K(\mathfrak{m})^\vee])}{\left|\mathcal{K}^T_{C\le B}(N)\right|} \cdot \frac{\left|\mathcal{K}^T_{C\le B}(N)\right|}{\left|\mathcal{K}^T_{C\le B}\right|}.$$

Using the function $\mathbb{1}_{\mathcal{E}(U^\vee_{T,R},N)}$ in Conjecture 8.38 gives

$$\lim_{B\to\infty} \frac{\left|\mathcal{K}^T_{C\le B}(N)\right|}{\left|\mathcal{K}^T_{C\le B}\right|} = \mathbb{P}^{\mathrm{BL}}(N),$$

and the claim follows. □

Corollary 9.7. *Assume that Conjecture 8.38 holds. Let $N \in \mathcal{M}_V$ and let $\Theta \in \mathcal{E}(U^\vee_{T,R}, N)$. Then*

$$\lim_{B\to\infty} \frac{\left|\left\{ (K,\iota)\in\mathcal{K}^T_{C\le B}(N) \;\middle|\; [R\otimes_{\mathbb{Z}G}\mathrm{S}^{\mathrm{Ara}}_K(\mathfrak{m})^\vee] = \Theta \right\}\right|}{\left|\mathcal{K}^T_{C\le B}(N)\right|} = \frac{|[\Theta]_{G\text{-eq. alg.}}|}{\left|\mathrm{Ext}^1_R(U^\vee_{T,R}, N)\right|}.$$

9.3 Ray Class Group Sequences

The aim of this section is to describe the consequences of Conjecture 8.38 for the distribution of the dual ray class group sequence $R\otimes_{\mathbb{Z}G}\mathrm{S}^{\mathrm{fin}}_K(\mathfrak{m})^\vee$, which we recall is given by

$$0 \longrightarrow R\otimes_{\mathbb{Z}G}\mathrm{Cl}^\vee_K \longrightarrow R\otimes_{\mathbb{Z}G}\mathrm{Cl}_K(\mathfrak{m})^\vee \longrightarrow R\otimes_{\mathbb{Z}G}\left(\frac{(\mathcal{O}_K/\mathfrak{m}_0)^\times}{\rho(\mathcal{O}_K^\times)}\right)^\vee \longrightarrow 0.$$

For this, we imitate the approach of [BP25]. We first deal with item (1) from the beginning of this chapter and investigate by which space the sequences $R\otimes_{\mathbb{Z}G}\mathrm{S}^{\mathrm{fin}}_K(\mathfrak{m})^\vee$ are modelled as (K,ι) runs over $\mathcal{K}^T$.

Lemma 8.19 shows that for $(K,\iota)\in\mathcal{K}^T$, the left hand side of $R\otimes_{\mathbb{Z}G}\mathrm{S}^{\mathrm{fin}}_K(\mathfrak{m})^\vee$ is the torsion submodule of $R\otimes_{\mathbb{Z}G}(\mathrm{Pic}^0_K)^\vee$. This means that when running over the subfamily $\mathcal{K}^T(N)$ of $\mathcal{K}^T$ for $N\in\mathcal{M}_V$, then via an isomorphism $R\otimes_{\mathbb{Z}G}(\mathrm{Pic}^0_K)^\vee \cong N$ we may identify $R\otimes_{\mathbb{Z}G}\mathrm{Cl}^\vee_K$ with N_{tors}.

We also have information on the right hand side of $R\otimes_{\mathbb{Z}G}\mathrm{S}^{\mathrm{fin}}_K(\mathfrak{m})^\vee$: By Section 7.3.2 and Proposition 7.24, it is given by the kernel of

$$\omega_{\mathrm{d}}(R\otimes_{\mathbb{Z}G}\mathrm{S}^{\mathrm{Ara}}_K(\mathfrak{m})^\vee)\colon R\otimes_{\mathbb{Z}G}\left(\frac{(\mathcal{O}_K/\mathfrak{m}_0)^\times}{\rho(\mu(K))}\right)^\vee \to \left(\left(\frac{R\otimes_{\mathbb{Z}G}(\mathrm{Pic}^0_K)^\vee}{(R\otimes_{\mathbb{Z}G}(\mathrm{Pic}^0_K)^\vee)_{\mathrm{tors}}}\right)^*\right)^\vee.$$

Again, it is useful to first consider the subfamily $\mathcal{K}^T(N)$ of $\mathcal{K}^T$ for $N\in\mathcal{M}_V$. Here, if $(K,\iota)\in\mathcal{K}^T(N)$, then via an isomorphism $R\otimes_{\mathbb{Z}G}(\mathrm{Pic}^0_K)^\vee \cong N$ we may identify

$\left(\left(\frac{R\otimes_{\mathbb{Z}G}(\mathrm{Pic}^0_K)^\vee}{(R\otimes_{\mathbb{Z}G}(\mathrm{Pic}^0_K)^\vee)_{\mathrm{tors}}}\right)^*\right)^\vee$ with $((N/N_{\mathrm{tors}})^*)^\vee$ and as explained in Construction 8.28, we may identify $R\otimes_{\mathbb{Z}G}\left(\frac{(\mathcal{O}_K/\mathfrak{m}_0)^\times}{\rho(\mu(K))}\right)^\vee$ with $U^\vee_{T,R}$ via a G-equivariant $\mathcal{O}_F$-algebra isomorphism. Thus, we can identify $\omega_{\mathrm{d}}(R\otimes_{\mathbb{Z}G}\mathrm{S}^{\mathrm{Ara}}_K(\mathfrak{m})^\vee)$ with a homomorphism $\omega \in \mathrm{Hom}_R(U^\vee_{T,R}, ((N/N_{\mathrm{tors}})^*)^\vee$ in such a way that the isomorphism $R \otimes_{\mathbb{Z}G} \left(\frac{(\mathcal{O}_K/\mathfrak{m}_0)^\times}{\rho(\mu(K))}\right)^\vee \cong U^\vee_{T,R}$ restricts to an isomorphism between $R \otimes_{\mathbb{Z}G} \left(\frac{(\mathcal{O}_K/\mathfrak{m}_0)^\times}{\rho(\mathcal{O}_K^\times)}\right)^\vee$ and $\ker\omega$.

$$\begin{tikzcd}
0 \arrow[d] & 0 \arrow[d, dotted] \\
R \otimes_{\mathbb{Z}G} \left(\frac{(\mathcal{O}_K/\mathfrak{m}_0)^\times}{\rho(\mathcal{O}_K^\times)}\right)^\vee \arrow[r, dotted, "\sim"] \arrow[d] & \ker\omega \arrow[d, dotted] \\
R \otimes_{\mathbb{Z}G} \left(\frac{(\mathcal{O}_K/\mathfrak{m}_0)^\times}{\rho(\mu(K))}\right)^\vee \arrow[r, "\sim"] \arrow[d, "\omega_{\mathrm{d}}(R\otimes_{\mathbb{Z}G}\mathrm{S}^{\mathrm{Ara}}_K(\mathfrak{m})^\vee)"'] & U^\vee_{T,R} \arrow[d, dashed, "\omega"] \\
\left(\left(\frac{R\otimes_{\mathbb{Z}G}(\mathrm{Pic}^0_K)^\vee}{(R\otimes_{\mathbb{Z}G}(\mathrm{Pic}^0_K)^\vee)_{\mathrm{tors}}}\right)^*\right)^\vee \arrow[r, "\sim"] & ((N/N_{\mathrm{tors}})^*)^\vee
\end{tikzcd}$$

This suggests to subdivide $\mathcal{K}^T(N)$ even further in the following way:

Definition 9.8. Let $N \in \mathcal{M}_V$. Let $\mathcal{H}_N$ be a system of representatives for

$$\mathrm{Hom}_R(U^\vee_{T,R}, ((N/N_{\mathrm{tors}})^*)^\vee)/(\mathrm{Aut}_{G\text{-eq. alg.}}(U^\vee_{T,R}) \times \mathrm{Aut}\, N).$$

For $\omega \in \mathcal{H}_N$ we define $\mathcal{K}^T(N,\omega)$ to be the set of $(K,\iota) \in \mathcal{K}^T$ with $R \otimes_{\mathbb{Z}G} (\mathrm{Pic}^0_K)^\vee \cong N$ and such that there are an R-module isomorphism $\chi\colon R \otimes_{\mathbb{Z}G} (\mathrm{Pic}^0_K)^\vee \xrightarrow{\sim} N$ and an isomorphism

$$\alpha\colon R \otimes_{\mathbb{Z}G} \left(\frac{(\mathcal{O}_K/\mathfrak{m}_0)^\times}{\rho(\mu(K))}\right)^\vee \xrightarrow{\sim} \left(R \otimes_{\mathbb{Z}G} \frac{(\mathcal{O}_K/\mathfrak{m}_0)^\times}{\rho(\mu(K))}\right)^\vee \xrightarrow{\sim} U^\vee_{T,R},$$

where the left hand map is the natural isomorphism from Proposition 7.17 and where the right hand map is a G-equivariant $\mathcal{O}_F$-algebra isomorphism induced from an isomorphism from Proposition 8.25, that make the diagram

$$\begin{tikzcd}
R \otimes_{\mathbb{Z}G} \left(\frac{(\mathcal{O}_K/\mathfrak{m}_0)^\times}{\rho(\mu(K))}\right)^\vee \arrow[r, "\alpha"] \arrow[d, "\omega_{\mathrm{d}}(R\otimes_{\mathbb{Z}G}\mathrm{S}^{\mathrm{Ara}}_K(\mathfrak{m})^\vee)"'] & U^\vee_{T,R} \arrow[d, "\omega"] \\
\left(\left(\frac{R\otimes_{\mathbb{Z}G}(\mathrm{Pic}^0_K)^\vee}{(R\otimes_{\mathbb{Z}G}(\mathrm{Pic}^0_K)^\vee)_{\mathrm{tors}}}\right)^*\right)^\vee \arrow[r, "((\overline{\chi})^*)^\vee"'] & ((N/N_{\mathrm{tors}})^*)^\vee
\end{tikzcd}$$

commute.

Construction 9.9. Let $(K,\iota) \in \mathcal{K}^T(N,\omega)$. Then by choosing isomorphisms χ and α that make the above diagram commute, we can identify $R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{fin}}(\mathfrak{m})^\vee$ with an element of $\mathrm{Ext}^1_R(\ker\omega, N_{\mathrm{tors}})$. While this identification depends on the choice of χ and α, we may uniquely identify $R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{fin}}(\mathfrak{m})^\vee$ with an element of $\mathrm{Ext}^1_R(\ker\omega, N_{\mathrm{tors}})/(H_\omega \times \mathrm{Aut}\, N_{\mathrm{tors}})$, where

$$H_\omega := \left\{ \kappa \in \mathrm{Aut}(\ker\omega) \,\middle|\, \exists\, \upsilon \in \mathrm{Aut}_{G\text{-eq. alg.}}(U^\vee_{T,R}) : \kappa = \upsilon\big|_{\ker\omega} \right\}.$$

This way, for $(K,\iota) \in \mathcal{K}^T$, we may uniquely identify $R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{fin}}(\mathfrak{m})^\vee$ with an element of

$$\bigsqcup_{N \in \mathcal{M}_V} \bigsqcup_{\omega \in \mathcal{H}_N} \mathrm{Ext}^1_R(\ker\omega, N_{\mathrm{tors}})/(H_\omega \times \mathrm{Aut}\, N_{\mathrm{tors}}).$$

We denote this element by $[R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{fin}}(\mathfrak{m})^\vee]$.

Definition 9.10. For $N \in \mathcal{M}_V$ and $\omega \in \mathcal{H}_N$ we let $\mathcal{E}_{\mathrm{tors}}(U^\vee_{T,R}, N, \omega)$ be a system of representatives for $\mathrm{Ext}^1_R(\ker\omega, N_{\mathrm{tors}})/(H_\omega \times \mathrm{Aut}\, N_{\mathrm{tors}})$. Define

$$\begin{aligned}
\mathcal{E}_{\mathrm{tors}}(U^\vee_{T,R}, N) &:= \bigsqcup_{\omega \in \mathcal{H}_N} \mathcal{E}_{\mathrm{tors}}(U^\vee_{T,R}, N, \omega),\\
\mathcal{E}_{\mathrm{tors}}(U^\vee_{T,R}, \mathcal{M}_V) &:= \bigsqcup_{N \in \mathcal{M}_V} \mathcal{E}_{\mathrm{tors}}(U^\vee_{T,R}, N).
\end{aligned}$$

As explained above, these spaces model the sequence $R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{fin}}(\mathfrak{m})^\vee$ for number fields in the families $\mathcal{K}^T(N,\omega)$, $\mathcal{K}^T(N)$ and $\mathcal{K}^T$, respectively. To finish this discussion, we note the subspace of $\mathcal{E}(U^\vee_{T,R}, \mathcal{M}_V)$ that corresponds to $\mathcal{K}^T(N,\omega)$ when modelling $R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee$.

Definition 9.11. Let $N \in \mathcal{M}_V$. Denote by

$$\omega_{\mathrm{d},N} := \omega_{\mathrm{d},R}^{U^\vee_{T,R},N} \colon \mathrm{Ext}^1_R(U^\vee_{T,R}, N) \to \mathrm{Hom}_R(U^\vee_{T,R}, ((N/N_{\mathrm{tors}})^*)^\vee)$$

the homomorphism from Construction 7.22 and by $\overline{\omega_{\mathrm{d},N}}$ the induced map on $(\mathrm{Aut}_{G\text{-eq. alg.}}(U^\vee_{T,R}) \times \mathrm{Aut}\, N)$-isomorphism classes, which is well-defined by Proposition 7.23.

Proposition 9.12. *Let $N \in \mathcal{M}_V$ and $\omega \in \mathcal{H}_N$. Then*

$$(K,\iota) \in \mathcal{K}^T(N,\omega) \qquad\Longleftrightarrow\qquad [R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee] \in \overline{\omega_{\mathrm{d},N}}^{-1}([\omega]).$$

Proof. This follows from naturality of $\omega_{\mathrm{d},N}$, see Proposition 7.23. □

Definition 9.13. Let $N \in \mathcal{M}_V$ and $\omega \in \mathcal{H}_N$. Denote by $\mathcal{E}(U^\vee_{T,R}, N, \omega)$ the subset of $\mathcal{E}(U^\vee_{T,R}, N)$ that corresponds to $\overline{\omega_{\mathrm{d},N}}^{-1}([\omega])$.

In order to derive implications on the distribution of $R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{fin}}(\mathfrak{m})^\vee$ from our main conjecture, we next take care of item (2) from the beginning of this chapter and set out to define a function

$$\tau\colon \mathcal{E}(U_{T,R}^\vee, \mathcal{M}_V) \to \mathcal{E}_{\mathrm{tors}}(U_{T,R}^\vee, \mathcal{M}_V)$$

with $\tau([R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee]) = [R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{fin}}(\mathfrak{m})^\vee]$. Then the pushforward distribution of $\mathbb{P}_T$ under τ will give the distribution of $R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{fin}}(\mathfrak{m})^\vee$.

For the construction of τ we will work on the subsets $\mathcal{E}(U_{T,R}^\vee, N, \omega)$ that partition $\mathcal{E}(U_{T,R}^\vee, \mathcal{M}_V)$. The map τ should be given by mapping a short exact sequence to its torsion sequence, defined in Section 7.3.1. We split the construction into two parts, where we keep track of the homomorphism whose kernel determines the Ext-space of the torsion sequence in the first step.

Definition 9.14. Let $N \in \mathcal{M}_V$. Define

$$\Sigma(U_{T,R}^\vee, N) := \left\{ (\omega, \Delta) \,\middle|\, \omega \in \mathrm{Hom}_R(U_{T,R}^\vee, ((N/N_{\mathrm{tors}})^*)^\vee), \Delta \in \mathrm{Ext}_R^1(\ker \omega, N_{\mathrm{tors}}) \right\}.$$

We have a natural action of $\mathrm{Aut}_{G\text{-eq. alg.}}(U_{T,R}^\vee) \times \mathrm{Aut}\, N$ on $\Sigma(U_{T,R}^\vee, N)$ defined by

$$(f,g).(\omega,\Delta) := \Big((f, (\overline{g}^*)^\vee).\omega, (g_{\mathrm{tors}})_* \circ (f^{-1}|_{\ker((f,(\overline{g}^*)^\vee).\omega)})^*(\Delta) \Big)$$

for $f \in \mathrm{Aut}_{G\text{-eq. alg.}}(U_{T,R}^\vee)$, $g \in \mathrm{Aut}\, N$ and $(\omega, \Delta) \in \Sigma(U_{T,R}^\vee, N)$. We also define maps

$$\pi_N\colon \Sigma(U_{T,R}^\vee, N) \to \mathrm{Hom}_R(U_{T,R}^\vee, ((N/N_{\mathrm{tors}})^*)^\vee), \ (\omega, \Delta) \mapsto \omega$$

and

$$\sigma_N\colon \mathrm{Ext}_R^1(U_{T,R}^\vee, N) \to \Sigma(U_{T,R}^\vee, N), \ \Theta \mapsto (\omega_{\mathrm{d},N}(\Theta), \Theta_{\mathrm{tors}}).$$

Here, if Θ is given by the short exact sequence $0 \to N \xrightarrow{\gamma} L \xrightarrow{\delta} U_{T,R}^\vee \to 0$, we use Proposition 7.24 to regard Θ_{tors} as the short exact sequence

$$0 \longrightarrow N_{\mathrm{tors}} \xrightarrow{\gamma|_{N_{\mathrm{tors}}}} L_{\mathrm{tors}} \xrightarrow{\delta|_{L_{\mathrm{tors}}}} \ker \omega_{\mathrm{d},N}(\Theta) \longrightarrow 0.$$

We obtain the following generalised version of [BP25, Proposition 3.8].

Proposition 9.15. *Let $N \in \mathcal{M}_V$. Then π_N and σ_N are $(\mathrm{Aut}_{G\text{-eq. alg.}}(U_{T,R}^\vee) \times \mathrm{Aut}\, N)$-equivariant and surjective. Moreover, for $\omega \in \mathrm{Hom}_R(U_{T,R}^\vee, ((N/N_{\mathrm{tors}})^*)^\vee)$ it holds that*

$$\left|\pi_N^{-1}(\omega)\right| = \left|\mathrm{Ext}_R^1(\ker \omega, N_{\mathrm{tors}})\right|$$

and for $(\omega, \Delta) \in \Sigma(U_{T,R}^\vee, N)$ it holds that

$$\left|\sigma_N^{-1}(\omega, \Delta)\right| = \frac{\left|\mathrm{Ext}_R^1(U_{T,R}^\vee, N_{\mathrm{tors}})\right|}{\left|\mathrm{Ext}_R^1(\ker \omega, N_{\mathrm{tors}})\right|}.$$

Proof. The claims on π_N are clear, so we just investigate σ_N. To check equivariance, let $\Theta \in \operatorname{Ext}^1_R(U^\vee_{T,R}, N)$, $f \in \operatorname{Aut}_{G\text{-eq. alg.}}(U^\vee_{T,R})$ and $g \in \operatorname{Aut} N$. We know from Proposition 7.23 that $\omega_{\mathrm{d},N}((f,g).\Theta) = (f, (\overline{g}^*)^\vee).\omega_{\mathrm{d},N}(\Theta)$. To check equivariance in the second component, write

$$\Theta\colon \qquad 0 \longrightarrow N \xrightarrow{\gamma} L \xrightarrow{\delta} U^\vee_{T,R} \longrightarrow 0.$$

In the following, we use the notation $(-)'$ for maps as laid out in Construction 2.7. One readily verifies that the map

$$L_{\mathrm{tors}} \to \frac{N_{\mathrm{tors}} \oplus (L_{\mathrm{tors}} \times_{\ker \omega_{\mathrm{d}}(\Theta)} \ker \omega_{\mathrm{d}}((f,g).\Theta))}{\left\{\, (g(n), -(\gamma|_{N_{\mathrm{tors}}})'(n)) \,\middle|\, n \in N_{\mathrm{tors}} \,\right\}}, \; x \mapsto \overline{(0, (x, f \circ \delta(x)))},$$

makes the diagram

$$\begin{tikzcd}
0 \arrow[r] & N_{\mathrm{tors}} \arrow[r, "(\gamma \circ g^{-1})|_{N_{\mathrm{tors}}}"] \arrow[d, equal] & L_{\mathrm{tors}} \arrow[r, "(f\circ\delta)'"] \arrow[d] & \ker(\omega_{\mathrm{d}}((f,g).\Theta)) \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & N_{\mathrm{tors}} \arrow[r] & \frac{N_{\mathrm{tors}} \oplus (L_{\mathrm{tors}} \times_{\ker \omega_{\mathrm{d}}(\Theta)} \ker \omega_{\mathrm{d}}((f,g).\Theta))}{\left\{ (g(n), -(\gamma|_{N_{\mathrm{tors}}})'(n)) \,\middle|\, n \in N_{\mathrm{tors}} \right\}} \arrow[r] & \ker(\omega_{\mathrm{d}}((f,g).\Theta)) \arrow[r] & 0
\end{tikzcd}$$

commute, in which the upper sequence is $((f,g).\Theta)_{\mathrm{tors}}$ and the lower sequence is $(g_{\mathrm{tors}})_* \circ (f^{-1}|_{\ker((f,(\overline{g}^*)^\vee).\omega_{\mathrm{d}}(\Theta))})^*(\Theta_{\mathrm{tors}})$. This shows the equivariance of σ_N.

To show surjectivity, let $(\omega, \Delta) \in \Sigma(U^\vee_{T,R}, N)$. Denote by $i\colon N_{\mathrm{tors}} \hookrightarrow N$ and $j\colon \ker \omega \hookrightarrow U^\vee_{T,R}$ the inclusions. We have a commutative diagram

$$\begin{tikzcd}
\operatorname{Ext}^1_R(U^\vee_{T,R}, N_{\mathrm{tors}}) \arrow[r, hook, "i_*"] \arrow[d, two heads, "j^*"] & \operatorname{Ext}^1_R(U^\vee_{T,R}, N) \arrow[d, two heads, "j^*"] \\
\operatorname{Ext}^1_R(\ker \omega, N_{\mathrm{tors}}) \arrow[r, hook, "i_*"] & \operatorname{Ext}^1_R(\ker \omega, N),
\end{tikzcd}$$

in which the vertical maps are surjective by Proposition 3.34 and the horizontal maps are injective as N/N_{tors} is torsionfree.

We claim that for $\Theta \in \operatorname{Ext}^1_R(U^\vee_{T,R}, N)$ with $\omega_{\mathrm{d},N}(\Theta) = \omega$ it holds that

$$\Theta_{\mathrm{tors}} = \Delta \qquad \Longleftrightarrow \qquad j^*(\Theta) = i_*(\Delta). \tag{9.16}$$

To prove this statement, write

$$\Delta\colon \qquad 0 \longrightarrow N_{\mathrm{tors}} \xrightarrow{\varepsilon} W \xrightarrow{\varphi} \ker \omega \longrightarrow 0$$

and

$$\Theta\colon \qquad 0 \longrightarrow N \xrightarrow{\gamma} L \xrightarrow{\delta} U^\vee_{T,R} \longrightarrow 0.$$

For the forward implication, suppose that $\Theta_{\mathrm{tors}} = \Delta$. Then there is a homomorphism $\eta\colon W \to L_{\mathrm{tors}}$ that makes the diagram

$$\begin{tikzcd}
\Delta\colon & 0 \arrow[r] & N_{\mathrm{tors}} \arrow[r, "\varepsilon"] \arrow[d, equal] & W \arrow[r, "\varphi"] \arrow[d, "\eta"] & \ker\omega \arrow[r] \arrow[d, equal] & 0 \\
\Theta_{\mathrm{tors}}\colon & 0 \arrow[r] & N_{\mathrm{tors}} \arrow[r, "\gamma|_{N_{\mathrm{tors}}}"'] & L_{\mathrm{tors}} \arrow[r, "\delta'"'] & \ker\omega \arrow[r] & 0
\end{tikzcd}$$

commute. One checks that the map

$$\kappa\colon \frac{N \oplus W}{\{\,(n, -\varepsilon(n)) \,|\, n \in N_{\mathrm{tors}}\,\}} \to L \times_{U_{T,R}^{\vee}} \ker\omega,\ \overline{(n,w)} \mapsto (\gamma(n) + \eta(w), \varphi(w))$$

is well-defined and renders the diagram

$$\begin{tikzcd}
i_*(\Delta)\colon & 0 \arrow[r] & N \arrow[r] \arrow[d, equal] & \frac{N\oplus W}{\{\,(n,-\varepsilon(n)) \,|\, n\in N_{\mathrm{tors}}\,\}} \arrow[r, "\varphi'"] \arrow[d, "\kappa"] & \ker\omega \arrow[r] \arrow[d, equal] & 0 \\
j^*(\Theta)\colon & 0 \arrow[r] & N \arrow[r, "\gamma'"'] & L \times_{U_{T,R}^{\vee}} \ker\omega \arrow[r] & \ker\omega \arrow[r] & 0
\end{tikzcd}$$

commutative, which proves the forward implication. Conversely, suppose that $j^*(\Theta) = i_*(\Delta)$. Then there is a homomorphism κ that makes the diagram above commute. Let $\iota_W\colon W \to \frac{N\oplus W}{\{\,(n,-\varepsilon(n)) \,|\, n\in N_{\mathrm{tors}}\,\}}$ and $\pi_L\colon L \times_{U_{T,R}^{\vee}} \ker\omega \to L$ be the natural maps and define

$$\eta := \pi_L \circ \kappa \circ \iota_W \colon W \to L.$$

Since N_{tors} and $\ker\omega$ are finite, so is W, whence the image of η is in fact contained in L_{tors}. One verifies that η defines an equivalence between Δ and Θ_{tors}. This completes the proof of (9.16).

By Proposition 7.23, $\omega_{\mathrm{d},N}$ is surjective with kernel $i_*(\mathrm{Ext}^1_R(U_{T,R}^{\vee}, N_{\mathrm{tors}}))$. Hence, we can choose $\Theta' \in \mathrm{Ext}^1_R(U_{T,R}^{\vee}, N)$ with $\omega_{\mathrm{d},N}(\Theta') = \omega$. Define $\Delta' := (\Theta')_{\mathrm{tors}} \in \mathrm{Ext}^1_R(\ker\omega, N_{\mathrm{tors}})$. Since j^* is surjective, there is $\widetilde{\Delta} \in \mathrm{Ext}^1_R(U_{T,R}^{\vee}, N_{\mathrm{tors}})$ with $j^*(\widetilde{\Delta}) = \Delta - \Delta'$. Define $\Theta := \Theta' + i_*(\widetilde{\Delta}) \in \mathrm{Ext}^1_R(U_{T,R}^{\vee}, N)$. Then $\omega_{\mathrm{d},N}(\Theta) = \omega_{\mathrm{d},N}(\Theta') = \omega$ and by (9.16) further

$$j^*(\Theta) = j^*(\Theta') + j^* \circ i_*(\widetilde{\Delta}) = i_*(\Delta') + i_*(\Delta - \Delta') = i_*(\Delta).$$

Using again (9.16), this shows that $\sigma(\Theta) = (\omega, \Delta)$. So σ_N is surjective. The criterion (9.16) also shows that

$$\sigma_N^{-1}(\omega, \Delta) = \omega_{\mathrm{d},N}^{-1}(\omega) \cap j^{-1}(i_*(\Delta)) = \left\{\, \Theta + i_*(\widetilde{\Theta}) \,\middle|\, \widetilde{\Theta} \in \ker(j^* \circ i_*) \,\right\}$$

which gives $\left|\sigma_N^{-1}(\omega, \Delta)\right| = |\ker(j^* \circ i_*)|$. But by injectivity of i_* we have

$$\ker(j^* \circ i_*) = \ker(i_* \circ j^*) = \ker j^*.$$

The claim on $\left|\sigma_N^{-1}(\omega, \Delta)\right|$ now follows from the first isomorphism theorem. □

Construction 9.17. Let $N \in \mathcal{M}_V$ and let $\omega \in \mathcal{H}_N$. Since $\pi_N \circ \sigma_N = \omega_{\mathrm{d},N}$ and σ_N is surjective by Proposition 9.15, we have $\sigma_N(\omega_{\mathrm{d},N}^{-1}([\omega])) = \pi_N^{-1}([\omega])$. We now define a map

$$\varepsilon_{N,\omega} \colon \pi_N^{-1}([\omega]) \to \operatorname{Ext}^1_R(\ker\omega, N_{\mathrm{tors}})$$

as follows: For each $\psi \in [\omega]$ we fix $f_\psi \in \operatorname{Aut}_{G\text{-eq. alg.}}(U^\vee_{T,R})$ and $g_\psi \in \operatorname{Aut} N$ with

$$\psi = (f_\psi, (\overline{g_\psi}^*)^\vee).\omega = ((\overline{g_\psi}^*)^\vee) \circ \omega \circ f_\psi^{-1}.$$

Then $f_\psi|_{\ker\omega}$ defines an isomorphism from $\ker\omega$ onto $\ker\psi$ and we define $\varepsilon_{N,\omega}(\psi, \Delta) := (f_\psi|_{\ker\omega})^*(\Delta)$.

By Proposition 9.15, both maps π_N and σ_N factor through the $(\operatorname{Aut}_{G\text{-eq. alg.}}(U^\vee_{T,R}) \times \operatorname{Aut} N)$-actions on their respective domain and codomain. We denote the induced maps on the sets of $(\operatorname{Aut}_{G\text{-eq. alg.}}(U^\vee_{T,R}) \times \operatorname{Aut} N)$-equivalence classes by $\overline{\pi_N}$ and $\overline{\sigma_N}$, respectively. Moreover, one sees from the definition of the action of $\operatorname{Aut}_{G\text{-eq. alg.}}(U^\vee_{T,R}) \times \operatorname{Aut} N$ on $\Sigma(U^\vee_{T,R}, N)$ that $\varepsilon_{N,\omega}$ descends to a map on equivalence classes

$$\overline{\varepsilon_{N,\omega}} \colon \overline{\pi_N}^{-1}([\omega]) \to \operatorname{Ext}^1_R(\ker\omega, N_{\mathrm{tors}})/(H_\omega \times \operatorname{Aut} N_{\mathrm{tors}}).$$

We define

$$\tau_{N,\omega} \colon \overline{\omega_{\mathrm{d},N}}^{-1}([\omega]) \xrightarrow{\overline{\sigma_N}} \overline{\pi_N}^{-1}([\omega]) \xrightarrow{\overline{\varepsilon_{N,\omega}}} \operatorname{Ext}^1_R(\ker\omega, N_{\mathrm{tors}})/(H_\omega \times \operatorname{Aut} N_{\mathrm{tors}}),$$

and we denote the associated map $\mathcal{E}(U^\vee_{T,R}, N, \omega) \to \mathcal{E}_{\mathrm{tors}}(U^\vee_{T,R}, N, \omega)$ by the same letter.

The following is clear by construction:

Proposition 9.18. *Let $N \in \mathcal{M}_V$ and let $\omega \in \mathcal{H}_N$. Let $(K, \iota) \in \mathcal{K}^T(N, \omega)$. Then $\tau_{N,\omega}([R \otimes_{\mathbb{Z}G} \mathrm{S}^{\mathrm{Ara}}_K(\mathfrak{m})^\vee]) = [R \otimes_{\mathbb{Z}G} \mathrm{S}^{\mathrm{fin}}_K(\mathfrak{m})^\vee]$.*

We now compute the pushforward distribution under $\tau_{N,\omega}$.

Proposition 9.19. *Let $N \in \mathcal{M}_V$ and let $\omega \in \mathcal{H}_N$. Denote by $\mathbb{P}_{T,N,\omega}$ the restriction and renormalisation of $\mathbb{P}_T$ to $\mathcal{E}(U^\vee_{T,R}, N, \omega)$. Then for $\Delta \in \mathcal{E}_{\mathrm{tors}}(U^\vee_{T,R}, N, \omega)$ it holds that*

$$(\tau_{N,\omega})_* \mathbb{P}_{T,N,\omega}(\Delta) = \frac{|[\Delta]|}{\left|\operatorname{Ext}^1_R(\ker\omega, N_{\mathrm{tors}})\right|},$$

where $[\Delta]$ denotes the class of Δ with respect to the $(H_\omega \times \operatorname{Aut} N_{\mathrm{tors}})$-action.

Proof. We first calculate the distribution $\mathbb{P}_{T,N,\omega}$ using the restriction and renormalisation $\mathbb{P}_{T,N}$ of $\mathbb{P}_T$ to $\mathcal{E}(U^\vee_{T,R}, N)$. It holds that

$$\begin{aligned}
\mathbb{P}_{T,N}(\mathcal{E}(U^\vee_{T,R}, N, \omega)) &= \sum_{\substack{\Theta \in \mathcal{E}(U^\vee_{T,R}, N) \\ \overline{\omega_{\mathrm{d},N}}([\Theta]) = [\omega]}} \mathbb{P}_{T,N}(\Theta) \\
&= \frac{1}{\left|\operatorname{Ext}^1_R(U^\vee_{T,R}, N)\right|} \sum_{\substack{\Theta \in \operatorname{Ext}^1_R(U^\vee_{T,R}, N) \\ [\omega_{\mathrm{d},N}(\Theta)] = [\omega]}} 1 \\
&= \frac{1}{\left|\operatorname{Ext}^1_R(U^\vee_{T,R}, N)\right|} \sum_{\psi \in [\omega]} \sum_{\Theta \in \omega^{-1}_{\mathrm{d},N}(\psi)} 1 \\
&= \frac{|[\omega]| \cdot \left|\operatorname{Ext}^1_R(U^\vee_{T,R}, N_{\mathrm{tors}})\right|}{\left|\operatorname{Ext}^1_R(U^\vee_{T,R}, N)\right|},
\end{aligned}$$

where we have used Propositions 9.5 and 7.23. It follows that for $\Theta \in \mathcal{E}(U^\vee_{T,R}, N, \omega)$ we have

$$\mathbb{P}_{T,N,\omega}(\Theta) = \frac{\mathbb{P}_{T,N}(\Theta)}{\mathbb{P}_{T,N}(\mathcal{E}(U^\vee_{T,R}, N, \omega))} = \frac{|[\Theta]_{G\text{-eq. alg.}}|}{|[\omega]| \cdot \left|\operatorname{Ext}^1_R(U^\vee_{T,R}, N_{\mathrm{tors}})\right|}.$$

For the pushforward, note first that $\tau_{N,\omega}$ is obtained from the map

$$\omega^{-1}_{\mathrm{d},N}([\omega]) \xrightarrow{\sigma_N} \pi_N^{-1}([\omega]) \xrightarrow{\varepsilon_{N,\omega}} \operatorname{Ext}^1_R(\ker \omega, N_{\mathrm{tors}})$$

by passing to $(\operatorname{Aut}_{G\text{-eq. alg.}}(U^\vee_{T,R}) \times \operatorname{Aut} N)$-equivalence classes. By Proposition 9.15 and as $\varepsilon_{N,\omega}$ is surjective with fibres of size $|[\omega]|$, we have that $\varepsilon_{N,\omega} \circ \sigma_N|_{\omega^{-1}_{\mathrm{d},N}([\omega])}$ is surjective with fibre of size

$$\left|\left(\varepsilon_{N,\omega} \circ \sigma_N|_{\omega^{-1}_{\mathrm{d},N}([\omega])}\right)^{-1}(\Delta)\right| = \frac{|[\omega]| \cdot \left|\operatorname{Ext}^1_R(U^\vee_{T,R}, N_{\mathrm{tors}})\right|}{\left|\operatorname{Ext}^1_R(\ker \omega, N_{\mathrm{tors}})\right|}$$

at $\Delta \in \operatorname{Ext}^1_R(\ker \omega, N_{\mathrm{tors}})$. It follows that for $\Delta \in \mathcal{E}_{\mathrm{tors}}(U^\vee_{T,R}, N, \omega)$ we have

$$\begin{aligned}
(\tau_{N,\omega})_* \mathbb{P}_{T,N,\omega}(\Delta) &= \sum_{\substack{\Theta \in \mathcal{E}(U^\vee_{T,R}, N, \omega) \\ \tau_{N,\omega}(\Theta) = \Delta}} \mathbb{P}_{T,N,\omega}(\Theta) \\
&= \frac{1}{|[\omega]| \cdot \left|\operatorname{Ext}^1_R(U^\vee_{T,R}, N_{\mathrm{tors}})\right|} \sum_{\substack{\Theta \in \omega^{-1}_{\mathrm{d},N}([\omega]) \\ (\varepsilon_{N,\omega} \circ \sigma_N)(\Theta) \in [\Delta]}} 1 \\
&= \frac{1}{|[\omega]| \cdot \left|\operatorname{Ext}^1_R(U^\vee_{T,R}, N_{\mathrm{tors}})\right|} \sum_{\Delta' \in [\Delta]} \sum_{\Theta \in \left(\varepsilon_{N,\omega} \circ \sigma_N|_{\omega^{-1}_{\mathrm{d},N}([\omega])}\right)^{-1}(\Delta')} 1 \\
&= \frac{|[\Delta]|}{\left|\operatorname{Ext}^1_R(\ker \omega, N_{\mathrm{tors}})\right|},
\end{aligned}$$

as claimed. □

Definition 9.20. Define $\tau\colon \mathcal{E}(U_{T,R}^\vee, \mathcal{M}_V) \to \mathcal{E}_{\mathrm{tors}}(U_{T,R}^\vee, \mathcal{M}_V)$ to be the map obtained by gluing together the maps $\tau_{N,\omega}\colon \mathcal{E}(U_{T,R}^\vee, N, \omega) \to \mathcal{E}_{\mathrm{tors}}(U_{T,R}^\vee, N, \omega)$ for $N \in \mathcal{M}_V$ and $\omega \in \mathcal{H}_N$.

As a result of Proposition 9.18 we have:

Corollary 9.21. *Assume that Conjecture 8.38 holds. Let $f\colon \mathcal{E}_{\mathrm{tors}}(U_{T,R}^\vee, \mathcal{M}_V) \to \mathbb{C}$ be 'reasonable' and assume that $f \circ \tau$ is again 'reasonable'. Then*

$$\lim_{B\to\infty} \frac{\sum_{(K,\iota)\in\mathcal{K}_{C\le B}^T} f([R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{fin}}(\mathfrak{m})^\vee])}{\left|\mathcal{K}_{C\le B}^T\right|} = \sum_{\Delta\in\mathcal{E}_{\mathrm{tors}}(U_{T,R}^\vee, \mathcal{M}_V)} f(\Delta)\cdot \tau_*\mathbb{P}_T(\Delta).$$

Here, the distribution $\tau_*\mathbb{P}_T$ is given as follows.

Proposition 9.22. *Suppose that $\Delta \in \mathcal{E}_{\mathrm{tors}}(U_{T,R}^\vee, \mathcal{M}_V)$ is given by*

$$0 \longrightarrow N_{\mathrm{tors}} \longrightarrow L \longrightarrow \ker\omega \longrightarrow 0$$

where $N \in \mathcal{M}_V$ and $\omega \in \mathcal{H}_N$. Then

$$\tau_*\mathbb{P}_T(\Delta) = \mathbb{P}^{\mathrm{BL}}(N) \cdot \frac{|[\omega]|}{\left|\mathrm{Hom}_R(U_{T,R}^\vee, ((N/N_{\mathrm{tors}})^*)^\vee)\right|} \cdot \frac{|[\Delta]|}{\left|\mathrm{Ext}_R^1(\ker\omega, N_{\mathrm{tors}})\right|}.$$

Proof. We have

$$\begin{aligned}\tau_*\mathbb{P}_T(\Delta) &= \mathbb{P}_T(\tau_{N,\omega}^{-1}(\Delta))\\ &= \mathbb{P}_T(\mathcal{E}(U_{T,R}^\vee, N, \omega)) \cdot \mathbb{P}_{T,N,\omega}(\tau_{N,\omega}^{-1}(\Delta))\\ &= \mathbb{P}_T(\mathcal{E}(U_{T,R}^\vee, N)) \cdot \mathbb{P}_{T,N}(\mathcal{E}(U_{T,R}^\vee, N, \omega)) \cdot \mathbb{P}_{T,N,\omega}(\tau_{N,\omega}^{-1}(\Delta)).\end{aligned}$$

Now Remark 8.35 gives $\mathbb{P}_T(\mathcal{E}(U_{T,R}^\vee, N)) = \mathbb{P}^{\mathrm{BL}}(N)$ and Proposition 9.19 shows that $\mathbb{P}_{T,N,\omega}(\tau_{N,\omega}^{-1}(\Delta)) = \frac{|[\Delta]|}{\left|\mathrm{Ext}_R^1(\ker\omega, N_{\mathrm{tors}})\right|}$. By the proof of the latter, we also have

$$\mathbb{P}_{T,N}(\mathcal{E}(U_{T,R}^\vee, N, \omega)) = \frac{|[\omega]| \cdot \left|\mathrm{Ext}_R^1(U_{T,R}^\vee, N_{\mathrm{tors}})\right|}{\left|\mathrm{Ext}_R^1(U_{T,R}^\vee, N)\right|}.$$

It follows from Propositions 3.9, 4.41 and 4.42 that

$$\begin{aligned}\left|\mathrm{Ext}_R^1(U_{T,R}^\vee, N)\right| &= \left|\mathrm{Ext}_R^1(U_{T,R}^\vee, N_{\mathrm{tors}})\right| \cdot \left|\mathrm{Ext}_R^1(U_{T,R}^\vee, N/N_{\mathrm{tors}})\right|\\ &= \left|\mathrm{Ext}_R^1(U_{T,R}^\vee, N_{\mathrm{tors}})\right| \cdot \left|\mathrm{Hom}_R(U_{T,R}^\vee, ((N/N_{\mathrm{tors}})^*)^\vee)\right|,\end{aligned}$$

finishing the proof. □

As a special case, we have:

Corollary 9.23. *Assume that Conjecture 8.38 holds. Let $N \in \mathcal{M}_V$ and let $\omega \in \mathcal{H}_N$. Let $\Delta \in \mathcal{E}_{\mathrm{tors}}(U_{T,R}^\vee, N, \omega)$. Then*

$$\lim_{B\to\infty} \frac{\left|\left\{ (K,\iota) \in \mathcal{K}^T_{C\le B}(N,\omega) \,\middle|\, [R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{fin}}(\mathfrak{m})^\vee] = [\Delta] \right\}\right|}{\left|\mathcal{K}^T_{C\le B}(N,\omega)\right|} = \frac{|[\Delta]|}{\left|\mathrm{Ext}^1_R(\ker\omega, N_{\mathrm{tors}})\right|}.$$

9.4 Reduction Map on the Unit Group

Recall that associated to $(K,\iota) \in \mathcal{K}^T$ we have the natural reduction map

$$\overline{\rho_K(\mathfrak{m})}\colon \frac{\mathcal{O}_K^\times}{\mu(K)} \to \frac{(\mathcal{O}_K/\mathfrak{m}_0)^\times}{\rho(\mu(K))}.$$

In the present section, we derive from Conjecture 8.38 that $\mathrm{id}_R \otimes \overline{\rho_K(\mathfrak{m})}$ is equidistributed over a suitable space. The key for this is the fact that $\mathrm{id}_R \otimes \overline{\rho_K(\mathfrak{m})}$ can be recovered from $R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee$ by the results of Sections 6.4.2 and 7.3.2.

As usual, we first describe by which space the R-module homomorphism $\mathrm{id}_R \otimes \overline{\rho_K(\mathfrak{m})}$ can be modelled as (K,ι) runs over $\mathcal{K}^T$.

Construction 9.24. We consider $(K,\iota) \in \mathcal{K}^T(N)$ where $N \in \mathcal{M}_V$. By Proposition 8.25 there is a G-equivariant $\mathcal{O}_F$-algebra isomorphism

$$R \otimes_{\mathbb{Z}G} \frac{(\mathcal{O}_K/\mathfrak{m}_0)^\times}{\rho(\mu(K))} \cong U_{T,R}$$

which allows us to identify the codomain of $\mathrm{id}_R \otimes \overline{\rho_K(\mathfrak{m})}$ with $U_{T,R}$. For the domain, we pick an isomorphism $R \otimes_{\mathbb{Z}G} (\mathrm{Pic}_K^0)^\vee \cong N$ and an isomorphism $N/N_{\mathrm{tors}} \cong P_V$ which together with the isomorphisms from Construction 6.23 and Proposition 7.18 provide us with an isomorphism

$$\begin{aligned} R \otimes_{\mathbb{Z}G} \frac{\mathcal{O}_K^\times}{\mu(K)} &\cong R \otimes_{\mathbb{Z}G} \left(\frac{(\mathrm{Pic}_K^0)^\vee}{((\mathrm{Pic}_K^0)^\vee)_{\mathrm{tors}}} \right)^* \\ &\cong \left(R \otimes_{\mathbb{Z}G} \frac{(\mathrm{Pic}_K^0)^\vee}{((\mathrm{Pic}_K^0)^\vee)_{\mathrm{tors}}} \right)^* \\ &\cong (N/N_{\mathrm{tors}})^* \\ &\cong P_V^*. \end{aligned}$$

Using the above isomorphisms, we may uniquely identify $\mathrm{id}_R \otimes \overline{\rho_K(\mathfrak{m})}$ with an element of

$$\mathrm{Hom}_R(P_V^*, U_{T,R})/\operatorname{Aut} P_V^* \times \mathrm{Aut}_{G\text{-eq. alg.}}(U_{T,R}),$$

regardless of the choice of isomorphisms at all instances where there was one. We will denote that element by $[\mathrm{id}_R \otimes \overline{\rho_K(\mathfrak{m})}]$.

To derive implications on the distribution of $[\mathrm{id}_R \otimes \overline{\rho_K(\mathfrak{m})}]$ from our main conjecture, we now define an appropriate function on the probability space $\mathcal{E}(U_{T,R}^\vee, \mathcal{M}_V)$.

Construction 9.25. For $N \in \mathcal{M}_V$ we have maps

$$\begin{aligned} \mathrm{Ext}^1_R(U_{T,R}^\vee, N) &\xrightarrow{\omega_{\mathrm{d}}} \mathrm{Hom}_R(U_{T,R}^\vee, ((N/N_{\mathrm{tors}})^*)^\vee) && \text{(Construction 7.22)} \\ &\xleftarrow{\vee} \mathrm{Hom}_R((N/N_{\mathrm{tors}})^*, U_{T,R}) && \text{(Corollary 4.9)} \\ &\xrightarrow{\sim} \mathrm{Hom}_R(P_V^*, U_{T,R}) && (N/N_{\mathrm{tors}} \cong P_V) \end{aligned}$$

which by naturality factor through the actions of automorphism groups to give rise to a map

$$\rho_N \colon \mathcal{E}(U_{T,R}^\vee, N) \to \mathrm{Hom}_R(P_V^*, U_{T,R}) / \operatorname{Aut} P_V^* \times \operatorname{Aut}_{G\text{-eq. alg.}}(U_{T,R}).$$

The maps ρ_N glue together to a map

$$\rho \colon \mathcal{E}(U_{T,R}^\vee, \mathcal{M}_V) \to \mathrm{Hom}_R(P_V^*, U_{T,R}) / \operatorname{Aut} P_V^* \times \operatorname{Aut}_{G\text{-eq. alg.}}(U_{T,R}).$$

Crucially, we have:

Proposition 9.26. *Let $(K, \iota) \in \mathcal{K}^T$. Then*

$$\rho([R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee]) = [\mathrm{id}_R \otimes \overline{\rho_K(\mathfrak{m})}]$$

Proof. This follows from Propositions 6.24 and 7.26 and naturality of ω_{d} and $(\cdot)^\vee$. □

We next determine the pushforward distribution under ρ_N and ρ.

Proposition 9.27. *Let $\varphi \in \mathrm{Hom}_R(P_V^*, U_{T,R})$. Let $N \in \mathcal{M}_V$. Then*

$$\rho_* \mathbb{P}_T([\varphi]) = (\rho_N)_* \mathbb{P}_{T,N}([\varphi]) = \frac{|[\varphi]|}{|\mathrm{Hom}_R(P_V^*, U_{T,R})|}.$$

Proof. Let $N \in \mathcal{M}_V$. We denote by

$$\overline{\omega_{\mathrm{d}}} \colon \mathcal{E}(U_{T,R}^\vee, N) \to \mathrm{Hom}_R(U_{T,R}^\vee, ((N/N_{\mathrm{tors}})^*)^\vee) / \operatorname{Aut}_{G\text{-eq. alg.}}(U_{T,R}^\vee) \times \operatorname{Aut}(N/N_{\mathrm{tors}})^*)^\vee$$

the map that is induced by the homomorphism from Construction 7.19. Let $\psi \in \mathrm{Hom}_R(U_{T,R}^\vee, ((N/N_{\mathrm{tors}})^*)^\vee)$. Using Propositions 9.5 and 7.23, we have

$$\begin{aligned}
\overline{\omega_{\mathrm{d}}}_* \mathbb{P}_{T,N}([\psi]) &= \sum_{\substack{\Theta \in \mathcal{E}(U_{T,R}^\vee, N) \\ \overline{\omega_{\mathrm{d}}}(\Theta) = [\psi]}} \mathbb{P}_{T,N}(\Theta) \\
&= \frac{1}{\left|\mathrm{Ext}_R^1(U_{T,R}^\vee, N)\right|} \sum_{\substack{\Theta \in \mathrm{Ext}_R^1(U_{T,R}^\vee, N) \\ [\omega_{\mathrm{d}}(\Theta)] = [\psi]}} 1 \\
&= \frac{1}{\left|\mathrm{Ext}_R^1(U_{T,R}^\vee, N)\right|} \sum_{\chi \in [\psi]} \sum_{\substack{\Theta \in \mathrm{Ext}_R^1(U_{T,R}^\vee, N) \\ \omega_{\mathrm{d}}(\Theta) = \chi}} 1 \\
&= \frac{\left|\mathrm{Ext}_R^1(U_{T,R}^\vee, N_{\mathrm{tors}})\right| \cdot |[\psi]|}{\left|\mathrm{Ext}_R^1(U_{T,R}^\vee, N)\right|} \\
&= \frac{|[\psi]|}{\left|\mathrm{Hom}_R(U_{T,R}^\vee, ((N/N_{\mathrm{tors}})^*)^\vee)\right|}.
\end{aligned}$$

Since the remaining two maps in the construction of ρ_N are isomorphisms, it follows that for $\varphi \in \mathrm{Hom}_R(P_V^*, U_{T,R})$ we have $(\rho_N)_* \mathbb{P}_{T,N}([\varphi]) = |[\varphi]| \,/\, |\mathrm{Hom}_R(P_V^*, U_{T,R})|$. For ρ we then obtain

$$\begin{aligned}
\rho_* \mathbb{P}_T([\varphi]) &= \sum_{\substack{\Theta \in \mathcal{E}(U_{T,R}^\vee, \mathcal{M}_V) \\ \rho(\Theta) = [\varphi]}} \mathbb{P}_T(\Theta) \\
&= \sum_{N \in \mathcal{M}_V} \sum_{\substack{\Theta \in \mathcal{E}(U_{T,R}^\vee, N) \\ \rho_N(\Theta) = [\varphi]}} \mathbb{P}_{T,N}(\Theta) \cdot \mathbb{P}_T(\mathcal{E}(U_{T,R}^\vee, N)) \\
&= \sum_{N \in \mathcal{M}_V} \mathbb{P}_T(\mathcal{E}(U_{T,R}^\vee, N)) \cdot (\rho_N)_* \mathbb{P}_{T,N}([\varphi]) \\
&= \frac{|[\varphi]|}{\left|\mathrm{Hom}_R(P_V^*, U_{T,R})\right|},
\end{aligned}$$

as claimed. □

Corollary 9.28. *Assume that Conjecture 8.38 holds. Let $N \in \mathcal{M}_V$ and let $\varphi \in \mathrm{Hom}_R(P_V^*, U_{T,R})$. Then*

$$\lim_{B \to \infty} \frac{\left| \left\{ (K, \iota) \in \mathcal{K}_{C \le B}^T(N) \,\middle|\, [\mathrm{id}_R \otimes \overline{\rho_K(\mathfrak{m})}] = [\varphi] \right\} \right|}{\left| \mathcal{K}_{C \le B}^T(N) \right|} = \frac{|[\varphi]|}{\left|\mathrm{Hom}_R(P_V^*, U_{T,R})\right|}.$$

Corollary 9.29. *Assume that Conjecture 8.38 holds. Let $\varphi \in \operatorname{Hom}_R(P_V^*, U_{T,R})$. Then*

$$\lim_{B\to\infty} \frac{\left|\left\{ (K,\iota) \in \mathcal{K}^T_{C\le B} \,\middle|\, [\mathrm{id}_R \otimes \overline{\rho_K(\mathfrak{m})}] = [\varphi] \right\}\right|}{\left|\mathcal{K}^T_{C\le B}\right|} = \frac{|[\varphi]|}{\left|\operatorname{Hom}_R(P_V^*, U_{T,R})\right|}.$$

We end this section by showing that the distribution of the reduction map and the distribution of the Arakelov class group are independent as (K,ι) runs over $\mathcal{K}^T$. This can be seen as a generalisation of [BP25, Corollary 4.9]. Recall the map $\sigma\colon \mathcal{E}(U_{T,R}^\vee, \mathcal{M}_V) \to \mathcal{M}_V$ from Theorem 8.34 that sends Θ to the unique element of $\mathcal{M}_V$ that is isomorphic to the left hand module of Θ.

Proposition 9.30. *Let*

$$(\sigma,\rho)\colon \mathcal{E}(U_{T,R}^\vee, \mathcal{M}_V) \to \mathcal{M}_V \times \operatorname{Hom}_R(P_V^*, U_{T,R})/\operatorname{Aut} P_V^* \times \operatorname{Aut}_{G\text{-eq. alg.}}(U_{T,R})$$

be the map that sends Θ to $(\sigma(\Theta), \rho(\Theta))$. Then $(\sigma,\rho)_*\mathbb{P}_T$ equals the product measure of $\sigma_*\mathbb{P}_T$ and $\rho_*\mathbb{P}_T$.

Proof. Let $N \in \mathcal{M}_V$ and let $\varphi \in \operatorname{Hom}_R(P_V^*, U_{T,R})$. Then we have

$$\begin{aligned}(\sigma,\rho)_*\mathbb{P}_T(N,[\varphi]) &= \sum_{\substack{\Theta\in\mathcal{E}(U_{T,R}^\vee,\mathcal{M}_V)\\ \sigma(\Theta)=N\\ \rho(\Theta)=[\varphi]}} \mathbb{P}_T(\Theta)\\ &= \mathbb{P}_T(\mathcal{E}(U_{T,R}^\vee, N)) \cdot \sum_{\substack{\Theta\in\mathcal{E}(U_{T,R}^\vee,N)\\ \rho_N(\Theta)=[\varphi]}} \mathbb{P}_{T,N}(\Theta)\\ &= \sigma_*\mathbb{P}_T(N)\cdot \rho_*\mathbb{P}_T([\varphi]),\end{aligned}$$

where in the final step we have used Theorem 8.34 (ii), Remark 8.35 and Proposition 9.27. □

9.5 Average Torsion of Ray Class Groups

We keep using the notation from Setup 8.37, but we make the following choices. Let $I = \langle \sum_{g\in G} g\rangle$, let ℓ be a prime with $\ell \nmid |G|$, let $S = \{\ell\}$. We denote the primitive central idempotents of $\mathbb{Q}G$ by $e_0, e_1, \dots, e_c$ where we let $e_0 := \frac{1}{|G|}\sum_{g\in G} g$, so that $I = \langle e_0\rangle$ and so that notation for A aligns with the notation from Section 1.4, which we are also going to use in this section.

We investigate the consequences of Conjecture 8.38 for the function

$$f_T\colon \mathcal{E}(U_{T,R}^\vee, \mathcal{M}_V) \to \mathbb{C},\ (0 \to N \to L \to U_{T,R}^\vee \to 0) \mapsto |L[\ell]|,$$

which will lead to results on the average torsion of ray class groups. These results generalise statements from [PS17, Section 2.2] and [BP25, Section 4.2].

We first deal with $\mathrm{Av}(f_T)$ and describe

$$f_T([R \otimes_{\mathbb{Z}G} \mathrm{S}_K^{\mathrm{Ara}}(\mathfrak{m})^\vee]) = \left|(R \otimes_{\mathbb{Z}G} \mathrm{Pic}_K^0(\mathfrak{m})^\vee)[\ell]\right|$$

for $(K, \iota) \in \mathcal{K}^T$.

Proposition 9.31. *Let $(K, \iota) \in \mathcal{K}^T$. Then*

$$\left|(R \otimes_{\mathbb{Z}G} \mathrm{Pic}_K^0(\mathfrak{m})^\vee)[\ell]\right| = \frac{|\mathrm{Cl}_K(\mathfrak{m})[\ell]|}{|\mathrm{Cl}_K(\mathfrak{m})[\ell]^G|}.$$

Proof. First, by Lemma 8.19 we have

$$(R \otimes_{\mathbb{Z}G} \mathrm{Pic}_K^0(\mathfrak{m})^\vee)[\ell] = (R \otimes_{\mathbb{Z}G} \mathrm{Cl}_K(\mathfrak{m})^\vee)[\ell].$$

Next, Proposition 7.17, self-duality of finite abelian groups and Lemma 7.15 (ii) give

$$\begin{aligned}\left|(R \otimes_{\mathbb{Z}G} \mathrm{Cl}_K(\mathfrak{m})^\vee)[\ell]\right| &= \left|(R \otimes_{\mathbb{Z}G} \mathrm{Cl}_K(\mathfrak{m}))^\vee[\ell]\right| \\ &= |(R \otimes_{\mathbb{Z}G} \mathrm{Cl}_K(\mathfrak{m}))[\ell]| \\ &= |R \otimes_{\mathbb{Z}G} \mathrm{Cl}_K(\mathfrak{m})[\ell]|\,.\end{aligned}$$

Now as explained at the beginning of Chapter 7, we have

$$R \otimes_{\mathbb{Z}G} \mathrm{Cl}_K(\mathfrak{m})[\ell] = \mathrm{Cl}_K(\mathfrak{m})[\ell]/e_0\,\mathrm{Cl}_K(\mathfrak{m})[\ell].$$

One sees directly that $e_0\,\mathrm{Cl}_K(\mathfrak{m})[\ell] = \mathrm{Cl}_K(\mathfrak{m})[\ell]^G$. The claim follows. □

Proposition 9.32. *Assume that $\ell \nmid |\mathrm{Cl}_F|$. Let $(K, \iota) \in \mathcal{K}^T$. Then*

$$\mathrm{Cl}_K(\mathfrak{m})[\ell]^G \cong U_T[\ell]^G$$

as abelian groups.

Proof. The idea is to chase through the diagram from Theorem 6.18 to show that $\mathrm{Cl}_K(\mathfrak{m})[\ell]^G$ is isomorphic to $\frac{(\mathcal{O}_K/\mathfrak{m}_0)^\times}{\rho(\mu(K))}[\ell]^G$ and then use Proposition 8.25 to conclude. The short exact sequence $\mathrm{S}_K^{\mathrm{fin}}(\mathfrak{m})$ induces an exact sequence of $\mathbb{Z}_{(\ell)}G$-modules

$$\begin{tikzcd} 0 \arrow[r] & \frac{(\mathcal{O}_K/\mathfrak{m}_0)^\times}{\rho(\mathcal{O}_K^\times)}[\ell] \arrow[r] & \mathrm{Cl}_K(\mathfrak{m})[\ell] \arrow[r] & \mathrm{Cl}_K[\ell]. \end{tikzcd}$$

Looking at the e_0-component, we obtain

$$\begin{tikzcd} 0 \arrow[r] & \frac{(\mathcal{O}_K/\mathfrak{m}_0)^\times}{\rho(\mathcal{O}_K^\times)}[\ell]^G \arrow[r] & \mathrm{Cl}_K(\mathfrak{m})[\ell]^G \arrow[r] & \mathrm{Cl}_K[\ell]^G. \end{tikzcd}$$

By assumption and since $\ell \nmid |G|$, we have $\mathrm{Cl}_K[\ell]^G = \mathrm{Cl}_F[\ell] = 0$, whence

$$\mathrm{Cl}_K(\mathfrak{m})[\ell]^G = \frac{(\mathcal{O}_K/\mathfrak{m}_0)^\times}{\rho(\mathcal{O}_K^\times)}[\ell]^G. \tag{9.33}$$

We next would like to study the effect of the functor $(-)[\ell]^G$ on the left hand column of the diagram in Theorem 6.18, in order to link $\frac{(\mathcal{O}_K/\mathfrak{m}_0)^\times}{\rho(\mathcal{O}_K^\times)}[\ell]^G$ to $\frac{(\mathcal{O}_K/\mathfrak{m}_0)^\times}{\rho(\mu(K))}[\ell]^G$. Note that for a G-module M there is an isomorphism of abelian groups

$$\mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}/\ell, M) \to M[\ell]^G,\ \varphi \mapsto \varphi(1)$$

where we regard $\mathbb{Z}/\ell$ with the trivial G-structure. We infer that the functor

$$_{\mathbb{Z}G}\mathsf{Mod} \to \mathsf{Ab},\ M \mapsto M[\ell]^G$$

is isomorphic to the functor $\mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}/\ell, -)$. Thus, applying $(-)[\ell]^G$ to the short exact sequence

$$0 \longrightarrow \frac{\rho(\mathcal{O}_K^\times)}{\rho(\mu(K))} \longrightarrow \frac{(\mathcal{O}_K/\mathfrak{m}_0)^\times}{\rho(\mu(K))} \longrightarrow \frac{(\mathcal{O}_K/\mathfrak{m}_0)^\times}{\rho(\mathcal{O}_K^\times)} \longrightarrow 0$$

from Theorem 6.18, we obtain a long exact sequence

$$0 \to \frac{\rho(\mathcal{O}_K^\times)}{\rho(\mu(K))}[\ell]^G \to \frac{(\mathcal{O}_K/\mathfrak{m}_0)^\times}{\rho(\mu(K))}[\ell]^G \to \frac{(\mathcal{O}_K/\mathfrak{m}_0)^\times}{\rho(\mathcal{O}_K^\times)}[\ell]^G \to \mathrm{Ext}^1_{\mathbb{Z}G}\left(\mathbb{Z}/\ell, \frac{\rho(\mathcal{O}_K^\times)}{\rho(\mu(K))}\right). \tag{9.34}$$

We are going to show that both the left and right hand term of this exact sequence are zero. First we prove that $(\mathcal{O}_K^1(\mathfrak{m}) \otimes_{\mathbb{Z}} \mathbb{R}/\mathbb{Z})[\ell]^G = 0$ which by the top row of the diagram in Theorem 6.18 will imply that $\frac{\rho(\mathcal{O}_K^\times)}{\rho(\mu(K))}[\ell]^G = 0$. By the proof of Proposition 6.15, there is an isomorphism of $\mathbb{Z}G$-modules

$$\mathcal{O}_K^1(\mathfrak{m}) \otimes_{\mathbb{Z}} \mathbb{R}/\mathbb{Z} \cong \frac{(\prod_{\mathfrak{p}|\infty}\mathbb{R})^0}{\mathrm{Log}(\mathcal{O}_K^1(\mathfrak{m}))},$$

where $\mathrm{Log}(\mathcal{O}_K^1(\mathfrak{m}))$ is a complete lattice in $(\prod_{\mathfrak{p}|\infty}\mathbb{R})^0$ by Theorem 6.8. Note that

$$\frac{(\prod_{\mathfrak{p}|\infty}\mathbb{R})^0}{\mathrm{Log}(\mathcal{O}_K^1(\mathfrak{m}))}[\ell] = \frac{\frac{1}{\ell}\mathrm{Log}(\mathcal{O}_K^1(\mathfrak{m}))}{\mathrm{Log}(\mathcal{O}_K^1(\mathfrak{m}))} \cong \frac{\mathrm{Log}(\mathcal{O}_K^1(\mathfrak{m}))}{\ell\,\mathrm{Log}(\mathcal{O}_K^1(\mathfrak{m}))}.$$

This leads us to consider the effect of the functor $(-)^G$ on the short exact sequence

$$0 \longrightarrow \ell\,\mathrm{Log}(\mathcal{O}_K^1(\mathfrak{m})) \longrightarrow \mathrm{Log}(\mathcal{O}_K^1(\mathfrak{m})) \longrightarrow \frac{\mathrm{Log}(\mathcal{O}_K^1(\mathfrak{m}))}{\ell\,\mathrm{Log}(\mathcal{O}_K^1(\mathfrak{m}))} \longrightarrow 0. \tag{9.35}$$

We first show that $((\prod_{\mathfrak{p}|\infty}\mathbb{R})^0)^G = 0$. To this end, let $(x_\mathfrak{p})_\mathfrak{p} \in ((\prod_{\mathfrak{p}|\infty}\mathbb{R})^0)^G$. Since G operates transitively on $\{\mathfrak{p} \mid \infty\}$, there is $x \in \mathbb{R}$ with $x_\mathfrak{p} = x$ for all $\mathfrak{p}$. But $0 = \mathrm{Tr}((x_\mathfrak{p})_\mathfrak{p}) = |\{\mathfrak{p} \mid \infty\}| \cdot x$, which gives $x = 0$ and therefore $(x_\mathfrak{p})_\mathfrak{p} = 0$. Next, note that $H^1\left(G, \frac{\operatorname{Log}(\mathcal{O}_K^1(\mathfrak{m}))}{\ell \operatorname{Log}(\mathcal{O}_K^1(\mathfrak{m}))}\right) = 0$ as multiplication by $|G|$ is both the zero map and an isomorphism on this group. Hence, applying $(-)^G$ to the short exact sequence (9.35), we obtain an exact sequence

$$0 \longrightarrow \left(\frac{\operatorname{Log}(\mathcal{O}_K^1(\mathfrak{m}))}{\ell \operatorname{Log}(\mathcal{O}_K^1(\mathfrak{m}))}\right)^G \longrightarrow H^1(G, \ell \operatorname{Log}(\mathcal{O}_K^1(\mathfrak{m}))) \longrightarrow H^1(G, \operatorname{Log}(\mathcal{O}_K^1(\mathfrak{m}))) \longrightarrow 0.$$

In this sequence, the middle and right hand term are finite by [CF67, Corollary 2 on page 105], and they have the same cardinality, since $\operatorname{Log}(\mathcal{O}_K^1(\mathfrak{m})) \cong \ell \operatorname{Log}(\mathcal{O}_K^1(\mathfrak{m}))$. It follows that $\left(\frac{\operatorname{Log}(\mathcal{O}_K^1(\mathfrak{m}))}{\ell \operatorname{Log}(\mathcal{O}_K^1(\mathfrak{m}))}\right)^G = 0$ which implies

$$(\mathcal{O}_K^1(\mathfrak{m}) \otimes_{\mathbb{Z}} \mathbb{R}/\mathbb{Z})[\ell]^G \cong \frac{(\prod_{\mathfrak{p}|\infty} \mathbb{R})^0}{\operatorname{Log}(\mathcal{O}_K^1(\mathfrak{m}))}[\ell]^G \cong \left(\frac{\operatorname{Log}(\mathcal{O}_K^1(\mathfrak{m}))}{\ell \operatorname{Log}(\mathcal{O}_K^1(\mathfrak{m}))}\right)^G = 0.$$

Then by the top row of the diagram in Theorem 6.18 we also have $\frac{\rho(\mathcal{O}_K^\times)}{\rho(\mu(K))}[\ell]^G = 0$.

Now for the right hand term of (9.34), by Proposition 2.1 we have that

$$\begin{aligned}\operatorname{Ext}^1_{\mathbb{Z}G}\left(\mathbb{Z}/\ell, \frac{\rho(\mathcal{O}_K^\times)}{\rho(\mu(K))}\right) &= \operatorname{Ext}^1_{\mathbb{Z}G}\left(\mathbb{Z}/\ell, \frac{\rho(\mathcal{O}_K^\times)}{\rho(\mu(K))}\right)[\ell^\infty] \\ &= \mathbb{Z}_{(\ell)} \otimes_{\mathbb{Z}} \operatorname{Ext}^1_{\mathbb{Z}G}\left(\mathbb{Z}/\ell, \frac{\rho(\mathcal{O}_K^\times)}{\rho(\mu(K))}\right) \\ &\cong \operatorname{Ext}^1_{\mathbb{Z}_{(\ell)}G}\left(\mathbb{Z}/\ell, \frac{\rho(\mathcal{O}_K^\times)}{\rho(\mu(K))}[\ell^\infty]\right),\end{aligned}$$

and analogously

$$\frac{\rho(\mathcal{O}_K^\times)}{\rho(\mu(K))}[\ell]^G \cong \operatorname{Hom}_{\mathbb{Z}G}\left(\mathbb{Z}/\ell, \frac{\rho(\mathcal{O}_K^\times)}{\rho(\mu(K))}\right) \cong \operatorname{Hom}_{\mathbb{Z}_{(\ell)}G}\left(\mathbb{Z}/\ell, \frac{\rho(\mathcal{O}_K^\times)}{\rho(\mu(K))}[\ell^\infty]\right).$$

But as $\ell \nmid |G|$, $\mathbb{Z}_{(\ell)}G$ is a maximal $\mathbb{Z}_{(\ell)}$-order in $\mathbb{Q}G$ by [Rei03, Theorem 41.1], so Proposition 3.32 shows that

$$\begin{aligned}\left|\operatorname{Ext}^1_{\mathbb{Z}G}\left(\mathbb{Z}/\ell, \frac{\rho(\mathcal{O}_K^\times)}{\rho(\mu(K))}\right)\right| &= \left|\operatorname{Ext}^1_{\mathbb{Z}_{(\ell)}G}\left(\mathbb{Z}/\ell, \frac{\rho(\mathcal{O}_K^\times)}{\rho(\mu(K))}[\ell^\infty]\right)\right| \\ &= \left|\operatorname{Hom}_{\mathbb{Z}_{(\ell)}G}\left(\mathbb{Z}/\ell, \frac{\rho(\mathcal{O}_K^\times)}{\rho(\mu(K))}[\ell^\infty]\right)\right| \\ &= \left|\frac{\rho(\mathcal{O}_K^\times)}{\rho(\mu(K))}[\ell]^G\right| \\ &= 1.\end{aligned}$$

Thus, the sequence (9.34) gives

$$\frac{(\mathcal{O}_K/\mathfrak{m}_0)^\times}{\rho(\mathcal{O}_K^\times)}[\ell]^G = \frac{(\mathcal{O}_K/\mathfrak{m}_0)^\times}{\rho(\mu(K))}[\ell]^G. \tag{9.36}$$

Finally, by definition of $\mathcal{K}^T$ and by Proposition 8.25 we have

$$\frac{(\mathcal{O}_K/\mathfrak{m}_0)^\times}{\rho(\mu(K))}[\ell] = \frac{(\mathcal{O}_K/\mathfrak{m}_0)^\times}{\rho(\mu_{\ell'}(K))}[\ell] = (\mathcal{O}_K/\mathfrak{m}_0)^\times[\ell] \cong U_T[\ell]$$

as G-modules which together with (9.33) and (9.36) implies the claim. □

We now determine $\mathbb{E}(f_T)$. For this, we need a few auxiliary results.

Recall that by definition, Z_i is the integral closure of $\mathbb{Z}_{(\ell)}$ in K_i. In particular, $\operatorname{Max}(Z_i)$ is finite.

Lemma 9.37. *$Z_i/\mathbb{Z}_{(\ell)}$ is unramified at ℓ for all $i \in \{1, \dots, c\}$.*

Proof. Let $i \in \{1, \dots, c\}$. Since localisation commutes with integral closure, we have that $Z_i/\mathbb{Z}_{(\ell)}$ is unramified at ℓ if and only if $\mathcal{O}_{K_i}/\mathbb{Z}$ is unramified at ℓ. As $\ell \nmid |G|$, the latter follows from [Rei03, Theorem 41.7]. □

Construction 9.38.

(a) As in [BL20, Proposition 3.6 and its proof], we define a probability distribution $\mathbb{P}_V$ on $\mathcal{M}$ by

$$\mathbb{P}_V(M_0) := \frac{1}{|\operatorname{Hom}_R(P_V, M_0)| \cdot |\operatorname{Aut} M_0|} \cdot \left(\sum_{L_0 \in \mathcal{M}} \frac{1}{|\operatorname{Hom}_R(P_V, L_0)| \cdot |\operatorname{Aut} L_0|} \right)^{-1}$$

for $M_0 \in \mathcal{M}$. By loc. cit. it satisfies $\mathbb{P}^{\mathrm{BL}}(P_V \oplus M_0) = \mathbb{P}_V(M_0)$ for all $M_0 \in \mathcal{M}$.

(b) For $i \in \{1, \dots, c\}$ and $\mathfrak{p} \in \operatorname{Max}(Z_i)$ let $\mathcal{M}_{i,\mathfrak{p}}$ be a set of representatives of isomorphism classes of finite $\widehat{R}_{i,\mathfrak{p}}$-modules. Use the shorthand $P_{i,\mathfrak{p}} := (\widehat{P_V})_{i,\mathfrak{p}}$. In analogy to the above, we define a probability distribution $\mathbb{P}_{i,\mathfrak{p}}$ on $\mathcal{M}_{i,\mathfrak{p}}$ by

$$\mathbb{P}_{i,\mathfrak{p}}(M) := \frac{1}{\left|\operatorname{Hom}_{\widehat{R}_{i,\mathfrak{p}}}(P_{i,\mathfrak{p}}, M)\right| \cdot |\operatorname{Aut} M|} \cdot \left(\sum_{L \in \mathcal{M}_{i,\mathfrak{p}}} \frac{1}{\left|\operatorname{Hom}_{\widehat{R}_{i,\mathfrak{p}}}(P_{i,\mathfrak{p}}, L)\right| \cdot |\operatorname{Aut} L|} \right)^{-1}$$

for $M \in \mathcal{M}_{i,\mathfrak{p}}$.

Note that in both cases, the sums appearing converge by [CM90, Theorem 3.6].

Lemma 9.39. *Suppose that $h \colon \mathcal{M} \to \mathbb{R}_{\geq 0}$ and $h_{i,\mathfrak{p}} \colon \mathcal{M}_{i,\mathfrak{p}} \to \mathbb{R}_{\geq 0}$ for $i \in \{1, \dots, c\}$ and $\mathfrak{p} \in \operatorname{Max}(Z_i)$ are functions which satisfy $h(M_0) = \prod_{i=1}^c \prod_{\mathfrak{p} \in \operatorname{Max}(Z_i)} h_{i,\mathfrak{p}}((\widehat{M_0})_{i,\mathfrak{p}})$ for all $M_0 \in \mathcal{M}$. Then*

$$\sum_{M_0 \in \mathcal{M}} h(M_0) = \prod_{i=1}^{c} \prod_{\mathfrak{p} \in \operatorname{Max}(Z_i)} \sum_{M \in \mathcal{M}_{i,\mathfrak{p}}} h_{i,\mathfrak{p}}(M)$$

if the sum on the left hand side converges.

Proof. Observe that

$$\begin{aligned}\sum_{M\in\mathcal{M}} h(M) &= \sum_{M\in\mathcal{M}} h(M)\left(\prod_{i=1}^{c}\prod_{\mathfrak{p}\in\operatorname{Max}(Z_i)}\sum_{L_{i,\mathfrak{p}}\in\mathcal{M}_{i,\mathfrak{p}}} \mathbb{1}(\widehat{M}_{i,\mathfrak{p}}\cong L_{i,\mathfrak{p}})\right)\\ &= \sum_{M\in\mathcal{M}}\prod_{i=1}^{c}\prod_{\mathfrak{p}\in\operatorname{Max}(Z_i)}\sum_{L_{i,\mathfrak{p}}\in\mathcal{M}_{i,\mathfrak{p}}} h_{i,\mathfrak{p}}(L_{i,\mathfrak{p}})\mathbb{1}(\widehat{M}_{i,\mathfrak{p}}\cong L_{i,\mathfrak{p}}).\end{aligned}$$

Upon changing the order of summation, we see that it remains to show that given $L_{i,\mathfrak{p}}\in\mathcal{M}_{i,\mathfrak{p}}$ for all $i\in\{1,\ldots,c\}$ and $\mathfrak{p}\in\operatorname{Max}(Z_i)$, it holds that

$$\sum_{M\in\mathcal{M}}\prod_{i=1}^{c}\prod_{\mathfrak{p}\in\operatorname{Max}(Z_i)}\mathbb{1}(\widehat{M}_{i,\mathfrak{p}}\cong L_{i,\mathfrak{p}}) = 1.$$

By Lemma 3.3, the left hand side is at most 1. To show that it equals 1, we now construct a module $M\in\mathcal{M}$ with $\widehat{M}_{i,\mathfrak{p}}\cong L_{i,\mathfrak{p}}$ for all $i\in\{1,\ldots,c\}$ and $\mathfrak{p}\in\operatorname{Max}(Z_i)$. We may regard each $L_{i,\mathfrak{p}}$ as a finite R_i-module via the natural ring homomorphism $R_i\to\widehat{Z}_{i,\mathfrak{p}}\otimes_{Z_i}R_i=\widehat{R}_{i,\mathfrak{p}}$. Since $L_{i,\mathfrak{p}}$ is also a finite $\widehat{Z}_{i,\mathfrak{p}}$-module, it is annihilated by a power of $\widehat{\mathfrak{p}}$ and therefore (as a Z_i-module) annihilated by a power of $\mathfrak{p}$, so $L_{i,\mathfrak{p}}=L_{i,\mathfrak{p}}[\mathfrak{p}^\infty]$ as R_i-modules. Note that the natural $\widehat{R}_{i,\mathfrak{p}}$-structure on the $R_{i,\mathfrak{p}}$-module $L_{i,\mathfrak{p}}$ from Lemma 3.3 agrees with the original $\widehat{R}_{i,\mathfrak{p}}$-structure. We define $M_i:=\bigoplus_{\mathfrak{q}\in\operatorname{Max}(Z_i)}L_{i,\mathfrak{q}}$, an R_i-module as explained above. Then Lemma 3.3 gives

$$\widehat{Z}_{i,\mathfrak{p}}\otimes_{Z_i}M_i=\widehat{Z}_{i,\mathfrak{p}}\otimes_{Z_i}L_{i,\mathfrak{p}}\cong L_{i,\mathfrak{p}}$$

as $\widehat{R}_{i,\mathfrak{p}}$-modules. Regarding each M_i as an R-module in the obvious way, it follows that the module $M:=\bigoplus_{i=1}^{c}M_i$ indeed satisfies $\widehat{M}_{i,\mathfrak{p}}\cong L_{i,\mathfrak{p}}$ for all $i\in\{1,\ldots,c\}$ and $\mathfrak{p}\in\operatorname{Max}(Z_i)$. □

The lemma in particular shows that

$$\mathbb{P}_V(M_0)=\prod_{i=1}^{c}\prod_{\mathfrak{p}\in\operatorname{Max}(Z_i)}\mathbb{P}_{i,\mathfrak{p}}\big((\widehat{M_0})_{i,\mathfrak{p}}\big)$$

for $M_0\in\mathcal{M}$.

Lemma 9.40. *Let V and W be finite-dimensional vector spaces over a finite field. Then*

$$\sum_{f\in\operatorname{Hom}(V,W)}|\ker f|=\frac{|\operatorname{Hom}(V,W)|}{|W|}\cdot(|V|+|W|-1).$$

Proof. Note that

$$\begin{aligned}\sum_{f\in\mathrm{Hom}(V,W)} |\ker f| &= \sum_{f\in\mathrm{Hom}(V,W)} \sum_{v\in V} \mathbb{1}(f(v)=0)\\ &= \sum_{v\in V} \sum_{f\in\mathrm{Hom}(V,W)} \mathbb{1}(f(v)=0)\\ &= \sum_{v\in V} |\{\, f\in \mathrm{Hom}(V,W) \mid f(v)=0 \,\}|\,.\end{aligned}$$

By [FA66, Theorem 3], for $0\neq v\in V$ it holds that

$$\frac{\mathrm{Hom}(V,W)}{\{\, f\in\mathrm{Hom}(V,W)\mid f(v)=0\,\}} \cong W.$$

Hence,

$$\begin{aligned}\sum_{f\in\mathrm{Hom}(V,W)} |\ker f| &= |\mathrm{Hom}(V,W)| + \sum_{0\neq v\in V} |\{\, f\in\mathrm{Hom}(V,W)\mid f(v)=0\,\}|\\ &= |\mathrm{Hom}(V,W)| + (|V|-1)\cdot\frac{|\mathrm{Hom}(V,W)|}{|W|},\end{aligned}$$

from which the claim follows. □

Lemma 9.41 ([CL84, Proof of Example 5.12])**.** *Let Z' be a Dedekind domain, let J be an ideal of Z' and let M be a finite Z'-module. Then*

$$|\{\, x\in M \mid \mathrm{ann}_{Z'}(x)=J\,\}| = \left|\mathrm{Aut}_{Z'}(Z'/J)\right|\cdot\left|\left\{\, W\le M \,\middle|\, W\cong_{Z'} Z'/J \,\right\}\right|.$$

As the main result of this section, we now determine the expected value of f_T. This is a generalisation of [PS17, Proposition 2.11] and [BP25, Lemma 4.16]. As in those results, the key ingredient in the proof below is the map δ_ℓ from Section 3.4. Aside from this, our proof takes a different approach. In order to be able to use Corollary 3.29 and since it simplifies many calculations in the proof, we assume below that G is abelian. By suitably adapting the arguments, it may be possible to obtain similar statements also for nonabelian G for which the assumptions of Corollary 3.29 are satisfied.

Theorem 9.42. *Assume that G is abelian. Then*

$$\mathbb{E}(f_T) = \prod_{i=1}^{c} \prod_{\substack{\mathfrak{q}\in\mathrm{Max}(\mathcal{O}_{K_i})\\ \mathfrak{q}\mid\ell}} \left(\frac{|U_T[\ell]_i[\mathfrak{q}^\infty]|}{\ell^{f(\mathfrak{q}|\ell)\cdot\dim_{K_i}(V_i)}}+1\right),$$

where $U_T[\ell]_i$ denotes the i-th isotypical component of the $\mathbb{Z}_{(\ell)}G$-module $U_T[\ell]$.

Note that $U_T[\ell]_i$ is an $e_i\mathbb{Z}_{(\ell)}G$-module and $e_i\mathbb{Z}_{(\ell)}G$ is a $Z_i = (\mathbb{Z}_{(\ell)} \otimes_{\mathbb{Z}} \mathcal{O}_{K_i})$-order by [Rei03, Theorem 10.5], so the expression $U_T[\ell]_i[\mathfrak{q}^\infty]$ makes sense.

Proof. By definition and Theorem 8.34, we have

$$\begin{aligned}\mathbb{E}(f_T) &= \sum_{\Theta \in \mathcal{E}(U^\vee_{T,R}, \mathcal{M}_V)} f_T(\Theta) \cdot \mathbb{P}_T(\Theta) \\ &= \sum_{N \in \mathcal{M}_V} \sum_{\Theta \in \mathcal{E}(U^\vee_{T,R}, N)} f_T(\Theta) \cdot \mathbb{P}^{\mathrm{BL}}(N) \cdot \frac{\left|[\Theta]_{G\text{-eq. alg.}}\right|}{\left|\mathrm{Ext}^1_R(U^\vee_{T,R}, N)\right|} \\ &= \sum_{N \in \mathcal{M}_V} \frac{\mathbb{P}^{\mathrm{BL}}(N)}{\left|\mathrm{Ext}^1_R(U^\vee_{T,R}, N)\right|} \sum_{\Theta \in \mathrm{Ext}^1_R(U^\vee_{T,R}, N)} f_T(\Theta).\end{aligned}$$

By Lemma 9.37 it holds that $v_{i,\mathfrak{p}}(\ell) \leq 1$ for all $i \in \{1, \ldots, c\}$ and $\mathfrak{p} \in \mathrm{Max}(Z_i)$. Moreover, since G is abelian, we have $A_i = K_i$ for all $i \in \{1, \ldots, c\}$ and therefore $e_{i,\mathfrak{p}} = 1$ for all $i \in \{1, \ldots, c\}$ and $\mathfrak{p} \in \mathrm{Max}(Z_i)$. Thus, Corollary 3.29 shows that the map

$$\delta^N_\ell \colon \mathrm{Ext}^1_R(U^\vee_{T,R}, N) \to \mathrm{Hom}_R(U^\vee_{T,R}[\ell], N/\ell N)$$

is surjective for any $N \in \mathcal{M}_V$. We have

$$\sum_{\Theta \in \mathrm{Ext}^1_R(U^\vee_{T,R}, N)} f_T(\Theta) = \sum_{\alpha \in \mathrm{Hom}_R(U^\vee_{T,R}[\ell], N/\ell N)} \sum_{\Theta \in (\delta^N_\ell)^{-1}(\alpha)} f_T(\Theta).$$

But by definition of δ^N_ℓ, if $\Theta \in (\delta^N_\ell)^{-1}(\alpha)$, then there is an exact sequence

$$0 \longrightarrow N[\ell] \longrightarrow L[\ell] \longrightarrow U^\vee_{T,R}[\ell] \xrightarrow{\alpha} \alpha(U^\vee_{T,R}[\ell]) \longrightarrow 0$$

where L is the middle term of the short exact sequence Θ. It follows that

$$f_T(\Theta) = |L[\ell]| = \frac{|N[\ell]| \cdot \left|U^\vee_{T,R}[\ell]\right|}{\left|\alpha(U^\vee_{T,R}[\ell])\right|},$$

whence

$$\begin{aligned}\mathbb{E}(f_T) &= \sum_{N \in \mathcal{M}_V} \frac{\mathbb{P}^{\mathrm{BL}}(N)}{\left|\mathrm{Ext}^1_R(U^\vee_{T,R}, N)\right|} \sum_{\alpha \in \mathrm{Hom}_R(U^\vee_{T,R}[\ell], N/\ell N)} \left|\ker \delta^N_\ell\right| \cdot \frac{|N[\ell]| \cdot \left|U^\vee_{T,R}[\ell]\right|}{\left|\alpha(U^\vee_{T,R}[\ell])\right|} \\ &= \sum_{N \in \mathcal{M}_V} \frac{\mathbb{P}^{\mathrm{BL}}(N)}{\left|\mathrm{Hom}_R(U^\vee_{T,R}[\ell], N/\ell N)\right|} \cdot |N[\ell]| \cdot \sum_{\alpha \in \mathrm{Hom}_R(U^\vee_{T,R}[\ell], N/\ell N)} |\ker \alpha|.\end{aligned}$$

Using Lemma 8.18 we can rewrite this as

$$\mathbb{E}(f_T) = \sum_{N_0 \in \mathcal{M}} \frac{\mathbb{P}_V(N_0)}{\left|\mathrm{Hom}_R\left(U^\vee_{T,R}[\ell], \frac{P_V \oplus N_0}{\ell(P_V \oplus N_0)}\right)\right|} \cdot |N_0[\ell]| \cdot \sum_{\alpha \in \mathrm{Hom}_R\left(U^\vee_{T,R}[\ell], \frac{P_V \oplus N_0}{\ell(P_V \oplus N_0)}\right)} |\ker \alpha|.$$

Now we split up everything into local parts via Lemma 9.39. With the shorthand notation $P_{i,\mathfrak{p}} := (\widehat{P_V})_{i,\mathfrak{p}}$ and $U_{i,\mathfrak{p}} := (\widehat{U_{T,R}^\vee[\ell]})_{i,\mathfrak{p}}$ we have

$$\begin{aligned}\mathbb{E}(f_T) = \prod_{i=1}^{c} \prod_{\mathfrak{p}\in \operatorname{Max}(Z_i)} \sum_{M\in\mathcal{M}_{i,\mathfrak{p}}} & \frac{\mathbb{P}_{i,\mathfrak{p}}(M)}{\left|\operatorname{Hom}_{\widehat{R}_{i,\mathfrak{p}}}\left(U_{i,\mathfrak{p}}, \frac{P_{i,\mathfrak{p}}\oplus M}{\ell(P_{i,\mathfrak{p}}\oplus M)}\right)\right|} \cdot |M[\ell]| \\ & \cdot \sum_{\alpha\in \operatorname{Hom}_{\widehat{R}_{i,\mathfrak{p}}}\left(U_{i,\mathfrak{p}}, \frac{P_{i,\mathfrak{p}}\oplus M}{\ell(P_{i,\mathfrak{p}}\oplus M)}\right)} |\ker\alpha|\,.\end{aligned}$$

We next investigate the sum over α. Let $i \in \{1,\dots,c\}$, let $\mathfrak{p} \in \operatorname{Max}(Z_i)$ and let $M \in \mathcal{M}_{i,\mathfrak{p}}$. Since G is abelian, we have $R_i = Z_i$ and therefore $\widehat{R}_{i,\mathfrak{p}} = \widehat{Z}_{i,\mathfrak{p}}$. By Lemma 9.37 it holds that $\ell\widehat{Z}_{i,\mathfrak{p}} = \widehat{\mathfrak{p}}$. Since both $U_{i,\mathfrak{p}}$ and $(P_{i,\mathfrak{p}}\oplus M)/\ell(P_{i,\mathfrak{p}}\oplus M)$ are annihilated by ℓ, it follows that

$$\begin{aligned}\operatorname{Hom}_{\widehat{R}_{i,\mathfrak{p}}}\left(U_{i,\mathfrak{p}}, \frac{P_{i,\mathfrak{p}}\oplus M}{\ell(P_{i,\mathfrak{p}}\oplus M)}\right) &= \operatorname{Hom}_{\widehat{Z}_{i,\mathfrak{p}}}\left(U_{i,\mathfrak{p}}, \frac{P_{i,\mathfrak{p}}\oplus M}{\ell(P_{i,\mathfrak{p}}\oplus M)}\right) \\ &= \operatorname{Hom}_{\widehat{Z}_{i,\mathfrak{p}}/\widehat{\mathfrak{p}}}\left(U_{i,\mathfrak{p}}, \frac{P_{i,\mathfrak{p}}\oplus M}{\ell(P_{i,\mathfrak{p}}\oplus M)}\right).\end{aligned}$$

Thus, Lemma 9.40 gives

$$\begin{aligned}&\sum_{\alpha\in \operatorname{Hom}_{\widehat{R}_{i,\mathfrak{p}}}\left(U_{i,\mathfrak{p}}, \frac{P_{i,\mathfrak{p}}\oplus M}{\ell(P_{i,\mathfrak{p}}\oplus M)}\right)} |\ker\alpha| \\ &\qquad = \frac{\left|\operatorname{Hom}_{\widehat{R}_{i,\mathfrak{p}}}\left(U_{i,\mathfrak{p}}, \frac{P_{i,\mathfrak{p}}\oplus M}{\ell(P_{i,\mathfrak{p}}\oplus M)}\right)\right|}{|P_{i,\mathfrak{p}}/\ell P_{i,\mathfrak{p}}|\cdot|M[\ell]|} \cdot (|U_{i,\mathfrak{p}}| + |P_{i,\mathfrak{p}}/\ell P_{i,\mathfrak{p}}|\cdot|M[\ell]| - 1)\end{aligned}$$

which yields

$$\begin{aligned}\mathbb{E}(f_T) &= \prod_{i=1}^{c} \prod_{\mathfrak{p}\in \operatorname{Max}(Z_i)} \sum_{M\in\mathcal{M}_{i,\mathfrak{p}}} \frac{\mathbb{P}_{i,\mathfrak{p}}(M)}{|P_{i,\mathfrak{p}}/\ell P_{i,\mathfrak{p}}|} \cdot (|U_{i,\mathfrak{p}}| + |P_{i,\mathfrak{p}}/\ell P_{i,\mathfrak{p}}|\cdot|M[\ell]| - 1) \\ &= \prod_{i=1}^{c} \prod_{\mathfrak{p}\in \operatorname{Max}(Z_i)} \left(\frac{|U_{i,\mathfrak{p}}| - 1}{|P_{i,\mathfrak{p}}/\ell P_{i,\mathfrak{p}}|} + \sum_{M\in\mathcal{M}_{i,\mathfrak{p}}} \mathbb{P}_{i,\mathfrak{p}}(M)\cdot|M[\ell]|\right).\end{aligned}$$

Let $i \in \{1,\dots,c\}$, let $\mathfrak{p} \in \operatorname{Max}(Z_i)$ and let $M \in \mathcal{M}_{i,\mathfrak{p}}$. Using again that $\ell\widehat{Z}_{i,\mathfrak{p}} = \widehat{\mathfrak{p}}$, we have

$$M[\ell] = \left\{ x\in M \,\middle|\, \operatorname{ann}_{\widehat{Z}_{i,\mathfrak{p}}}(x) \mid \widehat{\mathfrak{p}} \right\} = \left\{ x\in M \,\middle|\, \operatorname{ann}_{\widehat{Z}_{i,\mathfrak{p}}}(x) = \widehat{\mathfrak{p}} \right\} \cup \{0\}\,.$$

Then Lemma 9.41 gives

$$|M[\ell]| = 1 + \left|\operatorname{Aut}_{\widehat{Z}_{i,\mathfrak{p}}}(\widehat{Z}_{i,\mathfrak{p}}/\widehat{\mathfrak{p}})\right| \cdot \left|\left\{ W \le M \,\middle|\, W \cong \widehat{Z}_{i,\mathfrak{p}}/\widehat{\mathfrak{p}} \right\}\right|.$$

Taking into account that $\widehat{R}_{i,\mathfrak{p}} = \widehat{Z}_{i,\mathfrak{p}}$, by [CM90, Theorem 2.6 and Example 4.5 (ii)] we have

$$\sum_{M \in \mathcal{M}_{i,\mathfrak{p}}} \mathbb{P}_{i,\mathfrak{p}}(M) \cdot \left| \left\{ W \leq M \,\middle|\, W \cong \widehat{Z}_{i,\mathfrak{p}}/\widehat{\mathfrak{p}} \right\} \right| = \frac{1}{\left| \widehat{Z}_{i,\mathfrak{p}}/\widehat{\mathfrak{p}} \right|^{u(P_{i,\mathfrak{p}})} \cdot \left| \mathrm{Aut}_{\widehat{Z}_{i,\mathfrak{p}}}(\widehat{Z}_{i,\mathfrak{p}}/\widehat{\mathfrak{p}}) \right|}$$
$$= \frac{1}{|Z_i/\mathfrak{p}|^{u_i(P_V)} \cdot \left| \mathrm{Aut}_{\widehat{Z}_{i,\mathfrak{p}}}(\widehat{Z}_{i,\mathfrak{p}}/\widehat{\mathfrak{p}}) \right|},$$

where we use the notation $\underline{u} = (u_i)_i$ from [CM90, Definition 2.2]. It follows that

$$\mathbb{E}(f_T) = \prod_{i=1}^{c} \prod_{\mathfrak{p} \in \mathrm{Max}(Z_i)} \left(\frac{|U_{i,\mathfrak{p}}| - 1}{|P_{i,\mathfrak{p}}/\ell P_{i,\mathfrak{p}}|} + 1 + \frac{1}{|Z_i/\mathfrak{p}|^{u_i(P_V)}} \right).$$

Note that by [CM90, Corollary 2.8] and since G is abelian we have

$$|P_{i,\mathfrak{p}}/\ell P_{i,\mathfrak{p}}| = \left|P_{i,\mathfrak{p}}/\widehat{\mathfrak{p}} P_{i,\mathfrak{p}}\right| = \left|P_{i,\mathfrak{p}}/\mathfrak{p}' P_{i,\mathfrak{p}}\right| = |Z_i/\mathfrak{p}|^{u_i(P_V)} = |Z_i/\mathfrak{p}|^{\dim_{K_i}(V_i)},$$

which yields

$$\mathbb{E}(f_T) = \prod_{i=1}^{c} \prod_{\mathfrak{p} \in \mathrm{Max}(Z_i)} \left(\frac{|U_{i,\mathfrak{p}}|}{|Z_i/\mathfrak{p}|^{\dim_{K_i}(V_i)}} + 1 \right).$$

Let $i \in \{1, \ldots, c\}$ and $\mathfrak{p} \in \mathrm{Max}(Z_i)$. By Lemmas 3.3 and 4.19 and Corollary 4.18 we have

$$U_{i,\mathfrak{p}} = \widehat{U_{T,R}^{\vee}[\ell]}_{i,\mathfrak{p}} = (\widehat{U_{T,R}^{\vee}})_{i,\mathfrak{p}}[\ell] \cong ((\widehat{U_{T,R}})_{i,\mathfrak{p}})^{\vee}[\ell],$$

which together with self-duality of finite abelian groups gives

$$|U_{i,\mathfrak{p}}| = \left| (\widehat{U_{T,R}})_{i,\mathfrak{p}}[\ell] \right| = \left| \widehat{U_{T,R}[\ell]}_{i,\mathfrak{p}} \right|.$$

Now by definition of $U_{T,R}$ and Lemma 7.15 (iii) it holds that

$$U_{T,R}[\ell] = R \otimes_{\mathbb{Z}G} U_T[\ell] = U_T[\ell]_1 \oplus \cdots \oplus U_T[\ell]_c,$$

so $\widehat{U_{T,R}[\ell]}_{i,\mathfrak{p}} = \widehat{U_T[\ell]}_{i,\mathfrak{p}} \cong U_T[\ell]_i[\mathfrak{p}^\infty]$. The maximal ideals of Z_i are in natural bijection with the maximal ideals of $\mathcal{O}_{K_i}$ lying over ℓ, and it is clear that this bijection preserves residue field degrees and primary components. The claim follows. □

Corollary 9.43. *Use Setup 8.37 with G abelian and $S = \{\ell\}$ where ℓ is a prime with $\ell \nmid |\mathrm{Cl}_F| \cdot |G|$. Assume that Conjecture 8.38 holds for f_T. Then*

$$\lim_{B \to \infty} \frac{\sum_{(K,\iota) \in \mathcal{K}_{C \leq B}^T} |\mathrm{Cl}_K(\mathfrak{m})[\ell]|}{\left| \mathcal{K}_{C \leq B}^T \right|} = \left| U_T[\ell]^G \right| \cdot \prod_{i=1}^{c} \prod_{\substack{\mathfrak{q} \in \mathrm{Max}(\mathcal{O}_{K_i}) \\ \mathfrak{q} | \ell}} \left(\frac{|U_T[\ell]_i[\mathfrak{q}^\infty]|}{\ell^{f(\mathfrak{q}|\ell) \cdot \dim_{K_i}(V_i)}} + 1 \right).$$

Proof. This is immediate from Propositions 9.31 and 9.32 and Theorem 9.42. □

Taking Proposition 8.22 into account, the above statement immediately implies Corollary 1.16 about the average torsion of $\mathrm{Cl}_K(\mathfrak{m})$ on the whole family $\mathcal{K}$:

Corollary 9.44. *Use Setup 8.37 with G abelian and $S = \{\ell\}$ where ℓ is a prime with $\ell \nmid |\mathrm{Cl}_F| \cdot |G|$, but do not fix T. Assume that for all viable collections of G-structured $F_\mathfrak{p}$-algebras $T = (T_\mathfrak{p})_{\mathfrak{p}|\mathfrak{m}_F}$, Conjecture 8.38 holds for f_T. Then the limit*

$$\lim_{B\to\infty} \frac{\sum_{(K,\iota)\in\mathcal{K}_{C\le B}} |\mathrm{Cl}_K(\mathfrak{m})[\ell]|}{|\mathcal{K}_{C\le B}|}$$

exists and equals

$$\sum_{\substack{T=(T_\mathfrak{p})_{\mathfrak{p}|\mathfrak{m}_F} \\ \text{viable } /\cong}} \mathrm{Pr}_C(T) \cdot \left|U_T[\ell]^G\right| \cdot \prod_{i=1}^{c} \prod_{\substack{\mathfrak{q}\in\mathrm{Max}(\mathcal{O}_{K_i}) \\ \mathfrak{q}|\ell}} \left(\frac{|U_T[\ell]_i[\mathfrak{q}^\infty]|}{\ell^{f(\mathfrak{q}|\ell)\cdot \dim_{K_i}(V_i)}} + 1 \right),$$

where T runs over viable collections of G-structured $F_\mathfrak{p}$-algebras up to isomorphism.

10 Average Torsion of Ray Class Groups of Cyclic Fields of Prime Degree

The aim of this chapter is to make explicit the formula for the average torsion of ray class groups from Corollary 9.44 in the case of cyclic fields of prime degree.

Throughout this chapter let q be a prime number.

10.1 Families of Cyclic Extensions of Prime Degree

Let F be a number field and fix an algebraic closure $\overline{F}$ of F. Let $0 \neq \mathfrak{m}_F \trianglelefteq \mathcal{O}_F$. We discuss how to model families of C_q-extensions of F in terms of Setup 8.37.

Note first that $\mathbb{Q}C_q \cong \mathbb{Q} \times \mathbb{Q}(\zeta_q)$, so the only choice for I that leads to nontrivial statements is $I = \langle \sum_{h \in C_q} h \rangle$. Then $A = \mathbb{Q}(\zeta_q)$. All primes except q are good for A. In order to obtain a nonempty family $\mathcal{K}$, we may choose for S any finite set of primes different from q with the property that $\mu_p \nsubseteq F$ for all $p \in S$. With the above choices and W as the appropriate finitely generated $\mathbb{Q}C_q$-module, the family $\mathcal{K}$ in Setup 8.37 models the family of C_q-extensions of F with signature given by W.

Later on, we will focus on the case $F = \mathbb{Q}$. Note that if $q > 2$, then every C_q-extension of $\mathbb{Q}$ is necessarily totally real. The family of such extensions in the setup from above is modelled by taking $W = \mathbb{Q}(\zeta_q)$. If $q = 2$, then a C_q-extension of $\mathbb{Q}$ can be totally imaginary or totally real. The totally real C_2-extensions of $\mathbb{Q}$, i.e. the real quadratic number fields, are modelled by $W = \mathbb{Q}(-1)$. The totally imaginary C_2-extensions of $\mathbb{Q}$, i.e. the imaginary quadratic number fields, are modelled $W = 0$.

10.1.1 C_q-Structured Algebras

We next discuss the viable collections $T = (T_{\mathfrak{p}})_{\mathfrak{p} \mid \mathfrak{m}_F}$ of C_q-structured $F_{\mathfrak{p}}$-algebras.

We have the following general result.

Proposition 10.1. *Let F be a number field. Let P be a finite set of places of F and let $T = (T_v)_{v \in P}$ be a collection of C_q-structured F_v-algebras. Then T is viable for C_q and F. Moreover, for any fair counting function C on $E_{C_q}(F)$ we have*

$$\mathrm{Pr}_C(T) = \prod_{v \in P} \mathrm{Pr}_C(T_v)$$

and

$$\mathrm{Pr}_C(T_v) = N(v)^{-c_v(T_v)/m_C} \cdot \left(\sum_{T_v' \in A_{C_q}(F_v)} N(v)^{-c_v(T_v')/m_C} \right)^{-1}.$$

Proof. That T is viable follows from [Woo10, page 108]. The second claim follows from [Woo10, Corollary 2.4] and the third claim from [Woo10, Corollary 2.2]. □

We now classify the C_q-structured F_v-algebras and give their probabilities.

Proposition 10.2. *Let F be a field. Then the C_q-structured F-algebras up to isomorphism are given by:*

- *F^q with $C_q \hookrightarrow \mathrm{Aut}_F(F^q) = S_q$ mapping a generator of C_q to $(1\ 2 \cdots q)$,*
- *the C_q-extensions of F.*

Proof. This is just an application of Proposition 8.8. □

Proposition 10.3. *Let F be a field. Let G be a finite abelian group. Denote by $E'_G(F)$ a system of representatives of G-extensions of F up to isomorphism as F-algebras. Then the map*

$$E'_G(F) \times \mathrm{Aut}(G) \to E_G(F),\ \ ((K, \iota_K), \alpha) \mapsto (K, \iota_K \circ \alpha)$$

is a bijection.

Proof. This is straightforward. □

Proposition 10.4. *Let $F/\mathbb{Q}_p$ be a finite extension. We give the number of C_q-extensions of F up to F-isomorphism.*

(i) Suppose that $q \neq p$. Then:

(a) There is 1 unramified C_q-extension of F up to F-isomorphism, namely $F(\zeta_{p^{fq}-1})$ where f is the residue field degree of $F/\mathbb{Q}_p$.

(b) If $|\mu_q(F)| = 1$, then there is no totally tamely ramified C_q-extension of F. If $|\mu_q(F)| = q$, then there are $\left|\mathcal{O}_F^\times/(\mathcal{O}_F^\times)^q\right| = |\mu_q(F)| = q$ totally tamely ramified C_q-extensions of F up to F-isomorphism. If $\pi \in \mathcal{O}_F$ is a uniformiser, these are given by $F(\sqrt[q]{u\pi})$ where u runs over a system of representatives for the classes in $\mathcal{O}_F^\times/(\mathcal{O}_F^\times)^q$.

(ii) Suppose that $q = p$. Then:

(a) There is 1 unramified C_p-extension of F up to F-isomorphism, namely $F(\zeta_{p^{fp}-1})$ where f is the residue field degree of $F/\mathbb{Q}_p$.

(b) If $|\mu_p(F)| = 1$, then there are $p + \cdots + p^{|F:\mathbb{Q}_p|}$ many totally wildly ramified C_p-extensions of F up to F-isomorphism. If $|\mu_p(F)| = p$, then there are $p + \cdots + p^{|F:\mathbb{Q}_p|+1}$ many totally wildly ramified C_p-extensions of F up to F-isomorphism.

Proof. Note that since q is prime, every C_q-extension K/F is either unramified or totally ramified. The statements on unramified extensions are well-known.

Suppose that $q \neq p$. If there is a totally tamely ramified C_q-extension K/F, then by [CF67, Proposition 1 on page 32], we have $|\mu_q(F)| = q$. Now assume that $|\mu_q(F)| = q$. By loc. cit. there is a bijection

$$\{\text{uniformisers of } \mathcal{O}_F\} / \sim \ \xrightarrow{\sim} \{\text{tot. tamely ram. } C_q\text{-ext. of } F\} / \cong_F, \ [\pi] \mapsto [F(\sqrt[q]{\pi})],$$

where $\pi' \sim \pi$ if and only if $\overline{\pi'\pi^{-1}} \in ((\mathcal{O}_F/\mathfrak{p})^\times)^q$, where $\mathfrak{p}$ is the maximal ideal of $\mathcal{O}_F$. As in the proof of Proposition 10.7 below, since $q \neq p$, the natural map

$$\frac{\mathcal{O}_F^\times}{(\mathcal{O}_F^\times)^q} \to \frac{(\mathcal{O}_F/\mathfrak{p})^\times}{((\mathcal{O}_F/\mathfrak{p})^\times)^q}$$

is a bijection, from which it follows that $\pi' \sim \pi$ if and only if $\pi'\pi^{-1} \in (\mathcal{O}_F^\times)^q$. Hence, if $\pi \in \mathcal{O}_F$ is a uniformiser, then the map

$$\mathcal{O}_F^\times/(\mathcal{O}_F^\times)^q \to \{\text{uniformisers of } \mathcal{O}_F\} / \sim, \ \overline{u} \mapsto [\pi u]$$

is a bijection. This proves part (b) of (i).

The claims in part (b) of (ii) are [Sha47, Consequence 2] for $|\mu_p(F)| = 1$ and [Yam95, Theorem 1] for $|\mu_p(F)| = p$. □

Proposition 10.5. *Let F be a number field and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_F$.*

(i) Suppose $\mathfrak{p} \nmid q$ and $|\mu_q(F_\mathfrak{p})| = 1$. Then the C_q-structured $F_\mathfrak{p}$-algebras up to isomorphism are given by

- $F_\mathfrak{p}^q$,
- *1 unramified C_q-extension $L/F_\mathfrak{p}$ with $q-1$ different C_q-structures.*

Let C be either the norm of the product of the ramified primes or the norm of the conductor or the norm of the discriminant. Then in the respective cases we have

- $\mathrm{Pr}_C(F_\mathfrak{p}^q) = \frac{1}{q}$,
- $\mathrm{Pr}_C(L) = \frac{1}{q}$.

(ii) Suppose $\mathfrak{p} \nmid q$ and $|\mu_q(F_\mathfrak{p})| = q$. Then the C_q-structured $F_\mathfrak{p}$-algebras up to isomorphism are given by

- $F_\mathfrak{p}^q$,
- *1 unramified C_q-extension $L/F_\mathfrak{p}$ with $q-1$ different C_q-structures,*
- *q totally tamely ramified C_q-extensions $L/F_\mathfrak{p}$ with $q-1$ different C_q-structures each.*

Let C be either the norm of the product of the ramified primes or the norm of the conductor or the norm of the discriminant. Then in the respective cases we have

- $\mathrm{Pr}_C(F_{\mathfrak{p}}^q) = \frac{N(\mathfrak{p})}{qN(\mathfrak{p})+q(q-1)}$,
- $\mathrm{Pr}_C(L) = \frac{N(\mathfrak{p})}{qN(\mathfrak{p})+q(q-1)}$,
- $\mathrm{Pr}_C(L) = \frac{1}{qN(\mathfrak{p})+q(q-1)}$.

(iii) Suppose $\mathfrak{p} \mid q$ and $|\mu_q(F_{\mathfrak{p}})| = 1$. Then the C_q-structured $F_{\mathfrak{p}}$-algebras up to isomorphism are given by

- $F_{\mathfrak{p}}^q$,
- *1 unramified C_q-extension $L/F_{\mathfrak{p}}$ with $q-1$ different C_q-structures,*
- *$q+\cdots+q^{|F_{\mathfrak{p}}:\mathbb{Q}_q|}$ totally wildly ramified C_q-extensions $L/F_{\mathfrak{p}}$ with $q-1$ different C_q-structures each.*

Let C be the norm of the product of the ramified primes. Then in the respective cases we have

- $\mathrm{Pr}_C(F_{\mathfrak{p}}^q) = \frac{N(\mathfrak{p})}{qN(\mathfrak{p})+(q+\cdots q^{|F_{\mathfrak{p}}:\mathbb{Q}_q|})(q-1)}$,
- $\mathrm{Pr}_C(L) = \frac{N(\mathfrak{p})}{qN(\mathfrak{p})+(q+\cdots q^{|F_{\mathfrak{p}}:\mathbb{Q}_q|})(q-1)}$,
- $\mathrm{Pr}_C(L) = \frac{1}{qN(\mathfrak{p})+(q+\cdots q^{|F_{\mathfrak{p}}:\mathbb{Q}_q|})(q-1)}$.

(iv) Suppose $\mathfrak{p} \mid q$ and $|\mu_q(F_{\mathfrak{p}})| = q$. Then the C_q-structured $F_{\mathfrak{p}}$-algebras up to isomorphism are given by

- $F_{\mathfrak{p}}^q$,
- *1 unramified C_q-extension $L/F_{\mathfrak{p}}$ with $q-1$ different C_q-structures,*
- *$q+\cdots+q^{|F_{\mathfrak{p}}:\mathbb{Q}_q|+1}$ totally wildly ramified C_q-extensions $L/F_{\mathfrak{p}}$ with $q-1$ different C_q-structures each.*

Let C be the norm of the product of the ramified primes. Then in the respective cases we have

- $\mathrm{Pr}_C(F_{\mathfrak{p}}^q) = \frac{N(\mathfrak{p})}{qN(\mathfrak{p})+(q+\cdots q^{|F_{\mathfrak{p}}:\mathbb{Q}_q|+1})(q-1)}$,
- $\mathrm{Pr}_C(L) = \frac{N(\mathfrak{p})}{qN(\mathfrak{p})+(q+\cdots q^{|F_{\mathfrak{p}}:\mathbb{Q}_q|+1})(q-1)}$,
- $\mathrm{Pr}_C(L) = \frac{1}{qN(\mathfrak{p})+(q+\cdots q^{|F_{\mathfrak{p}}:\mathbb{Q}_q|+1})(q-1)}$.

Proof. The respective lists of C_q-structured $F_{\mathfrak{p}}$-algebras are obtained from Propositions 10.2, 10.3 and 10.4. The probabilities are easily calculated using Proposition 10.1 and Example 8.11. □

In cases (iii) and (iv) the probabilities for C the norm of the conductor and the norm of the discriminant depend on the conductor and the discriminant, respectively, of the totally wildly ramified C_q-extensions of $F_{\mathfrak{p}}$. Given knowledge of the latter, these probabilities can be calculated explicitly using Proposition 10.1. We will do this below in the case $q = 2$.

10.2 Generalities on Average Torsion

Use Setup 8.37 with the specifications $G = C_q$, $I = \langle \sum_{h \in C_q} h \rangle$, $S = \{\ell\}$, where ℓ is a prime with $\ell \nmid |\mathrm{Cl}_F| \cdot q$, and do not fix T. Conditional on Conjecture 8.38, Corollary 9.44 shows that the limit

$$\lim_{B \to \infty} \frac{\sum_{(K,\iota) \in \mathcal{K}_{C \leq B}} |\mathrm{Cl}_K(\mathfrak{m})[\ell]|}{|\mathcal{K}_{C \leq B}|}$$

exists and equals

$$\mathrm{Av}_{\mathcal{K},C}(\ell) := \sum_{T = (T_{\mathfrak{p}})_{\mathfrak{p} | \mathfrak{m}_F}/\cong} \mathrm{Pr}_C(T) \cdot \left| U_T[\ell]^G \right| \cdot \prod_{\substack{\mathfrak{q} \in \mathrm{Max}(\mathbb{Z}[\zeta_q]) \\ \mathfrak{q} | \ell}} \left(\frac{|U_T[\ell]_1[\mathfrak{q}^\infty]|}{\ell^{f(\mathfrak{q}|\ell) \cdot \dim_{\mathbb{Q}(\zeta_q)}(W_1)}} + 1 \right).$$

Recall here that all collections $T = (T_{\mathfrak{p}})_{\mathfrak{p} | \mathfrak{m}_F}$ of C_q-structured $F_{\mathfrak{p}}$-algebras are viable by Proposition 10.1. Note that in the notation of Section 9.5, $A = A_1 = \mathbb{Q}(\zeta_q)$, $e_0 = \frac{1}{q} \sum_{h \in C_q} h$ and $e_1 = \frac{1}{q}(q - 1 - \sum_{1 \neq h \in C_q} h)$. Note further that by Proposition 10.1, all terms in $\mathrm{Av}_{\mathcal{K},C}(\ell)$ involving T can be expressed as products whose factors only depend on one $T_{\mathfrak{p}}$ at a time.

Our aim in this section is to provide tools to explicitly calculate all terms occurring in $\mathrm{Av}_{\mathcal{K},C}(\ell)$ for the case $F = \mathbb{Q}$ and for

- ℓ inert in $\mathbb{Q}(\zeta_q)$,
- ℓ totally split in $\mathbb{Q}(\zeta_q)$, that is, $\ell \equiv 1 \mod q$.

Note that if $F = \mathbb{Q}$, then $\dim_{\mathbb{Q}(\zeta_q)}(W_1) = 1$. The probabilities $\mathrm{Pr}_C(T)$ have already been discussed in the previous section.

10.2.1 Torsion in Unit Groups of Residue Rings of p-Adic Fields

The following statements can be used to calculate $|U_T[\ell]|$ and $\left| U_T[\ell]^G \right|$.

Proposition 10.6. *Let $K/\mathbb{Q}_p$ be a finite extension of degree d with valuation ring $\mathcal{O}_K$. Let e be the ramification index and f be the residue field degree. Let $r \in \mathbb{Z}_{\geq 1}$ and let ℓ be a prime. Then we have*

$$\left| \frac{\mathcal{O}_K^\times}{(\mathcal{O}_K^\times)^\ell} \right| = p^{d \cdot v_p(\ell)} \cdot |\mu_\ell(K)|.$$

If moreover $K/\mathbb{Q}_p$ is Galois with Galois group G, then for $\ell \neq p$ it holds that

$$\left|\left(\frac{\mathcal{O}_K^\times}{(\mathcal{O}_K^\times)^\ell}\right)^G\right| = \begin{cases} \ell, & \ell \mid p-1, \\ 1, & \ell \nmid p-1. \end{cases}$$

If $p \nmid d = |G|$, we also have

$$\left|\left(\frac{\mathcal{O}_K^\times}{(\mathcal{O}_K^\times)^p}\right)^G\right| = \begin{cases} 4, & p = 2, \\ p, & p > 2. \end{cases}$$

Proof. The first statement is [Neu99, Corollary II.5.8]. Now assume that $K/\mathbb{Q}_p$ is Galois with Galois group G. Denote by $\mathfrak{p}$ the maximal ideal of $\mathcal{O}_K$. First, we deal with the case $\ell \neq p$. Then by [Neu99, Proposition II.5.7] ℓ-powering is an isomorphism on $1 + \mathfrak{p}\mathcal{O}_K$. Thus, the snake lemma applied to

$$\begin{tikzcd}
1 \arrow[r] & 1+\mathfrak{p}\mathcal{O}_K \arrow[r] \arrow[d, "(\cdot)^\ell"] & \mathcal{O}_K^\times \arrow[r] \arrow[d, "(\cdot)^\ell"] & (\mathcal{O}_K/\mathfrak{p})^\times \arrow[r] \arrow[d, "(\cdot)^\ell"] & 1 \\
1 \arrow[r] & 1+\mathfrak{p}\mathcal{O}_K \arrow[r] & \mathcal{O}_K^\times \arrow[r] & (\mathcal{O}_K/\mathfrak{p})^\times \arrow[r] & 1
\end{tikzcd}$$

gives an isomorphism of G-modules

$$\frac{\mathcal{O}_K^\times}{(\mathcal{O}_K^\times)^\ell} \cong \frac{(\mathcal{O}_K/\mathfrak{p})^\times}{((\mathcal{O}_K/\mathfrak{p})^\times)^\ell}.$$

Now the inertia subgroup $I \trianglelefteq G$ acts trivially on $\mathcal{O}_K/\mathfrak{p}$, and $G/I \cong \mathrm{Gal}(\mathbb{F}_{p^f}/\mathbb{F}_p)$ which implies that

$$\left(\frac{\mathcal{O}_K^\times}{(\mathcal{O}_K^\times)^\ell}\right)^G \cong \left(\frac{(\mathcal{O}_K/\mathfrak{p})^\times}{((\mathcal{O}_K/\mathfrak{p})^\times)^\ell}\right)^G = \left(\frac{(\mathcal{O}_K/\mathfrak{p})^\times}{((\mathcal{O}_K/\mathfrak{p})^\times)^\ell}\right)^{G/I} \cong \left(\frac{\mathbb{F}_{p^f}^\times}{(\mathbb{F}_{p^f}^\times)^\ell}\right)^{\mathrm{Gal}(\mathbb{F}_{p^f}/\mathbb{F}_p)}.$$

We have $\mathrm{Gal}(\mathbb{F}_{p^f}/\mathbb{F}_p) = \langle\sigma\rangle$ where σ is the Frobenius homomorphism, and $\mathbb{F}_{p^f}^\times = \langle\zeta\rangle$ for some $\zeta \in \mathbb{F}_{p^f}^\times$. If $\ell \nmid p^f - 1$, then $\mathbb{F}_{p^f}^\times/(\mathbb{F}_{p^f}^\times)^\ell = 1$ and also the fixed points are trivial. From now on assume that $\ell \mid p^f - 1$. Then $\mathbb{F}_{p^f}^\times/(\mathbb{F}_{p^f}^\times)^\ell$ has size ℓ. So the set of fixed points either has size 1 or ℓ, and we can characterise the latter case as follows:

$$\begin{aligned}
\left|\left(\frac{\mathbb{F}_{p^f}^\times}{(\mathbb{F}_{p^f}^\times)^\ell}\right)^{\mathrm{Gal}(\mathbb{F}_{p^f}/\mathbb{F}_p)}\right| = \ell \quad &\iff \quad \overline{\zeta} = \sigma(\overline{\zeta}) = \overline{\zeta}^p \\
&\iff \quad \zeta^{p-1} \in (\mathbb{F}_{p^f}^\times)^\ell = \langle\zeta^\ell\rangle \\
&\iff \quad \exists t \in \mathbb{Z} : p^f - 1 \mid (p-1) - t\ell \\
&\iff \quad \ell \mid p - 1
\end{aligned}$$

where for the last equality we have used that $\ell \mid p^f - 1$. This proves the claim for $\ell \neq p$.

Finally, assume that $p \nmid d = |G|$. Consider the exact sequence of G-modules

$$1 \longrightarrow \mu_p(K) \longrightarrow \mathcal{O}_K^\times \xrightarrow{(\cdot)^p} (\mathcal{O}_K^\times)^p \longrightarrow 1.$$

Since $p \nmid |G|$, multiplication by $|G|$ is both the zero map and an isomorphism on $H^i(G, \mu_p(K))$ for all $i \geq 1$ which shows that $H^i(G, \mu_p(K)) = 1$ for all $i \geq 1$. Hence, the above sequence induces a long exact sequence

$$\cdots \longrightarrow \mathbb{Z}_p^\times \xrightarrow{(\cdot)^p} ((\mathcal{O}_K^\times)^p)^G \longrightarrow 1 \longrightarrow H^1(G, \mathcal{O}_K^\times) \longrightarrow H^1(G, (\mathcal{O}_K^\times)^p) \longrightarrow 1 \longrightarrow \cdots$$

We conclude that $((\mathcal{O}_K^\times)^p)^G = (\mathbb{Z}_p^\times)^p$ and $H^1(G, \mathcal{O}_K^\times) \cong H^1(G, (\mathcal{O}_K^\times)^p)$. Note moreover that the valuation exact sequence

$$1 \longrightarrow \mathcal{O}_K^\times \longrightarrow K^\times \longrightarrow \mathbb{Z} \longrightarrow 1$$

of G-modules together with Hilbert 90 shows that $H^1(G, \mathcal{O}_K^\times) \cong \mathbb{Z}/e\mathbb{Z}$ is cyclic of order e, and in particular finite. Now consider the canonical exact sequence of G-modules

$$1 \longrightarrow (\mathcal{O}_K^\times)^p \longrightarrow \mathcal{O}_K^\times \longrightarrow \frac{\mathcal{O}_K^\times}{(\mathcal{O}_K^\times)^p} \longrightarrow 1.$$

Since $\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^p$ is a p-group, we have $H^1(G, \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^p) = 1$ by the same argument as before, so that the induced long exact sequence gives an exact sequence

$$1 \longrightarrow \frac{\mathbb{Z}_p^\times}{(\mathbb{Z}_p^\times)^p} \longrightarrow \left(\frac{\mathcal{O}_K^\times}{(\mathcal{O}_K^\times)^p}\right)^G \longrightarrow H^1(G, (\mathcal{O}_K^\times)^p) \longrightarrow H^1(G, \mathcal{O}_K^\times) \longrightarrow 1$$

It follows that

$$\left|\left(\frac{\mathcal{O}_K^\times}{(\mathcal{O}_K^\times)^p}\right)^G\right| = \left|\frac{\mathbb{Z}_p^\times}{(\mathbb{Z}_p^\times)^p}\right|,$$

and we conclude using the first statement of the proposition. □

Proposition 10.7. *Let $K/\mathbb{Q}_p$ be a finite extension of degree d with valuation ring $\mathcal{O}_K$. Let e be the ramification index and f be the residue field degree. Let $r \in \mathbb{Z}_{\geq 1}$ and let ℓ be a prime.*

(i) Suppose that $\ell \neq p$. Then

$$\left|\frac{(\mathcal{O}_K/p^r)^\times}{((\mathcal{O}_K/p^r)^\times)^\ell}\right| = |\mu_\ell(K)| = \begin{cases} \ell, & \ell \mid p^f - 1, \\ 1, & \ell \nmid p^f - 1. \end{cases}$$

If moreover $K/\mathbb{Q}_p$ is Galois with Galois group G, then

$$\left|\left(\frac{(\mathcal{O}_K/p^r)^\times}{((\mathcal{O}_K/p^r)^\times)^\ell}\right)^G\right| = \begin{cases} \ell, & \ell \mid p - 1, \\ 1, & \ell \nmid p - 1. \end{cases}$$

(ii) For $\ell = p$ we further distinguish two cases:

(a) Suppose that $r \geq 2$. Then

$$\left|\frac{(\mathcal{O}_K/p^r)^\times}{((\mathcal{O}_K/p^r)^\times)^p}\right| = \begin{cases} 2^d, & p = 2, r = 2, \\ p^d \cdot |\mu_p(K)|, & \text{else.} \end{cases}$$

If moreover $K/\mathbb{Q}_p$ is Galois with Galois group G and $p \nmid d = |G|$, then

$$\left|\left(\frac{(\mathcal{O}_K/p^r)^\times}{((\mathcal{O}_K/p^r)^\times)^p}\right)^G\right| = \begin{cases} 2, & p = 2, r = 2, \\ 4, & p = 2, r > 2, \\ p, & p \neq 2. \end{cases}$$

(b) For $r = 1$ we have

$$\left|\frac{(\mathcal{O}_K/p)^\times}{((\mathcal{O}_K/p)^\times)^p}\right| = p^{f(e - \lceil \frac{e}{p} \rceil)}.$$

If moreover $K/\mathbb{Q}_p$ is Galois with Galois group G and $p \nmid d = |G|$, then

$$\left|\left(\frac{(\mathcal{O}_K/p)^\times}{((\mathcal{O}_K/p)^\times)^p}\right)^G\right| = 1.$$

Proof. For any ℓ and r, the surjective homomorphism $\mathcal{O}_K^\times \to (\mathcal{O}_K/p^r)^\times$ induces an exact sequence

$$\begin{tikzcd} 1 \arrow[r] & \frac{(\mathcal{O}_K^\times)^\ell \cdot (1 + p^r\mathcal{O}_K)}{(\mathcal{O}_K^\times)^\ell} \arrow[r] & \frac{\mathcal{O}_K^\times}{(\mathcal{O}_K^\times)^\ell} \arrow[r] & \frac{(\mathcal{O}_K/p^r)^\times}{((\mathcal{O}_K/p^r)^\times)^\ell} \arrow[r] & 1. \end{tikzcd}$$

Note that for the left hand term it holds that

$$\frac{(\mathcal{O}_K^\times)^\ell \cdot (1 + p^r\mathcal{O}_K)}{(\mathcal{O}_K^\times)^\ell} \cong \frac{(1 + p^r\mathcal{O}_K)}{(1 + p^r\mathcal{O}_K) \cap (\mathcal{O}_K^\times)^\ell},$$

so that we have an exact sequence

$$\begin{tikzcd} 1 \arrow[r] & \frac{1 + p^r\mathcal{O}_K}{(1 + p^r\mathcal{O}_K) \cap (\mathcal{O}_K^\times)^\ell} \arrow[r] & \frac{\mathcal{O}_K^\times}{(\mathcal{O}_K^\times)^\ell} \arrow[r] & \frac{(\mathcal{O}_K/p^r)^\times}{((\mathcal{O}_K/p^r)^\times)^\ell} \arrow[r] & 1. \end{tikzcd} \tag{10.8}$$

This will be the central object of the proof. If $K/\mathbb{Q}_p$ is Galois with Galois group G, then it is an exact sequence of G-modules.

Suppose that $\ell \neq p$. Then [Neu99, Proposition II.5.7] shows that ℓ-powering is an isomorphism on $1 + p^r\mathcal{O}_K$, so that

$$1 + p^r\mathcal{O}_K = (1 + p^r\mathcal{O}_K)^\ell \subseteq (1 + p^r\mathcal{O}_K) \cap (\mathcal{O}_K^\times)^\ell \subseteq 1 + p^r\mathcal{O}_K.$$

Hence, the left hand term in (10.8) is trivial and we have

$$\frac{\mathcal{O}_K^\times}{(\mathcal{O}_K^\times)^\ell} \cong \frac{(\mathcal{O}_K/p^r)^\times}{((\mathcal{O}_K/p^r)^\times)^\ell}.$$

Claim (i) then follows from Proposition 10.6.

Suppose from now on that $\ell = p$. We first fix some notation. We denote by $\mathfrak{p}$ the maximal ideal of $\mathcal{O}_K$ and write $U^{(n)} := 1 + \mathfrak{p}^n\mathcal{O}_K$ for $n \in \mathbb{Z}_{\geq 1}$. Note that $(p) = \mathfrak{p}^e$. Furthermore let π be a uniformiser for $\mathcal{O}_K$, so that $\mathfrak{p} = (\pi)$. We write v_K for the normalised discrete valuation on K. We will repeatedly make use of the following fact, cf. [Neu99, Proposition II.5.5]: The p-adic logarithm and exponential function furnish algebraic and topological isomorphisms

$$1 + \mathfrak{p}^n\mathcal{O}_K = U^{(n)} \cong \mathfrak{p}^n \qquad \text{for } n > \frac{e}{p-1}. \tag{10.9}$$

If $K/\mathbb{Q}_p$ is Galois with Galois group G, then these isomorphisms are also isomorphisms of G-modules, as can be seen from the definition of the exponential function, using that the elements of G are continuous. Moreover, we will use that

$$(\mathcal{O}_K^\times)^p \cap U^{(1)} = (U^{(1)})^p \tag{10.10}$$

which follows from [Neu99, Proposition II.5.3].

Suppose that $r \geq 2$. Then, unless $p = 2$ and $r = 2$, we have $er > e(r-1) > \frac{e}{p-1}$ in which case the isomorphisms from (10.9) fit into a commutative diagram

$$\begin{tikzcd}
1 + p^{r-1}\mathcal{O}_K \arrow[r, "\sim"] & p^{r-1}\mathcal{O}_K \\
1 + p^r\mathcal{O}_K \arrow[r, "\sim"] \arrow[u, hook] & p^r\mathcal{O}_K. \arrow[u, hook]
\end{tikzcd}$$

Since $p(p^{r-1}\mathcal{O}_K) = p^r\mathcal{O}_K$, this shows that $(1 + p^{r-1}\mathcal{O}_K)^p = 1 + p^r\mathcal{O}_K$. It follows that

$$(1 + p^r\mathcal{O}_K) \cap (\mathcal{O}_K^\times)^p = (1 + p^{r-1}\mathcal{O}_K)^p \cap (\mathcal{O}_K^\times)^p = (1 + p^{r-1}\mathcal{O}_K)^p = 1 + p^r\mathcal{O}_K.$$

So from (10.8) we get

$$\frac{\mathcal{O}_K^\times}{(\mathcal{O}_K^\times)^p} \cong \frac{(\mathcal{O}_K/p^r)^\times}{((\mathcal{O}_K/p^r)^\times)^p},$$

and we can again conclude using Proposition 10.6.

It remains to deal with the case $p = 2$ and $r = 2$. Here, the left hand term in (10.8) turns out to be nontrivial, and we will now explicitly calculate its size. To begin with, we claim that

$$(1 + 4\mathcal{O}_K) \cap (\mathcal{O}_K^\times)^2 = (1 + 2\mathcal{O}_K)^2. \tag{10.11}$$

It is evident that the right hand set is contained in the left hand set. Conversely, let $x \in (1+4\mathcal{O}_K) \cap (\mathcal{O}_K^\times)^2$. By (10.10) we can write $x = (1+\pi y)^2$ for some $y \in \mathcal{O}_K$. Then since $x \in 1+4\mathcal{O}_K$ we must have

$$v_K(\pi^{e+1}y + \pi^2 y^2) = v_K(2\pi y + \pi^2 y^2) \geq v_K(4) = 2e,$$

or equivalently

$$v_K(\pi^{e-1}y + y^2) \geq 2e - 2.$$

If $v_K(y) < e-1$, then $v_K(y^2) = 2v_K(y) < v_K(y) + e - 1 = v_K(\pi^{e-1}y)$ which implies $v_K(\pi^{e-1}y + y^2) = v_K(y^2) = 2v_K(y) < 2e-2$, a contradiction. So we must have $v_K(y) \geq e-1$ which gives $1 + \pi y \in 1 + \pi^e \mathcal{O}_K = 1 + 2\mathcal{O}_K$. Thus, $x \in (1+2\mathcal{O}_K)^2$, establishing (10.11).

We will calculate the size of the left hand side of (10.8) using the chain of subgroups

$$(1+4\mathcal{O}_K)^2 \subseteq (1+2\mathcal{O}_K)^2 \subseteq 1+4\mathcal{O}_K.$$

First, we have $1+4\mathcal{O}_K = 1+\mathfrak{p}^{2e} \cong \mathfrak{p}^{2e} = 4\mathcal{O}_K$ by (10.9). This gives isomorphisms of abelian groups

$$\frac{1+4\mathcal{O}_K}{(1+4\mathcal{O}_K)^2} \cong \frac{4\mathcal{O}_K}{2\cdot 4\mathcal{O}_K} \cong \frac{\mathcal{O}_K}{2\mathcal{O}_K} = \frac{\mathcal{O}_K}{\mathfrak{p}^e\mathcal{O}_K},$$

showing that the size of the left hand term is $|\mathcal{O}_K/\mathfrak{p}|^e = 2^{f\cdot e} = 2^d$. Secondly, using [Neu99, Proposition II.3.10], we have

$$\left|\frac{1+2\mathcal{O}_K}{1+4\mathcal{O}_K}\right| = \left|\frac{U^{(e)}}{U^{(2e)}}\right| = \prod_{i=e}^{2e-1}\left|\frac{U^{(i)}}{U^{(i+1)}}\right| = \prod_{i=e}^{2e-1} 2^f = 2^{f\cdot e} = 2^d. \tag{10.12}$$

Thirdly, there is an exact sequence

$$1 \longrightarrow \tfrac{\mu_2(K)\cdot(1+4\mathcal{O}_K)}{1+4\mathcal{O}_K} \longrightarrow \tfrac{1+2\mathcal{O}_K}{1+4\mathcal{O}_K} \xrightarrow{(\cdot)^2} \tfrac{(1+2\mathcal{O}_K)^2}{(1+4\mathcal{O}_K)^2} \longrightarrow 1.$$

For the left hand term it holds that

$$\frac{\mu_2(K)\cdot(1+4\mathcal{O}_K)}{1+4\mathcal{O}_K} \cong \frac{\mu_2(K)}{\mu_2(K)\cap(1+4\mathcal{O}_K)} = \mu_2(K) = \{\pm 1\}$$

since $1+4\mathcal{O}_K \cong 4\mathcal{O}_K$ is torsionfree. Hence, the exact sequence and (10.12) give

$$\left|\frac{(1+2\mathcal{O}_K)^2}{(1+4\mathcal{O}_K)^2}\right| = \frac{1}{2}\cdot\left|\frac{1+2\mathcal{O}_K}{1+4\mathcal{O}_K}\right| = 2^{d-1}.$$

Then using (10.11) and all the above results we obtain

$$\begin{aligned}\left|\frac{1+4\mathcal{O}_K}{(1+4\mathcal{O}_K)\cap(\mathcal{O}_K^\times)^2}\right| &= \left|\frac{1+4\mathcal{O}_K}{(1+2\mathcal{O}_K)^2}\right| \\ &= \left|\frac{1+4\mathcal{O}_K}{(1+4\mathcal{O}_K)^2}\right| \cdot \left|\frac{(1+2\mathcal{O}_K)^2}{(1+4\mathcal{O}_K)^2}\right|^{-1} \\ &= 2^d\cdot 2^{-d+1} \\ &= 2. \end{aligned} \tag{10.13}$$

The exact sequence (10.8) and Proposition 10.6 therefore give

$$\left|\frac{(\mathcal{O}_K/2^2)^\times}{((\mathcal{O}_K/2^2)^\times)^2}\right| = \left|\frac{\mathcal{O}_K^\times}{(\mathcal{O}_K^\times)^2}\right| \cdot \left|\frac{1+4\mathcal{O}_K}{(1+4\mathcal{O}_K)\cap(\mathcal{O}_K^\times)^2}\right|^{-1} = 2^d \cdot 2 \cdot 2^{-1} = 2^d.$$

Now assume further that $K/\mathbb{Q}_2$ is Galois with Galois group G, and that $2 \nmid d = |G|$. Then the left hand side of (10.8) has trivial first cohomology, since multiplication by $|G|$ is both the zero map and an isomorphism on it. Together with (10.11), this means that we obtain an exact sequence

$$1 \longrightarrow \left(\tfrac{1+4\mathcal{O}_K}{(1+2\mathcal{O}_K)^2}\right)^G \longrightarrow \left(\tfrac{\mathcal{O}_K^\times}{(\mathcal{O}_K^\times)^2}\right)^G \longrightarrow \left(\tfrac{(\mathcal{O}_K/2^2)^\times}{((\mathcal{O}_K/2^2)^\times)^2}\right)^G \longrightarrow 1. \tag{10.14}$$

To compute the size of the left hand term, we proceed as follows: Again, since $2 \nmid |G|$, the exact sequence of G-modules

$$1 \longrightarrow \mu_2(K) \longrightarrow 1+2\mathcal{O}_K \xrightarrow{(\cdot)^2} (1+2\mathcal{O}_K)^2 \longrightarrow 1$$

induces an exact sequence

$$1 \longrightarrow \mu_2(\mathbb{Q}_2) \longrightarrow 1+2\mathbb{Z}_2 \xrightarrow{(\cdot)^2} ((1+2\mathcal{O}_K)^2)^G \longrightarrow 1$$

which shows that $((1+2\mathcal{O}_K)^2)^G = (1+2\mathbb{Z}_2)^2$. Therefore, from the long exact sequence associated to the canonical sequence

$$1 \longrightarrow (1+2\mathcal{O}_K)^2 \longrightarrow 1+4\mathcal{O}_K \longrightarrow \tfrac{1+4\mathcal{O}_K}{(1+2\mathcal{O}_K)^2} \longrightarrow 1$$

we obtain an injection

$$\frac{1+4\mathbb{Z}_2}{(1+2\mathbb{Z}_2)^2} \hookrightarrow \left(\frac{1+4\mathcal{O}_K}{(1+2\mathcal{O}_K)^2}\right)^G.$$

Now by (10.13), the size of the left hand term is 2, whereas the size of the right hand term is at most 2. So the size of the right hand term must be 2. We conclude from (10.14) and Proposition 10.6 that

$$\begin{aligned}\left|\left(\frac{(\mathcal{O}_K/2^2)^\times}{((\mathcal{O}_K/2^2)^\times)^2}\right)^G\right| &= \left|\left(\frac{\mathcal{O}_K^\times}{(\mathcal{O}_K^\times)^2}\right)^G\right| \cdot \left|\left(\frac{1+4\mathcal{O}_K}{(1+2\mathcal{O}_K)^2}\right)^G\right|^{-1} \\ &= 4 \cdot 2^{-1} \\ &= 2,\end{aligned}$$

finishing part (ii) (a) of the proposition.

Suppose finally that $r = 1$. The proof in this case follows similar steps as the $p = 2$, $r = 2$ case above. We again explicitly calculate the size of the left hand size of (10.8). We claim that

$$(1+p\mathcal{O}_K) \cap (\mathcal{O}_K^\times)^p = (1+\mathfrak{p}^{\lceil \frac{e}{p} \rceil}\mathcal{O}_K)^p. \tag{10.15}$$

If $x \in (1+\mathfrak{p}^{\lceil \frac{e}{p} \rceil}\mathcal{O}_K)^p$, then there is $y \in \mathcal{O}_K$ such that $x = (1+\pi^{\lceil \frac{e}{p} \rceil}y)^p$. It follows that

$$x = \sum_{k=0}^{p} \binom{p}{k} (\pi^{\lceil \frac{e}{p} \rceil} y)^k = 1 + \sum_{k=1}^{p-1} \binom{p}{k} (\pi^{\lceil \frac{e}{p} \rceil} y)^k + \pi^{p \cdot \lceil \frac{e}{p} \rceil} y^p.$$

Since p divides the middle term on the right hand side and $p \cdot \lceil \frac{e}{p} \rceil \geq e$, it follows that $x \in 1 + p\mathcal{O}_K$. Conversely, let $x \in (1+p\mathcal{O}_K) \cap (\mathcal{O}_K^\times)^p$. Then by (10.10) we can write $x = (1+\pi y)^p$ for some $y \in \mathcal{O}_K$. Expanding this expression yields $\pi^p y^p \in p\mathcal{O}_K = \pi^e \mathcal{O}_K$, whence $p + pv_K(y) \geq e$. It follows that $1 + v_K(y) \geq \lceil \frac{e}{p} \rceil$, that is, $1 + \pi y \in 1 + \mathfrak{p}^{\lceil \frac{e}{p} \rceil}\mathcal{O}_K$. So (10.15) is proved.

To compute the size of the left hand side of (10.8), we consider the chain of subgroups

$$(1+p\mathcal{O}_K)^p \subseteq (1+\mathfrak{p}^{\lceil \frac{e}{p} \rceil}\mathcal{O}_K)^p \subseteq 1 + p\mathcal{O}_K.$$

We first compute the size of the quotient of the right hand term by the left hand term. If $p > 2$, then $e > \frac{e}{p-1}$ and (10.9) gives an isomorphism $1 + p\mathcal{O}_K \cong p\mathcal{O}_K$. It follows that

$$\left| \frac{1+p\mathcal{O}_K}{(1+p\mathcal{O}_K)^p} \right| = \left| \frac{p\mathcal{O}_K}{p^2\mathcal{O}_K} \right| = \left| \frac{\mathcal{O}_K}{p\mathcal{O}_K} \right| = \left| \frac{\mathcal{O}_K}{\mathfrak{p}^e\mathcal{O}_K} \right| = |\mathcal{O}_K/\mathfrak{p}|^e = p^d.$$

If $p = 2$, then (10.12) and (10.13) give

$$\left| \frac{1+2\mathcal{O}_K}{(1+2\mathcal{O}_K)^2} \right| = \left| \frac{1+2\mathcal{O}_K}{1+4\mathcal{O}_K} \right| \cdot \left| \frac{1+4\mathcal{O}_K}{(1+2\mathcal{O}_K)^2} \right| = 2^d \cdot 2 = 2^{d+1}.$$

Next, for arbitrary p again, by [Neu99, Proposition II.3.10] we have

$$\left| \frac{1+\mathfrak{p}^{\lceil \frac{e}{p} \rceil}\mathcal{O}_K}{1+p\mathcal{O}_K} \right| = \left| \frac{U^{(\lceil \frac{e}{p} \rceil)}}{U^{(e)}} \right| = \prod_{i=\lceil \frac{e}{p} \rceil}^{e-1} \left| \frac{U^{(i)}}{U^{(i+1)}} \right| = \prod_{i=\lceil \frac{e}{p} \rceil}^{e-1} p^f = p^{f \cdot (e - \lceil \frac{e}{p} \rceil)}.$$

Now consider the exact sequence

$$\begin{tikzcd} 1 \arrow[r] & \frac{\mu_p(K)\cdot(1+p\mathcal{O}_K)}{1+p\mathcal{O}_K} \arrow[r] & \frac{1+\mathfrak{p}^{\lceil \frac{e}{p} \rceil}\mathcal{O}_K}{1+p\mathcal{O}_K} \arrow[r, "(\cdot)^p"] & \frac{(1+\mathfrak{p}^{\lceil \frac{e}{p} \rceil}\mathcal{O}_K)^p}{(1+p\mathcal{O}_K)^p} \arrow[r] & 1. \end{tikzcd}$$

Its left hand term is

$$\frac{\mu_p(K)\cdot(1+p\mathcal{O}_K)}{1+p\mathcal{O}_K} \cong \frac{\mu_p(K)}{\mu_p(K) \cap (1+p\mathcal{O}_K)} = \begin{cases} 1, & p = 2 \\ \mu_p(K), & p > 2, \end{cases}$$

where we used that $1 + p\mathcal{O}_K \cong p\mathcal{O}_K$ is torsionfree if $p > 2$. Thus the exact sequence gives

$$\begin{aligned} \left| \frac{(1+\mathfrak{p}^{\lceil \frac{e}{p} \rceil}\mathcal{O}_K)^p}{(1+p\mathcal{O}_K)^p} \right| &= \left| \frac{1+\mathfrak{p}^{\lceil \frac{e}{p} \rceil}\mathcal{O}_K}{1+p\mathcal{O}_K} \right| \cdot \left| \frac{\mu_p(K)\cdot(1+p\mathcal{O}_K)}{1+p\mathcal{O}_K} \right|^{-1} \\ &= \begin{cases} 2^{f\cdot(e-\lceil \frac{e}{2} \rceil)}, & p = 2, \\ p^{f\cdot(e-\lceil \frac{e}{p} \rceil)} \cdot |\mu_p(K)|^{-1}, & p > 2. \end{cases} \end{aligned}$$

We now put (10.15) and all these intermediate results together to obtain

$$\begin{aligned}\left|\frac{1+p\mathcal{O}_K}{(1+p\mathcal{O}_K)\cap(\mathcal{O}_K^\times)^p}\right| &= \left|\frac{1+p\mathcal{O}_K}{(1+\mathfrak{p}^{\lceil \frac{e}{p}\rceil}\mathcal{O}_K)^p}\right| \\ &= \left|\frac{1+p\mathcal{O}_K}{(1+p\mathcal{O}_K)^p}\right|\cdot\left|\frac{(1+\mathfrak{p}^{\lceil \frac{e}{p}\rceil}\mathcal{O}_K)^p}{(1+p\mathcal{O}_K)^p}\right|^{-1} \\ &= \begin{cases} 2^{d+1}\cdot 2^{-f\cdot(e-\lceil\frac{e}{2}\rceil)}, & p=2,\\ p^d\cdot p^{-f\cdot(e-\lceil\frac{e}{p}\rceil)}\cdot|\mu_p(K)|\,, & p>2.\end{cases}\end{aligned} \tag{10.16}$$

This, (10.8) and Proposition 10.6 give

$$\begin{aligned}\left|\frac{(\mathcal{O}_K/p)^\times}{((\mathcal{O}_K/p)^\times)^p}\right| &= \left|\frac{\mathcal{O}_K^\times}{(\mathcal{O}_K^\times)^p}\right|\cdot\left|\frac{1+p\mathcal{O}_K}{(1+p\mathcal{O}_K)\cap(\mathcal{O}_K^\times)^p}\right|^{-1} \\ &= \begin{cases} 2^d\cdot 2\cdot 2^{-d-1}\cdot 2^{f\cdot(e-\lceil\frac{e}{2}\rceil)}, & p=2,\\ p^d\cdot|\mu_p(K)|\cdot p^{-d}\cdot p^{f\cdot(e-\lceil\frac{e}{p}\rceil)}\cdot|\mu_p(K)|^{-1}\,, & p>2,\end{cases} \\ &= p^{f\cdot(e-\lceil\frac{e}{p}\rceil)}.\end{aligned}$$

Finally, suppose that $K/\mathbb{Q}_p$ is Galois with Galois group G and $p\nmid d=|G|$. Then since the left hand side in (10.8) is a p-group, it has trivial first cohomology, so that there is an exact sequence

$$1\longrightarrow\left(\tfrac{1+p\mathcal{O}_K}{(1+p\mathcal{O}_K)\cap(\mathcal{O}_K^\times)^p}\right)^G\longrightarrow\left(\tfrac{\mathcal{O}_K^\times}{(\mathcal{O}_K^\times)^p}\right)^G\longrightarrow\left(\tfrac{(\mathcal{O}_K/p)^\times}{((\mathcal{O}_K/p)^\times)^p}\right)^G\longrightarrow 1. \tag{10.17}$$

We calculate the size of the left hand side. Using the fact that $((\mathcal{O}_K^\times)^p)^G=(\mathbb{Z}_p^\times)^p$ as shown in the proof of Proposition 10.6, the exact sequence

$$1\longrightarrow(1+p\mathcal{O}_K)\cap(\mathcal{O}_K^\times)^p\longrightarrow 1+p\mathcal{O}_K\longrightarrow\tfrac{1+p\mathcal{O}_K}{(1+p\mathcal{O}_K)\cap(\mathcal{O}_K^\times)^p}\longrightarrow 1$$

gives rise to an injection

$$\frac{1+p\mathbb{Z}_p}{(1+p\mathbb{Z}_p)\cap(\mathbb{Z}_p^\times)^p}\hookrightarrow\left(\frac{1+p\mathcal{O}_K}{(1+p\mathcal{O}_K)\cap(\mathcal{O}_K^\times)^p}\right)^G.$$

Now by (10.16), the left hand term has size 4 if $p=2$ and size p if $p>2$. On the other hand, by (10.17) and Proposition 10.6, the right hand term has size at most 4 if $p=2$ and size at most p if $p>2$. It follows that

$$\left|\left(\frac{1+p\mathcal{O}_K}{(1+p\mathcal{O}_K)\cap(\mathcal{O}_K^\times)^p}\right)^G\right|=\left|\frac{1+p\mathbb{Z}_p}{(1+p\mathbb{Z}_p)\cap(\mathbb{Z}_p^\times)^p}\right|=\left|\left(\frac{\mathcal{O}_K^\times}{(\mathcal{O}_K^\times)^p}\right)^G\right|.$$

Then (10.17) shows that

$$\left|\left(\frac{(\mathcal{O}_K/p)^\times}{((\mathcal{O}_K/p)^\times)^p}\right)^G\right|=1.$$

This finishes the proof. □

10.2.2 Primary Components of $U_T[\ell]_1$ for $\ell \equiv 1 \mod q$

We now discuss how to calculate the terms $|U_T[\ell]_1[\mathfrak{q}^\infty]|$ for $\ell \equiv 1 \mod q$ and $\mathfrak{q}$ a prime of $\mathbb{Z}[\zeta_q]$ above ℓ. It suffices to consider the case $T = T_p$, where $p \mid \mathfrak{m}_\mathbb{Q}$ and T_p is a C_q-structured $\mathbb{Q}_p$-algebra. We need a few lemmas.

Lemma 10.18. *Let ℓ be a prime with $\ell \equiv 1 \mod q$. Denote by $\mathfrak{q}_1, \dots, \mathfrak{q}_{q-1}$ the primes of $\mathbb{Z}[\zeta_q]$ above ℓ. Fix a generator g of C_q. Let M be a $\mathbb{Z}_{(\ell)}C_q$-module that is annihilated by ℓ. Let $n \in \mathbb{Z}$ such that n is congruent to a primitive q-th root of unity modulo ℓ. Let $N_i := \{ x \in M \mid gx = n^i x \}$ for $i = 1, \dots, q-1$. Then*

$$\{M_1[\mathfrak{q}_1^\infty], \dots, M_1[\mathfrak{q}_{q-1}^\infty]\} = \{N_1, \dots, N_{q-1}\}.$$

Proof. We have that $M_1 = e_1 M$ is an $e_1\mathbb{Z}_{(\ell)}C_q \cong \mathbb{Z}_{(\ell)}[\zeta_q]$-module, where the isomorphism is given by

$$e_1\mathbb{Z}_{(\ell)}C_q \xrightarrow{\sim} \mathbb{Z}_{(\ell)}[\zeta_q],\ e_1(a_0 + a_1 g + \cdots + a_{q-1}g^{q-1}) \mapsto a_0 + a_1\zeta_q + \cdots + a_{q-1}\zeta_q^{q-1}.$$

This means that the action of $\mathbb{Z}_{(\ell)}[\zeta_q]$ on M_1 is given as follows: for $x \in M$ we have

$$\zeta_q.(e_1 x) = (e_1 g)(e_1 x) = g.(e_1 x).$$

By definition of n, it holds that

$$t^{q-1} + \cdots + t + 1 = (t - \overline{n})(t - \overline{n}^2)\cdots(t - \overline{n}^{q-1}) \in \mathbb{F}_\ell[t].$$

Thus, by the Dedekind–Kummer Theorem we have

$$(\ell) = (\ell, \zeta_q - n)(\ell, \zeta_q - n^2)\cdots(\ell, \zeta_q - n^{q-1}) \subseteq \mathbb{Z}[\zeta_q].$$

Without loss of generality, $\mathfrak{q}_i = (\ell, \zeta_q - n^i)$ for $i = 1, \dots, q-1$. Using that $\ell M = 0$, for $y \in M_1$ it holds that

$$y \in M_1[\mathfrak{q}_i^\infty] \iff \operatorname{ann}_{\mathbb{Z}[\zeta_q]}(y) \mid \mathfrak{q}_i \iff \zeta_q - n^i \in \operatorname{ann}_{\mathbb{Z}[\zeta_q]}(y) \iff \zeta_q y = n^i y.$$

It follows that

$$M_1[\mathfrak{q}_i^\infty] = \{ y \in M_1 \mid g.y = n^i y \} = \{ y \in M \mid g.y = n^i y \},$$

where the right hand equality follow from the fact that $1 + n + \cdots + n^{q-1} \equiv 0 \mod \ell$, giving $e_0 y = 0$ for the y in the right hand sets. □

Lemma 10.19. *Let p be a prime with $p \equiv 1 \mod q$. Let $L/\mathbb{Q}_p$ be cyclic of degree q with Galois group $\operatorname{Gal}(L/\mathbb{Q}_p) = \langle\sigma\rangle$. Denote by $\mathfrak{p}$ the maximal ideal of $\mathcal{O}_L$. Then for each $i \in \{1, \dots, q-1\}$ there is $x_i \in \mathcal{O}_L$ with $\sigma(x_i) = \zeta_q^i x_i$; if L is unramified we can additionally ensure $v_\mathfrak{p}(x_i) = 1$ and if L is totally ramified we can additionally ensure $v_\mathfrak{p}(x_i) \in \{1, \dots, q-1\}$.*

Proof. Note that since $p \equiv 1 \mod q$ we have $\zeta_q \in \mathbb{Q}_p$. Let $i \in \{1, \dots, q-1\}$.

Suppose first that L is unramified. By Kummer theory, there is $y_i \in L$ with $\sigma(y_i) = \zeta_q^i y_i$. We can write $y_i = \frac{a_i}{b_i}$ with $a_i \in \mathcal{O}_L$ and $b_i \in \mathbb{Z}_p$. Then $\sigma(a_i) = \zeta_q^i a_i$. Now since $L/\mathbb{Q}_p$ is unramified, p is a uniformiser in $\mathcal{O}_L$. Write $a_i = u_i \cdot p^{k_i}$ with $u_i \in \mathcal{O}_L^\times$ and $k_i \in \mathbb{Z}$. We get $\sigma(u_i) = \zeta_q^i u_i$ and may hence take $x_i := pu_i$.

Now suppose $L/\mathbb{Q}_p$ is totally tamely ramified. Then there is a uniformiser π of $\mathbb{Z}_p$ with $L = \mathbb{Q}_p(\sqrt[q]{\pi})$. We have $v_\mathfrak{p}(\sqrt[q]{\pi}) = 1$ and $\sigma(\sqrt[q]{\pi}) \in \left\{\zeta_q \sqrt[q]{\pi}, \dots, \zeta_q^{q-1} \sqrt[q]{\pi}\right\}$. Hence, one of $\sqrt[q]{\pi}, \dots, \sqrt[q]{\pi}^{q-1}$ will do the job. □

Lemma 10.20. *Let p be a prime with $p \equiv 1 \mod q$. Let $L/\mathbb{Q}_p$ be cyclic of degree q. Let $n \in \mathbb{Z}$ such that n is congruent to a primitive q-th root of unity modulo p. Then for $\zeta_q \in L$ it holds that $n \equiv \zeta_q^i \mod p\mathcal{O}_L$ for some $i \in \{1, \dots, q-1\}$.*

Proof. Suppose that $x \in \mathcal{O}_L$ is such that $\overline{x}^q = \overline{1} \in \mathcal{O}_L/p$. We are going to show that there is $\zeta \in \mu_q(L)$ with $\overline{x} = \overline{\zeta}$. Since $\mathcal{O}_L^\times \to (\mathcal{O}_L/p)^\times$ is surjective, we may assume that $x \in \mathcal{O}_L^\times$. We can write $x = \zeta u$ with $\zeta \in \mu_{p^f-1}(L)$ and $u \in U^{(1)}$ where $f = f(L/\mathbb{Q}_p)$. We have $x^q = \zeta^q u^q \in 1 + p\mathcal{O}_L \subseteq U^{(1)}$, which forces $\zeta^q = 1$. Hence, $u^q \in 1 + p\mathcal{O}_L$. But raising to the q-th power is an isomorphism on $1 + p\mathcal{O}_L$ by [Neu99, Proposition II.5.7], so $u \in 1 + p\mathcal{O}_L$. It follows that $\overline{x} = \overline{\zeta}$ as claimed.

We have $\mathbb{F}_p \subseteq \mathcal{O}_L/p$, so by assumption $\overline{n} \in \mathcal{O}_L/p$ satisfies $\overline{n}^q = \overline{1}$ and $\overline{n} \neq \overline{1}$. The claim then follows from what has been shown in the first paragraph. □

We can now obtain the sizes of the primary components of $U_{T_p}[\ell]_1$.

Proposition 10.21. *Suppose that $q \geq 3$. Let ℓ be a prime with $\ell \equiv 1 \mod q$. Let $p \mid \mathfrak{m}_\mathbb{Q}$ and let T_p be a C_q-structured $\mathbb{Q}_p$-algebra.*

(i) Suppose that $T_p = \mathbb{Q}_p^q$. Then $\left|U_{T_p}[\ell]_1[\mathfrak{q}_i^\infty]\right| = \left|U_{T_p}[\ell]^G\right|$ for all $i \in \{1, \dots, q-1\}$.

(ii) Suppose that T_p is an unramified C_q-extension of $\mathbb{Q}_p$. Then $\left|U_{T_p}[\ell]_1[\mathfrak{q}_i^\infty]\right| = 1$ for all $i \in \{1, \dots, q-1\}$ unless

- *$p^q \equiv 1(\ell)$ and $p \not\equiv 1(\ell)$, in which case $\left|U_{T_p}[\ell]_1[\mathfrak{q}_i^\infty]\right| = \ell$ for one $i \in \{1, \dots, q-1\}$ and $\left|U_{T_p}[\ell]_1[\mathfrak{q}_i^\infty]\right| = 1$ for all other i; or*
- *$p = \ell$ and $v_\ell(\mathfrak{m}_\mathbb{Q}) \geq 2$, in which case $\left|U_{T_p}[\ell]_1[\mathfrak{q}_i^\infty]\right| = \ell$ for all $i \in \{1, \dots, q-1\}$.*

(iii) Suppose that T_p is a totally ramified C_q-extension of $\mathbb{Q}_p$. Then $\left|U_{T_p}[\ell]_1[\mathfrak{q}_i^\infty]\right| = 1$ for all $i \in \{1, \dots, q-1\}$ unless

- *$p = \ell$ and $v_\ell(\mathfrak{m}_\mathbb{Q}) = 1$, in which case $\left|U_{T_p}[\ell]_1[\mathfrak{q}_i^\infty]\right| = \ell$ for all $i \in \{1, \dots, q-1\}$; or*

- *$p = \ell$ and $v_\ell(\mathfrak{m}_\mathbb{Q}) \geq 2$, in which case we further distinguish two subcases: If $|\mu_p(T_p)| = p$, then $\left|U_{T_p}[\ell]_1[\mathfrak{q}_i^\infty]\right| = \ell^2$ for one $i \in \{1, \ldots, q-1\}$ and $\left|U_{T_p}[\ell]_1[\mathfrak{q}_j^\infty]\right| = \ell$ for all other i. If $|\mu_p(T_p)| = 1$, then $\left|U_{T_p}[\ell]_1[\mathfrak{q}_i^\infty]\right| = \ell$ for all $i \in \{1, \ldots, q-1\}$.*

Proof. Let g be a generator of C_q. Suppose first that $T_p = \mathbb{Q}_p^q$. By Proposition 10.2 we can assume that g acts on T_p via $(1\ 2 \cdots q)$. We have $U_{T_p}[\ell] = ((\mathbb{Z}_p/p^{v_p(\mathfrak{m}_\mathbb{Q})})^\times[\ell])^q$ and therefore

$$U_{T_p}[\ell]^G = \left\{ (\mu, \ldots, \mu) \,\middle|\, \mu \in (\mathbb{Z}_p/p^{v_p(\mathfrak{m}_\mathbb{Q})})^\times[\ell] \right\}.$$

Let $n \in \mathbb{Z}$ such that n is congruent to a primitive q-th root of unity modulo ℓ and let $N_i := \left\{ x \in U_{T_p}[\ell] \,\middle|\, gx = n^i x \right\}$ for $i = 1, \ldots, q-1$. Then it is easy to see that

$$N_i = \left\{ (\mu, \mu^{n^{-i}}, \ldots, \mu^{n^{-(q-2)i}}, \mu^{n^i}) \,\middle|\, \mu \in (\mathbb{Z}_p/p^{v_p(\mathfrak{m}_\mathbb{Q})})^\times[\ell] \right\}.$$

Claim (i) follows from this and Lemma 10.18.

Now suppose that $T_p = L$ for $L/\mathbb{Q}_p$ cyclic of degree q. In all cases except $p = \ell$ the claims in (ii) and (iii) are immediate from Proposition 10.7, which for $p \neq \ell$ gives $\left|U_{T_p}[\ell]_1\right| = \left|U_{T_p}[\ell]\right| / \left|U_{T_p}[\ell]^G\right| \in \{1, \ell\}$. Assume from now on that $p = \ell$. Here, $U_{T_p}[\ell] = (\mathcal{O}_L/p^{v_p(\mathfrak{m}_\mathbb{Q})})^\times[p]$. We instead study $\frac{(\mathcal{O}_L/p^{v_p(\mathfrak{m}_\mathbb{Q})})^\times}{((\mathcal{O}_L/p^{v_p(\mathfrak{m}_\mathbb{Q})})^\times)^p}$, all of whose isotypical and primary components have the same size as the corresponding components of $U_{T_p}[\ell]$, which follows from the exact sequence

$$0 \to (\mathcal{O}_L/p^{v_p(\mathfrak{m}_\mathbb{Q})})^\times[p] \to (\mathcal{O}_L/p^{v_p(\mathfrak{m}_\mathbb{Q})})^\times[p^\infty] \overset{(\cdot)^p}{\to} (\mathcal{O}_L/p^{v_p(\mathfrak{m}_\mathbb{Q})})^\times[p^\infty] \to \frac{(\mathcal{O}_L/p^{v_p(\mathfrak{m}_\mathbb{Q})})^\times}{((\mathcal{O}_L/p^{v_p(\mathfrak{m}_\mathbb{Q})})^\times)^p} \to 0.$$

Recall the short exact sequence of C_q-modules (10.8) which in the case of our interest reads

$$1 \longrightarrow \frac{1+p^{v_p(\mathfrak{m}_\mathbb{Q})}\mathcal{O}_L}{(1+p^{v_p(\mathfrak{m}_\mathbb{Q})}\mathcal{O}_L) \cap (\mathcal{O}_L^\times)^p} \longrightarrow \frac{\mathcal{O}_L^\times}{(\mathcal{O}_L^\times)^p} \longrightarrow \frac{(\mathcal{O}_L/p^{v_p(\mathfrak{m}_\mathbb{Q})})^\times}{((\mathcal{O}_L/p^{v_p(\mathfrak{m}_\mathbb{Q})})^\times)^p} \longrightarrow 1. \tag{10.22}$$

From the snake lemma applied to

$$\begin{tikzcd}
1 \arrow[r] & 1+\mathfrak{p}\mathcal{O}_L \arrow[r] \arrow[d, "(\cdot)^p"] & \mathcal{O}_L^\times \arrow[r] \arrow[d, "(\cdot)^p"] & (\mathcal{O}_L/\mathfrak{p})^\times \arrow[r] \arrow[d, "(\cdot)^p"] & 1 \\
1 \arrow[r] & 1+\mathfrak{p}\mathcal{O}_L \arrow[r] & \mathcal{O}_L^\times \arrow[r] & (\mathcal{O}_L/\mathfrak{p})^\times \arrow[r] & 1
\end{tikzcd}$$

we obtain an isomorphism

$$\frac{U^{(1)}}{(U^{(1)})^p} \xrightarrow{\sim} \frac{\mathcal{O}_L^\times}{(\mathcal{O}_L^\times)^p}$$

of G-modules. Note that the condition $\ell \equiv 1 \mod q$ forces $\ell \geq q+1$ and even $\ell > q+1$ as $q \neq 2$. Hence, $p = \ell > q+1$. This gives $\frac{e}{p-1} < 1$, where e is the ramification index of $L/\mathbb{Q}_p$. Hence, as in the proof of Proposition 10.7, the exponential function furnishes an isomorphism of G-modules

$$\frac{\mathfrak{p}}{p\mathfrak{p}} \xrightarrow{\sim} \frac{U^{(1)}}{(U^{(1)})^p}.$$

Let $n \in \mathbb{Z}$ such that n is congruent to a primitive q-th root of unity modulo ℓ. By Lemma 10.20 we have $n \equiv \zeta_q^j \mod p\mathcal{O}_L$ for some $j \in \{1, \dots, q-1\}$. Now let $i \in \{1, \dots, q-1\}$. By Lemma 10.19 there is $0 \neq \overline{x} \in \mathfrak{p}/p\mathfrak{p}$ such that $g\overline{x} = \overline{\zeta_q^{ij} x} = n^i \overline{x}$.

Suppose that $v_\ell(\mathfrak{m}_\mathbb{Q}) \geq 2$. Then as in the proof of Proposition 10.6, the left hand side of (10.22) is trivial. Hence, the above and Lemma 10.18 show that $\left|U_{T_p}[\ell]_1[\mathfrak{q}_i^\infty]\right| > 1$. The claims for $v_\ell(\mathfrak{m}_\mathbb{Q}) \geq 2$ follow from this and Proposition 10.6.

Suppose finally that $v_\ell(\mathfrak{m}_\mathbb{Q}) = 1$. If $L/\mathbb{Q}_p$ is unramified, then $\left|U_{T_p}[\ell]\right| = 1$, so clearly $\left|U_{T_p}[\ell]_1[\mathfrak{q}_i^\infty]\right| = 1$. Assume now that $L/\mathbb{Q}_p$ is ramified. Then by Lemma 10.19 we can choose x such that $v_\mathfrak{p}(x) \in \{1, \dots, q-1\}$. By the arguments above, we have $\left|U_{T_p}[\ell]_1[\mathfrak{q}_i^\infty]\right| > 1$ provided that

$$\overline{\exp(x)} \notin \frac{1 + p\mathcal{O}_L}{(1 + p\mathcal{O}_L) \cap (\mathcal{O}_L^\times)^p}.$$

Assume for the sake of a contradiction that there is $y \in 1 + p\mathcal{O}_L$ such that $\overline{\exp(x)} = \overline{y} \in \mathcal{O}_L^\times/(\mathcal{O}_L^\times)^p$. Then there is $z \in (U^{(1)})^p$ with $\exp(x) = yz$. It follows that $x = \log y + \log z \in p\mathcal{O}_L$ which gives $v_\mathfrak{p}(x) \geq q$, a contradiction. □

10.3 Average Torsion of Ray Class Groups of Quadratic Fields

Following the approach of [PS17, Section 2.2] and [BP25, Section 4.2], we use the results from the previous section to give explicit formulas for the average ℓ-torsion, ℓ odd, of ray class groups of imaginary and real quadratic fields. In doing so, we restate [PS17, Conjecture 2.15] and [BP25, Proposition 4.15] and extend those results to the case where quadratic fields are ordered by the product of the ramified primes

Use Setup 8.37 with $F = \mathbb{Q}$, $G = C_2$ and $I = \langle \sum_{h \in C_2} h \rangle$ and do not fix T. Let ℓ be an odd prime. If $W = 0$, then $\mathcal{K}$ is the family of imaginary quadratic fields and we have

$$\begin{aligned} \mathrm{Av}_{\mathcal{K},C}(\ell) &= \sum_{T=(T_p)_{p|\mathfrak{m}_\mathbb{Q}}/\cong} \mathrm{Pr}_C(T) \cdot \left|U_T[\ell]^G\right| \cdot (|U_T[\ell]_1| + 1) \\ &= \sum_{T=(T_p)_{p|\mathfrak{m}_\mathbb{Q}}/\cong} \mathrm{Pr}_C(T) \cdot (|U_T[\ell]| + \left|U_T[\ell]^G\right|), \end{aligned}$$

where T runs over collections of C_2-structured $\mathbb{Q}_p$-algebras. Using Proposition 10.1 we can express this as

$$\mathrm{Av}_{\mathcal{K},C}(\ell) = \prod_{p \mid \mathfrak{m}_{\mathbb{Q}}} \sum_{T_p/\cong} \mathrm{Pr}_C(T_p) \cdot \left|U_{T_p}[\ell]\right| + \prod_{p \mid \mathfrak{m}_{\mathbb{Q}}} \sum_{T_p/\cong} \mathrm{Pr}_C(T_p) \cdot \left|U_{T_p}[\ell]^G\right|.$$

If $W = \mathbb{Q}(-1)$, then $\mathcal{K}$ is the family of real quadratic fields. Here, one obtains

$$\mathrm{Av}_{\mathcal{K},C}(\ell) = \frac{1}{\ell} \prod_{p \mid \mathfrak{m}_{\mathbb{Q}}} \sum_{T_p/\cong} \mathrm{Pr}_C(T_p) \cdot \left|U_{T_p}[\ell]\right| + \prod_{p \mid \mathfrak{m}_{\mathbb{Q}}} \sum_{T_p/\cong} \mathrm{Pr}_C(T_p) \cdot \left|U_{T_p}[\ell]^G\right|.$$

The table below gives the probabilities of the C_2-structured $\mathbb{Q}_p$-algebras. The second column gives the base algebra and the third column how many C_2-structured $\mathbb{Q}_p$-algebras up to isomorphism there are with such a base algebra. This data comes from Proposition 10.5. Except in the case where C is the discriminant and $p = 2$, the probabilities can be read off from the same proposition. In the exceptional cases, we have used Proposition 10.1 to calculate the probabilities. Here, for the ramified extensions of $\mathbb{Q}_2$, one calculates the 2-adic valuation of the discriminants of $\mathbb{Q}_2(\sqrt{-1})$ and $\mathbb{Q}_2(\sqrt{3})$ to be 2 and for the remaining ramified extensions to be 3.

		Number of	$\mathrm{Pr}_C(T_p)$	$\mathrm{Pr}_C(T_p)$
p	T_p	such T_p	C prod. of ram. primes	C discriminant
$p \neq 2$	$\mathbb{Q}_p^2$	1	$\frac{p}{2(p+1)}$	$\frac{p}{2(p+1)}$
	$L/\mathbb{Q}_p$ unram.	1	$\frac{p}{2(p+1)}$	$\frac{p}{2(p+1)}$
	$L/\mathbb{Q}_p$ ram.	2	$\frac{1}{2(p+1)}$	$\frac{1}{2(p+1)}$
$p = 2$	$\mathbb{Q}_p^2$	1	$\frac{1}{5}$	$\frac{1}{3}$
	$L/\mathbb{Q}_p$ unram.	1	$\frac{1}{5}$	$\frac{1}{3}$
	$\mathbb{Q}_2(\sqrt{-1})$	1	$\frac{1}{10}$	$\frac{1}{12}$
	$\mathbb{Q}_2(\sqrt{3})$	1	$\frac{1}{10}$	$\frac{1}{12}$
	$\mathbb{Q}_2(\sqrt{2})$	1	$\frac{1}{10}$	$\frac{1}{24}$
	$\mathbb{Q}_2(\sqrt{-2})$	1	$\frac{1}{10}$	$\frac{1}{24}$
	$\mathbb{Q}_2(\sqrt{6})$	1	$\frac{1}{10}$	$\frac{1}{24}$
	$\mathbb{Q}_2(\sqrt{-6})$	1	$\frac{1}{10}$	$\frac{1}{24}$

From Proposition 10.7 one further obtains the following table.

p	T_p	$\lvert U_{T_p}[\ell]\rvert$	$\lvert U_{T_p}[\ell]^G\rvert$
$p \not\equiv 0, \pm 1 (\ell)$	$\mathbb{Q}_p^2$	1	1
	$L/\mathbb{Q}_p$ unram.	1	1
	$L/\mathbb{Q}_p$ ram.	1	1
$p \equiv -1(\ell)$	$\mathbb{Q}_p^2$	1	1
	$L/\mathbb{Q}_p$ unram.	ℓ	1
	$L/\mathbb{Q}_p$ ram.	1	1
$p \equiv 1(\ell)$	$\mathbb{Q}_p^2$	ℓ^2	ℓ
	$L/\mathbb{Q}_p$ unram.	ℓ	ℓ
	$L/\mathbb{Q}_p$ ram.	ℓ	ℓ
$p = \ell$, $v_\ell(\mathfrak{m}_\mathbb{Q}) = 1$	$\mathbb{Q}_p^2$	1	1
	$L/\mathbb{Q}_p$ unram.	1	1
	$L/\mathbb{Q}_p$ ram.	ℓ	1
$p = \ell$, $v_\ell(\mathfrak{m}_\mathbb{Q}) \geq 2$	$\mathbb{Q}_p^2$	ℓ^2	ℓ
	$L/\mathbb{Q}_p$ unram.	ℓ^2	ℓ
	$L/\mathbb{Q}_p$ ram.	$\ell^2 \cdot \lvert\mu_\ell(L)\rvert$	ℓ

In the $p = \ell$, $v_\ell(\mathfrak{m}_\mathbb{Q}) \geq 2$ case, note that if $L/\mathbb{Q}_p$ is unramified, then $|\mu_\ell(L)| = 1$ as $\mathbb{Q}_p(\zeta_p)$ is totally ramified over $\mathbb{Q}_p$ and therefore cannot be contained in L. On the other hand, since $\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p$ has degree $p-1$ by [Neu99, Proposition II.7.13], in order for a quadratic ramified extension $L/\mathbb{Q}_p$ to satisfy $|\mu_\ell(L)| = \ell$, it needs to hold that $p = \ell = 3$. In the latter case, there are 2 ramified extensions of $\mathbb{Q}_3$ up to isomorphism by Proposition 10.4, and $\mathbb{Q}_3(\zeta_3)$ is the only one to contain the third roots of unity.

Putting the above together, we obtain the following results.

Corollary 10.23. *Write $\mathcal{K}^-$ for the family of imaginary quadratic number fields. Let $\mathfrak{m}_\mathbb{Q}$ be a positive integer and let ℓ be an odd prime. Let C be a fair counting function on $\mathcal{K}^-$. Let $\mathcal{P}_1 := \{\, p \mid \mathfrak{m}_\mathbb{Q} : p \equiv 1 \mod \ell \,\}$ and define $\mathcal{P}_{\pm 1}$ analogously. Assume that Conjecture 8.38 holds. Then the limit*

$$\mathrm{Av}_C^-(\ell) := \lim_{B\to\infty} \frac{\sum_{K\in\mathcal{K}^-_{C\leq B}} |\mathrm{Cl}_K(\mathfrak{m}_\mathbb{Q}, \varnothing)[\ell]|}{\left|\mathcal{K}^-_{C\leq B}\right|}$$

exists. If C is the discriminant, then

$$\mathrm{Av}_C^-(\ell) = \begin{cases} \ell^{|\mathcal{P}_1|} \cdot \left(1 + \prod_{p\in\mathcal{P}_{\pm 1}} \frac{p(\ell+1)+2}{2(p+1)}\right), & \ell \nmid \mathfrak{m}_\mathbb{Q}, \\ \ell^{|\mathcal{P}_1|} \cdot \left(1 + \frac{2\ell}{\ell+1} \prod_{p\in\mathcal{P}_{\pm 1}} \frac{p(\ell+1)+2}{2(p+1)}\right), & \ell \parallel \mathfrak{m}_\mathbb{Q}, \\ \ell^{|\mathcal{P}_1|+1} \cdot \left(1 + \ell \prod_{p\in\mathcal{P}_{\pm 1}} \frac{p(\ell+1)+2}{2(p+1)}\right), & \ell > 3, \ell^2 \mid \mathfrak{m}_\mathbb{Q}, \\ 3^{|\mathcal{P}_1|+1} \cdot \left(1 + \frac{15}{4} \prod_{p\in\mathcal{P}_{\pm 1}} \frac{2p+1}{p+1}\right), & \ell = 3, \ell^2 \mid \mathfrak{m}_\mathbb{Q}. \end{cases}$$

If C is the product of the ramified primes, then for $\ell > 3$ we have

$$\mathrm{Av}_C^-(\ell) = \begin{cases} \ell^{|\mathcal{P}_1|} \cdot \left(1 + \prod_{p \in \mathcal{P}_{\pm 1}} \frac{p(\ell+1)+2}{2(p+1)}\right), & \ell \nmid \mathfrak{m}_{\mathbb{Q}}, \\ \ell^{|\mathcal{P}_1|} \cdot \left(1 + \frac{2\ell}{\ell+1} \prod_{p \in \mathcal{P}_{\pm 1}} \frac{p(\ell+1)+2}{2(p+1)}\right), & \ell \parallel \mathfrak{m}_{\mathbb{Q}}, \\ \ell^{|\mathcal{P}_1|+1} \cdot \left(1 + \ell \prod_{p \in \mathcal{P}_{\pm 1}} \frac{p(\ell+1)+2}{2(p+1)}\right), & \ell^2 \mid \mathfrak{m}_{\mathbb{Q}}, \end{cases}$$

and for $\ell = 3$ we have

$$\mathrm{Av}_C^-(3) = \begin{cases} 3^{|\mathcal{P}_1|} \cdot \left(1 + \prod_{p \in \mathcal{P}_{\pm 1}} \frac{2p+1}{p+1}\right), & 3 \nmid \mathfrak{m}_{\mathbb{Q}}, 2 \nmid \mathfrak{m}_{\mathbb{Q}}, \\ 3^{|\mathcal{P}_1|} \cdot \left(1 + \frac{7}{5} \prod_{p \in \mathcal{P}_{\pm 1} \setminus \{2\}} \frac{2p+1}{p+1}\right), & 3 \nmid \mathfrak{m}_{\mathbb{Q}}, 2 \mid \mathfrak{m}_{\mathbb{Q}}, \\ 3^{|\mathcal{P}_1|} \cdot \left(1 + \frac{3}{2} \prod_{p \in \mathcal{P}_{\pm 1}} \frac{2p+1}{p+1}\right), & 3 \parallel \mathfrak{m}_{\mathbb{Q}}, 2 \nmid \mathfrak{m}_{\mathbb{Q}}, \\ 3^{|\mathcal{P}_1|} \cdot \left(1 + \frac{21}{10} \prod_{p \in \mathcal{P}_{\pm 1} \setminus \{2\}} \frac{2p+1}{p+1}\right), & 3 \parallel \mathfrak{m}_{\mathbb{Q}}, 2 \mid \mathfrak{m}_{\mathbb{Q}}, \\ 3^{|\mathcal{P}_1|+1} \cdot \left(1 + \frac{15}{4} \prod_{p \in \mathcal{P}_{\pm 1}} \frac{2p+1}{p+1}\right), & 3^2 \mid \mathfrak{m}_{\mathbb{Q}}, 2 \nmid \mathfrak{m}_{\mathbb{Q}}, \\ 3^{|\mathcal{P}_1|+1} \cdot \left(1 + \frac{21}{4} \prod_{p \in \mathcal{P}_{\pm 1} \setminus \{2\}} \frac{2p+1}{p+1}\right), & 3^2 \mid \mathfrak{m}_{\mathbb{Q}}, 2 \mid \mathfrak{m}_{\mathbb{Q}}. \end{cases}$$

Proof. The results are obtained from the formula

$$\mathrm{Av}_C^-(\ell) = \prod_{p \mid \mathfrak{m}_{\mathbb{Q}}} \sum_{T_p/\cong} \mathrm{Pr}_C(T_p) \cdot \left|U_{T_p}[\ell]\right| + \prod_{p \mid \mathfrak{m}_{\mathbb{Q}}} \sum_{T_p/\cong} \mathrm{Pr}_C(T_p) \cdot \left|U_{T_p}[\ell]^G\right|$$

by plugging in the appropriate values from the two tables. We illustrate this procedure for the case C the discriminant and $\ell \nmid \mathfrak{m}_{\mathbb{Q}}$. Since by the second table, $\left|U_{T_p}[\ell]^G\right|$ only depends on p and not the individual T_p, we immediately have

$$\prod_{p \mid \mathfrak{m}_{\mathbb{Q}}} \sum_{T_p/\cong} \mathrm{Pr}_C(T_p) \cdot \left|U_{T_p}[\ell]^G\right| = \ell^{|\mathcal{P}_1|}.$$

For $p \mid \mathfrak{m}_{\mathbb{Q}}$ define

$$S_p := \sum_{T_p/\cong} \mathrm{Pr}_C(T_p) \cdot \left|U_{T_p}[\ell]\right|.$$

For $p \mid \mathfrak{m}_{\mathbb{Q}}$ with $p \equiv -1(\ell)$ and $p \neq 2$, the tables give

$$S_p = \frac{p}{2(p+1)} + \frac{p}{2(p+1)} \cdot \ell + 2 \cdot \frac{1}{2(p+1)} = \frac{p(\ell+1)+2}{2(p+1)}.$$

For $p \mid \mathfrak{m}_{\mathbb{Q}}$ with $p \equiv -1(\ell)$ and $p = 2$, the tables give

$$S_p = \frac{1}{3} + \frac{1}{3} \cdot \ell + \frac{1}{12} \cdot 2 + \frac{1}{24} \cdot 4 = \frac{2\ell+4}{6} = \frac{p(\ell+1)+2}{2(p+1)},$$

so the $p \equiv -1(\ell)$ case can be treated uniformly. For $p \mid \mathfrak{m}_{\mathbb{Q}}$ with $p \equiv 1(\ell)$, the tables give

$$S_p = \frac{p}{2(p+1)} \cdot \ell^2 + \frac{p}{2(p+1)} \cdot \ell + 2 \cdot \frac{1}{2(p+1)} \cdot \ell = \ell \cdot \frac{p(\ell+1)+2}{2(p+1)}.$$

It follows that

$$\prod_{p\mid\mathfrak{m}_{\mathbb{Q}}} S_p = \ell^{|\mathcal{P}_1|} \cdot \prod_{p\in\mathcal{P}_{\pm1}} \frac{p(\ell+1)+2}{2(p+1)},$$

which proves the statement in the case C the discriminant and $\ell \nmid \mathfrak{m}_{\mathbb{Q}}$. The proofs of the remaining statements follow the same procedure. The case distinction between $\ell = 3$ and $\ell > 3$ stems from the fact that for $p = \ell$, there is a quadratic ramified extension of $\mathbb{Q}_p$ containing ζ_ℓ if and only if $p = \ell = 3$, as explained above. □

The above result for C the discriminant has already been obtained in [PS17, Section 2.2] and has been proven for $\ell = 3$ by Varma [Var22, Theorem 1 (b)].

Corollary 10.24. *Write $\mathcal{K}^+$ for the family of real quadratic number fields. Let $\mathfrak{m}_{\mathbb{Q}}$ be a positive integer and let ℓ be an odd prime. Let C be a fair counting function on $\mathcal{K}^+$. Let $\mathcal{P}_1 := \{\, p \mid \mathfrak{m}_{\mathbb{Q}} : p \equiv 1 \mod \ell \,\}$ and define $\mathcal{P}_{\pm1}$ analogously. Assume that Conjecture 8.38 holds. Then the limit*

$$\mathrm{Av}_C^+(\ell) := \lim_{B\to\infty} \frac{\sum_{K\in\mathcal{K}^+_{C\le B}} |\mathrm{Cl}_K(\mathfrak{m}_{\mathbb{Q}},\varnothing)[\ell]|}{\left|\mathcal{K}^+_{C\le B}\right|}$$

exists. If C is the discriminant, then

$$\mathrm{Av}_C^+(\ell) = \begin{cases} \ell^{|\mathcal{P}_1|}\cdot\left(1+\frac{1}{\ell}\prod_{p\in\mathcal{P}_{\pm1}}\frac{p(\ell+1)+2}{2(p+1)}\right), & \ell\nmid\mathfrak{m}_{\mathbb{Q}},\\ \ell^{|\mathcal{P}_1|}\cdot\left(1+\frac{2}{\ell+1}\prod_{p\in\mathcal{P}_{\pm1}}\frac{p(\ell+1)+2}{2(p+1)}\right), & \ell\parallel\mathfrak{m}_{\mathbb{Q}},\\ \ell^{|\mathcal{P}_1|+1}\cdot\left(1+\prod_{p\in\mathcal{P}_{\pm1}}\frac{p(\ell+1)+2}{2(p+1)}\right), & \ell>3, \ell^2\mid\mathfrak{m}_{\mathbb{Q}},\\ 3^{|\mathcal{P}_1|+1}\cdot\left(1+\frac{5}{4}\prod_{p\in\mathcal{P}_{\pm1}}\frac{2p+1}{p+1}\right), & \ell=3, \ell^2\mid\mathfrak{m}_{\mathbb{Q}}.\end{cases}$$

If C the product of the ramified primes, then for $\ell > 3$ we have

$$\mathrm{Av}_C^+(\ell) = \begin{cases} \ell^{|\mathcal{P}_1|}\cdot\left(1+\frac{1}{\ell}\prod_{p\in\mathcal{P}_{\pm1}}\frac{p(\ell+1)+2}{2(p+1)}\right), & \ell\nmid\mathfrak{m}_{\mathbb{Q}},\\ \ell^{|\mathcal{P}_1|}\cdot\left(1+\frac{2}{\ell+1}\prod_{p\in\mathcal{P}_{\pm1}}\frac{p(\ell+1)+2}{2(p+1)}\right), & \ell\parallel\mathfrak{m}_{\mathbb{Q}},\\ \ell^{|\mathcal{P}_1|+1}\cdot\left(1+\prod_{p\in\mathcal{P}_{\pm1}}\frac{p(\ell+1)+2}{2(p+1)}\right), & \ell^2\mid\mathfrak{m}_{\mathbb{Q}},\end{cases}$$

and for $\ell = 3$ we have

$$\mathrm{Av}_C^+(3) = \begin{cases} 3^{|\mathcal{P}_1|}\cdot\left(1+\frac{1}{3}\prod_{p\in\mathcal{P}_{\pm1}}\frac{2p+1}{p+1}\right), & 3\nmid\mathfrak{m}_{\mathbb{Q}}, 2\nmid\mathfrak{m}_{\mathbb{Q}},\\ 3^{|\mathcal{P}_1|}\cdot\left(1+\frac{7}{15}\prod_{p\in\mathcal{P}_{\pm1}\setminus\{2\}}\frac{2p+1}{p+1}\right), & 3\nmid\mathfrak{m}_{\mathbb{Q}}, 2\mid\mathfrak{m}_{\mathbb{Q}},\\ 3^{|\mathcal{P}_1|}\cdot\left(1+\frac{1}{2}\prod_{p\in\mathcal{P}_{\pm1}}\frac{2p+1}{p+1}\right), & 3\parallel\mathfrak{m}_{\mathbb{Q}}, 2\nmid\mathfrak{m}_{\mathbb{Q}},\\ 3^{|\mathcal{P}_1|}\cdot\left(1+\frac{7}{10}\prod_{p\in\mathcal{P}_{\pm1}\setminus\{2\}}\frac{2p+1}{p+1}\right), & 3\parallel\mathfrak{m}_{\mathbb{Q}}, 2\mid\mathfrak{m}_{\mathbb{Q}},\\ 3^{|\mathcal{P}_1|+1}\cdot\left(1+\frac{5}{4}\prod_{p\in\mathcal{P}_{\pm1}}\frac{2p+1}{p+1}\right), & 3^2\mid\mathfrak{m}_{\mathbb{Q}}, 2\nmid\mathfrak{m}_{\mathbb{Q}},\\ 3^{|\mathcal{P}_1|+1}\cdot\left(1+\frac{7}{4}\prod_{p\in\mathcal{P}_{\pm1}\setminus\{2\}}\frac{2p+1}{p+1}\right), & 3^2\mid\mathfrak{m}_{\mathbb{Q}}, 2\mid\mathfrak{m}_{\mathbb{Q}}.\end{cases}$$

Proof. The proof is analogous to that of Corollary 10.23. □

The above result for C the discriminant has already been obtained in [BP25, Section 4.2] and has been proven for $\ell = 3$ by Varma [Var22, Theorem 1 (a)].

10.4 Average Torsion of Ray Class Groups of Cyclic Cubic Fields

Using the results from the previous sections, we show how to obtain explicit formulas for the average ℓ-torsion, $\ell \neq 2, 3$, of ray class groups of cyclic cubic fields.

Use Setup 8.37 with $F = \mathbb{Q}$, $G = C_3$ and $I = \langle \sum_{h\in C_3} h\rangle$ and do not fix T. Then $\mathcal{K}$ is the family of cyclic cubic extensions of $\mathbb{Q}$. Let ℓ be a prime with $\ell \neq 2, 3$. If $\ell \equiv 2 \mod 3$, then ℓ is inert in $\mathbb{Q}(\zeta_3)$ and

$$\begin{aligned}\mathrm{Av}_{\mathcal{K},C}(\ell) &= \sum_{T=(T_p)_{p\mid\mathfrak{m}_\mathbb{Q}}/\cong} \mathrm{Pr}_C(T)\cdot\left|U_T[\ell]^G\right|\cdot\left(\frac{|U_T[\ell]_1|}{\ell^2}+1\right)\\ &= \sum_{T=(T_p)_{p\mid\mathfrak{m}_\mathbb{Q}}/\cong} \mathrm{Pr}_C(T)\cdot\left(\frac{|U_T[\ell]|}{\ell^2}+\left|U_T[\ell]^G\right|\right),\end{aligned}$$

where T runs over collections of C_3-structured $\mathbb{Q}_p$-algebras. If $\ell \equiv 1 \mod 3$, then ℓ is totally split in $\mathbb{Q}(\zeta_3)$, say $(\ell) = \mathfrak{q}_1\mathfrak{q}_2$. Here,

$$\mathrm{Av}_{\mathcal{K},C}(\ell) = \sum_{T=(T_p)_{p\mid\mathfrak{m}_\mathbb{Q}}/\cong} \mathrm{Pr}_C(T)\cdot\left|U_T[\ell]^G\right|\cdot\left(\frac{|U_T[\ell]_1[\mathfrak{q}_1^\infty]|}{\ell}+1\right)\cdot\left(\frac{|U_T[\ell]_1[\mathfrak{q}_2^\infty]|}{\ell}+1\right),$$

where again T runs over collections of C_3-structured $\mathbb{Q}_p$-algebras. From Proposition 10.5 one reads off the following table for the probabilities of the C_3-structured $\mathbb{Q}_p$-algebras, where again the third column indicates how many C_3-structured $\mathbb{Q}_p$-algebras up to isomorphism there are with base algebra as given in the second column.

p	T_p	Number of such T_p	$\mathrm{Pr}_C(T_p)$ C prod. of ram. primes
$p \equiv 2(3)$	$\mathbb{Q}_p^3$	1	$\frac{1}{3}$
	$L/\mathbb{Q}_p$ unram.	2	$\frac{1}{3}$
$p \equiv 1(3)$	$\mathbb{Q}_p^3$	1	$\frac{p}{3p+6}$
	$L/\mathbb{Q}_p$ unram.	2	$\frac{p}{3p+6}$
	$L/\mathbb{Q}_p$ ram.	6	$\frac{1}{3p+6}$
$p = 3$	$\mathbb{Q}_p^3$	1	$\frac{p}{3p+6}$
	$L/\mathbb{Q}_p$ unram.	2	$\frac{p}{3p+6}$
	$L/\mathbb{Q}_p$ ram.	6	$\frac{1}{3p+6}$

From Propositions 10.7 and 10.21 one further obtains the following table.

				In case $\ell \equiv 1(3)$
p	T_p	$\lvert U_{T_p}[\ell]\rvert$	$\lvert U_{T_p}[\ell]^G\rvert$	$\{\lvert U_{T_p}[\ell]_1[\mathfrak{q}_1^\infty]\rvert, \lvert U_{T_p}[\ell]_1[\mathfrak{q}_2^\infty]\rvert\}$
$p^3 \not\equiv 1(\ell)$, $p \neq \ell$	$\mathbb{Q}_p^3$	1	1	$\{1\}$
	$L/\mathbb{Q}_p$ unram.	1	1	$\{1\}$
	$L/\mathbb{Q}_p$ ram.	1	1	$\{1\}$
$p^2+p+1 \equiv 0(\ell)$	$\mathbb{Q}_p^3$	1	1	$\{1\}$
	$L/\mathbb{Q}_p$ unram.	ℓ	1	$\{1, \ell\}$
	$L/\mathbb{Q}_p$ ram.	1	1	$\{1\}$
$p \equiv 1(\ell)$	$\mathbb{Q}_p^3$	ℓ^3	ℓ	$\{\ell\}$
	$L/\mathbb{Q}_p$ unram.	ℓ	ℓ	$\{1\}$
	$L/\mathbb{Q}_p$ ram.	ℓ	ℓ	$\{1\}$
$p = \ell$, $v_\ell(\mathfrak{m}_\mathbb{Q}) = 1$	$\mathbb{Q}_p^3$	1	1	$\{1\}$
	$L/\mathbb{Q}_p$ unram.	1	1	$\{1\}$
	$L/\mathbb{Q}_p$ ram.	ℓ^2	1	$\{\ell\}$
$p = \ell$, $v_\ell(\mathfrak{m}_\mathbb{Q}) \geq 2$	$\mathbb{Q}_p^3$	ℓ^3	ℓ	$\{\ell\}$
	$L/\mathbb{Q}_p$ unram.	ℓ^3	ℓ	$\{\ell\}$
	$L/\mathbb{Q}_p$ ram.	ℓ^3	ℓ	$\{\ell\}$

Note that the statement $p^2+p+1 \equiv 0(\ell)$ or $p \equiv 1(\ell)$ is equivalent to $p^3 \equiv 1(\ell)$. In the $p = \ell$, $v_\ell(\mathfrak{m}_\mathbb{Q}) \geq 2$ case, further note that if $L/\mathbb{Q}_p$ is unramified, then $|\mu_\ell(L)| = 1$ as $\mathbb{Q}_p(\zeta_p)$ is totally ramified over $\mathbb{Q}_p$ and therefore cannot be contained in L. Moreover, since $\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p$ has degree $p-1$ by [Neu99, Proposition II.7.13], even if $L/\mathbb{Q}_p$ is ramified, we must have $|\mu_\ell(L)| = 1$. Hence the factor $|\mu_\ell(L)|$ from Proposition 10.7 (ii) (a) does not appear in the case $p = \ell$, $v_\ell(\mathfrak{m}_\mathbb{Q}) \geq 2$.

The tables lead to explicit formulas for the average ℓ-torsion, $\ell \neq 2, 3$, of ray class groups of cyclic cubic fields. In particular, we obtain Corollary 1.17, which constitutes the case $\ell \equiv 2 \mod 3$.

Corollary 10.25. *Denote by $\mathcal{K}^{C_3}$ the family of pairs (K, ι) where $K \subseteq \overline{\mathbb{Q}}$ is a Galois extension of $\mathbb{Q}$ and ι is an isomorphism $C_3 \xrightarrow{\sim} \mathrm{Gal}(K/\mathbb{Q})$. Let $\mathfrak{m}_\mathbb{Q}$ be a positive integer. For $a, b \in \mathbb{Z}$ define $\mathcal{P}(a,b) := \{\, p \mid \mathfrak{m}_\mathbb{Q} : p \equiv a \mod b \,\}$. For $(K,\iota) \in \mathcal{K}^{C_3}$ let $C(K,\iota)$ be the norm of the product of the primes of $\mathbb{Q}$ that ramify in K. Let $2 \neq \ell$ be a prime with $\ell \equiv 2 \mod 3$. Assume that Conjecture 8.38 holds. Then the limit*

$$\lim_{B\to\infty} \frac{\sum_{(K,\iota)\in\mathcal{K}^{C_3}_{C\leq B}} |\mathrm{Cl}_K(\mathfrak{m}_\mathbb{Q}, \varnothing)[\ell]|}{\left|\mathcal{K}^{C_3}_{C\leq B}\right|}$$

exists and equals

$$\begin{cases} \ell^{|\mathcal{P}(1,\ell)|}\left(1 + \frac{1}{\ell^2}\left(\frac{\ell^2+2}{3}\right)^{|\mathcal{P}(2\ell+1,3\ell)|}\prod_{p\in\mathcal{P}(1,3\ell)}\frac{p(\ell^2+2)+6}{3p+6}\right), & \ell^2 \nmid \mathfrak{m}_\mathbb{Q}, \\ \ell^{|\mathcal{P}(1,\ell)|+1}\left(1 + \left(\frac{\ell^2+2}{3}\right)^{|\mathcal{P}(2\ell+1,3\ell)|}\prod_{p\in\mathcal{P}(1,3\ell)}\frac{p(\ell^2+2)+6}{3p+6}\right), & \ell^2 \mid \mathfrak{m}_\mathbb{Q}. \end{cases}$$

Proof. The formulas are obtained in the analogous way as in Corollary 10.23, namely by plugging the data from the two tables in this subsection into the formula

$$\begin{aligned}\mathrm{Av}_{\mathcal{K},C}(\ell) &= \sum_{T=(T_p)_{p\mid\mathfrak{m}_{\mathbb{Q}}}/\cong} \mathrm{Pr}_C(T)\cdot\left(\frac{|U_T[\ell]|}{\ell^2}+\left|U_T[\ell]^G\right|\right)\\ &= \frac{1}{\ell^2}\prod_{p\mid\mathfrak{m}_{\mathbb{Q}}}\sum_{T_p/\cong}\mathrm{Pr}_C(T_p)\cdot\left|U_{T_p}[\ell]\right| + \prod_{p\mid\mathfrak{m}_{\mathbb{Q}}}\sum_{T_p/\cong}\mathrm{Pr}_C(T_p)\cdot\left|U_{T_p}[\ell]^G\right|\end{aligned}$$

for the limit in the statement, where for the final equality we have used Proposition 10.1 and where we recall that T_p runs over C_3-structured $\mathbb{Q}_p$-algebras. We note that if $p^2+p+1\equiv 0 \mod \ell$, then $0\equiv 4p^2+4p+4=(2p+1)^2+3 \mod \ell$ which gives $\left(\frac{-3}{\ell}\right)=1$. However, $\left(\frac{-3}{\ell}\right)=\left(\frac{-1}{\ell}\right)\left(\frac{3}{\ell}\right)=\left(\frac{\ell}{3}\right)=\left(\frac{2}{3}\right)=-1$ by quadratic reciprocity and as $\ell\equiv 2 \mod 3$. Hence, the case $p^2+p+1\equiv 0 \mod \ell$ does not occur. So for $p\mid\mathfrak{m}_{\mathbb{Q}}$ there are the following nontrivial cases to distinguish:

(1) $p\equiv 1 \mod \ell$ and $p\equiv 2 \mod 3$, or equivalently, $p\equiv 2\ell+1 \mod 3\ell$;

(2) $p\equiv 1 \mod \ell$ and $p\equiv 1 \mod 3$, or equivalently, $p\equiv 1 \mod 3\ell$;

(3) $p=\ell\equiv 2 \mod 3$ and $v_\ell(\mathfrak{m}_{\mathbb{Q}})=1$;

(4) $p=\ell\equiv 2 \mod 3$ and $v_\ell(\mathfrak{m}_{\mathbb{Q}})\geq 2$.

The statement follows by plugging the respective values from the two tables into the formula for $\mathrm{Av}_{\mathcal{K},C}(\ell)$. □

In the same manner, a formula for $\ell\equiv 1 \mod 3$ can be obtained, albeit that formula will look more complicated.

References

[AM69] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969. MR0242802 ↑23

[BJL24] A. Bartel, H. Johnston, and H. W. Lenstra Jr., *Arakelov class groups of random number fields*, Math. Ann. **390** (2024), no. 3, 4405–4428. MR4803478 ↑13, 71, 137

[BL17] A. Bartel and H. W. Lenstra Jr., *Commensurability of automorphism groups*, Compos. Math. **153** (2017), no. 2, 323–346. MR3705226 ↑12, 17, 74, 75, 76, 77, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 93, 145

[BL20] ———, *On class groups of random number fields*, Proc. Lond. Math. Soc. (3) **121** (2020), no. 4, 927–953. MR4105790 ↑10, 11, 13, 14, 15, 16, 17, 111, 136, 137, 138, 139, 140, 145, 147, 150, 151, 153, 171

[BP25] A. Bartel and C. Pagano, *A heuristic for ray class groups of quadratic number fields* (2025), available at `https://arxiv.org/abs/2509.20185`. ↑7, 14, 15, 16, 19, 20, 21, 30, 42, 63, 97, 100, 105, 106, 107, 123, 125, 138, 139, 141, 155, 158, 167, 168, 173, 194, 199

[Bro82] K. S. Brown, *Cohomology of groups*, Graduate Texts in Mathematics, vol. 87, Springer-Verlag, New York-Berlin, 1982. MR672956 ↑63, 64

[Bum13] D. Bump, *Lie groups*, Second edition, Graduate Texts in Mathematics, vol. 225, Springer, New York, 2013. MR3136522 ↑54

[CEW97] V. Chothi, G. Everest, and T. Ward, *S-integer dynamical systems: periodic points*, J. Reine Angew. Math. **489** (1997), 99–132. MR1461206 ↑20, 59, 60

[CF67] J. W. S. Cassels and A. Fröhlich (eds.), *Algebraic number theory*, Academic Press, London; Thompson Book Co., Inc., Washington, DC, 1967. MR215665 ↑59, 61, 62, 64, 170, 180

[CL84] H. Cohen and H. W. Lenstra Jr., *Heuristics on class groups of number fields*, Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), 1984, pp. 33–62. MR756082 ↑7, 8, 9, 10, 173

[CM90] H. Cohen and J. Martinet, *Étude heuristique des groupes de classes des corps de nombres*, J. Reine Angew. Math. **404** (1990), 39–76. MR1037430 ↑10, 24, 138, 149, 171, 176

[Coh00] H. Cohen, *Advanced topics in computational number theory*, Graduate Texts in Mathematics, vol. 193, Springer-Verlag, New York, 2000. MR1728313 ↑97, 98, 104

[Con] K. Conrad, *The character group of* $\mathbf{Q}$, available at `https://kconrad.math.uconn.edu/blurbs/`. ↑59, 60, 63

[CR81] C. W. Curtis and I. Reiner, *Methods of representation theory. Vol. I*, Pure and Applied Mathematics, John Wiley & Sons, Inc., New York, 1981. MR632548 ↑35, 114, 133, 138

[DH71] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields. II*, Proc. Roy. Soc. London Ser. A **322** (1971), no. 1551, 405–420. MR491593 ↑13

[DW88] B. Datskovsky and D. J. Wright, *Density of discriminants of cubic extensions*, J. Reine Angew. Math. **386** (1988), 116–138. MR936994 ↑13

[FA66] S. D. Fisher and M. N. Alexander, *Classroom Notes: Matrices over a Finite Field*, Amer. Math. Monthly **73** (1966), no. 6, 639–641. MR1533848 ↑173

[FG71] R. O. Fulp and P. A. Griffith, *Extensions of locally compact abelian groups. I*, Trans. Amer. Math. Soc. **154** (1971), 341–356. MR272870 ↑57, 58, 59

[FK07] É. Fouvry and J. Klüners, *On the 4-rank of class groups of quadratic number fields*, Invent. Math. **167** (2007), no. 3, 455–513. MR2276261 ↑13

[Flo79] J. Flood, *Pontryagin duality for topological modules*, Proc. Amer. Math. Soc. **75** (1979), no. 2, 329–333. MR532161 ↑51, 52

[FW89] E. Friedman and L. C. Washington, *On the distribution of divisor class groups of curves over a finite field*, Théorie des nombres (Quebec, PQ, 1987), 1989, pp. 227–239. MR1024565 ↑8

[Ger87] F. Gerth III, *Densities for ranks of certain parts of p-class groups*, Proc. Amer. Math. Soc. **99** (1987), no. 1, 1–8. MR866419 ↑13

[HR79] E. Hewitt and K. A. Ross, *Abstract harmonic analysis. Vol. I*, Second edition, Grundlehren der Mathematischen Wissenschaften, vol. 115, Springer-Verlag, Berlin-New York, 1979. MR551496 ↑51, 53, 54, 55, 56, 59, 104, 106

[HS07] N. Hoffmann and M. Spitzweck, *Homological algebra with locally compact abelian groups*, Adv. Math. **212** (2007), no. 2, 504–524. MR2329311 ↑58

[HS97] P. J. Hilton and U. Stammbach, *A course in homological algebra*, Second edition, Graduate Texts in Mathematics, vol. 4, Springer-Verlag, New York, 1997. MR1438546 ↑27, 28, 42

[Isa76] I. M. Isaacs, *Character theory of finite groups*, Pure and Applied Mathematics, No. 69, Academic Press [Harcourt Brace Jovanovich, Publishers], New York-London, 1976. MR0460423 ↑112

[Kne67] M. Knebusch, *Elementarteilertheorie über Maximalordnungen*, J. Reine Angew. Math. **226** (1967), 175–183. MR214584 ↑38

[Lam91] T. Y. Lam, *A first course in noncommutative rings*, Graduate Texts in Mathematics, vol. 131, Springer-Verlag, New York, 1991. MR1125071 ↑39, 112, 113

[Lam99] ———, *Lectures on modules and rings*, Graduate Texts in Mathematics, vol. 189, Springer-Verlag, New York, 1999. MR1653294 ↑50

[Lan94] S. Lang, *Algebraic number theory*, Second edition, Graduate Texts in Mathematics, vol. 110, Springer-Verlag, New York, 1994. MR1282723 ↑141

[Lev73] M. D. Levin, *Locally compact modules*, J. Algebra **24** (1973), 25–55. MR310125 ↑51

[LOWW25] R. Lemke Oliver, J. Wang, and M. M. Wood, *The average size of 3-torsion in class groups of 2-extensions*, Forum Math. Pi **13** (2025), Paper No. e19, 43. MR4959456 ↑13

[Mal08] G. Malle, *Cohen–Lenstra heuristic and roots of unity*, J. Number Theory **128** (2008), no. 10, 2823–2835. MR2441080 ↑10, 137

[ML63] S. Mac Lane, *Homology*, Grundlehren der mathematischen Wissenschaften, vol. 114, Academic Press, Inc., Publishers, New York; Springer-Verlag, Berlin-Göttingen-Heidelberg, 1963. MR156879 ↑44, 64

[ML71] ———, *Categories for the working mathematician*, Graduate Texts in Mathematics, Vol. 5, Springer-Verlag, New York-Berlin, 1971. MR0354798 ↑77

[Mor77] S. A. Morris, *Pontryagin duality and the structure of locally compact abelian groups*, London Mathematical Society Lecture Note Series, No. 29, Cambridge University Press, Cambridge-New York-Melbourne, 1977. MR0442141 ↑51, 53

[Mos67] M. Moskowitz, *Homological algebra in locally compact abelian groups*, Trans. Amer. Math. Soc. **127** (1967), 361–404. MR215016 ↑54, 57, 58, 59, 73

[Neu99] J. Neukirch, *Algebraic number theory*, Grundlehren der mathematischen Wissenschaften, vol. 322, Springer-Verlag, Berlin, 1999. MR1697859 ↑9, 99, 100, 101, 102, 103, 183, 185, 186, 187, 189, 192, 196, 200

[PS17] C. Pagano and E. Sofos, *4-ranks and the general model for statistics of ray class groups of imaginary quadratic number fields* (2017), available at https://arxiv.org/abs/1710.07587. ↑7, 14, 15, 16, 20, 21, 30, 42, 138, 139, 141, 168, 173, 194, 198

[Rei03] I. Reiner, *Maximal orders*, London Mathematical Society Monographs. New Series, vol. 28, The Clarendon Press, Oxford University Press, Oxford, 2003. MR1972204 ↑24, 25, 26, 33, 35, 36, 37, 38, 39, 40, 46, 49, 50, 85, 88, 111, 114, 115, 121, 142, 170, 171, 174

[Rot09] J. J. Rotman, *An introduction to homological algebra*, Second edition, Universitext, Springer, New York, 2009. MR2455920 ↑28, 43

[Sch08] R. Schoof, *Computing Arakelov class groups*, Algorithmic number theory: lattices, number fields, curves and cryptography, 2008, pp. 447–495. MR2467554 ↑102

[Sch99] J.-P. Schneiders, *Quasi-abelian categories and sheaves*, Mém. Soc. Math. Fr. (N.S.) **76** (1999), vi+134. MR1779315 ↑58

[Sha47] I. Shafarevitch, *On p-extensions*, Rec. Math. [Mat. Sbornik] N.S. **20/62** (1947), 351–363. MR20546 ↑180

[Smi26a] A. Smith, *The distribution of ℓ^∞-Selmer groups in degree ℓ twist families I*, J. Amer. Math. Soc. **39** (2026), no. 1, 1–72. MR4969355 ↑13

[Smi26b] ———, *The distribution of ℓ^∞-Selmer groups in degree ℓ twist families II*, J. Amer. Math. Soc. **39** (2026), no. 2, 453–514. MR4999533 ↑13

[Sta25] Stacks Project Authors, *Stacks project*, 2025. See https://stacks.math.columbia.edu. ↑34, 116

[SW23] W. Sawin and M. M. Wood, *Conjectures for distributions of class groups of extensions of number fields containing roots of unity* (2023), available at https://arxiv.org/abs/2301.00791. ↑13, 137

[Var22] I. Varma, *The mean number of 3-torsion elements in ray class groups of quadratic fields*, Israel J. Math. **252** (2022), no. 1, 149–185. MR4526829 ↑14, 20, 198, 199

[Wei94] C. A. Weibel, *An introduction to homological algebra*, Cambridge Studies in Advanced Mathematics, vol. 38, Cambridge University Press, Cambridge, 1994. MR1269324 ↑26, 28, 45, 49, 50, 65, 76, 77

[Woo10] M. M. Wood, *On the probabilities of local behaviors in abelian field extensions*, Compos. Math. **146** (2010), no. 1, 102–128. MR2581243 ↑15, 130, 132, 133, 134, 136, 137, 141, 142, 179

[WW21] W. Wang and M. M. Wood, *Moments and interpretations of the Cohen–Lenstra–Martinet heuristics*, Comment. Math. Helv. **96** (2021), no. 2, 339–387. MR4277275 ↑10, 13

[Yam95] M. Yamagishi, *On the number of Galois p-extensions of a local field*, Proc. Amer. Math. Soc. **123** (1995), no. 8, 2373–2380. MR1264832 ↑180