On Non-Noetherian Iwasawa Theory

Dingli Liang

A dissertation submitted in partial fulfillment

of the requirements for the degree of

Doctor of Philosophy

of

University College London.

Department of Mathematics

University College London

January 1, 2026

I, Dingli Liang, confirm that the work presented in this thesis is my own, except for those parts which are explicitly stated to be based on joint work or previously published articles. Where information has been derived from other sources, this has been clearly indicated in the text.

Abstract

In this thesis, we investigate two non-Noetherian rings of arithmetic interest: the p-adic completed group ring $\mathbb{Z}_p[[\mathbb{Z}_p^{\mathbb{N}}]]$, where $\mathbb{Z}_p^{\mathbb{N}}$ denotes the direct product of countably infinitely many copies of $\mathbb{Z}_p$, and the integral completed group ring $\mathbb{Z}[[G]]$ associated to compact p-adic Lie groups. We further study the module theory over these rings and explore arithmetic applications of the resulting algebraic structures.

For the first ring $\mathbb{Z}_p[[\mathbb{Z}_p^{\mathbb{N}}]]$, we establish a general structure theorem for finitely presented torsion modules over a class of commutative rings that need not be Noetherian. This theorem is then applied to the study of the Weil-étale cohomology groups of $\mathbb{G}_m$ for curves over finite fields. A particularly striking outcome is that we prove an Iwasawa Main Conjecture under mild assumptions. As an application, we show that the inverse limit, taken with respect to norm maps, of the p-primary parts of degree-zero divisor class groups can only form a finitely generated $\mathbb{Z}_p[[\mathbb{Z}_p^{\mathbb{N}}]]$-module under a small class of $\mathbb{Z}_p^{\mathbb{N}}$-extensions.

For the second ring $\mathbb{Z}[[G]]$, we study its coherence properties. We prove that for every compact p-adic Lie group G of rank d, the ring $\mathbb{Z}[[G]]$ is not coherent, but is $d+3$-coherent. This result contributes to a better understanding of the homological behavior of modules over this non-Noetherian Iwasawa algebra.

Impact Statement

This thesis contributes to pure mathematics, specifically within Algebraic Number Theory and Iwasawa Theory. The primary impact of this research lies in advancing the theoretical understanding of non-Noetherian algebraic structures and their arithmetic applications, addressing technical limitations that have previously constrained research in this area.

Beneficial Use within Academia:

1. **Establishing a New Algebraic Framework:** Traditional Iwasawa theory relies heavily on Noetherian rings. This thesis bridges a critical gap by establishing a general structure theorem for finitely presented torsion modules over a class of non-Noetherian rings, specifically $\mathbb{Z}_p[[\mathbb{Z}_p^{\mathbb{N}}]]$. By replacing previously "ad hoc" arithmetic definitions with intrinsic algebraic characterizations, this work provides future scholars with a standardized toolkit. This framework allows for a more conceptual approach to studying characteristic ideals, which can be utilized by researchers to explore broader classes of infinite extensions of global fields.

2. **Advancing Arithmetic of Function Fields:** The application of the newly developed structure theorems has led to part of proof of an Iwasawa Main Conjecture for degree-one Weil-étale cohomology groups under mild assumptions. This result strengthens and generalizes existing literature regarding divisor class groups and Drinfeld modular towers. It offers researchers deeper insights into the arithmetic behavior of global

function fields, potentially influencing future work on the special values of L-functions and geometric extensions.

3. **Foundations for Non-Commutative Integral Iwasawa Theory:** The thesis also impacts Integral Iwasawa Theory by investigating the homological properties of the integral completed group ring $\mathbb{Z}[[G]]$. By proving that these rings are $(d+3)$-coherent for compact p-adic Lie groups of rank d, this research resolves open questions regarding their coherence. This finding lays a crucial algebraic foundation for the development of non-commutative integral Iwasawa theory, opening new pathways for investigating class group growth in non-abelian extensions.

Broader Impact: While this research is primarily theoretical, it contributes to the fundamental advancement of mathematical knowledge. By clarifying complex algebraic structures, it supports the long-term vitality of Number Theory, a discipline that historically underpins modern advancements in cryptography and information theory.

Acknowledgements

This is likely to be a lengthy chapter. I must firstly thank my supervisor Professor David Burns. I would like to express my heartfelt gratitude for his invaluable help and unwavering support throughout my PhD. Were it not for his kindness and timely help at a pivotal moment, I would not have been able to overcome the crisis and continue with my PhD journey. Had it not been for his patience and understanding, I would not have been able to complete my PhD study. My deepest gratitude goes to him for his considerate care and dedicated mentorship.

I would also like to express my deepest gratitude to my supervisor, Professor Edward Segal. Without his understanding and belief in me, I would not have had the opportunity to continue my research.

I would like to thank my parents and my uncle's family. Without their unconditional support, I would not have been able to complete this PhD.

Furthermore, it is a pleasure to thank Alexandre Daoud and Yu Kuang for their contributions to the two joint works. The discussions with them were extremely helpful to me.

I am very grateful to Andrea Bandini, Francesc Bars, Meng Fai Lim, Werner Bley and Cristian Popescu for their interest, generous encouragement and helpful advice for the work of Part I. I also sincerely thank Alexandre Daoud, Cornelius Greither and Xin Wan for their work on this and related projects contributing to the development of Part II. Many thanks to Vladimir Dokchitser and Luis Garcia Martinez for their interest in our work.

I would like to thank my friends Dominik Bullach and Daniel Macias Castillo, whose experience and guidance have been of great help during my PhD studies. I am also grateful to Daniel Isaac Puignau Chacón, and I sincerely wish him all the best in everything.

Finally, I would like to express my heartfelt thanks to all my friends. Without their companionship, I could not have made it through the journey of completing my PhD. I am especially grateful to Yibo Wang, whose generous support in offering me a part-time position during my final year provided crucial financial assistance that made the completion of this degree possible. I would also like to thank Haoyu Chi, whose companionship helped me through one of the most emotionally vulnerable periods of my life. My thanks also go to all the friends in the F&F group.

Thank you to Haorang Liang, Wenhan Zhang, Mengxin Xi, Yuan Yang and all our KCL PhD friends for their meaningful academic discussions and valued friendship. I am also grateful to my friends Ziyang Gu and Ziqiang Zheng, whose support as roommates was a great help in daily life.

Contents

Part I: Non-Noetherian Iwasawa theory for function fields

Chapter 0

Introduction

0.1 Overview

The goal of this thesis is to advance the understanding of non-Noetherian algebra that arises naturally in the development of Iwasawa theory, by establishing a structural algebraic framework and exploring its arithmetic applications. We focus on two main objects of study:

- $\mathbb{Z}_p[[\mathbb{Z}_p^{\mathbb{N}}]]$, the completed p-adic group ring of the direct product $\mathbb{Z}_p^{\mathbb{N}}$ of a countably infinite number of copies of $\mathbb{Z}_p$;
- $\mathbb{Z}[[G]]$, the integral completed group ring associated to compact p-adic Lie groups G.

This introduction is devoted to the former. For an introduction to the latter, see Part II, Chapter 6.

Let us briefly review the motivation for studying the algebra $\mathbb{Z}_p[[\mathbb{Z}_p^{\mathbb{N}}]]$. This motivation is closely tied to the number of independent $\mathbb{Z}_p$-extensions of global fields. Let us first recall the number field case. Fix a prime number p and a number field K. For each prime $\mathfrak{p}$ of K lying over p, let $U_{\mathfrak{p}}$ denote the group of local units of $K_{\mathfrak{p}}$, and $U_{1,\mathfrak{p}}$ denote the subgroup of units congruent to 1 modulo $\mathfrak{p}$. Set $U = \prod_{\mathfrak{p}|p} U_{\mathfrak{p}}$ and $U_1 = \prod_{\mathfrak{p}|p} U_{1,\mathfrak{p}}$. There is a diagonal embedding $e : \mathcal{O}_K^{\times} \hookrightarrow U$, sending each global unit ϵ to $(\epsilon, \ldots, \epsilon) \in U$. Let $E_1 \subset \mathcal{O}_K^{\times}$

be the subgroup whose image lies in U_1, and let $\bar{E}_1$ denote its closure. It is well known that there exists at least one $\mathbb{Z}_p$-extension of K, but there may be several independent such extensions. The number d of independent $\mathbb{Z}_p$-extensions of K is related to the $\mathbb{Z}_p$-rank of $\bar{E}_1$ (See Washington [79, Thm. 13.4]). According to the well-known Leopoldt's Conjecture, for every number field K, this number d is expected to satisfy $d = r_2 + 1 = \mathrm{rank}_{\mathbb{Z}_p}(\bar{E}_1) - r_1 + 2$, where r_1, r_2 denote the numbers of real and complex embeddings of K, respectively. Leopoldt's conjecture is known in many cases; in particular, it holds for every finite abelian extension of $\mathbb{Q}$ or of an imaginary quadratic field (see, for example, Ferri–Johnston [39, Thm 1.1] and the references therein; see also Washington [79, Cor. 5.32]). Let K' be the compositum field of all the $\mathbb{Z}_p$-extensions of K. Then we have $\mathrm{Gal}(K'/K) \cong \mathbb{Z}_p^d$. This compositum field, which is the canonical example for $\mathbb{Z}_p^d$-extensions, has been extensively utilized by many researchers, for example Greenberg [45] which studies Iwasawa invariants. In particular, he proved that if K has only one prime lying over p, then the μ-invariant is bounded as the $\mathbb{Z}_p$-extension varies over all such extensions. This shows that studying the compositum field is a meaningful and worthwhile pursuit.

In contrast, it is of interest to investigate the analogous situation for global function fields. Let us now recall the notion of $\mathbb{Z}_p$-extensions in the context of global function fields. Suppose k denotes a global function field with the constant field $\mathbb{F}_q$. The first example that naturally comes to mind when discussing such extensions is the constant field — that is, an extension of k obtained by forming a tower of finite field extensions of the constant field. In this case, the base field $\mathbb{F}_q$ is extended by a union of finite fields $\mathbb{F}_{q^{p^n}}$. It should be noted that this type of $\mathbb{Z}_p$-extension exhibits different properties from the cyclotomic $\mathbb{Z}_p$-extension of number fields. For instance, any constant field extension of a global function field is unramified (See [68, Prop. 8.5]). Since such $\mathbb{Z}_p$-extensions involve only the extension of the constant field, they arguably carry relatively trivial arithmetic information about global function fields.

However, for global function fields, the most significant departure from the number field case arises in the case of geometric extensions of k — these are algebraic extensions K/k whose constant field coincides with that of k. As previously noted, the number of independent $\mathbb{Z}_p$-extensions is always finite in the case of number fields. By contrast, this is no longer true for global function fields. A prominent counterexample is provided by the $\mathbb{Z}_p$-extensions arising from Drinfeld modules (See [68, P. 199]). In particular, a Carlitz module is a rank-one Drinfeld module defined over $A = \mathbb{F}_q[T]$ with base field $k = \mathbb{F}_q(T)$. Since the existence of a Drinfeld module is often a delicate matter (See [68, P. 231]), we restrict our attention here to the Carlitz module Φ associated with A and use it to illustrate the constructions that follow.

Fix once and for all an algebraic closure $\bar{k}$ of k, and a non-zero prime ideal $\mathfrak{p} \subset A$ generated by an irreducible polynomial of degree $d \geq 1$. For each $n \in \mathbb{N}$, define $k_n := k(\Phi[\mathfrak{p}^{n+1}])$ as the field obtained by adjoining the $\mathfrak{p}^{n+1}$-torsion of Φ to k. Since $\mathfrak{p}^n \mid \mathfrak{p}^{n+1}$ implies $\Phi[\mathfrak{p}^n] \subseteq \Phi[\mathfrak{p}^{n+1}]$, we have a tower of fields:

$$k \subset k_0 \subset k_1 \subset \cdots \subset k_\infty := \bigcup_n k_n.$$

It is well known that each k_n/k is an abelian extension, with Galois group

$$G_n := \mathrm{Gal}(k_n/k) \cong (A/\mathfrak{p}^{n+1})^\times \cong (A/\mathfrak{p})^\times \times (1+\mathfrak{p}A)/(1+\mathfrak{p}^{n+1}A) =: \Delta \times \Gamma_n,$$

where $\Delta \cong \mathrm{Gal}(k_0/k) \cong (A/\mathfrak{p})^\times$ is a cyclic group of order $q^d - 1$, and $\Gamma_n = \mathrm{Gal}(k_n/k_0)$ is the p-Sylow subgroup of G_n. The extension k_n/k is totally ramified at $\mathfrak{p}$ and tamely ramified at the place ∞. In particular, k_n/k_0 is ramified only at $\mathfrak{p}$. This motivates the definition of the $\mathfrak{p}$-cyclotomic extension of k as

$$k^{\mathfrak{p},cyc} := k(\Phi[\mathfrak{p}^\infty]) = \bigcup_n k(\Phi[\mathfrak{p}^n])$$

which is a Galois extension with the Galois group

$$G_\infty := \mathrm{Gal}(k^{\mathfrak{p},cyc}/k) = \varprojlim_n \mathrm{Gal}(k_n/k) \cong \Delta \times \Gamma, \quad \text{where } \Gamma := \varprojlim_n \Gamma_n.$$

To analyze the group G_∞, we consider the completion of A at $\mathfrak{p}$. We have $A_\mathfrak{p} \cong \mathbb{F}_\mathfrak{p}[[\pi_\mathfrak{p}]]$, where $\pi_\mathfrak{p}$ is the irreducible generator of $\mathfrak{p}$ and $\mathbb{F}_\mathfrak{p}$ is the residue field of $A_\mathfrak{p}$. The unit group $A_\mathfrak{p}^\times$ admits a filtration $U_n := 1 + \mathfrak{p}^n A_\mathfrak{p}$. Let $k_\mathfrak{p}$ be the completion of k at $\mathfrak{p}$ and $\mathcal{C}_\mathfrak{p}$ be the completion of an algebraic closure of $k_\mathfrak{p}$. We establish, once and for all, an embedding $\bar{k} \hookrightarrow \mathcal{C}_\mathfrak{p}$. Via the Galois action on the formal Drinfeld module $\Phi : A_\mathfrak{p} \to A_\mathfrak{p}\{\{\tau\}\}$ (See [67]), we obtain a $\mathfrak{p}$-cyclotomic character $\kappa : G_\infty \to A_\mathfrak{p}^\times$ which is, in fact, an isomorphism. Then we know $\Gamma \cong U_1$ since $\Gamma_n \cong U_1/U_{n+1} \cong (1+\mathfrak{p}A_\mathfrak{p})/(1+\mathfrak{p}^{n+1}A_\mathfrak{p})$. Since $n \to +\infty$, the minimal number of generators of U_1/U_{n+1} tends to infinity (See [68, Prop. 1.6]), it is obvious that $U_1 \cong \mathbb{Z}_p^\mathbb{N}$. Let K be the subfield of $k^{\mathfrak{p},cyc}$ fixed by Γ. Then K/k is a $\mathbb{Z}_p^\mathbb{N}$-extension of k, which is totally ramified at $\mathfrak{p}$. This provides a natural and concrete example demonstrating why the development of Iwasawa theory for $\mathbb{Z}_p^\mathbb{N}$-extensions of function fields is both meaningful and necessary.

There has been considerable pioneering work on this topic. Let K/k be a $\mathbb{Z}_p^\mathbb{N}$-extension of a global function field k. The major difficulty in this setting is that the completed p-adic group ring $\mathbb{Z}_p[[\mathbb{Z}_p^\mathbb{N}]]$ of $\mathbb{Z}_p^\mathbb{N}$ is not Noetherian, which prevents the direct application of classical techniques in Iwasawa theory. In response to this challenge, Bandini, Bars, and Longhi were the first to introduce the notion of "pro-characteristic ideal" under certain conditions, as a generalization of the classical Iwasawa-theoretic characteristic ideal (See [7, Def. 1.3]). They applied this concept to the study of several natural Iwasawa modules over K/k. For instance, the authors investigated degree-zero divisor class groups in [7, 9], as well as the Pontrjagin duals of the p-primary Selmer groups of abelian varieties defined over global function fields in [8, 9]. These efforts culminated in their joint proof, with Anglès, of a main conjecture for divisor class groups over Carlitz-Hayes cyclotomic extensions of k (see [3]). More recently, Bandini and Coscelli [10], as well as Bley and Popescu [12], have extended such results to broader classes of Drinfeld modular towers. However, a significant issue arises in that the definitions of "pro-characteristic ideals" used in the aforementioned works heavily depend on specific arithmetic contexts. In particular, the definitions vary depending on the Iwasawa module under consideration, each requiring arithmetic assumptions to define a pro-characteristic ideal tailored to that module (See [7, Thm 1.2, Def. 1.3], [8, Thm. 1.2]). As a result, the definition appears somewhat ad hoc—crafted to align with arithmetic phenomena rather than arising as an intrinsic algebraic characterization of the modules over the complete group ring $\mathbb{Z}_p[[\mathbb{Z}_p^{\mathbb{N}}]]$.

By adopting a more conceptual algebraic approach, Part I of this thesis aims to strengthen the theoretical foundations established in earlier works. As a starting point, we identify a natural class of commutative rings — which notably includes all rings of the form $\mathbb{Z}_p[[\mathbb{Z}_p^{\mathbb{N}} \times G]]$ for finite abelian groups G — that are generally non-Noetherian, yet still admit a structure theorem for a broad class of finitely presented torsion modules (see Theorem 2.2.1). This result is potentially of independent interest and, in particular, leads naturally to a generalized notion of the characteristic ideal, which both extends and refines the pro-characteristic ideal constructions used in previous literature.

We then prove that the inverse limits (with respect to corestriction) of the p-completions of the degree-one Weil-étale cohomology groups of $\mathbb{G}_m$ over finite extensions of k in K are finitely-presented torsion $\mathbb{Z}_p[[\mathbb{Z}_p^{\mathbb{N}}]]$-modules. By applying our structure theory to these modules, we obtain strengthened and more general versions of the main results in [3], [10] and [12] (see Theorem 4.3.2 and Remarks 4.4.2 and 4.4.3). Moreover, this approach also enables us to prove surprisingly that the inverse limit (with respect to norm maps) of the p-parts of the degree-zero divisor class groups of finite extensions of k in K is finitely generated as a $\mathbb{Z}_p[[\mathbb{Z}_p^{\mathbb{N}}]]$-module for a remarkably small class of extensions K/k (see Corollary 4.4.1). Finally, we present two major open questions whose resolution may lead to further advances in the theory.

0.2 Content

In this section, we present a summary of the content covered in Chapters 1-7 individually.

In Chapter 1, we introduce a general structure theorem for finitely presented torsion modules over a broad class of unital commutative rings, including certain non-Noetherian cases. After presenting several types of rings, we then establish the structure theorem for finitely presented modules over elementary divisor domains, which form a special subclass of Prüfer and Bézout domains.

In Chapter 2, to apply the structure theorems presented in 1, we introduce the notions of admissible modules and admissible rings. We then prove two structure theorems for finitely presented admissible modules. Furthermore, we investigate the admissibility relationship between certain kinds of $\mathbb{Z}_p$-algebras R and their group rings $\mathbb{Z}_p[G]$ for finite abelian groups G, which sets the stage for the arithmetic study of $\mathbb{Z}_p[[\mathbb{Z}_p^{\mathbb{N}} \times G]]$-extensions in Chapter 4.

In Chapter 3, in light of the two structure theorems we established in Chapter 2, we define two types of characteristic ideals and examine the relationship between them. Later, we develop a framework for inverse limits of compact rings and introduce the notion of $I_\bullet$-completeness for finitely presented modules. The $I_\bullet$-completeness is employed later in Section 4.2 to show that the definition of one of our two characteristic ideals encompasses the pro-characteristic ideal for quadratically-presented torsion modules.

In Chapter 4, following a brief introduction to Weil–étale cohomology theory and some preparatory steps to adapt our algebraic results for arithmetic applications, we show that the degree-one Weil–étale cohomology groups of $\mathbb{G}_m$ over finite extensions inside a $\mathbb{Z}_p^{\mathbb{N}} \times G$-extension form quadratically-presented torsion $\mathbb{Z}_p[[\mathbb{Z}_p^{\mathbb{N}} \times G]]$-modules. Furthermore, using the characteristic ideals defined earlier, we formulate an Iwasawa Main Conjecture and prove it under certain mild assumptions. Finally, we apply this result to the study of degree-zero divisor class groups.

In Chapter 5, we propose two meaningful questions to be addressed in future research. The first concerns the ring-theoretic properties of $\mathbb{Z}_p[[\mathbb{Z}^{\mathbb{N}}]]$; the second explores potential applications of our theory to the study of the arithmetic of number fields.

In Chapter 6, we introduce the motivation to develop integral Iwasawa theory and review recent progress in the field to clarify our interest in studying the properties of integral completed group rings associated with p-adic Lie groups in Chapter 7.

In Chapter 7, we complete the proof of a more general theorem showing that for every compact p-adic Lie group G of rank d, $\mathbb{Z}[[G]]$ is $d+3$-coherent rather than coherent. Along the way, we introduce the notion of pro-discrete $\mathbb{Z}[[G]]$-modules, establish a version of Nakayama's Lemma for such modules, and investigate the divisibility properties of Tor-groups.

0.3 Notation

In this thesis, $\mathbb{Z}$ denotes the ring of integers. $\mathbb{N}$ denotes the set of natural numbers. $\mathbb{Q}$ denotes the field of rational numbers. $\mathbb{C}$ denotes the field of complex numbers. $\mathbb{Q}_p$ denotes the field of p-adic numbers, that is, the completion of $\mathbb{Q}$ with respect to the p-adic valuation. $\mathbb{Z}_p$ denotes the ring of p-adic integers. $\mathbb{F}_q$ denotes the finite field with q elements, where q is a power of a prime number p. Throughout this thesis, A and R always denote unital rings, the precise assumptions on which will be specified as needed in context. M will be used to denote a module over such rings, with additional structure specified as needed.

$Spec(A)$ denotes the spectrum of a commutative ring A. All other notations will be introduced and explained as they arise in the text.

Chapter 1

Non-Noetherian algebra

In this chapter, we review several algebraic results concerning properties of commutative unital rings that are not necessarily Noetherian, along with modules over such rings.

We begin with Warfield's Structure Theorem (Theorem 1.1.2) which serves as the starting point for the structural results developed in Chapter 2. This theorem describes the structure of finitely presented modules over commutative rings whose localizations at all maximal ideals are valuation rings.

Next, we introduce various classes of rings, including semisimple rings, von Neumann regular rings, semihereditary rings, Prüfer domains, Bézout domains, elementary divisor domains. These classes form a hierarchy:

- "Von Neumann regular rings generalize semisimple rings";
- "Semihereditary rings generalize von Neumann regular rings";
- "An integral semihereditary ring is called a Prüfer domain";
- "A Bézout domain is a special case of a Prüfer domain";
- "An elementary divisor domain is a special case of a Bézout domain".

Finally we present the structure theorem (Theorem 1.6.1), which gives the structure of finitely presented modules over elementary divisor domains. We also highlight a key property of module presentations (Proposition 1.7.4) that will be used frequently in the chapters that follow.

1.1 Warfield's structure theorem

In this section, we follow Warfield [75] to show a decomposition property for finitely presented modules over certain commutative rings. Throughout this section, all rings are assumed to be commutative and unital. We begin by recalling the definition of a cyclic module.

Definition 1.1.1. *Let R be a commutative and unital ring. A cyclic R-module is a module generated by a single element, i.e. $M = Rx$. If M is a cyclic R-module, then it is isomorphic to $R/\operatorname{Ann}_R(x)$. In addition, if $\operatorname{Ann}_R(x)$ is a principal ideal, then the module M is said to be cyclically presented.*

Theorem 1.1.2 (Warfield's Structure Theorem)**.** *A commutative ring R has the property that every finitely presented module is a summand of a direct sum of cyclic modules if and only if the localisation $R_{\mathfrak{m}}$ is a generalized valuation ring for each maximal ideal $\mathfrak{m}$ in R.*

To prove this theorem, we first introduce the notion of a generalized valuation ring, which extends the concept of valuation rings to the setting of non-integral rings.

Definition 1.1.3. *A commutative ring is a generalized valuation ring if it satisfies one of the three equivalent conditions:*

- *for every element a and b, either a divides b or b divides a;*
- *the ideals of R are totally ordered by inclusion;*
- *R is a local ring and every finitely generated ideal is principal.*

Proposition 1.1.4. *If M is a finitely presented module over a generalized valuation ring, then M is a direct sum of cyclically presented modules.*

Proof. See [75, Thm. 1]. □

The third item of the Definition 1.1.3 describes the relationship between generalized valuation rings and local rings. We now present a result that further elucidates this relationship in the context of finitely presented modules.

Proposition 1.1.5. *If R is a commutative local ring and every finitely presented module is a summand of a direct sum of cyclic modules, then R is a generalized valuation ring.*

To prove this result, we need the following two lemmas.

Lemma 1.1.6. *Let R be a commutative local ring which is not a generalized valuation ring. Then for every $n > 0$, there are finitely presented modules which are indecomposable and cannot be generated by fewer than n elements.*

Proof. See [75, Thm. 2]. □

Lemma 1.1.7. *Any indecomposable summand of a direct sum of cyclic modules over a commutative local ring is again a cyclic module.*

Proof. See [6, Thm. 1] □

Proof of Proposition 1.1.5. Assume R is not a generalized valuation ring. Then by Lemma 1.1.6, there exists a finitely presented indecomposable module M which is generated by no fewer than two elements. By the hypothesis of Proposition 1.1.5, M is a summand of a direct sum of cyclic modules. Thus we know it is again a cyclic module by Lemma 1.1.7. We obtain a contradiction. □

To complete the proof of Theorem 1.1.2, we need the following notion.

Definition 1.1.8. *Let R be a commutative ring. An R-submodule A of an R-module B is relatively divisible if for all $r \in R, rA = A \cap rB$. An R-module P is RD-projective if for every short exact sequence $0 \to A \to B \to C \to 0$ with A relatively divisible in B, the map $\operatorname{Hom}(P, B) \to \operatorname{Hom}(P, C)$ is surjective.*

Proposition 1.1.9. *Let R be a commutative ring and M a finitely generated R-module. Then M is RD-projective if and only if M is finitely presented and for each maximal ideal $\mathfrak{m}$ of R, the localisation $M_{\mathfrak{m}}$ is a direct sum of cyclically presented $R_{\mathfrak{m}}$-modules.*

Proof. See [76, Prop. 4]. □

Proposition 1.1.10. *Let R be a commutative ring. Then an R-module is RD-projective if and only if it is a summand of a direct sum of cyclically presented modules.*

Proof. See [76, Prop. 1, Cor. 1] □

Proof of Theorem 1.1.2. It is well known that if a ring R satisfies the conditions of Theorem 1.1.2, then so does $R_{\mathfrak{m}}$ for every maximal ideal $\mathfrak{m}$. This follows from the fact that every finitely presented $R_{\mathfrak{m}}$-module is of the form $M_{\mathfrak{m}}$, where M is a finitely presented R-module. The necessity then follows from Proposition 1.1.5. Conversely, by Proposition 1.1.10, it suffices to prove that every finitely presented module is RD-projective. By Proposition 1.1.9, a finitely generated R-module M is RD-projective if and only if M is finitely presented and $M_{\mathfrak{m}}$ is RD-projective for every $\mathfrak{m}$. Applying Proposition 1.1.10 and Proposition 1.1.4, we obtain the desired result. □

1.2 Semisimple rings

In this section, we recall some properties of semisimple rings, which will play an important role in our theory. We begin by recalling the definition.

Definition 1.2.1. *A module is called left (or right) semisimple if it is a direct sum of left (or right) simple modules. A ring is called semisimple if as the left (or right) module over itself, the ring is a semisimple left (or right) module.*

In the proposition below, we list some alternative equivalent definitions of semisimple rings (see [69, Chap. 4, §4.1, Prop. 4.5]).

Proposition 1.2.2. *The following conditions on a ring R are equivalent.*

(i) R is semisimple.

(ii) Every left (or right) R-module M is semisimple.

(iii) Every left (or right) R-module M is injective.

(iv) Every short exact sequence of left (or right) R-modules splits.

(v) Every left (or right) R-module M is projective.

(vi) The global dimension (gl.dim) of R is equal to 0.

As is well known, semisimple rings play a key role in many areas of mathematics, including commutative algebra, representation theory, and algebraic number theory. The examples below illustrate the ubiquity of such rings.

Example 1.2.3. *We list several kinds of rings as examples of semisimple rings.*

(i) Every field is semisimple. More generally, any division ring is also semisimple.

(ii) Every Artinian ring is semisimple over itself.

(iii) If R is semisimple, then so is $M_n(R)$.

(iv) If R and S are semisimple, so is $R \times S$.

(v) By Maschke's Theorem and Proposition 1.2.2(ii), for every finite group G over a field $\mathbb{F}$ with characteristic not dividing the order of G, $\mathbb{F}[G]$ is semisimple. As an application, for $\mathbb{F} = \mathbb{Q}_p$ and $G = \mathrm{Gal}(L/K)$ for any finite extension $K/\mathbb{Q}_p$, we know $\mathbb{Q}_p[G]$ is semisimple.

Next, we recall a well-known result that describes the structure of semisimple rings: the Wedderburn–Artin Theorem.

Proposition 1.2.4 (Wedderburn-Artin)**.** *Let R be a semisimple ring. Then R is isomorphic to a product of finitely many $M_{n_i}(D_i)$ for some integers n_i and division ring D_i, where D_i and n_i, up to permutation of the index, are uniquely determined.*

By Proposition 1.2.4, we know that any commutative semisimple ring is isomorphic to a finite direct product of fields. On the other hand, by identifying matrix rings over division rings with simple Artinian rings, one obtains another version of the theorem. (see [2, Chap 4, §13, Thm. 13.6]).

Proposition 1.2.5. *A ring R is semisimple if and only if it is a finite product of simple Artinian rings.*

1.3 von Neumann regular rings

To extract further information from semisimple rings, we introduce a concept originally formulated by John von Neumann in [74], where he referred to such rings as "regular rings".

Definition 1.3.1. *A ring R is a von Neumann regular ring if for every element*

$a \in R$ there exists an x in R such that $a = axa$.

Note that if a is a unit in R, then $x = a^{-1}$ satisfies the equation $a = axa$. Intuitively, the element x in this equation can be viewed as a weak inverse of a. A ring is said to be von Neumann regular if every element in the ring admits at least one such weak inverse. Several examples of von Neumann regular rings can be found in [49, P. 110].

Example 1.3.2. *We list several kinds of rings as examples of von Neumann regular rings*

(i) Each field is von Neumann regular by taking $x = a^{-1}$ for every $a \neq 0$ and taking x equal to any element for $a = 0$. Moreover, any division ring is von Neumann regular.

(ii) The matrix ring $M_n(R)$ for $n \geq 1$ over every von Neumann regular ring R is von Neumann regular again.

(iii) Let K be a division ring and let V be a (possibly infinite-dimensional) left K-vector space. Then the endomorphism ring $\mathrm{End}_K(V)$ is von Neumann regular.

From the perspective of ideals and modules, we can gain further insight into the structure of von Neumann regular rings, as illustrated in the following proposition.

Proposition 1.3.3. *The following conditions are equivalent.*

(i) R is a von Neumann regular ring.

(ii) Every principal left (resp. right) ideal of R is generated by an idempotent.

(iii) Every principal left (resp. right) ideal of R is a direct summand of the left (resp. right) R-module R.

(iv) Every finitely generated left (resp. right) ideal of R is generated by an idempotent element.

Proof. For all items above, we just prove the claims about left ideals as the right ideal cases can be deduced by symmetrical arguments.

(i) $\Leftrightarrow$ *(ii)*: (ii) means that for every $a \in R$, there is an idempotent $e \in R$ such that $Ra = Re$. By (i), we know for every $a \in R$, there exists an x such that $a = axa$. Let $e = xa$. It is easy to check e is an idempotent and $Re \subseteq Ra$. Besides, we have $a = axa = ae$. Hence $Ra \subseteq Re$. Conversely, suppose $Ra = Re$ for some idempotent e, then we have $e = xa$ and $a = ye$ for some $x, y \in R$. Then we have $axa = ae = yee = ye = a$ for every $a \in R$.

(ii) $\Leftrightarrow$ *(iii)*: Since for every idempotent $e \in R$, $R = Re \oplus R(1-e)$, then we know every principal right ideal is a direct summand if it is generated by an idempotent e. Conversely, since any direct summand of R is generated by an idempotent, *(ii)* can be deduced from *(iii)* naturally.

(ii) $\Leftrightarrow$ *(iv)*: By (ii) and inductive method, we only need to prove the sum of two principal left ideals is principal. By (ii) we know any principle left ideal is generated by idempotent. Let Re_1 and Re_2 generated by idempotents e_1 and e_2. By (ii), we know the left ideal $Re_2(1-e_1)$ is generated by an idempotent f. Thus there exist $b, c \in R$ such that $e_2(1-e_1) = bf$ and $f = ce_2(1-e_1)$. Since $e_2 = e_2e_1 + bf$ and $fe_1 = ce_2(1-e_1)e_1 = 0$. Thus we can have some computations as follows.

$$
\begin{aligned}
e_1 &= e_1 + f - fe_1 - f^2 = (1-f)(e_1+f), \\
e_2 &= e_2e_1 + bf = e_2e_1 + e_2f - e_2f^2 - e_2(fe_1) + b(fe_1) + bf^2 \\
&= (e_2 - e_2f + bf)(e_1+f),
\end{aligned}
$$

Hence we can know $Re_1 + Re_2 \subseteq R(e_1 + f)$. By

$$e_1 + f = e_1 + ce_2(1 - e_1) = (1 - ce_2)e_1 + ce_2,$$

we know $R(e_1 + f) \subseteq Re_1 + Re_2$. The proof of converse arrow is obvious. □

Corollary 1.3.4. *All semisimple rings are von Neumann regular.*

Proof. By Proposition 1.2.2 (iv), every left ideal of a semisimple ring is a direct summand. So is every finitely generated ideal. Since every direct summand is generated by an idempotent, and by Proposition 1.3.3 (ii), we obtain the result. □

To illustrate certain local–global properties of von Neumann regular rings, we now present the following proposition.

Lemma 1.3.5. *A commutative ring is von Neumann regular if and only if for every maximal ideal* $\mathfrak{m}$ *of* R *the localization ring* $R_{\mathfrak{m}}$ *is a field.*

Proof. See ([37, Thm 1]). Note that in this paper, the author refers to localization rings as "quotient rings". □

We also require the following two lemmas concerning the homological dimension properties of von Neumann regular rings. Before stating the next lemma, we briefly recall the notion of weak global dimension. The (left) global dimension $\operatorname{gl.dim}(R)$ of a ring R is defined as

$$\operatorname{gl.dim}(R) := \sup\{\operatorname{pd}_R(M) : M \text{ is a left } R\text{-module}\},$$

where $\operatorname{pd}_R(M)$ denotes the projective dimension of M. Similarly, the (left) weak global dimension w.gl.dim(R) of R is defined as

$$\text{w.gl.dim}(R) := \sup\{\operatorname{fd}_R(M) : M \text{ is a left } R\text{-module}\},$$

where $\mathrm{fd}_R(M)$ is the flat dimension of M. Equivalently, w.gl.dim$(R) \leq n$ if and only if $\mathsf{Tor}_{n+1}^R(M,N) = 0$ for all R-modules M and N. In particular, one always has

$$\text{w.gl.dim}(R) \ \leq \ \text{gl.}\dim(R),$$

so the weak global dimension is a priori a weaker invariant than the global dimension.

Lemma 1.3.6. *A commutative local ring R is a valuation ring if and only if its weak global dimension (denoted by w.gl.dim) is less than or equal to 1. In particular, it is a field if and only if w.gl.dim$(R) = 0$.*

Proof. See [37, Thm 4]. □

Lemma 1.3.7. *Let R be a ring, M, N be R-modules and S be a multiplicatively closed subset of R. For every integer $n \geq 0$, we have $\mathsf{Tor}_n^R(M,N)_S \cong \mathsf{Tor}_n^{R_S}(M_S, N_S)$. Thus w.gl.dim$(R)= \sup_{\mathfrak{m}}\{\text{w.gl.dim}(R_{\mathfrak{m}})\}$, where $\mathfrak{m}$ runs over all maximal ideals of R.*

Proof. See [21, VII, Ex 9, 10, 11]. □

Proposition 1.3.8. *A commutative ring R is von Neumann regular if and only if w.gl.dim$(R) = 0$.*

Proof. It is obvious by Lemma 1.3.5, Lemma 1.3.6 and Lemma 1.3.7. □

The following proposition motivates the introduction of the notions of admissible modules and admissible rings in Chapter 2.

Proposition 1.3.9. *For a commutative ring R, w.gl.dim$(R) \leq 1$ if and only if the localization ring $R_{\mathfrak{m}}$ of R at every maximal ideal $\mathfrak{m}$ of R is a valuation ring.*

Proof. It is obvious by Lemma 1.3.6 and Lemma 1.3.7. □

1.4 Semihereditary rings and Prüfer domains

The main focus of this section is on certain properties of semihereditary rings, a notion that generalizes von Neumann regular rings. We begin by recalling the definition of a semihereditary ring.

Definition 1.4.1. *If a commutative ring R has the property that every finitely generated ideal of R is projective as an R-module, we call it a semihereditary ring.*

One can also define left (resp. right) semihereditary rings by replacing ideals with left (resp. right) ideals in the definition. Since our work primarily focuses on the commutative case, we present the definition accordingly. Furthermore, if every ideal of a ring is projective, the ring is called a hereditary ring. A commutative semihereditary integral domain is referred to as a Prüfer domain.

Example 1.4.2. *There are several examples of semihereditary rings.*

i) Each field is semihereditary.

ii) Each Dedekind domain is a hereditary ring. Indeed, every ideal I of a Dedekind domain R is finitely generated. For a finitely generated R-module, being projective is equivalent to being locally free. For every ideal $I \subset R$ and prime ideal $\mathfrak{p} \in \mathrm{Spec}(R)$, the localisation $I_{\mathfrak{p}}$ is a free $R_{\mathfrak{p}}$-module of rank one. Thus, Prüfer domains can be viewed as a generalization of Dedekind domains to the non-Noetherian setting. Furthermore, semihereditary (resp. hereditary) rings extend this notion to the non-integral and noncommutative context. For example, the matrix ring $M_n(R)$ over a Prüfer domain R is a semihereditary ring (see [52, P.44 Example 2.32(c)]).

iii) The direct product of any two semihereditary(resp. hereditary) rings is also semihereditary(resp. hereditary) (see [52, P.44 Example 2.32(c)]).

The following corollary, derived from Proposition 1.3.3(iv) and Definition 1.4.1, demonstrates that semihereditary rings generalize the notion of von Neumann regular rings.

Corollary 1.4.3. *Each von Neumann regular ring is semihereditary.*

As observed, the direct product of any two semihereditary (resp. hereditary) rings is again semihereditary (resp. hereditary). We now present an equivalent characterization of a semihereditary ring R in terms of its total quotient ring $Q(R)$.

Proposition 1.4.4. *A commutative ring R is semihereditary if and only if the total quotient ring $Q(R)$ is von Neumann regular ring and the localization ring $R_{\mathfrak{m}}$ is a valuation ring for every maximal ideal $\mathfrak{m}$ of R.*

Proof. See [37, Thm 2]. □

The Proposition 1.4.4 offers a perspective for recovering semihereditary rings from von Neumann regular rings. Consequently, using the weak global dimension properties of von Neumann regular rings, we can characterize semihereditary rings as follows (see [37, Thm 5]).

Proposition 1.4.5. *For every commutative ring R and its total quotient ring $Q(R)$, the following two statements are equivalent:*

i) R is a semihereditary ring.

ii) $w.gl.dim(R) \leq 1$ and $w.gl.dim(Q(R)) = 0$.

Proof. By Proposition 1.4.4, Proposition 1.3.8 and Proposition 1.3.9. □

Finally we explore the properties of Prüfer domains. We briefly recall the notion of an invertible ideal. Let R be a commutative ring. A (fractional) ideal I of R is called invertible if there exists a (fractional) ideal J of R such that $IJ = R$.

Proposition 1.4.6. *The following conditions listed below are equivalent.*

i) *R is a Prüfer domain.*

ii) *For every maximal ideal $\mathfrak{m}$ in R, the localization $R_{\mathfrak{m}}$ of R at $\mathfrak{m}$ is a valuation domain.*

iii) *Every non-zero finitely generated ideal is invertible.*

Proof. See [13, P.558 12]. □

A characterization of the direct product of a finite number of Prüfer domains in terms of homological dimensions is given as follows (see [37, P.117 Cor]).

Proposition 1.4.7. *For every commutative ring R and its total quotient ring $Q(R)$, the following two statements are equivalent:*

i) *R is a direct product of a finite number of Prüfer domains.*

ii) *$w.gl.dim(R) \leq 1$ and $gl.dim(Q(R)) = 0$.*

Proof. It is obvious by Lemma 1.3.6. □

1.5 Bézout domains and elementary divisor domains

In the previous section, we studied the properties of Prüfer domains. An important subclass of Prüfer domains is the class of Bézout domains, which are defined as follows.

Definition 1.5.1. *A commutative ring is a Bézout ring if its finitely generated ideals are principal.*

By the definition above, Bézout's identity holds for every pair of elements in a Bézout domain. It is evident that principal ideals in a commutative domain are projective, as they are free of rank one. Hence, every Bézout domain is a Prüfer domain. A natural question arises: which Prüfer domains are in fact Bézout domains? To address this question, we first recall the definition of semilocal rings.

Definition 1.5.2. *A commutative ring is semilocal if it only has finitely many maximal ideals.*

It is clear that a local ring is a special case of a semilocal ring. The finiteness of maximal ideals in semilocal rings leads to the following proposition, which answers the question raised above.

Proposition 1.5.3. *Semilocal Prüfer domains are Bézout domains.*

Proof. See [41, III. Thm. 5.1]. □

On the other hand, we can use the notion of GCD-domain, i.e. every pair of elements in the domain admits a greatest common divisor, to give another comprehensive answer of the question about the relation between Prüfer and Bézout domains.

Proposition 1.5.4. *A commutative ring R is a Bézout domain if and only if R is both a Prüfer domain and a GCD-domain.*

Proof. For the only if part, we just need to prove every pair of elements in Bézout domain has a greatest common divisor. This is because that for all $a, b \in R$, there exists an $c \in R$ such that $aR + bR = cR$. Thus c divides a and b, and for every $r \in R$, if r divides a and b, then r divides c.

For the if part, by Proposition 1.4.6(iii), we only need to prove that in a GCD-domain every invertible ideal is principal. Let I be an invertible ideal of a GCD-domain $R, I = (a_1/b_1)R + \cdots + (a_n/b_n)R$. Since R is a GCD-domain. here we can assume for each $1 \leq i \leq n, (a_i, b_i) = 1$. Since R is also an LCM-domain, we can find c as the least common multiple of all b_i's and d as the greatest common divisor of all a_i's, thus $I^{-1} = (c/d)R$. We hence know there exist m_i's of I such that $m_1(c/d) + \cdots + m_n(c/d) = 1$. Then we know $I = uR$, where $u = m_1 + \cdots + m_n$, because for every $x \in I$, $x = x \cdot m_1(c/d) + \cdots + m_n(c/d) = uxc/d$. □

Proposition 1.5.5. *A commutative ring R is a principal ideal domain if and only if R is both a unique factorization domain and a Bézout domain.*

Proof. The only if part is trivial. For any $a, b \in I$, where I is an ideal in R, we have $(\gcd(a, b)) = (a, b) \subseteq I$. Thus an ideal $I \neq 0$ is generated by an element a with fewest prime factors. We can find it by the following steps. Pick any $0 \neq c \in I$. If $I \neq (c)$, then there exists some $d \in I$ such that $c \nmid d$, so $e = \gcd(c, d) \in I$ and e has fewer prime factors than a. □

Example 1.5.6. *There are several examples for Bézout domains.*

i) Each principal ideal domain is a Bézout domain.

ii) Each valuation ring is a Bézout domain since the ideals are totally ordered. Thus every non-Noetherian valuation ring is an example of a non-noetherian Bézout domain ,for example, the valuation ring of $\mathbb{C}_p$.

iii) The ring of algebraic integers $\bar{\mathbb{Z}} \subseteq \bar{\mathbb{Q}}$ is a Bézout domain (see [34, 2.4]).

An important subclass of Bézout domains is that of elementary divisor domains, which play a central role in the structure theorem for finitely presented modules.

Definition 1.5.7. *A commutative ring R is said to be an elementary divisor ring(EDR) if every rectangular $m \times n$ matrix A over R admits diagonal reduction, i.e. there are invertible square matrices P and Q of orders m and n respectively such that $PAQ = D$ where D is a diagonal matrix with entries d_i satisfying the divisibility relations $d_i \mid d_{i+1}$ for all $1 \leq i \leq \min\{m, n\}$. We say A is equivalent to D.*

To investigate the relationship between elementary divisor rings (EDRs) and Bézout domains, we consider the following proposition, which provides a matrix-theoretic characterization of Bézout domains.

Proposition 1.5.8. *R is a Bézout domain if and only if every diagonal matrix over R admits diagonal reduction.*

Proof. See ([41, III. Prop. 6.1]). □

Corollary 1.5.9. *Elementary divisor domains are Bézout domains.*

The following proposition characterizes those Bézout domains that are elementary divisor rings (EDRs).

Proposition 1.5.10. *For a Bézout domain R the following properties are equivalent.*

i) R is an elementary divisor domain.

ii) Every 2×2 matrix admits diagonal reduction.

iii) If $a, b, c \in R$ satisfy $aR + bR + cR = R$, then there exist $p, q \in R$ such that

$$paR + (pb + qc)R = R.$$

Proof. See ([48, Thm 5.1, Thm 5.2]). □

The Proposition 1.5.10(ii) is particularly useful, as it reduces the problem of proving that a Bézout domain is an elementary divisor domain to the case of 2×2 matrices. We now provide a more direct description of the relationship between elementary divisor domains and Bézout domains. To do so, we first introduce the following definition.

Definition 1.5.11. *We say a ring of finite character (of countable character) if every non-zero element of the ring is contained in a finite (countable) number of maximal ideals.*

For instance, Dedekind domains and semilocal rings are both examples of rings with finite character. In contrast, the ring of all algebraic integers, denoted $\bar{\mathbb{Z}}$ is not a ring of countable character, as every non-unit is contained in uncountably many maximal ideals. We now introduce a more direct criterion — beyond the matrix-theoretic characterization in Proposition 1.5.10(ii) — under which a Bézout domain is also an elementary divisor domain.

Proposition 1.5.12. *Bézout domains of countable character are elementary divisor domains.*

Proof. By Proposition 1.5.8 and 1.5.10(ii), we only need to prove that every 2×2 matrix can be reduced to a diagonal matrix. The remainder of the proof can be found in [41, III. Thm. 6.5]. □

Corollary 1.5.13. *For a semilocal integral domain R the following are equivalent:*

i) R is a Prüfer domain;

ii) R is a Bézout domain;

iii) R is an elementary divisor domain.

Proof. The equivalence between (i) and (ii) is given by Proposition 1.5.3. The equivalence between (ii) and (iii) is given by Corollary 1.5.9 and Proposition 1.5.12. □

1.6 The structure theorem of finitely presented modules

In this section, we prove a fundamental structure theorem for finitely presented R-modules over an elementary divisor domain. This theorem also characterizes the class of domains over which finitely presented modules decompose into direct sums of cyclic modules (See [48], [55]).

Theorem 1.6.1. *A domain R satisfies the property that every finitely presented R-module is a direct sum of cyclic R-modules if and only if it is an elementary divisor domain. Moreover, every finitely presented R-module M can be decomposed in a unique way as*

$$M \cong R/d_1R \oplus \cdots \oplus R/d_nR, \quad d_i \mid d_{i+1} \ (1 \leq i \leq n-1). \tag{1.1}$$

To prove the theorem, we first recall the following proposition concerning finitely presented modules over Bézout domains.

Proposition 1.6.2. *Let R be a Bézout domain and let M be a finitely presented R-module which is a direct sum of cyclic modules. Then*

$$M \cong R/d_1R \oplus \cdots \oplus R/d_nR, \quad d_i \mid d_{i+1} \ (1 \leq i \leq n-1). \tag{1.2}$$

Here the annihilator ideals d_iR are uniquely determined by M.

Proof. Since every finitely generated ideal of R is principal, every cyclic summand of M is cyclically presented. Thus M has a free presentation

$$R^n \to R^n \to M \to 0,$$

where the first arrow is a diagonal matrix. By Proposition 1.5.8, the matrix admits a diagonal reduction. The uniqueness of the form 1.2 is given by Proposition 1.6.4. □

Proposition 1.6.3. *A domain R has the property that every finitely presented R-module is a summand of a direct sum of cyclic modules if and only if R is a Prüfer domain.*

Proof. It is obvious by Theorem 1.1.2 and Proposition 1.4.6. □

The sufficiency of Theorem 1.6.1 can be proved now. Since every elementary divisor domain is both a Prüfer domain and a Bézout domain, Propositions 1.6.3 and 1.6.2 ensure the existence of the normal form (1.1). The uniqueness of this form is guaranteed by the following proposition.

Proposition 1.6.4. *Let R be a commutative ring, and let an R-module M satisfy*

$$M \cong \bigoplus_{i=1}^{m} R/I_i \cong \bigoplus_{j=1}^{n} R/J_j,$$

i.e. M has two direct decompositions by cyclic summands. If $I_1 \geq \cdots \geq I_m$ and $J_1 \geq \cdots \geq J_n$, then $m = n$ and $I_i = J_i$ for all $1 \leq i \leq m$. Moreover, the number of the non-zero summands of M cannot exceed the minimal cardinality of systems of generators of the module M.

Proof. See [41, V. Prop. 2.10]. □

The necessity of Theorem 1.6.1 is not directly relevant to our work and can be found in [41, V. Thm. 3.4].

1.7 Presentations of modules

In this section, we study the notion of n-presentations of modules. Let R be a commutative ring. Recall that an R-module M is said to be finitely presented if there exists an exact sequence

$$F_1 \to F_0 \to M \to 0, \tag{1.3}$$

where F_0 and F_1 are finitely generated free R-modules. For such modules, we now state the following useful lemma.

Lemma 1.7.1. *Let M be a finitely presented R-module. If there exists an exact sequence*

$$0 \to K \to N \to M \to 0,$$

where N is a finitely generated R-module, then K is finitely generated.

Proof. Consider the commutative diagram

$$\begin{array}{ccccccccc} & & F_1 & \longrightarrow & F_0 & \longrightarrow & M & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle id_M} & & \\ 0 & \longrightarrow & K & \longrightarrow & N & \longrightarrow & M & \longrightarrow & 0 \end{array}$$

where α, β are given by the projectivity properties of F_0 and F_1, respectively. By snake lemma $\text{Coker}(\beta) \cong \text{Coker}(\alpha)$, and so we have an exact sequence

$$0 \to \text{Im}(\beta) \to K \to \text{Coker}(\alpha) \to 0.$$

Since $\text{Im}(\beta)$ and $\text{Coker}(\alpha)$ are both finitely generated, thus K is finitely generated too. □

If we refer to the exact sequence 1.3 as a finite 1-presentation of M, then, by analogy, we can define an n-presentation of M as follows.

Definition 1.7.2. *An n-presentation of M is an exact sequence*

$$F_n \to F_{n-1} \to \cdots \to F_0 \to M \to 0$$

with F_i free R-modules. In addition, if F_i is finitely generated, this presentation is called a finite n-presentation of M. Sometimes, such an R-module M with finite n-presentations is called n-presented in the later chapters.

It is obvious that a finitely generated R-module M has a 0-presentation. We now introduce a numerical invariant $\lambda(M)$ to study n-presentation, defined as follows.

Definition 1.7.3. *If M is a finitely generated R-module, then we define*

$$\lambda(M) = \sup\{n \mid \textit{there is a finite } n\textit{-presentation of } M\}.$$

If M is not finitely generated, we put $\lambda(M) = -1$.

It is clear that M is finitely generated if and only if $\lambda(M) \geq 0$ and M is finitely presented if and only if $\lambda(M) \geq 1$. The following proposition describes the relationship between modules that are connected by an exact sequence.

Proposition 1.7.4. *Let $0 \to P \to N \to M \to 0$ be an exact sequence of R-modules, then we have*

1) $\lambda(N) \geq \inf\{\lambda(P), \lambda(M)\}$.

2) $\lambda(M) \geq \inf\{\lambda(N), \lambda(P) + 1\}$.

3) $\lambda(P) \geq \inf\{\lambda(N), \lambda(M) - 1\}$.

4) If $N = M \oplus P$ then $\lambda(N) = \inf\{\lambda(M), \lambda(P)\}$. In particular, N is finitely presented if and only if M and P are both finitely presented.

To prove 1) of Proposition 1.7.4, we need the following lemma.

Lemma 1.7.5. *Let $N' \xrightarrow{u} N \xrightarrow{v} N'' \to 0$ be an exact sequence of R-modules and $P' \xrightarrow{\alpha'} N' \to 0$ and $P'' \xrightarrow{\alpha''} N'' \to 0$ be two surjective maps. If P'' is a projective R-module then there exists a surjective map $\alpha : P' \oplus P'' \to N \to 0$ such that the following diagram commutes:*

$$
\begin{array}{ccccccc}
P' & \xrightarrow{i} & P' \oplus P'' & \xrightarrow{p} & P'' & & \\
\downarrow{\scriptstyle \alpha'} & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \alpha''} & & \\
N' & \xrightarrow{u} & N & \xrightarrow{v} & N'' & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \\
0 & & 0 & & 0 & &
\end{array}
$$

where i and p are the corresponding inclusion and projection maps.

Proof. See [44, Thm 1.1.4]. □

Proof of Proposition 1.7.4.

1) Utilizing Lemma 1.7.5 to combine an $\lambda(P)$-presentation and an $\lambda(M)$-presentation together, we can construct an $\inf\{\lambda(P), \lambda(M)\}$-presentation of N.

2) Let $n \leq \inf\{\lambda(N), \lambda(P) + 1\}$. We want to show for each n, $\lambda(M) \geq n$. Using induction, if $n \leq 0$, the statement is obvious. For $n \geq 1$, by a $\lambda(M)$-presentation of M and an $n-1$-presentation of P, we can obtain an $n - 1 = \inf\{\lambda(M), n - 1\}$-presentation of N. If $\lambda(M) < n$, then we have $\lambda(N) \geq n > \lambda(M) = n - 1$. Thus the kernel at $n - 1$ stage of the composite presentation of N which is constructed by a $\lambda(P)$-presentation of P and a $\lambda(M)$-presentation of M is a finitely generated module onto which a finitely generated free module can be mapped. This can help us increase the $\lambda(M)$-presentation. So we obtain a contradiction.

3) Similar to the proof of 2).

4) If $N = M \oplus P$, we have $0 \to P \to N \to M \to 0$ and $0 \to M \to N \to P \to 0$. Use 1),2),3) to get the result.

□

A ring R is said to be n-coherent if every R-module that admits a finite n-presentation also admits a finite $(n+1)$-presentation. Rings with this property will be the primary focus of our study, particularly in Part II of this thesis.

Chapter 2

The structure theorem

As noted in the introduction, many foundational contributions to Iwasawa theory over function fields have been developed using the extrinsic notion of the pro-characteristic ideal. The main obstruction to obtaining an intrinsic definition of characteristic ideals — one that avoids reliance on field extensions and inverse limits — is the lack of a well-behaved structure theorem.

In classical Iwasawa theory, the setting typically involves a Noetherian Iwasawa algebra, such as $\Lambda = \mathbb{Z}_p[[\mathbb{Z}_p]]$. For a finitely generated torsion Λ-module M, one has a pseudo-isomorphism of the form:

$$M \sim \bigoplus_{i=1}^{s} \Lambda/p^{m_i} \oplus \bigoplus_{i=1}^{t} \Lambda/F_j^{n_j},$$

where p is a rational prime, the F_j are distinguished polynomials of Λ, and "$\sim$" denoting a pseudo-isomorphism. This structure theorem expresses M, up to pseudo-isomorphism, as a direct sum of elementary modules over Λ, and the integers r, m_i, n_j, and the prime ideals (F_j) are uniquely determined by M. A challenging problem arises: can this structure theorem be extended to broader settings beyond Noetherian Iwasawa algebras?

The answer is, perhaps unexpectedly, affirmative—and the implications may even surpass initial expectations.

In this chapter, we establish a structure theorem 2.2.1 for a special class of finitely presented torsion modules—referred to as admissible modules—over an arbitrary unital commutative ring A. However, the generality of the ring introduces two notable limitations. First, in this setting, the roles of p and F_j in the classical Iwasawa-theoretic decomposition are replaced by general principal ideals, making it impossible, in general, to give an explicit description of these ideals. Second, the module M is not necessarily pseudo-isomorphic to a direct sum of elementary modules; rather, it appears as a direct summand of a module that is pseudo-isomorphic to such a sum. Nevertheless, under the mild additional assumption that the total quotient ring $Q(A)$ is semisimple, we obtain the improved version (Theorem 2.2.3), in which the principal ideals are replaced by powers of height-one prime ideals. The proofs of both structure theorems rely critically on the algebraic foundations developed in Chapter 1.

Furthermore, to apply Warfield's Structure Theorem (Theorem 1.1.2) for height-one prime ideals, we introduce the notion of an admissible module over a commutative ring R in Definition 2.1.1. To meet the assumptions of Theorem 2.2.3, we define the concept of an admissible ring in Definition 2.3.1 and observe that it encompasses many rings commonly encountered in arithmetic contexts. Finally, we investigate the relationship between admissibility for a $\mathbb{Z}_p$-algebra R that is an integrally closed domain of characteristic zero, and admissibility for the group ring $R[G]$, where G is a finite abelian group.

This chapter is a joint work with David Burns and Alexandre Daoud.

2.1 Admissible modules

In this section we fix a commutative unital ring A and write $Q(A)$ for its total quotient ring. We also write $\mathrm{ht}(\mathfrak{p})$ for the height of each $\mathfrak{p}$ in $\mathrm{Spec}(A)$ and consider the sets

$$\mathcal{P} = \mathcal{P}_A := \{\mathfrak{p} \in \mathrm{Spec}(A) : \mathrm{ht}(\mathfrak{p}) = 1\} \quad \text{and}$$
$$\mathcal{P}^{\mathrm{fg}} = \mathcal{P}_A^{\mathrm{fg}} := \{\mathfrak{p} \in \mathcal{P} : \mathfrak{p} \text{ is finitely generated}\}.$$

Given an A-module M, we write $M_\mathfrak{p}$ for its localisation at $\mathfrak{p}$ in $\mathrm{Spec}(A)$. We also write $M_{\mathrm{tor}} = M_{A\text{-}\mathrm{tor}}$ for the A-submodule of M comprising all elements m that are annihilated by a non-zero divisor of A (that may depend on m) and refer to M as a "torsion A-module" if $M = M_{\mathrm{tor}}$ (or, equivalently, $Q(A) \otimes_A M = (0)$). We then define a (possibly empty) subset of $\mathcal{P}$ by setting

$$\mathcal{P}(M) = \mathcal{P}_A(M) := \mathcal{P} \cap \mathrm{Support}(M_{\mathrm{tor}}) = \{\mathfrak{p} \in \mathcal{P} : (M_{\mathrm{tor}})_\mathfrak{p} \neq (0)\}.$$

Finally, we write M_{tf} for the quotient of M by M_{tor}.

The following notion will play a key role in the sequel.

Definition 2.1.1. *A finitely generated A-module M will be said to be admissible if it has both of the following properties:*

(P_1) for every $\mathfrak{p} \in$ Spec(A) that is maximal amongst those contained in $\bigcup_{\mathfrak{q} \in \mathcal{P}(M)} \mathfrak{q}$, the localisation $A_\mathfrak{p}$ is a valuation ring (that is, its ideals are totally ordered by inclusion).

(P_2) $\mathcal{P}(M)$ is a finite subset of $\mathcal{P}^{fg}$.

Remark 2.1.2. *We consider several examples below to concretize the definition of the admissible module. Later these examples will be used repeatedly.*

(i) If $\mathcal{P}(M)$ is finite (as required by (P_2) and automatically satisfied if A is Noetherian), then the prime avoidance lemma implies (P_1) is valid if and only if $A_\mathfrak{q}$ is a valuation ring for every $\mathfrak{q}$ in $\mathcal{P}(M)$. In particular, if $A_\mathfrak{p}$ is a valuation ring for all $\mathfrak{p}$ in $\mathcal{P}$ (as is the case if A is either a Krull domain or valuation

domain of arbitrary dimension), then M is admissible if and only if M_{tor} is supported on only finitely many primes in $\mathcal{P}$, and each of which is finitely generated.

(ii) Prime ideals that are contained in a union of primes in $\mathcal{P}$ need not have height one. For example, if A is a Noetherian domain of dimension two, then Krull's Principal Ideal Theorem states that for every principal proper ideal I of A, each minimal prime ideal containing I has height at most one. This implies that every prime ideal of A is contained in $\bigcup_{\mathfrak{p}\in\mathcal{P}}\mathfrak{p}$, since for any prime ideal P in A and any non-zero element $x \in P$ there is a principal proper ideal (x) contained in a prime ideal p with height one. Hence the prime ideal in A with height two must be contained in $\bigcup_{\mathfrak{p}\in\mathcal{P}}\mathfrak{p}$.

As usual, a torsion A-module will be said to be *pseudo-null* if its localization vanishes at every prime in $\mathcal{P}$, and a map of A-modules will be said to be a *pseudo-isomorphism* if its kernel and cokernel are both pseudo-null.

2.2 Structure theorems

We are now in a position to prove two structural results that may be regarded as the starting point of our theory. These results apply to a broad class of modules: the first holds over arbitrary commutative rings, while the second requires a mild additional assumption on the base ring A, namely that its total quotient ring $Q(A)$ is semisimple.

The proof of Theorem 2.2.1 rely on the preceding algebraic decomposition result, Proposition 1.1.2, which can be applied using property (P_1) introduced in Definition 2.1.1. Notably, the condition (P_1) provides a favorable setting for localization.

The proof of the first structural theorem proceeds with minimal reliance on auxiliary lemmas, whereas the second theorem — an improved and more refined version — builds upon various algebraic results established in the previous chapter, like the refined structure theorem 1.6.1 of finitely presented modules, leading to a substantially more intricate argument.

Theorem 2.2.1. *Let M be a finitely-presented A-module with property (P_1). If M is torsion, then there exists an A-module N, a finite family of principal ideals $\{L_\tau\}_{\tau\in\mathcal{T}}$ of A and a pseudo-isomorphism of A-modules*

$$M \oplus N \to \bigoplus\nolimits_{\tau\in\mathcal{T}} A/L_\tau. \tag{2.1}$$

Proof of Thm 2.2.1. To prove the theorem we assume that M is A-torsion. We also note that if $\mathcal{P}(M) = \emptyset$, then M is pseudo-null and there is nothing to prove. We therefore assume that $\mathcal{P}(M) \neq \emptyset$, set $S := A \setminus \bigcup_{\mathfrak{p}\in\mathcal{P}(M)} \mathfrak{p}$ and write $(-)'$ for the localisation functor $S^{-1}(-)$.

The maximal ideals of A' are in one-to-one correspondence with the primes of A that are maximal amongst those contained in $\bigcup_{\mathfrak{p}\in\mathcal{P}(M)} \mathfrak{p}$. Hence, from condition (P_1), it follows that the localisation of A' at each maximal ideal is a valuation ring. We may therefore apply the Warfield's structure theorem 1.1.2 to deduce the existence of an A'-module N' and a finite collection $\{a'_\tau\}_{\tau\in\mathcal{T}}$ of elements of $A' \setminus (A')^\times$ for which there is an isomorphism of A'-modules

$$\psi : M' \oplus N' \cong \bigoplus\nolimits_{\tau\in\mathcal{T}} A'/(a'_\tau). \tag{2.2}$$

We now choose elements $\{a_\tau\}_{\tau\in\mathcal{T}}$ of $A \setminus S = \bigcup_{\mathfrak{p}\in\mathcal{P}(M)} \mathfrak{p}$ with $(a_\tau)' = (a'_\tau)$ for each $\tau \in \mathcal{T}$. Then, since both M and $\bigoplus_{\tau\in\mathcal{T}} A/(a_\tau)$ are finitely-presented A-modules (the former by assumption and the latter clearly), the canonical maps

$$\begin{aligned} \mathrm{Hom}_A\big(M, \bigoplus\nolimits_{\tau\in\mathcal{T}} A/(a_\tau)\big)' &\xrightarrow{\sim} \mathrm{Hom}_{A'}\big(M', \bigoplus\nolimits_{\tau\in\mathcal{T}} A'/(a'_\tau)\big), \\ \mathrm{Hom}_A\big(\bigoplus\nolimits_{\tau\in\mathcal{T}} A/(a_\tau), M\big)' &\xrightarrow{\sim} \mathrm{Hom}_{A'}\big(\bigoplus\nolimits_{\tau\in\mathcal{T}} A'/(a'_\tau), M'\big), \\ \mathrm{End}_A(M)' &\xrightarrow{\sim} \mathrm{End}_{A'}(M') \end{aligned} \tag{2.3}$$

are all bijective. This implies the existence of homomorphisms of A-modules

$$\iota_1 : M \to \bigoplus\nolimits_{\tau\in\mathcal{T}} A/(a_\tau) \quad \text{and} \quad \iota_2 : \bigoplus\nolimits_{\tau\in\mathcal{T}} A/(a_\tau) \to M$$

such that, for suitable elements s_1 and s_2 of S, the maps ι'_1/s_1 and ι'_2/s_2 are respectively equal to the composites

$$M' \xrightarrow{(\mathrm{id},0)} M'\oplus N' \xrightarrow{\psi} \bigoplus\nolimits_{\tau\in\mathcal{T}} A'/(a'_\tau) \quad \text{and} \quad \bigoplus\nolimits_{\tau\in\mathcal{T}} A'/(a'_\tau) \xrightarrow{\psi^{-1}} M'\oplus N' \xrightarrow{(\mathrm{id},0)} M'.$$

Set $N := \ker(\iota_2)$. Then, since the endomorphism $\iota'_2/s_2 \circ \iota'_1/s_1$ of M' is the identity map, which corresponds to the identity map in $\mathrm{End}_A(M)'$, the map $\iota_2 \circ \iota_1$ is given by multiplication by $s_2 s_1$ and the latter element is not contained in any prime in $\mathcal{P}(M)$. Hence the modules $\ker(\iota_1)$, $\mathrm{coker}(\iota_2)$ and $\iota_1(M) \cap N$ are all pseudo-null. In addition, by localising the exact commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \longrightarrow & \iota_1(M) + N & \xrightarrow{\iota_2} & (\iota_2\circ\iota_1)(M) & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle i_1} & & \downarrow{\scriptstyle i_2} & & \\ 0 & \longrightarrow & N & \longrightarrow & \bigoplus_{\tau\in\mathcal{T}} A/(a_\tau) & \xrightarrow{\iota_2} & \mathrm{im}(\iota_2) & \longrightarrow & 0 \end{array} \tag{2.4}$$

one checks that the inclusion

$$i_1 : \iota_1(M) + N \to \bigoplus\nolimits_{\tau\in\mathcal{T}} A/(a_\tau)$$

is also a pseudo-isomorphism. Actually, by diagram 2.4 and snake lemma, we have the short exact sequence

$$0 \to \operatorname{coker}(i_1) \to \operatorname{coker}(i_2) \to 0.$$

Since $\operatorname{coker}(\iota_2)$ is pseudo-null, we know $\operatorname{im}(\iota_2)_{\mathfrak{p}} = M_{\mathfrak{p}}$ for all $\mathfrak{p} \in \mathcal{P}$. Notice that we have the trivial short exact sequence

$$0 \longrightarrow (\iota_2 \circ \iota_1)(M) \xrightarrow{i_2} \operatorname{im}(\iota_2) \longrightarrow coker(i_2) \longrightarrow 0.$$

Since $(\iota_2 \circ \iota_1)(M)_{\mathfrak{p}} = M_{\mathfrak{p}}$ for all $\mathfrak{p} \in \mathcal{P}$, it follows that $\operatorname{coker}(\iota_2)_{\mathfrak{p}} = 0$ for all $\mathfrak{p} \in \mathcal{P}$, and hence the same holds for $\operatorname{coker}(\iota_1)$. Given these facts, the tautological short exact sequence

$$0 \to \iota_1(M) \cap N \xrightarrow{x \mapsto (x,x)} \iota_1(M) \oplus N \xrightarrow{(x,y) \mapsto x-y} \iota_1(M) + N \to 0$$

implies that the composite map

$$M \oplus N \xrightarrow{(\iota_1, \mathrm{id})} \iota_1(M) \oplus N \xrightarrow{(x,y) \mapsto x-y} \iota_1(M) + N \hookrightarrow \bigoplus_{\tau \in \mathcal{T}} A/(a_\tau) \tag{2.5}$$

is a pseudo-isomorphism. This proves (i) with $L_\tau = (a_\tau)$ for each $\tau \in \mathcal{T}$. □

The structural theorem 2.2.1 expresses a finitely presented torsion admissible A-module, up to pseudo-isomorphism, as a direct sum of quotient modules by principal ideals. Although the theorem holds for every commutative ring A, its main limitation lies in its dependence on the intermediate module N, which arises during the proof. In fact, since N is defined as the kernel of a specific morphism, its structure is generally difficult to describe explicitly.

Before stating the next theorem, we isolate the purely ring-theoretic input that will be used in its proof. This result concerns only a suitable localisation of A and its decomposition as a finite direct product of Prüfer domains.

Proposition 2.2.2. *Let A be a commutative ring and let $S \subset A$ be a multi-*

plicative set. Set $A' := S^{-1}A$. Assume that:

(i) the total quotient ring $Q(A)$ of A is semisimple; and

(ii) for every maximal ideal $\mathfrak{m}$ of A' the local ring $A'_{\mathfrak{m}}$ is a valuation ring.

Then A' has weak global dimension at most 1 and the total quotient ring $Q(A')$ has global dimension 0. In particular, there exists a finite index set T and Prüfer domains A'_t ($t \in T$) such that

$$A' \cong \prod_{t\in T} A'_t.$$

Proof. Since $Q(A)$ is semisimple, it has global dimension 0 by Corollary 1.2.2 (vi). Localising at S shows that $Q(A') \cong S^{-1}Q(A)$ is again semisimple. This is because $Q(A)$ is isomorphic to finite product of fields by Proposition 1.2.4. Hence $\operatorname{gl.dim}(Q(A')) = 0$ by Corollary 1.2.2 (vi). By assumption (ii), each localisation $A'_{\mathfrak{m}}$ at a maximal ideal $\mathfrak{m}$ of A' is a valuation ring. Hence Proposition 1.3.9 implies that $\text{w.gl.dim}(A') \leq 1$. We may now apply Proposition 1.4.7 with $R = A'$ to deduce that A' is a finite direct product of Prüfer domains, as claimed. □

The next theorem shows that, under the additional hypothesis that $Q(A)$ is semisimple, the auxiliary module N in Theorem 2.2.1 can in fact be dispensed with.

Theorem 2.2.3. *Let M be a finitely-presented A-module with property (P_1). If $Q(A)$ is semisimple, then the following claims are valid.*

(a) There exists a pseudo-isomorphism of A-modules $M \to M_{\mathrm{tor}} \oplus M_{\mathrm{tf}}$.

(b) Assume M is both admissible and torsion. Then for improving the pseudo-isomorphism (2.1) one can take the module N to be (0). Further, there exists a finite index set $\mathcal{S}$ and for each $\sigma \in \mathcal{S}$ a prime ideal $\mathfrak{p}_\sigma$ in $\mathcal{P}$

and a natural number a_σ, for which there exists a pseudo-isomorphism of A-modules $M \to \bigoplus_{\sigma\in\mathcal{S}} A/\mathfrak{p}_\sigma^{a_\sigma}$.

Proof of Thm 2.2.3. In the remainder of the argument we no longer require, except when explicitly stated, that M is a torsion module, but we do assume that the ring $Q(A)$ is semisimple. We keep the notation S and $A' = S^{-1}A$ introduced in the proof of Theorem 2.2.1. By Remark 2.1.2 and condition (P_1), the localisation $A'_{\mathfrak{m}}$ is a valuation ring for every maximal ideal $\mathfrak{m}$ of A'. Hence Proposition 2.2.2 yields a finite direct product decomposition

$$A' \;\cong\; \prod_{t\in T} A'_t$$

over a finite index set T in which each ring A'_t is a semi-hereditary (or Prüfer) domain.

In particular, if M is an admissible, torsion module, then $\mathcal{P}(M)$ is finite and, for each $t \in T$, the ring A'_t is a semi-local Prüfer domain because A' only has finitely many maximal ideals. Moreover, the A'_t-component of M' is both finitely-presented and torsion due to the structure of modules over direct product of some rings. In this case, therefore, we can apply the Corollary 1.5.13 and the stronger structure theorem 1.6.1 to each ring A'_t in order to deduce the existence of an isomorphism (2.2) for which the module N' is zero. Then, in this case, the module $\mathrm{coker}(\iota_1)' = \mathrm{coker}(\psi)$ vanishes and so $\mathrm{coker}(\iota_1)_{\mathfrak{p}}$, and hence also $N_{\mathfrak{p}}$, vanishes for all $\mathfrak{p}$ in $\mathcal{P}(M)$.

Next we suppose, in addition, that every prime ideal in $\mathcal{P}(M)$ is finitely generated and we claim this implies that every prime ideal of A' is finitely generated. To see this we note every prime ideal of A' is of the form $\mathfrak{B} = \mathfrak{B}_0 \times \prod_{t\in T\setminus\{t_0\}} A'_t$ where $\mathfrak{B}_0$ is a prime ideal of the domain A'_{t_0} for some $t_0 \in T$. If $\mathfrak{B}_0 = (0)$, then $\mathfrak{B}$ is finitely generated. If $\mathfrak{B}_0 \neq (0)$, then $\mathfrak{Q} := (0) \times \prod_{t\in T\setminus\{t_0\}} A'_t$ is a prime ideal of A' that is strictly contained in $\mathfrak{B}$. Now, since $\mathcal{P}(M)$ is assumed to be finite, the prime avoidance lemma implies that $\mathfrak{B}$ and $\mathfrak{Q}$ correspond to prime ideals $\mathfrak{p}$ and $\mathfrak{p}_1$ of A with $\mathfrak{p}_1 \subsetneq \mathfrak{p} \subseteq \mathfrak{q}$ for some $\mathfrak{q} \in \mathcal{P}(M)$. In particular, since $\mathfrak{q}$ has height one, this implies $\mathfrak{p} = \mathfrak{q}$ and hence that $\mathfrak{B}$ is finitely generated, as claimed.

At this stage, we can apply Cohen's Theorem [25, Th. 2] to deduce that A', and hence each of its components A'_t, is Noetherian. It follows that the localisation $A'_{\mathfrak{B}}$ of A' at each prime ideal $\mathfrak{B}$ is Noetherian, a domain (as each component A'_t of A' is a domain) and either a field (if $\mathfrak{B}$ corresponds to the zero ideal of some component A'_t) or a valuation ring (by Remark 2.1.2 and the assumption M is admissible). We further recall that every Noetherian valuation ring that is not a field is a discrete valuation ring (cf. [56, Th. 5.18]). Taken together, these facts imply that every component ring A'_t of A' is a Dedekind domain. We can therefore now appeal to the usual structure theorem for finitely generated torsion modules over such rings to deduce that the isomorphism (2.2) can be replaced by an isomorphism of the form $M' \cong \bigoplus_{\sigma\in\mathcal{S}} A'/(\mathfrak{p}_\sigma^{a_\sigma})'$ in which $\mathcal{S}$ is a finite index set, each $\mathfrak{p}_\sigma$ a prime ideal in $\mathcal{P}(M)$ and each a_σ a natural number. There are then also associated isomorphisms (2.3) in which $\mathcal{T}$ is replaced by $\mathcal{S}$ and each of the terms (a_τ) and (a'_τ) by $\mathfrak{p}_\tau^{a_\tau}$ and $(\mathfrak{p}_\tau^{a_\tau})'$ respectively, and so one can deduce the existence of corresponding analogues of the homomorphisms ι_1 and ι_2. In addition, in this case the module $N := \ker(\iota_2)$ is pseudo-null (since $N' = (0)$ and we already observed that $N_{\mathfrak{p}}$ vanishes for all $\mathfrak{p}$ in $\mathcal{P}(M)$) and so can be taken to be zero in the pseudo-isomorphism that arises from the analogue of the construction (2.5) in this case. This proves (ii)(b).

Finally, to prove (ii)(a), we do not assume either that M is torsion or that $M_{\rm tor}$ is admissible. We do however continue to assume that $Q(A)$ is semisimple and hence, by the above argument, that A' is a finite direct product of semi-hereditary domains. Thus, by the general result of [37, §5, Cor.], we know that $M'_{\rm tf}$ is a projective A'-module and hence that there exists an isomorphism of A'-modules of the form $M' \cong M'_{\rm tf} \oplus M'_{\rm tor}$.

Now, since M is a finitely-presented A-module, the natural map

$$\mathrm{Hom}_A(M, M_{\mathrm{tor}})' \to \mathrm{Hom}_{A'}(M', M'_{\mathrm{tor}})$$

is bijective. In particular, there exists a homomorphism $\phi : M \to M_{\mathrm{tor}}$ and an element $s_1 \in S$ with the property that ϕ'/s_1 corresponds under this identification to the projector of M' onto M'_{tor}. As such, ϕ'/s_1 restricts to the submodule M'_{tor} to give the identity. We can therefore find an element s_2 of S such that the map $\tau := s_2 \cdot \phi$ restricted to M_{tor} is equal to $s_1 s_2 \cdot \mathrm{id}_{M_{\mathrm{tor}}}$.

We now write π for the canonical projection $M \to M_{\mathrm{tf}}$ and consider the map

$$\kappa : M \to M_{\mathrm{tf}} \oplus M_{\mathrm{tor}}; \quad m \mapsto (\pi(m), \tau(m)).$$

One then checks that $\ker(\kappa) = \ker(\tau) \cap M_{\mathrm{tor}}$ and that $\mathrm{coker}(\kappa)$ is equal to the cokernel of the endomorphism of M_{tor} induced by τ and, since $s_1 s_2 \in S$, these modules are both pseudo-null. It follows that the above map κ is the required pseudo-isomorphism. □

2.3 Admissible rings

In view of Theorem 2.2.3, the following class of rings will be of interest to us in the sequel.

Definition 2.3.1. *A commutative unital ring A will be said to be admissible if it has both of the following properties:*

(P_3) $Q(A)$ is semisimple.

(P_4) Every finitely-presented torsion A-module is admissible (as in Definition 2.1.1).

It is clear that a Noetherian integrally closed domain (or equivalently, a

Noetherian Krull domain) is admissible in the above sense and also such that every finitely generated module is finitely-presented. For such rings, Theorem 2.2.1 simply recovers the classical structure theorem of Bourbaki [13, Chap. VII, § 4, Th. 4 and Th. 5]. However, Theorem 2.2.1 can also be applied in more general situations and, to end this section, we shall now discuss some examples that are relevant to later arguments.

Remark 2.3.2.

(i) Let A be an arbitrary Krull domain. Then $Q(A)$ is a field (and so semisimple), $\mathcal{P}_A$ is non-empty, the localisation of A at each prime in $\mathcal{P}_A$ is a discrete valuation ring and every non-zero ideal is contained in only finitely many primes in $\mathcal{P}_A$. Hence, if M is a non-zero finitely generated torsion A-module, then $\mathcal{P}_A(M)$ is finite (as it is the subset of $\mathcal{P}_A$ comprising primes containing the annihilator of M) and so M has property (P_1) (by Remark 2.1.2(i)) and also admits a pseudo-isomorphism (2.1) with $N = (0)$. In particular, A is admissible if $\mathcal{P}_A = \mathcal{P}_A^{fg}$. However, there are Krull domains A for which $\mathcal{P}_A \neq \mathcal{P}_A^{fg}$ (see, for instance, the examples discussed by Eakins and Heinzer in [35]) and no such ring is admissible. Indeed, in any such case, if $\mathfrak{p} \in \mathcal{P}_A$ is not finitely generated and $x \in \mathfrak{p} \setminus \{0\}$, then $M := A/(xA)$ is a finitely presented torsion A-module with $\mathfrak{p} \in \mathcal{P}_A(M)$.

(ii) If A is a unique factorisation domain, then A is a Krull domain for which every prime in $\mathcal{P}_A$ is principal and so the above discussion implies A is admissible. In fact, for such a ring, the only essential difference between the argument of Theorem 2.2.1 and that of Bourbaki referred to above is that we require the module M to be finitely-presented, rather than merely finitely generated, in order to guarantee the existence of the isomorphism (2.3).

In this subsection we assume to be given a $\mathbb{Z}_p$-algebra R that is an integrally closed domain of characteristic zero. For a fixed finite abelian group G, we compare the notions of admissibility introduced above relative to R and to the group ring $A := R[G]$ of G over R.

To do this, we write f for the ring inclusion $R \to A$, $f^* : \mathrm{Spec}(A) \to \mathrm{Spec}(R)$ for the induced morphism of spectra and $f^*(M)$ for each A-module M for the R-module obtained by restriction through f. We note that A is a free R-module of finite rank (as G is finite) so that f is a finite, flat ring morphism. In addition, since $|G|$ is invertible in the field of fractions $Q(R)$ of R, the algebra $Q(A)$ is equal to $Q(R)[G]$ and is therefore a finite product $\prod_{i\in I} K_i$ of finite degree field extensions K_i of $Q(R)$ (and so is semisimple).

We write $D(n)$ for the set of positive divisors of a natural number n. We also fix a primitive n-th root of unity ζ_n in $\mathbb{Q}_p^c$, set $L_n := \mathbb{Q}_p(\zeta_n)$ and write $\mathcal{O}_n$ for its valuation ring $\mathbb{Z}_p[\zeta_n]$. We then set $R_n := R \otimes_{\mathbb{Z}_p} \mathcal{O}_n$ and write ι_n for the ring inclusion $R \to R_n$.

Proposition 2.3.3. *Fix $R, G, A = R[G]$ and f as above, and write H for the maximal subgroup of G of order prime to p. Then the following claims are valid.*

(i) For $\mathfrak{q} \in Spec(R)$, the fibre $(f^*)^{-1}(\mathfrak{q}) := \{\mathfrak{p} \in Spec(A) : f^*(\mathfrak{p}) = \mathfrak{q}\}$ is finite and non-empty. For $\mathfrak{p} \in Spec(A)$, one has $ht(\mathfrak{p}) = ht(f^*(\mathfrak{p}))$ and so $\mathfrak{p} \in \mathcal{P}_A \iff f^*(\mathfrak{p}) \in \mathcal{P}_R$.

(ii) Fix $\mathfrak{q} \in \mathcal{P}_R$ and write $D_\mathfrak{q}(|G|)$ for $D(|G|)$ if $p \notin \mathfrak{q}$ and for $D(|H|)$ if $p \in \mathfrak{q}$.

(a) $(f^*)^{-1}(\mathfrak{q}) \subseteq \mathcal{P}_A^{fg} \iff (\iota_n^*)^{-1}(\mathfrak{q}) \subseteq \mathcal{P}_{R_n}^{fg}$ for every $n \in D_\mathfrak{q}(|G|)$.

(b) Assume $R_\mathfrak{q}$ is a valuation ring. Then $A_\mathfrak{p}$ is a valuation ring for all $\mathfrak{p} \in (f^*)^{-1}(\mathfrak{q})$ if and only if both $|G| \notin \mathfrak{q}$ and $f^*(A)_\mathfrak{q}$ is a maximal $R_\mathfrak{q}$-order in $Q(A)$.

(iii) For every finitely generated A-module M the following equivalences are valid:

(a) M is finitely-presented (over A) $\iff$ $f^*(M)$ is finitely-presented (over R);

(b) $f^*(M_{tor})$ is the R-torsion submodule of $f^*(M)$. In particular, M is a torsion A-module $\iff$ $f^*(M)$ is a torsion R-module;

(c) $\mathcal{P}_A(M) \subseteq (f^*)^{-1}(\mathcal{P}_R(f^*(M)))$ and so $\mathcal{P}_A(M)$ is finite if $\mathcal{P}_R(f^*(M))$ is finite;

(d) M is a pseudo-null A-module if $f^*(M)$ is a pseudo-null R-module.

Proof. Since f is both finite and flat it has the lying over, incomparability and going down properties and, in addition, its fibres are finite (cf. [59, Chap. 3, Th. 9.3, Th. 9.5 and Exer. 9.3]). The first assertion of (i) is thus clear. For the second assertion, it is enough to show $\mathrm{ht}(\mathfrak{p}) = \mathrm{ht}(f^*(\mathfrak{p}))$ for $\mathfrak{p} \in \mathrm{Spec}(A)$. For this, we claim first that $\mathrm{ht}(\mathfrak{p}) \geq \mathrm{ht}(f^*(\mathfrak{p}))$: indeed, this follows easily from the fact that if $\{\mathfrak{b}', \mathfrak{b}\} \subset \mathrm{Spec}(R)$ and $\mathfrak{a} \in \mathrm{Spec}(A)$ are such that $\mathfrak{b}' \subsetneq \mathfrak{b}$ and $f^*(\mathfrak{a}) = \mathfrak{b}$, then (by going down) there exists $\mathfrak{a}' \in \mathrm{Spec}(A)$ with $\mathfrak{a}' \subsetneq \mathfrak{a}$ and $f^*(\mathfrak{a}') = \mathfrak{b}'$. On the other hand, one has $\mathrm{ht}(\mathfrak{p}) \leq \mathrm{ht}(f^*(\mathfrak{p}))$ since for every inclusion $\mathfrak{a}' \subsetneq \mathfrak{a}$ with $\mathfrak{a}'$ and $\mathfrak{a}$ in $\mathrm{Spec}(A)$, incomparability implies that the inclusion $f^*(\mathfrak{a}') \subset f^*(\mathfrak{a})$ is also strict. This proves (i).

We next make a general observation. For this, we fix a natural number m, a quotient Q of G, an ideal J of $\mathcal{O}_m[Q]$, set $R_m[Q]/J := R_m \otimes_{\mathcal{O}_m} (\mathcal{O}_m[Q]/J)$ and use the canonical ring homomorphisms $f_{m,J} : R_m \to R_m \otimes_{\mathcal{O}_m} (\mathcal{O}_m[Q]/J)$ and $f_m^J : R_m[Q] \to R_m[Q]/J$. We assume $J \cap \mathcal{O}_m = (0)$ (in $\mathcal{O}_m[Q]$) and $\mathcal{O}_m[Q]/J$ is $\mathcal{O}_m$-free and hence that $f_{m,J} \circ \iota_m$ is an injective finite flat ring morphism $R \to R_m[Q]/J$. Via this morphism, we regard $R_m[Q]/J$ as an extension of R and note the argument of (i) implies that any prime ideal of $R_m[Q]/J$ lying over $\mathfrak{q}$ has height one. In addition, since $\ker(f_m^J) = R_m \otimes_{\mathcal{O}_m} J$ is finitely generated (as $\mathcal{O}_m[Q]/J$ is $\mathcal{O}_m$-free and $\mathcal{O}_m[Q]$ is Noetherian), for each $\mathfrak{p} \in \mathcal{P}_{R_m[Q]/J}$ one has

$$\big(\mathfrak{p}\cap R = \mathfrak{q} \iff (f_m^J)^{-1}(\mathfrak{p})\cap R = \mathfrak{q}\big) \text{ and } \big(\mathfrak{p} \in \mathcal{P}^{\rm fg}_{R_m[Q]/J} \iff (f_m^J)^{-1}(\mathfrak{p}) \in \mathcal{P}^{\rm fg}_{R_m[Q]}\big). \tag{2.6}$$

Turning now to the proof of (ii), we first note that, for each $n \in D(|G|)$, the morphism ι_n is finite and flat and so the argument of (i) implies $(\iota_n^*)^{-1}(\mathfrak{q}) \subseteq \mathcal{P}_{R_n}$. We next fix a homomorphism $\psi : G \to \mathbb{Q}_p^{c,\times}$ of exact order n. Then the kernel J_ψ of the induced $\mathbb{Z}_p$-linear ring homomorphism $\psi_* : \mathbb{Z}_p[G] \to \mathbb{Q}_p^c$ is such that $J_\psi \cap \mathbb{Z}_p = (0)$ and $\mathbb{Z}_p[G]/J_\psi \cong \mathrm{im}(\psi_*)$ is $\mathbb{Z}_p$-free (so that the criteria (2.6) are valid with $m = 1$, $Q = G$ and $J = J_\psi$). In particular, since the algebra $R[G]/J_\psi$ identifies with $R\otimes_{\mathbb{Z}_p}\mathrm{im}(\psi_*) = R_n$, this shows that the stated condition on the sets $(\iota_n^*)^{-1}(\mathfrak{q})$ in (ii)(a) are necessary.

To prove its sufficiency, we will show it implies, for every $m \in D(|G|)$ and every quotient Q of G, that each prime ideal of $R_m[Q]$ lying over $\mathfrak{q}$ is finitely generated. To prove this, we argue by induction on $|Q|$, with the case $|Q| = 1$ being obvious. To deal with the induction step, we fix $m \in D(|G|)$, a prime divisor ℓ of $|Q|$, a non-trivial element σ of Q that has ℓ-power order $t = \ell^d$ and is such that Q decomposes as a direct product $\langle\sigma\rangle \times Q'$ and a prime ideal $\mathfrak{p}$ of $R_m[Q]$ that lies over $\mathfrak{q}$. Now, if $\sigma^{t/\ell} - 1 \in \mathfrak{p}$, then $\mathfrak{p}$ is the full-preimage under the canonical projection $R_m[Q] \to R_m[Q/\langle\sigma^{t/\ell}\rangle]$ of a prime ideal and so, by induction (and an application of (2.6) with J the kernel of $\mathcal{O}_m[Q] \to \mathcal{O}_m[Q/\langle\sigma^{t/\ell}\rangle]$), is finitely generated. On the other hand, if $\sigma^{t/\ell}-1 \notin \mathfrak{p}$ and we set $T_\sigma := \sum_{j=0}^{\ell-1}(\sigma^{t/\ell})^j$, then the equality $(\sigma^{t/\ell}-1)T_\sigma = 0$ implies $T_\sigma \in \mathfrak{p}$. To deal with this case, we fix an injective homomorphism $\psi : \langle\sigma\rangle \to \mathcal{O}_t^\times$ and consider the induced (surjective) $\mathcal{O}_m$-linear ring homomorphism

$$\psi_{m,*} : \mathcal{O}_m[Q] = \mathbb{Z}_p[\langle\sigma\rangle]\otimes_{\mathbb{Z}_p}\mathcal{O}_m[Q'] \to \mathcal{O}_t\otimes_{\mathbb{Z}_p}\mathcal{O}_m[Q'] = (\mathcal{O}_t\otimes_{\mathbb{Z}_p}\mathcal{O}_m)[Q'] \cong \prod\nolimits_C \mathcal{O}_a[Q']$$

where $a = a(m,t) \in D(|G|)$ is the least common multiple of m and t and, with b denoting the greatest common divisor of m and t, we write C for a fixed set of coset representatives for $\mathrm{Gal}(L_a/L_b)$ in $\mathrm{Gal}(L_a/\mathbb{Q}_p)$, Then $\ker(\psi_{m,*}) = \mathcal{O}_m[Q]\cdot T_\sigma$ and so the containment $T_\sigma \in \mathfrak{p}$ implies $\mathfrak{p}$ is the full preimage under the projection $R_m \otimes_{\mathcal{O}_m} \psi_{m,*} : R_m[Q] \to \prod_C R_a[Q']$ of a prime ideal. Hence, by the induction hypothesis (and an application of (2.6) with $J = \ker(\psi_{m,*})$), it follows again that $\mathfrak{p}$ is finitely generated.

To complete the proof of (ii)(a) we now only need to show that if $G = H \times P$ with P a non-trivial p-group, then for any $\mathfrak{q} \in \mathcal{P}_R$ that contains p, one has $(f^*)^{-1}(\mathfrak{q}) \subseteq \mathcal{P}_A^{\mathrm{fg}}$ if $(\iota_n^*)^{-1}(\mathfrak{q}) \subseteq \mathcal{P}_{R_n}^{\mathrm{fg}}$ for all $n \in D(|H|)$. Now f factors as the composite $f_P \circ f_H$ of the finite, flat ring morphisms $f_H : R \to R[H]$ and $f_P : R[H] \to (R[H])[P] = A$ and by what we have just proved, the given condition implies that $(f_H^*)^{-1}(\mathfrak{q}) \subseteq \mathcal{P}_{R[H]}^{\mathrm{fg}}$. It is thus enough to note that if $\mathfrak{q}' \in (f_H^*)^{-1}(\mathfrak{q})$, then $p \in \mathfrak{q}'$ and so the only prime ideal in $(f_P^*)^{-1}(\mathfrak{q}')$ is $\mathfrak{q}' + I(P)\cdot R[G]$ which is finitely generated (over R) since $\mathfrak{q}'$ is.

Turning to (ii)(b) we assume $R_\mathfrak{q}$ is a valuation ring and note that, as R is a $\mathbb{Z}_p$-algebra, one has $|G| \in \mathfrak{q}$ if and only if both $p \in \mathfrak{q}$ and $p \mid |G|$. In particular, if this last condition is satisfied, then $(f^*)^{-1}(\mathfrak{q})$ contains the ideal $\mathfrak{p} = \mathfrak{q}' + I(P)\cdot R[G]$ discussed above. One then checks $A_\mathfrak{p}$ is equal to $(R[H])_{\mathfrak{q}'}[P]$ which is not an integral domain (as P is non-trivial) and so cannot be a valuation ring. To prove (ii)(b) it is thus enough to assume $|G| \notin \mathfrak{q}$ and show $A_\mathfrak{p}$ is a valuation ring for all $\mathfrak{p} \in \Sigma := (f^*)^{-1}(\mathfrak{q})$ if and only if $f^*(A)_\mathfrak{q}$ is a maximal $R_\mathfrak{q}$-order in $Q(A)$. In this case, there exist subrings $\mathcal{O}_i$ of K_i that are integral over $R_\mathfrak{q}$ and have K_i as their fraction field and are such that

$$f^*(A)_\mathfrak{q} = R_\mathfrak{q}[G] = \prod\nolimits_{i\in I} \mathcal{O}_i. \tag{2.7}$$

It follows that $f^*(A)_\mathfrak{q}$ is a maximal $R_\mathfrak{q}$-order if and only if each $\mathcal{O}_i$ is the integral closure $\mathcal{O}_i'$ of $R_\mathfrak{q}$ in K_i. In addition, writing $\Sigma(i)$ for the (finite) set of non-zero prime, and hence maximal, ideals of $\mathcal{O}_i$, the set $(f^*)^{-1}(\mathfrak{q})$ corresponds bijectively to $\bigcup_{i\in I}\Sigma(i)$ in the following way: for each $\mathfrak{p} \in \Sigma$, there exists a unique $i_\mathfrak{p} \in I$ and a unique $\mathfrak{P}_\mathfrak{p} \in \Sigma(i_\mathfrak{p})$ such that $A_\mathfrak{p} = \mathcal{O}_{i_\mathfrak{p},\mathfrak{P}_\mathfrak{p}}$ (and

$\mathfrak{P}_\mathfrak{p} \cap R = \mathfrak{q}$). In addition, by Chevalley's Extension Theorem, each ring $\mathcal{O}'_i$ is the intersection of the finitely many valuation subrings of K_i that extend $R_\mathfrak{q}$ and the localisation of $\mathcal{O}'_i$ at any of its maximal ideals is equal to one of these valuation rings (cf. [38, Lem. 3.2.6]).

We now assume $A_\mathfrak{p}$ is a valuation ring for every $\mathfrak{p} \in \Sigma$. In this case $\mathcal{O}_{i_\mathfrak{p},\mathfrak{P}}$ is a valuation ring that extends $R_\mathfrak{q}$ for every $\mathfrak{P} \in \Sigma(i_\mathfrak{p})$ and hence, since $\mathcal{O}_{i_\mathfrak{p}} = \bigcap_{\mathfrak{P}\in\Sigma(i_\mathfrak{p})}(\mathcal{O}_{i_\mathfrak{p}})_\mathfrak{P}$ (as $\mathcal{O}_{i_\mathfrak{p}}$ is an integral domain), one must have $\mathcal{O}'_{i_\mathfrak{p}} \subseteq \mathcal{O}_{i_\mathfrak{p}}$ and therefore also $\mathcal{O}_{i_\mathfrak{p}} = \mathcal{O}'_{i_\mathfrak{p}}$. Thus, in this case, (2.7) implies that $f^*(A)_\mathfrak{q}$ is integrally closed in $Q(A)$ and so is a maximal $R_\mathfrak{q}$-order.

Conversely, if $f^*(A)_\mathfrak{q}$ is a maximal $R_\mathfrak{q}$-order, then (2.7) implies that $\mathcal{O}_i = \mathcal{O}'_i$ for all $i \in I$. In particular, since the localisation of each $\mathcal{O}'_i$ at any of its maximal ideals is a valuation ring that extends $R_\mathfrak{q}$, it follows that the localisation $\mathcal{O}'_{i_\mathfrak{p},\mathfrak{P}_\mathfrak{p}}$ of A at each $\mathfrak{p} \in \Sigma$ is a valuation subring of some field K_i, as required to complete the proof of (ii).

The proof of (iii) relies crucially on the fact A is a free R-module of finite rank. In (iii)(a), the forward implication is clear and the reverse implication a consequence of Schanuel's Lemma. To prove (iii)(b) it is enough to prove the first assertion and then, since every non-zero element of R is a non-zero divisor of A, it is enough to show that any element m of M that is annihilated by a non-zero divisor a of A is also annihilated by a non-zero element of R. To prove this we write $f_a(X)$ for the monic polynomial of minimal degree in $R[X]$ with $f_a(a) = 0$ and note that the constant term of $f_a(X)$ is non-zero (since a is a non-zero divisor and $f_a(X)$ is chosen to be of minimal degree) and annihilates m. To prove (iii)(c), we note (iii)(b) implies $f^*(M_{\rm tor})$ is the R-torsion submodule of $f^*(M)$. We then fix $\mathfrak{p} \in \mathcal{P}_A(M)$ and an element m of $M_{\rm tor}$ with non-zero image in $M_{{\rm tor},\mathfrak{p}}$. Then $\mathfrak{p}$ contains the annihilator $\mathcal{A}(m)$ of m in A and so $f^*(\mathfrak{p})$ contains the annihilator $R \cap \mathcal{A}(m)$ of m in R. The image of m in $f^*(M_{\rm tor})_{f^*(\mathfrak{p})}$ is therefore non-zero so that $f^*(\mathfrak{p}) \in \mathcal{P}_R(f^*(M))$ and hence $\mathfrak{p} \in (f^*)^{-1}(\mathcal{P}_R(f^*(M))$, as required. Finally, (iii)(d) is true since (iii)(c) implies that $\mathcal{P}_A(M) = \emptyset$ if $\mathcal{P}_R(f^*(M)) = \emptyset$. □

We now consider, for each natural number n, the following subset of Spec(R)

$$\mathcal{P}_R^n := \{\mathfrak{q} \in \mathcal{P}_R : n \notin \mathfrak{q} \text{ and } (\iota_m^*)^{-1}(\mathfrak{q}) \subseteq \mathcal{P}_{R_m}^{\mathrm{fg}} \text{ for all } m \in D(n)\}.$$

Example 2.3.4. *By taking $m = 1$ $(\in D(n))$ in the above definition, it is clear $\mathcal{P}_R^n \subseteq \mathcal{P}_R^{fg}$. Under certain hypotheses on R, such as the following, it is possible to be much more precise.*

(i) If R is Noetherian, then clearly $\mathcal{P}_R^n = \{\mathfrak{q} \in \mathcal{P}_R : p \notin \mathfrak{q}\}$ if $p \mid n$ and $\mathcal{P}_R^n = \mathcal{P}_R$ if $p \nmid n$.

(ii) If R_m is a unique factorisation domain for each $m \in D(n)$, then every prime in $\mathcal{P}_{R_m}$ is principal and so again one has $\mathcal{P}_R^n = \{\mathfrak{q} \in \mathcal{P}_R : p \notin \mathfrak{q}\}$ if $p \mid n$ and $\mathcal{P}_R^n = \mathcal{P}_R$ if $p \nmid n$.

(iii) If $\mathcal{O}_n \subseteq R$, then, for each $m \in D(n)$, the $\mathbb{Z}_p$-algebra R_m is a finite direct product of copies of R and so one has $\mathcal{P}_R^n = \{\mathfrak{q} \in \mathcal{P}_R^{fg} : p \notin \mathfrak{q}\}$ if $p \mid n$ and $\mathcal{P}_R^n = \mathcal{P}_R^{fg}$ if $p \nmid n$. In particular, in all cases one has $\mathcal{P}_R^n = \mathcal{P}_R^{fg}$ for $n \in D(p-1)$.

(iv) Fix $\mathfrak{q} \in \mathcal{P}_R^{fg}$ with $p \notin \mathfrak{q}$ and set $\kappa := R/\mathfrak{q}$. Fix a field E containing $Q(\kappa)$ and $\mathbb{Q}_p^c$ and, for $m \in D(n)$, set $F_m = Q(\kappa) \cap L_m \subseteq E$, write $\mathcal{O}'_m$ for the valuation ring of F_m and assume $\mathcal{O}'_n \subseteq \kappa$ (as occurs, for example, if either $F_n = \mathbb{Q}_p$ or κ is integrally closed in $Q(\kappa)$). Then $\mathcal{O}_m$ is a free $\mathcal{O}'_m$-module of rank $[L_m : F_m]$ so that $\kappa_m := \kappa \otimes_{\mathcal{O}'_m} \mathcal{O}_m$ is isomorphic to a subring of the field $Q(\kappa) \otimes_{F_m} L_m$ and hence (0) is its unique prime ideal lying over the zero ideal (0_κ) of κ. In particular, since the algebra $\kappa \otimes_{\mathbb{Z}_p} \mathcal{O}_m$ is a finite direct product of copies of κ_m, each prime ideal that lies over (0_κ) is principal and so each prime ideal of R_m that lies over $\mathfrak{q}$ is finitely generated. It follows that $\mathfrak{q} \in \mathcal{P}_R^n$.

From Proposition 2.3.3 we now obtain the following useful criterion.

Proposition 2.3.5. *Let M be an A-module for which the R-module $f^*(M)$ is finitely-presented, admissible and torsion. Then M is a finitely-presented, admissible torsion A-module if both $\mathcal{P}_R(f^*(M)) \subseteq \mathcal{P}_R^{|G|}$ and, in addition, $R_{\mathfrak{q}}$ is Noetherian for every $\mathfrak{q} \in \mathcal{P}_R(f^*(M))$.*

Proof. Under the stated assumptions, Proposition 2.3.3(iii) implies that the A-module M is finitely-presented and torsion and that $\mathcal{P}_A(M)$ is finite since $\mathcal{P}_R(f^*(M))$ is finite. Then, since $\mathcal{P}_A(M) \subseteq (f^*)^{-1}(\mathcal{P}_R(f^*(M)))$, Proposition 2.3.3(ii)(a) implies $\mathcal{P}_A(M) \subseteq \mathcal{P}_A^{\mathrm{fg}}$ if $\mathcal{P}_R(f^*(M)) \subseteq \mathcal{P}_R^{|G|}$. Finally we note that if $\mathfrak{q} \in \mathcal{P}_R(f^*(M))$ is such that $R_{\mathfrak{q}}$ is Noetherian, then it is a Noetherian valuation ring that is not a field (as $\mathrm{ht}(\mathfrak{q}) = 1$) and hence a discrete valuation ring. In this case, therefore, the $R_{\mathfrak{q}}$-order $R_{\mathfrak{q}}[G]$ is maximal if and only if $|G| \notin \mathfrak{q}$ (cf. [29, Props. (27.1)]). The admissibility of M as an A-module now follows directly from Proposition 2.3.3(ii)(b) (and the first assertion of Remark 2.1.2(i)). □

Remark 2.3.6. *Fix a natural number n, let R be the completed p-adic group ring $\mathbb{Z}_p[[\mathbb{Z}_p^n]]$ and assume p divides $|G|$. Then $A = R[G]$ is Noetherian, $Q(A)$ is semisimple and Proposition 2.3.5 combines with Example 2.3.4(i) to imply that a finitely generated torsion A-module M is admissible if $pR \notin \mathcal{P}_R(f^*(M))$. By the classical structure theory of Iwasawa modules (cf. [62, Prop. (5.1.7)(ii)]), this condition is satisfied if and only if the submodule $M[p^\infty]$ of M of elements of finite (p-power) order is pseudo-null. Hence, in this case, Theorem 2.2.3(b) provides the following 'equivariant' refinement of the structure theorem for Iwasawa modules: if M is a finitely generated torsion A-module for which $M[p^\infty]$ is pseudo-null, then $\mathcal{P}_A(M)$ is finite and M is pseudo-isomorphic, as an A-module, to a finite direct sum of modules of the form $A/\mathfrak{p}^{e(\mathfrak{p})}$, with $\mathfrak{p} \in \mathcal{P}_A(M)$ and $e(\mathfrak{p}) \in \mathbb{N}$.*

Chapter 3

Characteristic ideals

In this chapter, we define the generalised characteristic ideals in Definition 3.1.1 drawing upon the algebraic results established in Chapter 2. However, the two structural forms presented in Theorem 2.2.1 and Theorem 2.2.3 are distinct: the former employs principal ideals, while the latter utilizes prime ideals. This distinction gives rise to two different types of characteristic ideals. In Proposition 3.1.2, we examine the relationship between them, which lays the groundwork for the formulation of an Iwasawa Main Conjecture in Theorem 4.3.2(iii). Moreover, we point out that for rings arising in our arithmetic setting and the modules defined over them, the characteristic ideal defined via prime ideals is contained within that defined via principal ideals, and their quotient is pseudo-null. In particular, if a module is quadratically presented over the ring, then the characteristic ideal defined by principal ideals coincides with the zeroth Fitting ideal.

In the second part of this chapter, we investigate the structure of modules over a ring expressed as the inverse limit of a system of rings. We first treat the general case and then deduce the compact case (Proposition 3.2.2): if a ring is the inverse limit of compact Hausdorff rings and a module over it is $I_\bullet$-complete (see the beginning of 3.2), then the two characteristic ideals also arise as inverse limits. This perspective aids in understanding the modules encountered in our arithmetic contexts in Chapter 4.2.

This chapter is a joint work with David Burns and Alexandre Daoud.

3.1 Generalised characteristic ideals

In this section we assume $Q(A)$ is semisimple. Then, for any finitely-presented, admissible, torsion A-module M, the set $\mathcal{P}_A(M)$ is finite and, by Theorem 2.2.3(b), for each $\mathfrak{p}$ in $\mathcal{P}_A(M)$ there exists a finite set $\{e(\mathfrak{p})_i\}_{1\leq i\leq n(\mathfrak{p})}$ of natural numbers $e(\mathfrak{p})_i$ for which there exists a pseudo-isomorphism of A-modules

$$M \to \bigoplus\nolimits_{\mathfrak{p}\in\mathcal{P}_A(M)} \bigoplus\nolimits_{1\leq i\leq n(\mathfrak{p})} A/\mathfrak{p}^{e(\mathfrak{p})_i}. \tag{3.1}$$

In addition, Theorem 2.2.1 implies the existence of a finite family of principal ideals $\{ L_\tau \}_{\tau\in\mathcal{T}}$ of A together with a pseudo-isomorphism of A-modules

$$M \to \bigoplus\nolimits_{\tau\in\mathcal{T}} A/L_\tau. \tag{3.2}$$

These pseudo-isomorphisms then naturally suggest the following definitions.

Definition 3.1.1. *Assume $Q(A)$ is semisimple and let M be a finitely-presented, admissible, torsion A-module. Then the lower and upper generalised characteristic ideals of M (with respect to the pseudo-isomorphisms (3.1) and (3.2)) are the ideals of A that are respectively obtained by setting*

$$\mathrm{char}_A(M) := \prod\nolimits_{\mathfrak{p}\in\mathcal{P}_A(M)} \mathfrak{p}^{\sum_{1\leq i\leq n(\mathfrak{p})} e(\mathfrak{p})_i}.$$

and

$$\mathrm{Char}_A(M) := \prod\nolimits_{\tau\in\mathcal{T}} L_\tau.$$

The distinguishing features of these ideals are that $\mathrm{char}_A(M)$ is defined via an explicit product of primes in $\mathcal{P}_A$, whilst $\mathrm{Char}_A(M)$ is defined to be principal. In the next result, we discuss the relation between them (and, in particular, justify the 'lower' and 'upper' terminology) and their dependence on the respective choices of pseudo-isomorphism, and also show that they retain some of the key properties of the characteristic ideals in classical Iwasawa theory (and see also Remark 3.1.3 below).

In the sequel we write $\mathrm{Fit}_A^0(M)$ for the initial Fitting ideal of a finitely-presented A-module M. We also refer to M as 'quadratically-presented' if, for some natural number d, it lies in an exact sequence of A-modules of the form

$$A^d \xrightarrow{\theta} A^d \to M \to 0. \tag{3.3}$$

Proposition 3.1.2. *Assume $Q(A)$ is semisimple.*

(i) If M is a finitely-presented, torsion A-module, then the following claims are valid.

(a) If M is admissible, then $\mathrm{char}_A(M)$ is independent of the choice of pseudo-isomorphism (3.1) and one has $char_A(M)_\mathfrak{p} = \mathrm{Char}_A(M)_\mathfrak{p}$ for all $\mathfrak{p}$ in $\mathcal{P}_A$.

(b) Assume $A = R[G]$, with R a $\mathbb{Z}_p$-algebra that is a Krull domain and G a finite abelian group. Then M is admissible if $\mathcal{P}_R(f^*(M)) \subseteq \mathcal{P}_R^{|G|}$. Assuming this to be the case, the following claims are also valid.

(i) $Char_A(M) = \bigcap_{\mathfrak{q}\in\mathcal{P}_R} f^*(char_A(M))_\mathfrak{q}$. In particular, $\mathrm{Char}_A(M)$ is independent of the choice of pseudo-isomorphism (3.2).

(ii) $char_A(M) \subseteq Char_A(M)$, with equality if and only if $char_A(M)$ is principal. In addition, the quotient $Char_A(M)/char_A(M)$ is pseudo-null.

(iii) If M is quadratically-presented, then $Char_A(M) = Fit_A^0(M)$.

(ii) Let $0 \to M_1 \to M_2 \to M_3 \to 0$ be an exact sequence of finitely generated A-modules. Then the following claims are valid.

(a) If M_2 is a finitely-presented, admissible, torsion A-module, then M_3 is a finitely-presented, admissible, torsion A-module and $\mathrm{char}_A(M_2) \subseteq \mathrm{char}_A(M_3)$.

(b) If M_1 and M_3 are finitely-presented, admissible, torsion A-modules, then M_2 is a finitely-presented, admissible, torsion A-module and

$$\mathrm{char}_A(M_2) = \mathrm{char}_A(M_1) \cdot \mathrm{char}_A(M_3).$$

Proof. To prove (i)(a) we fix $\mathfrak{p} \in \mathcal{P}_A(M)$ and note that, if M is admissible, then the ring $A_{\mathfrak{p}} = A'_{\mathfrak{p}'}$ that occurs in the proof of Theorem 2.2.3(a) is a discrete valuation ring. Writing $l_{\mathfrak{p}}(N)$ for the length of a finitely generated, torsion $A_{\mathfrak{p}}$-module N, one can then compute

$$\begin{aligned} e(\mathfrak{p}) := \sum_{1\le i\le n(\mathfrak{p})} e(\mathfrak{p})_i &= l_{\mathfrak{p}}\big(\bigoplus_{1\le i\le n(\mathfrak{p})} A_{\mathfrak{p}}/(\mathfrak{p}A_{\mathfrak{p}})^{e(\mathfrak{p})_i}\big) \\ &= l_{\mathfrak{p}}\big(\bigoplus_{\mathfrak{a}\in\mathcal{P}_A(M)} \bigoplus_{1\le i\le n(\mathfrak{a})} (A/\mathfrak{a}^{e(\mathfrak{a})_i})_{\mathfrak{p}}\big) = l_{\mathfrak{p}}(M_{\mathfrak{p}}), \end{aligned} \tag{3.4}$$

where the last equality follows from the pseudo-isomorphism (3.1). One therefore has

$$\mathrm{char}_A(M)_{\mathfrak{p}} = \mathfrak{p}^{e(\mathfrak{p})}A_{\mathfrak{p}} = (\mathfrak{p}A_{\mathfrak{p}})^{l_{\mathfrak{p}}(M_{\mathfrak{p}})}$$

which, in particular, implies the first assertion of (i)(a). In the same way, the pseudo-isomorphism (3.2) implies that each $A_{\mathfrak{p}}$-module $A_{\mathfrak{p}}/L_{\tau,\mathfrak{p}}$ is torsion and that

$$l_{\mathfrak{p}}(M_{\mathfrak{p}}) = \sum\nolimits_{\tau\in\mathcal{T}} l_{\mathfrak{p}}(A_{\mathfrak{p}}/L_{\tau,\mathfrak{p}}) = l_{\mathfrak{p}}\big(A_{\mathfrak{p}}/(\prod\nolimits_{\tau\in\mathcal{T}} L_\tau)_{\mathfrak{p}}\big) = l_{\mathfrak{p}}(A_{\mathfrak{p}}/\mathrm{Char}_A(M)_{\mathfrak{p}})$$

and hence $\mathrm{Char}_A(M)_{\mathfrak{p}} = (\mathfrak{p}A_{\mathfrak{p}})^{l_{\mathfrak{p}}(M_{\mathfrak{p}})} = \mathrm{char}_A(M)_{\mathfrak{p}}$. To complete the proof of (i)(a), it is now enough to note that if $\mathfrak{p} \in \mathcal{P}_A \setminus \mathcal{P}_A(M)$, then it is clear

$\mathrm{char}_A(M)_\mathfrak{p} = A_\mathfrak{p}$ and also that the pseudo-isomorphism (3.2) implies $L_{\tau,\mathfrak{p}} = A_\mathfrak{p}$ for all $\tau \in \mathcal{T}$ and hence $\mathrm{Char}_A(M)_\mathfrak{p} = A_\mathfrak{p}$.

To prove (i)(b) we assume R is a Krull domain and $A = R[G]$. Then $\mathcal{P}_R(f^*(M))$ is finite and $f^*(M)$ is admissible if $\mathcal{P}_R(f^*(M)) \subseteq \mathcal{P}_R^{\mathrm{fg}}$ (cf. Remark 2.3.2(i)). By applying the argument of Proposition 2.3.3(ii) in this case, we deduce that M is admissible provided $\mathcal{P}_R(f^*(M)) \subseteq \mathcal{P}_R^{|G|}$ (as we assume henceforth).

Before proceeding, we next show that

$$f^*(\mathrm{char}_A(M))_\mathfrak{q} = f^*(\mathrm{Char}_A(M))_\mathfrak{q} \quad \text{for every } \mathfrak{q} \in \mathcal{P}_R. \tag{3.5}$$

For this, we first assume that $\mathfrak{q} \notin \mathcal{P}_R(f^*(M))$. Then one has $f^*(M)_\mathfrak{q} = (0)$ so that the pseudo-isomorphisms (3.1) and (3.2) imply $f^*(\mathfrak{p}^{e(\mathfrak{p})_i})_\mathfrak{q} = f^*(A)_\mathfrak{q} = f^*(L_\tau)_\mathfrak{q}$ for each $\mathfrak{p} \in \mathcal{P}_A(M)$, integer i with $1 \le i \le n(\mathfrak{p})$ and $\tau \in \mathcal{T}$. This in turn implies $f^*(\mathrm{char}_A(M))_\mathfrak{q} = f^*(A)_\mathfrak{q} = f^*(\mathrm{Char}_A(M))_\mathfrak{q}$. It is thus enough to verify (3.5) for $\mathfrak{q} \in \mathcal{P}_R(f^*(M))$. For such $\mathfrak{q}$ one has $|G| \notin \mathfrak{q}$ and so, in order to deduce (3.5) from the final assertion of (i)(a), it is enough to show that, for any such $\mathfrak{q}$ and any ideal X of A the module $f^*(X)_\mathfrak{q}$ is uniquely determined by $\{X_\mathfrak{p} : \mathfrak{p} \in (f^*)^{-1}(\mathfrak{q})\}$. To see this, we note the argument of Proposition 2.3.3(ii) implies $f^*(A)_\mathfrak{q} = \prod_{i\in I}\mathcal{O}_i'$, with each $\mathcal{O}_i'$ the integral closure in K_i of the discrete valuation ring $R_\mathfrak{q}$. There is also a natural bijection $j : (f^*)^{-1}(\mathfrak{q}) \to \bigcup_{i\in I}\Sigma(i)$, where $\Sigma(i)$ denotes the (finite) set of maximal ideals of $\mathcal{O}_i'$, such that $X_\mathfrak{p} = (f^*(X)_\mathfrak{q})_{j(\mathfrak{p})}$ for $\mathfrak{p} \in (f^*)^{-1}(\mathfrak{q})$. In addition, each ring $\mathcal{O}_i'$ is a principal ideal domain (as a Dedekind domain with only finitely many prime ideals) and equal to $\bigcap_{\mathfrak{B}\in\Sigma(i)}\mathcal{O}'_{i,\mathfrak{B}}$. In particular, $f^*(X)_\mathfrak{q} = \bigoplus_{i\in I} X(i)$, with each $X(i) := \mathcal{O}_i' \otimes_A X$ an ideal of $\mathcal{O}_i'$. In addition, $X(i) = (0)$ if and only if $X(i)_\mathfrak{B} = (0)$ for any $\mathfrak{B} \in \Sigma(i)$ and, if $X(i) \neq (0)$, then it is isomorphic to $\mathcal{O}_i'$ and hence equal to $\bigcap_{\mathfrak{B}\in\Sigma(i)} X(i)_\mathfrak{B}$. The claimed result is therefore true since $X(i)_\mathfrak{B} = X_{j^{-1}(\mathfrak{B})}$ for each $\mathfrak{B} \in \Sigma(i)$.

Next we observe that the claimed equality in (i)(b)(i) combines with the in-dependence result in (i)(a) to directly imply the second claim of (i)(b)(i). To prove the equality of (i)(b)(i) and the first assertion of (i)(b)(ii) it is enough to show that

$$\mathrm{char}_A(M) \subseteq \bigcap\nolimits_{\mathfrak{q}\in\mathcal{P}_R} f^*(\mathrm{char}_A(M))_{\mathfrak{q}} = \bigcap\nolimits_{\mathfrak{q}\in\mathcal{P}_R} f^*(\mathrm{Char}_A(M))_{\mathfrak{q}} = \mathrm{Char}_A(M). \tag{3.6}$$

Here the inclusion is clear (since R is a domain) and the first equality follows from (3.5). Since R is assumed to be a Krull domain, the second equality will follow if $\mathrm{Char}_A(M)$ is free as a (finitely generated) R-module. To prove this it is enough to show that the principal ideal $\mathrm{Char}_A(M)$ of A contains a non-zero divisor (of A). To do this, we note first that each $\mathfrak{p} \in \mathcal{P}_A(M)$ contains a non-zero divisor (as if $m \in M$ has non-zero image in $M_{\mathfrak{p}}$, then $\mathfrak{p}$ contains every non-zero divisor that annihilates m). This implies the existence of a non-zero divisor a in $\mathrm{char}_A(M)$. Then, for $\mathfrak{q} \in \mathcal{P}_R$, one has $a \in f^*(\mathrm{char}_A(M))_{\mathfrak{q}} = f^*(\mathrm{Char}_A(M))_{\mathfrak{q}}$ and so $ra = b$ for some $r \in R \setminus \mathfrak{q}$ and $b \in \mathrm{Char}_A(M)$. The element b is then a non-zero divisor of the sort required to complete the proof of (3.6).

In a similar way, if $\mathrm{char}_A(M)$ is a principal ideal, then it is a free R-module (as it contains a non-zero divisor) and so the first inclusion in (3.6) is an equality. This proves the second assertion of (i)(b)(ii) and the third assertion then follows directly from the final assertion of (i)(a). Lastly, to prove (i)(b)(iii) we note that, for $\mathfrak{p} \in \mathcal{P}_A(M)$, the presentation (3.3) gives rise to an exact sequence of $A_{\mathfrak{p}}$-modules

$$A_{\mathfrak{p}}^d \xrightarrow{\theta_{\mathfrak{p}}} A_{\mathfrak{p}}^d \to M_{\mathfrak{p}} \to 0. \tag{3.7}$$

Hence, since $M_{\mathfrak{p}}$ is a torsion module over the discrete valuation ring $A_{\mathfrak{p}}$, one has

$$A_{\mathfrak{p}} \cdot \det(\theta_{\mathfrak{p}}) = \mathfrak{p}_{\mathfrak{p}}^{l_{\mathfrak{p}}(\mathrm{coker}(\theta_{\mathfrak{p}}))} = \mathfrak{p}_{\mathfrak{p}}^{l_{\mathfrak{p}}(M_{\mathfrak{p}})} = \mathfrak{p}_{\mathfrak{p}}^{e(\mathfrak{p})} = \mathrm{Char}_A(M)_{\mathfrak{p}}. \tag{3.8}$$

Here the first equality is valid since $A_{\mathfrak{p}}$ is an elementary divisor ring, the second follows from (3.7), the third from (3.4) and the last from the definition of $\mathrm{char}_A(M)$ and the final assertion of (i)(a).

Now, since M is torsion, the exact sequence (3.3) implies $\det(\theta)$ is a unit of $Q(A)$ (and hence a non-zero divisor of A). This implies $f^*(A\cdot\det(\theta))$ is a (finitely generated) free R-module and thereby implies the equality in (i)(b)(iii) via the computation

$$\mathrm{Fit}^0_A(M) = A\cdot\det(\theta) = \bigcap_{\mathfrak{q}\in\mathcal{P}_R} f^*(A\cdot\det(\theta))_{\mathfrak{q}} = \bigcap_{\mathfrak{q}\in\mathcal{P}_R} f^*(\mathrm{Char}_A(M))_{\mathfrak{q}} = \mathrm{Char}_A(M).$$

Here the first equality follows directly from the definition of initial Fitting ideal (and the resolution (3.3)), the second from the assumption R is a Krull domain and the last from (3.6). In addition, since $(A\cdot\det(\theta))_{\mathfrak{p}} = A_{\mathfrak{p}}\cdot\det(\theta_{\mathfrak{p}})$ for all $\mathfrak{p}\in\mathcal{P}_A$, the third equality is true since the equalities (3.8) imply that $f^*(A\cdot\det(\theta))_{\mathfrak{q}} = f^*(\mathrm{Char}_A(M))_{\mathfrak{q}}$ for all $\mathfrak{q}\in\mathcal{P}_R$ (in just the same way that the final assertion of (i)(a) implies (3.5)). This completes the proof of (i)(b).

Turning to (ii), we note that the assertions regarding modules being torsion and finitely-presented follow directly from the given exact sequence (and, in the latter case, the Proposition 1.7.4). In addition, for each prime ideal $\mathfrak{p}$ of A, the given sequence induces a short exact sequence of $A_{\mathfrak{p}}$-modules

$$0 \to M_{1,\mathfrak{p}} \to M_{2,\mathfrak{p}} \to M_{3,\mathfrak{p}} \to 0.$$

Assuming M_2 (or equivalently, both M_1 and M_3) to be torsion, these sequences imply an equality $\mathcal{P}(M_2) = \mathcal{P}(M_1)\cup\mathcal{P}(M_3)$ that combines with Remark 2.1.2 to imply both of the assertions regarding admissibility, and also combines with the fact, proved in (i)(a), that for each prime ideal p of A one has

$$\mathrm{char}_A(M)_{\mathfrak{p}} = (\mathfrak{p}A_{\mathfrak{p}})^{l_{\mathfrak{p}}(M_{\mathfrak{p}})}$$

to imply the stated inclusion, respectively equality, of characteristic ideals. □

Remark 3.1.3. *Fix natural numbers m and n and write R for the completed group ring $\mathbb{Z}_p[\zeta_m][[\mathbb{Z}_p^n]]$. Then R is both Noetherian and admissible in the sense of Definition 2.3.1 (for example, by Remark 2.3.2(ii)) and, in addition, every prime in $\mathcal{P}_R$ is principal. In this case, therefore, the argument of Proposition 3.1.2(i)(b) has two concrete consequences. Firstly, if $p \nmid |G|$, then the ring $R[G]$ is admissible (by Example 2.3.4(i)). Secondly, for every finitely generated (and hence finitely presented by Noetherianity), torsion R-module M, the ideals $\mathrm{char}_R(M)$ and $\mathrm{Char}_R(M)$ are equal and are easily seen to coincide with the classical characteristic ideal of M as an R-module.*

3.2 Inverse limit rings

In this section we assume to be given an inverse system of rings

$$(A_n,\ \phi_n : A_n \to A_{n-1})_{n\in\mathbb{N}}$$

in which every homomorphism ϕ_n is surjective. We study the associated inverse limit ring

$$A := \varprojlim_n A_n.$$

For every n we write $\phi_{\langle n\rangle} : A \to A_n$ for the induced (surjective) projection map, so that $\phi_n \circ \phi_{\langle n\rangle} = \phi_{\langle n-1\rangle}$ for all n, and we use the decreasing separated filtration

$$I_\bullet := (I_n)_{n\in\mathbb{N}}$$

of A that is obtained by setting $I_n := \ker(\phi_{\langle n\rangle})$ for every n. For an A-module M and non-negative integer n, we then define an A_n-module by setting

$$M_{(n)} := M/(I_n \cdot M) \cong (A/I_n) \otimes_A M \cong A_n \otimes_A M.$$

We also use similar notation for morphisms, so that $\theta_{(n)} : M_{(n)} \to N_{(n)}$ denotes the morphism $\mathrm{id}_{A_n} \otimes_A \theta$ induced by a given morphism of A-modules $\theta : M \to N$.

We say M is '$I_\bullet$-complete' if the natural map

$$\mu_M : M \to \varprojlim_n M_{(n)}$$

is bijective, where the inverse limit is taken with respect to the maps $\phi_{M,n} : M_{(n)} \to M_{(n-1)}$ induced by ϕ_n.

3.2.1 The general case

The following result records some useful general facts about the notion of $I_\bullet$-completeness. In this result we refer to the linear topology on A induced by the subgroups $\{I_n\}_n$ as the '$I_\bullet$-topology'.

Lemma 3.2.1. *The following claims are valid for every A-module M.*

(i) If M is finitely generated, then μ_M is surjective but need not be injective.

(ii) M is $I_\bullet$-complete if it is a finitely generated submodule of an $I_\bullet$-complete module. In particular, every finitely generated ideal of A is $I_\bullet$-complete.

(iii) Assume M is $I_\bullet$-complete and that there exists a natural number t for which both the I_t-adic topology on A is finer than the $I_\bullet$-topology and the A_t-module $M_{(t)}$ is finitely generated. Then M is generated as an A-module by any finite subset that projects to give a set of generators of $M_{(t)}$.

Proof. To prove (i) we fix a natural number d for which there exists an exact sequence of A-modules of the form

$$0 \to K \xrightarrow{\subseteq} A^d \xrightarrow{\varphi} M \to 0. \tag{3.9}$$

For each n, we set $K_n' := \ker(\varphi_{(n)})$ and use the exact commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & K'_n & \xrightarrow{\subseteq} & A^d_{(n)} & \xrightarrow{\varphi_{(n)}} & M_{(n)} & \longrightarrow & 0 \\
& & \downarrow{\scriptstyle \alpha_n} & & \downarrow{\scriptstyle (\phi_n)^d} & & \downarrow{\scriptstyle \phi_{M,n}} & & \\
0 & \longrightarrow & K'_{n-1} & \xrightarrow{\subseteq} & A^d_{(n-1)} & \xrightarrow{\varphi_{(n-1)}} & M_{(n-1)} & \longrightarrow & 0.
\end{array}$$

Write $I_{[n]}$ for the image of I_{n-1} in A_n. Then $\ker((\phi_n)^d) = I^d_{[n]}$ and $\ker(\phi_{M,n}) = I_{[n]} \cdot M_{(n)}$. Thus, since each map $(\phi_n)^d$ is surjective, the Snake Lemma applies to the above diagram to imply that each map α_n is also surjective. By passing to the limit over n of these diagrams we thus obtain the bottom row of the exact commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & K & \longrightarrow & A^d & \xrightarrow{\varphi} & M & \longrightarrow & 0 \\
& & \downarrow & & \downarrow{\scriptstyle (\mu_A)^d} & & \downarrow{\scriptstyle \mu_M} & & \\
0 & \longrightarrow & \varprojlim_n K'_n & \longrightarrow & (\varprojlim_n A_{(n)})^d & \longrightarrow & \varprojlim_n M_{(n)} & \longrightarrow & 0.
\end{array} \tag{3.10}$$

In addition, for each n the (surjective) map $\phi_{\langle n\rangle}$ induces an isomorphism $A_{(n)} \cong A_n$ so that the map $(\mu_A)^d$ is bijective (and hence A^d is $I_\bullet$-complete). From the above diagram, one can therefore deduce that μ_M is surjective.

To give an example in which μ_M is not injective we take A_n to be the power series ring $\mathbb{Z}_p[[X_1, \ldots, X_n]]$ over $\mathbb{Z}_p$ in n commuting indeterminates X_i and ϕ_n to be the projection map $A_n \to A_{n-1}$ induced by sending X_n to 0. In this case A identifies with one version (see [23]) of the power series ring over $\mathbb{Z}_p$ in a countable number of commuting indeterminates $\{X_i\}_{i\in\mathbb{N}}$. We then define K to be the (proper) ideal of A that is generated by the set $\{pX_1\} \cup \{X_n - pX_{n+1}\}_{n\in\mathbb{N}}$ and take M to be the quotient A/K. In this case, one computes that, for each n, the module $M_{(n)} \cong A_n/\phi_{\langle n\rangle}(K) \cong \mathbb{Z}_p$ and hence that μ_M is not injective.

To prove the first assertion of (ii) we fix an injective map $\theta : M \to N$ in which N is $I_\bullet$-complete. It is then enough to note that μ_M is injective as a consequence of the diagram

$$\begin{array}{ccc} M & \xrightarrow{\quad\theta\quad} & N \\ \downarrow{\scriptstyle \mu_M} & & \downarrow{\scriptstyle \mu_N} \\ \varprojlim_n M_{(n)} & \xrightarrow{(\theta_{(n)})_n} & \varprojlim_n N_{(n)} \end{array}$$

and the fact that μ_N is injective. The second assertion of (ii) is then an immediate consequence of the fact A is $I_\bullet$-complete (as shown above).

To prove (iii) we mimic the argument of [59, Th. 8.4]. To do this we fix a finite set of elements $\{m_\sigma\}_{\sigma\in\Sigma}$ of M with $M = (\sum_{\sigma\in\Sigma} Am_\sigma) + I_t \cdot M$. Then $M = (\sum_{\sigma\in\Sigma} Am_\sigma) + I_t^n \cdot M$ for every n and so, since for each $n \in \mathbb{N}$ there exists (by assumption) $n_1 \in \mathbb{N}$ with $(I_t)^{n_1} \subseteq I_n$, one therefore also has

$$M = (\sum\nolimits_{\sigma\in\Sigma} Am_\sigma) + I_n \cdot M \quad \text{for every } n. \tag{3.11}$$

We now fix $m \in M$ and set $m_0 := m$ and $I_0 := A$. Then, for each $n \in \mathbb{N}$, we inductively choose $\{a_{\sigma,n}\}_{\sigma\in\Sigma} \subseteq I_{n-1}$ and $m_n \in I_{n-1}I_n \cdot M \subset I_n \cdot M$ with $m_{n-1} = (\sum_{\sigma\in\Sigma} a_{\sigma.n}m_\sigma) + m_n$. That such elements can be chosen for $n = 1$ is a direct consequence of (3.11) with $n = 1$. Then, if one assumes their existence for $n = n_0$, their existence for $n_0 + 1$ is a consequence of the equality obtained after multiplying (3.11) with $n = n_0+1$ by I_{n_0}. Now, since A is $I_\bullet$-complete, for each $\sigma \in \Sigma$, there exists a unique element $a_\sigma \in A$ such that $a_\sigma - \sum_{i=1}^{i=n} a_{\sigma,i} \in I_n$ for all n. Then one checks that

$$m - (\sum\nolimits_{\sigma\in\Sigma} a_\sigma m_i) \in \bigcap\nolimits_{n\in\mathbb{N}} (I_n \cdot M) = (0)$$

where the last equality is valid since M is $I_\bullet$-complete. This shows that M is generated over A by $\{m_\sigma\}_{\sigma\in\Sigma}$, as required. □

3.2.2 The compact case

In the sequel we say that the inverse limit A is 'compact' if each ring A_n is endowed with a compact Hausdorff topology with respect to which the transition maps ϕ_n are continuous. In this case we endow A with the corresponding inverse limit topology, so that A is compact and, for every n, the ideal I_n is closed and the projection map $\phi_{\langle n\rangle}$ is continuous.

In particular, since A is compact, the inverse limit functor is exact on the category of finitely generated A-modules and this fact allows us to prove a finer version of Lemma 3.2.1.

Before stating the result, we note that if an A-module N is pseudo-null, then the associated A_n-module $N_{(n)}$ need not even be torsion. Such issues mean that, in general, one cannot hope to compute the characteristic ideal of a finitely-presented torsion A-module M directly in terms of the associated A_n-modules $M_{(n)}$.

Despite this difficulty, claim (iii) of the following result shows that such a reduction is possible for a natural family of compact rings A, at least after possibly replacing M by a pseudo-isomorphic module. (In Proposition 4.2.4 below we will also prove a more concrete version of this result for certain power series rings.)

Proposition 3.2.2. *Assume that A is compact. Then the following claims are valid for any finitely-presented A-module M.*

(i) M is $I_\bullet$-complete.

(ii) If M is an admissible, torsion module, then

$$\mathrm{char}_A(M) = \varprojlim_n \phi_{\langle n\rangle}(\mathrm{char}_A(M)) \quad \textit{and} \quad \mathrm{Char}_A(M) = \varprojlim_n \phi_{\langle n\rangle}(\mathrm{Char}_A(M)),$$

where the limits are taken with respect to the maps ϕ_n.

(iii) Assume A and A_n for each n are $\mathbb{Z}_p$-algebras and unique factorisation domains. Let M be a finitely-presented, torsion A-module. Then M is pseudo-isomorphic to an A-module $\widetilde{M}$ with the following properties: $\widetilde{M}$ is finitely-presented, torsion and $I_\bullet$-complete; there exists $n_0 \in \mathbb{N}$ such

that, for all $n \geq n_0$, the A_n-module $\widetilde{M}_{(n)}$ is finitely-presented and torsion; one has

$$\mathrm{Char}_A(M) = \mathrm{char}_A(M) = \varprojlim_{n \geq n_0} char_{A_n}(\widetilde{M}_{(n)}),$$

where the limit is taken with respect to the maps ϕ_n.

Proof. To prove (i) we fix an exact sequence of A-modules of the form (3.9). Then the A-module K is, by assumption, finitely generated and thus, by Lemma 3.2.1(ii), $I_\bullet$-complete. Hence, by passing to the limit over n of the induced exact sequences of (compact) A_n-modules $K_{(n)} \to A_n^d \to M_{(n)} \to 0$ one obtains an exact sequence of A-modules

$$0 \to K \xrightarrow{\subseteq} A^d \to \varprojlim_n M_{(n)} \to 0.$$

Comparing this to (3.9) one deduces the map μ_M is bijective, as required to prove (i).

In the rest of the argument we assume M is torsion. Then, since $\mathrm{char}_A(M)$ and $\mathrm{Char}_A(M)$ are both finitely generated ideals of A (cf. condition (P_2) in Definition 2.1.1), to prove (ii) it is enough to show that any finitely generated ideal N of A is equal to $\varprojlim_n \phi_{\langle n\rangle}(N)$, where the limit is taken with respect to the maps ϕ_n. To see this, we note that the above argument (with $M = A/N$, $d = 1$ and $K = N$) implies that the map $\mu_{A/N}$ is bijective. The stated equality then follows from the corresponding exact commutative diagram (3.10) and the fact that, in this case, one has $K'_n = \phi_{\langle n\rangle}(N)$ for every n.

To prove (iii) we note that if B is equal to either A or A_n for any n, then the given assumptions imply it is admissible (cf. Example 2.3.2(ii)) and also that every ideal in $\mathcal{P}_B$ is principal so that, for any finitely-presented torsion B-module N, one has $\mathrm{Char}_B(N) = \mathrm{char}_B(N)$ (by Proposition 3.1.2(i)(b)(ii) with $R = B$ and G trivial). In addition, by Theorem 2.2.3(b), any finitely-presented torsion A-module M is pseudo-isomorphic to a finite direct sum

$\widetilde{M} := \bigoplus_{\tau\in\mathcal{T}} A/L_\tau$, where, for each τ, $L_\tau = A\cdot a_\tau$ with $a_\tau \in A\setminus\{0\}$. In particular, $\widetilde{M}$ is finitely-presented and torsion and thus also $I_\bullet$-complete by (i). Further, for every n there is a natural isomorphism

$$\widetilde{M}_{(n)} \cong \bigoplus_{\tau\in\mathcal{T}} (A/L_\tau)_{(n)} \cong \bigoplus_{\tau\in\mathcal{T}} A_n/\phi_{\langle n\rangle}(L_\tau) = \bigoplus_{\tau\in\mathcal{T}} A_n/(A_n\cdot\phi_{\langle n\rangle}(a_\tau)). \tag{3.12}$$

In particular, if n_0 is the smallest integer for which $\phi_{\langle n\rangle}(a_\tau)\neq 0$ for all $\tau\in\mathcal{T}$, then for every $n\geq n_0$ the A_n-module $\widetilde{M}_{(n)}$ is finitely-presented and torsion. It is then enough to note that

$$\mathrm{Char}_A(M) = \prod_{\tau\in\mathcal{T}} L_\tau = \varprojlim_n \prod_{\tau\in\mathcal{T}} \phi_{\langle n\rangle}(L_\tau) = \varprojlim_n \mathrm{char}_{A_n}(\widetilde{M}_{(n)}).$$

Here the first equality follows directly from our definition of upper generalised characteristic ideal, the second from (ii) and the third is valid since, for each n, the isomorphism (3.12) combines with Proposition 3.1.2(i)(b) to imply that

$$\mathrm{char}_{A_n}(\widetilde{M}_{(n)}) = \mathrm{Char}_{A_n}(\widetilde{M}_{(n)}) = \prod_{\tau\in\mathcal{T}} \phi_{\langle n\rangle}(L_\tau).$$

□

Chapter 4

Arithmetic applications

Let p be a prime, k the function field of a smooth projective curve over the field of characteristic p and K/k a Galois extension such that $\mathrm{Gal}(K/k) \cong \mathbb{Z}_p^{\mathbb{N}} \times G$, where G is a finite abelian group. This section aims to apply the algebraic results developed in Chapter 2 and Chapter 3 to arithmetic contexts.

In the first part we provide a detailed introduction to Weil–étale cohomology theory as a refinement of étale cohomology, which allows us to extract deeper arithmetic information from function fields. We begin by presenting the background on the Weil group, which plays the role of the absolute Galois group in étale cohomology theory. We then introduce the Weil–étale site and topos, compute cohomology groups for certain sheaves, and establish the corresponding duality theorem (Proposition 4.1.14).

In the second part, by Lemma 4.2.1 and Proposition 4.2.4 we demonstrate that our notions of admissible rings and characteristic ideals are compatible with the rings and modules that naturally arise in arithmetic applications.

Subsequently, in Theorem 4.3.2, by applying the algebraic structure theorem established in Chapter 2, we prove that the degree-one Weil–étale cohomology groups of $\mathbb{G}_m$ over finite extensions of k in K are finitely presented torsion $\mathbb{Z}_p[[\mathbb{Z}_p^{\mathbb{N}}]]$-modules. From this, we prove an Iwasawa Main Conjecture holding under certain mild assumptions.

Finally, under mild assumptions, we investigate the pro-p completion of the Picard group in Corollary 4.4.1, whose finitely-generated property reflects behaviors of places of k ramified in K. Moreover, we show that our framework encompasses and extends several earlier works in the literature.

The results in Sections 2–4 are joint work with David Burns.

4.1 Weil-étale cohomology theory

Over the past several decades, étale cohomology has demonstrated its tremendous power. Numerous cohomology theories—serving as fundamental tools in algebraic number theory, arithmetic geometry, and algebraic geometry—have been unified under the framework of étale cohomology. In this section, we introduce the Weil–étale topology, which possesses better cohomological properties than the étale topology and retains richer arithmetic information.

Grothendieck originally introduced the notion of a Grothendieck topology via category theory to address the limitations of classical sheaf cohomology in capturing nontrivial information. In particular, because the Zariski topology is extremely coarse, the cohomology groups of many sheaves — such as constant sheaves over irreducible varieties — are often trivial. To overcome this issue, Grothendieck introduced the concept of a site, which generalizes the notion of a topological space. A site consists of a category together with a specified notion of covering families. In this framework, the category plays the role of a topological space, while coverings serve as analogues of open coverings in classical topology. Notably, the Zariski topology on a scheme X can be equivalently described using the Zariski site X_{zar}. To remedy the deficiencies of the Zariski site, Grothendieck defined the small étale site $X_{\text{ét}}$, whose objects are étale morphisms over X, arrows are X-morphisms, and coverings are surjective families of étale morphisms. The notion of sheaf can then be extended to the étale site using contravariant functor concept and the sheaf condition expressed via exact sequences. This provides the foundation for studying the category of étale sheaves $\mathbf{T}_{X,\text{ét}}$ which is an abelian category with enough injectives. Consequently, one can define the étale cohomology groups as the right derived functors of the global sections functor $\Gamma(X, -)$ on $\mathbf{T}_{X,\text{ét}}$.

Compared with classical sheaf cohomology, a significant advantage of étale cohomology is its ability to capture the action of the Galois group on sheaves. A prominent example is the correspondence between étale sheaves on a scheme X of finite type over finite field $k = \mathbb{F}_q$, and étale sheaves on the base change $\bar{X} = X \times_k k^{\text{sep}}$ equipped with a continuous action of the absolute Galois group $G_k = \text{Gal}(k^{\text{sep}}/k)$ (see [50, VIII, 1.1.3]). We will describe this correspondence more precisely in the following sections. This mechanism plays a central role in the proof of the Weil conjectures.

However, a major limitation of étale cohomology becomes apparent when we attempt to study the special values and leading terms of the zeta functions of varieties over finite fields. To address this issue, Lichtenbaum introduced a new Grothendieck topology in [58] called the Weil–étale topology, in which the role of the absolute Galois group is replaced by the Weil group (see proposition 4.1.7). We now proceed to introduce the definition and properties of the Weil group.

4.1.1 Weil groups

Let K be a local or global field, we can define the Weil group axiomatically (also see [72, 1.1]).

Definition 4.1.1. *Weil group for K is a triple data $(W_K, \phi_K, \{r_L\}_{L/K})$, where W_K is a topological group, $\phi_K : W_K \to G_K$ is a continuous homomorphism with dense image. Let $W_{L,K}$ be $\phi_K^{-1}(\text{Gal}(K^{\text{sep}}/L))$ where L runs through all the finite extensions of K within K^{sep}. The $r_L : A_L \to W_{L,K}^{ab}$ (A_L is $L^\times$ when L is a local field and idèle class group C_L when L is a global field) are isomorphisms* *between the topological groups satisfying the conditions (W1)- (W4).*

(W1) For every finite extension L/K, the homomorphism ϕ_K induces homomorphism $W_{L,K}^{ab} \to G_L^{ab}$, and the diagram below is commutative.

$$\begin{array}{ccccc} & & W_K & \xrightarrow{\phi} & G_K \\ & & \uparrow & & \uparrow \\ & & W_{L,K} & \xrightarrow{\phi} & G_L \\ & & {\scriptstyle ab}\downarrow & & \downarrow{\scriptstyle ab} \\ A_L & \xrightarrow{r_L} & W_{L,K}^{ab} & \xrightarrow{\phi_{L,K}^{ab}} & G_L^{ab} \end{array} \tag{4.1}$$

Moreover, the composition $\phi_{L,K}^{ab} \circ r_L$ of the bottom line is the local reciprocity homomorphism $\theta_L : A_L \to G_L^{ab}$.

(W2) For any $w \in W_K$ and $\sigma = \phi(w) \in G_K$ and every finite extension L/K, the diagram below is commutative.

$$\begin{array}{ccc} A_L & \xrightarrow{r_L} & W_L^{ab} \\ {\scriptstyle \sigma}\downarrow & & \downarrow{\scriptstyle w} \\ A_{\sigma(L)} & \xrightarrow{r_{\sigma(L)}} & W_{\sigma(L)}^{ab} \end{array}$$

Here the left vertical map is induced by σ and right vertical map is the conjugation by w.

(W3) If $L' \subset L$, the diagram below is commutative.

$$\begin{array}{ccc} A_{L'} & \xrightarrow{r_{L'}} & W_{L',K}^{ab} \\ \downarrow & & \downarrow{\scriptstyle t} \\ A_L & \xrightarrow{r_L} & W_{L,K}^{ab} \end{array}$$

Here the left vertical map is induced by the inclusion map and right vertical map is the transfer homomorphism defined as follows. For any topological group G and its finite index closed subgroup H, let s be a *section* $s : H\backslash G \to G$ *of the projection* $p : G \to H\backslash G$, *i.e* $p \circ s = id$. *For any* $g \in G$ *and* $x \in H\backslash G$, *we pick* $h_{g,x}$ *such that* $s(x)g = \boldsymbol{h}_{g,x}s(xg)$. *Then the transfer homomorphism is defined as*

$$t_H^G : G^{ab} \to H^{ab} \quad gG^c \to \prod_{x \in H\backslash G} \boldsymbol{h}_{g,x} \bmod H^c,$$

where G^c *is the closure of commutator subgroup of* G. *Here the map* t *on the commutative diagram is the transfer homomorphism decided by* $W_{L',K}$ *and its closed subgroup* $W_{L,K}$.

(W4) Let $W_{L/K} := W_K/W^c_{L,K}$. *Then there is a topological group isomorphism*

$$W_K \to \varprojlim_{L/K} W_{L/K},$$

where the inverse limit taken for all finite extension L/K *inside* K^{sep} *and if* $L' \subset L$, *the homomorphism between* $W_{L/K} \to W_{L'/K}$ *is the projection.*

Remark 4.1.2. *Let us give some interpretation of the definition 4.1.1.*

i) The second data in the definition of Weil group is required to be continuous. This is because if ϕ_K *is continuous, then we know* $W_{L,K}$ *is an open subgroup of* W_K. *Moreover, since the image of* ϕ_K *is dense,* ϕ_K *induces a bijection*

$$W_K/W_{L,K} \xrightarrow{\sim} \mathrm{Gal}(K^{sep}/K)/\,\mathrm{Gal}(K^{sep}/L) \xrightarrow{\sim} \mathrm{Hom}_K(L, K).$$

If L/K *is a Galois extension, then the bijection becomes a group homomorphism* $W_K/W_{L,K} \cong \mathrm{Gal}(L/K)$.

ii) Let $(W_K, \phi_K, \{r_L\}_{L/K})$ *be a Weil group of* K. *For any finite extension* L/K *inside* K^{sep}, *we can take the restriction for* ϕ_K *on* $W_{L,K}$ *and pick* $\{r_{L'}\}_{L'/L}$ *as* $r_{L'}$ *in* $\{r_L\}_{L/K}$ *(*L' *is also finite extension of* K*). Then* $W_{L,K}$ *is also a Weil group of* L. *Thus we can reduce the symbol* $W_{L,K}$ *to* W_L.

iii) In (W3), if H is a closed normal subgroup of G, then the composition

$$H^{ab} \hookrightarrow G^{ab} \xrightarrow{t_H^G} H^{ab}.$$

is the norm map $N : h \mapsto \prod_{x \in H\backslash G} h^x$, where $h^x = s(x)\boldsymbol{h}_{h,x}s(x)^{-1} = \boldsymbol{h}_{h,x}$. The transfer (Verlagerung) homomorphism plays a key role in the construction of reciprocity maps in class field theory, serving as a bridge that connects Galois groups on different layers.

There is a result (see [4, Chap 14. Thm 1, Thm 2]) that ensures the existence and uniqueness (up to isomorphism) of Weil group for a local or global field. So we can formulate Weil group for some types of fields.

Example 4.1.3. *Let us determine the Weil group for a local p-adic field and a global function field*

i) If K is a p-adic local field with residue field k, which is equal to $\mathbb{F}_q$, as we know G_k is isomorphic to $\hat{\mathbb{Z}}$. On the other hand the Galois group of the maximal unramified extension K^{ur} over K is also isomorphic to G_k, thus we have an tautological exact sequence

$$1 \longrightarrow I_K \longrightarrow G_K \longrightarrow G_k \cong \hat{\mathbb{Z}} \longrightarrow 1. \tag{4.2}$$

Here I_K denotes the absolute inertia subgroup. We can choose the W_K in the triple data as the inverse image in G_K of the discrete subgroup in G_k generated by the Frobenius endomorphism $\mathsf{Frob} : x \to x^q$, so we have $W_K/I_K \cong \mathbb{Z}$. Take $\phi : W_K \to G_K$ as the inclusion map. For the reciprocity maps, we can construct them from the local reciprocity map

$\theta_K : K^\times \to G_K^{ab}$. As we know, the classical diagram below is commutative.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{O}_K^\times & \longrightarrow & K^\times & \xrightarrow{v} & \mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow \cong & & \downarrow \theta_K & & \downarrow i & & \\ 1 & \longrightarrow & \mathrm{Gal}(K^{ab}/K^{ur}) & \longrightarrow & \mathrm{Gal}(K^{ab}/K) & \longrightarrow & \mathrm{Gal}(K^{ur}/K) & \longrightarrow & 1 \end{array}$$

The isomorphism between $\mathcal{O}_K^\times$ and $\mathrm{Gal}(K^{ab}/K^{ur})$ is given by the existence theorem of local class field theory (see [22, P. 144, Thm 3a]). Since $K^\times \cong \mathcal{O}_K^\times \times \mathbb{Z}$ and the profinite completion $\widehat{K^\times} \cong \mathrm{Gal}(K^{ab}/K) \cong \mathcal{O}_K^\times \times \hat{\mathbb{Z}}$, and the exact sequence 4.2 is split, we can define the maps r_L be θ_L and identify the W_L^{ab} with the image of θ_L. It is easy to check that r_L satisfy the conditions (W1)-(W4) (see [72, 1.4.1]).

ii) For a function field K of a curve C over a finite field k, we have the projection map $\pi : G_K \to \mathrm{Gal}(Kk^{\mathrm{sep}}/K) \cong G_k$, which is isomorphic to $\hat{\mathbb{Z}}$ and topologically generated by the Frobenius element. Then we have an analogue of exact sequence 4.2

$$1 \longrightarrow \mathrm{Gal}(K^{\mathrm{sep}}/Kk^{\mathrm{sep}}) \longrightarrow G_K \longrightarrow \mathrm{Gal}(Kk^{\mathrm{sep}}/K) \longrightarrow 1,$$

which is also split. Here $\mathrm{Gal}(Kk^{\mathrm{sep}}/K) \cong \mathrm{Gal}(k^{\mathrm{sep}}/k) \cong \hat{\mathbb{Z}}$. The Weil group W_K for function field K is $\pi^{-1}(\mathbb{Z})$ where $\mathbb{Z}$ denotes the discrete subgroup of $\mathrm{Gal}(Kk^{\mathrm{sep}}/K)$. By similar analysis and a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & C_K^0 & \longrightarrow & C_K & \xrightarrow{d} & \mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow \cong & & \downarrow \theta_K & & \downarrow i & & \\ 1 & \longrightarrow & \mathrm{Gal}(K^{ab}/H) & \longrightarrow & \mathrm{Gal}(K^{ab}/K) & \longrightarrow & \mathrm{Gal}(H/K) & \longrightarrow & 1 \end{array}$$

where d is a composition degree map given by $C_K \to \mathrm{Cl}(K) \xrightarrow{deg} \mathbb{Z}$ with the first arrow as the canonical map, C_K^0 is the degree-0 part, and H is the maximal constant field extension inside K^{ab}, we can a have similar *process as the p-adic local field case (see [72, 1.4.2])*

iii) As a special case of function field, a finite field $\mathbb{F}_q$ *has Weil group* $\mathbb{Z}$ *as the discrete subgroup of* $\mathrm{Gal}_{\mathbb{F}_q} \cong \hat{\mathbb{Z}}$.

We now analyze the motivation behind replacing absolute Galois groups with Weil groups. First, the abelianization of the Weil group W_K encodes more refined arithmetic information than that of G_K, particularly in relation to the idéle class group C_K. In the classical setting, we only obtain the Artin reciprocity map $\theta_K : C_K \to G_K^{ab}$, which is, in general, not injective. Second, in the global case, for each finite extension L/K, there exists a short exact sequence

$$1 \longrightarrow W_L^{ab} \longrightarrow W_{L,K} \longrightarrow W_K/W_L \longrightarrow 1.$$

Given that $W_L/W_L^c \cong C_L$ and $W_K/W_L \cong \mathrm{Gal}(L/K)$ for finite Galois extension L/K, it follows that $W_{L,K}$ is an extension of $\mathrm{Gal}(L/K)$ by C_L, corresponding to a fundamental class $u \in H^2(\mathrm{Gal}(L/K), C_L)$. By condition (W4) in definition 4.1.1, W_K is the projective limit of $W_{L/K}$, which demonstrates that W_K contains ample arithmetic information. Moreover, the original motivation for Weil's introduction of the Weil group was to resolve the discrepancy between Hecke L-functions and Artin L-functions. Indeed, not every Hecke L-function corresponds to an Artin L-function for a one-dimensional representation of the Galois group. However, Weil constructed the Weil group so that every Hecke L-function corresponds to an Artin L-function arising from a one-dimensional representation of the Weil group (see [80, P. 1-35]). This construction has since become classical in the study of automorphic forms and plays a central role in the Langlands program—for instance, in extending Weil groups to Deligne–Weil groups on the Galois side match automorphic data on the automorphic side, as in the study of the local Langlands correspondence for GL_n (see [72], [30, Chap 2], [20, Chap 7]). These developments highlight the foundational importance and potential of the Weil group in arithmetic research. Later, we will also see that Weil–étale cohomology enjoys better formal properties and can be regarded as more fundamental than classical étale cohomology.

4.1.2 Weil-étale sites and topoi

The content of this section is a reformulation of [58, §2]. Throughout this section, let k denote a finite field $\mathbb{F}_q$. Let X be a scheme of finite type over k and let $\bar{X}$ denote its base change to the algebraic closure of k. In analogy with the development of étale cohomology, we first define the site that will be used in the construction of Weil-étale cohomology theory.

Definition 4.1.4. *We define the Weil-étale topology as the following Grothendieck topology on the underlying category* $\mathrm{Cat}_{\mathcal{W}}(X)$.

- *Objects: All étale schemes of finite type over* $\bar{X}$.
- *Morphisms: Let* $\pi_1 : \bar{X} \to X, \pi_2 : \bar{X} \to k^{\mathrm{sep}}$ *be the two projections. If* $W \xrightarrow{f} \bar{X}$ *and* $Z \xrightarrow{g} \bar{X}$ *are two objects belonging to* $\mathrm{Cat}_{\mathcal{W}}(X)$ *where* W *is connected, then a morphism* ϕ *from* (W, f) *to* (Z, g) *is a morphism* ϕ *from* W *to* Z *such that*

  i) For π_1*, the diagram following is commutative.*

$$\begin{array}{ccc} W & \xrightarrow{\phi} & Z \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle g} \\ \bar{X} & & \bar{X} \\ {\scriptstyle \pi_1}\downarrow & & \downarrow{\scriptstyle \pi_1} \\ X & \xrightarrow[id]{} & X \end{array} \tag{4.3}$$

  ii) For π_2*, the diagram following is commutative where the bottom ar-*

row is an integral power of the Frobenius morphism on $\bar{k}$.

$$\begin{array}{ccc} W & \xrightarrow{\phi} & Z \\ {\scriptstyle f}\big\downarrow & & \big\downarrow{\scriptstyle g} \\ \bar{X} & & \bar{X} \\ {\scriptstyle \pi_2}\big\downarrow & & \big\downarrow{\scriptstyle \pi_2} \\ k^{\mathrm{sep}} & \xrightarrow[\mathsf{Frob}^n]{} & k^{\mathrm{sep}} \end{array} \tag{4.4}$$

For arbitrary W, a morphism on W is a collection of morphisms on the connected components of W.

- *Covering: The surjective families $\{W_i \to W\}$ belonging to $\mathrm{Cat}_{\mathcal{W}}(X)$.*

The Weil-étale site $X_{W\text{ét}}$ is the category $\mathrm{Cat}_{\mathcal{W}}(X)$ equipped with the Weil-étale topology.

Remark 4.1.5. *The Weil-étale site defined above closely resembles the structure of the small étale site. For instance, its coverings are induced by restricting the étale topology from the small étale site $\bar{X}_{\acute{e}t}$ to the subcategory $\mathrm{Cat}_{\mathcal{W}}(X)$. For this reason, Lichtenbaum[58] also refers to it as the Weil-étale small site.*

Next we introduce Weil-étale sheaves and the topos.

Definition 4.1.6. *A sheaf $\mathcal{F}$ on $X_{W\text{ét}}$ is a contravariant functor $\mathrm{Cat}_{\mathcal{W}}(X) \to$ AbGrp such that*

$$\mathcal{F}(W) \to \prod_{i\in I} \mathcal{F}(W_i) \rightrightarrows \prod_{(i,j)\in I\times I} \mathcal{F}(W_i \times_W W_j)$$

is exact for every object $W \to X$ and every covering $\{W_i \to W\}$. We use the notation $\mathbf{T}_{X,W\text{ét}}$ to denote the topos of Weil-étale sheaves.

We now provide an equivalent description of the Weil-étale topos. We begin by recalling the correspondence between étale sheaves on X and G_k-equivariant sheaves on the $\bar{X}$. Let $\mathcal{F}$ be an étale sheaf on $\bar{X}$, and let $\pi_1 : \bar{X} \to X$ denote the natural projection. For any $g \in G_k$ and any étale morphism $U \to \bar{X}$ of finite type, define $gU = U \times_{\bar{\mathbb{F}}_q, g^{-1}} \bar{\mathbb{F}}_q$. Then we can define the pullback $g^*\mathcal{F}(U) = \mathcal{F}(gU)$ and the pushward $g_*\mathcal{F}(U) = \mathcal{F}(g^{-1}U)$. We say G_k acts on $\mathcal{F}$ if for each $g \in G_k$ there exists an isomorphism $i_g : \mathcal{F} \to g^*\mathcal{F}$ such that $i_{gh} = i_g \circ i_h$. For any $f \in \mathcal{F}(U)$, we denote $i_g(f) \in \mathcal{F}(gU)$ by gf . Let $G_U \subset G_k$ denote the subgroup fixing the minimal finite extension $\mathbb{F}_{q^r}$ over which U has a model U' such that $U = U' \times_{\mathbb{F}_{q^r}} \bar{\mathbb{F}}_q$. This model exists because every scheme of finite type over $\bar{\mathbb{F}}_q$ is the base change of a scheme over some finite field $\mathbb{F}_{q^r}$. If G_k acts on $\mathcal{F}$, then so does G_U on $\mathcal{F}(U)$. We say that G_k acts continuously on $\mathcal{F}$ if for each U, the action of G_U on $\mathcal{F}(U)$ equipped with discrete topology is continuous. This correspondence yields an equivalence between the étale topos $\mathbf{T}_{X,\text{ét}}$ of étale sheaves on X and the topos $\mathbf{T}^{G_k}_{\bar{X},\text{ét}}$ of étale sheaves on $\bar{X}$ equipped with a continuous G_k-action as follows. Given an étale sheaf $\mathcal{G}$ on X, its pullback $\mathcal{G}_k = \pi_1^*\mathcal{G}$ to $\bar{X}$ carries a natural G_k-action since for every $g \in G_k$, there is an induced morphism $g : \bar{X} \to \bar{X}$ which induces a pullback $g^*\mathcal{G}_k$ and $g^*\mathcal{G}_k \cong \mathcal{G}_k$. This assigns $\mathcal{G}$ belonging to $\mathbf{T}_{X,\text{ét}}$ corresponding to $\mathcal{G}_k$ belonging to $\mathbf{T}^{G_k}_{\bar{X},\text{ét}}$. Conversely, given a sheaf $\mathcal{F}$ on the $\bar{X}$ with a continuous G_k-action, the corresponding étale sheaf on X is given by ${\pi_1}_*^{G_k}\mathcal{F}$, defined by $V \to \mathcal{F}(V \times_{\mathbb{F}_q} \bar{\mathbb{F}}_q)^{G_k}$. Moreover, using the isomorphism $H^i_{\text{ét}}(\bar{X}, g^*\mathcal{F}) \cong H^i_{\text{ét}}(X, \mathcal{F})$, we can extract cohomological information from the G_k-action on $\mathcal{F}$.

Notice that any G_k-equivariant sheaf as described above naturally carries the structure of a W_k-equivariant sheaf via the inclusion $W_k \hookrightarrow G_k$. In particular, for any $\mathcal{W}$ belonging to $\mathbf{T}_{X,W\text{ét}}$, the global section $\Gamma(\bar{X}, \mathcal{W})$ naturally form a W_k-module. Analogously, for the Weil group W_k and Weil-étale topos, a similar correspondence holds, mirroring the discussion above.

Proposition 4.1.7. *The category of Weil-étale sheaves on X is equivalent to the category of étale sheaves on $\bar{X}$ equipped with a W_k-action.*

Proof. See [58, Prop. 2.2]. □

Next we explain the connection between the Weil-étale topos $\mathbf{T}_{X,W\text{ét}}$ and the étale topos $\mathbf{T}_{X,\text{ét}}$. Inspired by constructing equivalence between $\mathbf{T}_{X,\text{ét}}$ and $\mathbf{T}^{G_k}_{\bar{X},\text{ét}}$, we can define two similar functors $\psi : \mathbf{T}_{X,W\text{ét}} \to \mathbf{T}_{X,\text{ét}}$ and $\phi : \mathbf{T}_{X,\text{ét}} \to \mathbf{T}_{X,W\text{ét}}$ between $\mathbf{T}_{X,\text{ét}}$ and $\mathbf{T}_{X,W\text{ét}}$. For every object $F \to X$ in $X_{\text{ét}}$ and every Weil-étale sheaf $\mathcal{G}$ in $\mathbf{T}_{X,W\text{ét}}$, we define $\psi(\mathcal{G})(F) := \mathcal{G}(F \times_X \bar{X})^{W_k}$. For every étale sheaf $\mathcal{F}$ on X, we set $\phi(\mathcal{F}) := \pi_1^*\mathcal{F}$. In general the two functors φ and ψ do not yield an equivalence of topoi. However, as a second-best result the pair (ϕ, ψ) forms an adjoint pair. Moreover, there exists a unit $\eta : id_{\mathbf{T}_{X,\text{ét}}} \to \psi \circ \phi$ which implies ϕ is actually fully faithful. This shows that $\mathbf{T}_{X,\text{ét}}$ is equivalent to a full subcategory of $\mathbf{T}_{X,W\text{ét}}$ (see [58, Prop. 2.4, (a),(b)]).

On the other hand, since $\mathbf{T}_{X,W\text{ét}}$ is a Grothendieck abelian category, it has enough injectives. By taking the functor $\Gamma(\bar{X}, -)^{W_k}$ as the zeroth cohomology functor, we can define the i-th Weil-étale cohomology functor as its i-th right derived functor. We denote the i-th Weil-étale cohomology group of an object $\mathcal{G}$ belonging to $\mathbf{T}_{X,W\text{ét}}$ by $H^i(X_{W\text{ét}}, \mathcal{G})$. The functors (ϕ, ψ) provide insights into the connection between Weil-étale and classical étale cohomology, via the homomorphisms induced between cohomology groups by the action of functors on the resolution complexes (see [58, Prop. 2.4, (e),(g)]).

Proposition 4.1.8. *Let $\mathcal{G}$ belong to $\mathbf{T}_{X,W\text{ét}}$ and $\mathcal{F}$ belong to $\mathbf{T}_{X,\text{ét}}$. There is $c_i : H^i_{\text{ét}}(X, \psi(\mathcal{G})) \to H^i(X_{W\text{ét}}, \mathcal{G})$ and $d_i : H^i_{\text{ét}}(X, \mathcal{F}) \to H^i(X_{W\text{ét}}, \phi(\mathcal{F}))$ such that the following assertions are correct.*

- *c_0 is an isomorphism.*
- *c_i are isomorphisms when $\mathcal{G}$ is a torsion sheaf.*
- *d_i are isomorphisms when $\mathcal{F}$ is a torsion sheaf.*

It also should be noted that the six standard functors for Weil-étale sheaves

— namely $(i^*, i_*, i^!)$ and $(j_!, j^*, j_*)$, corresponding respectively to the open immersion $j : U \hookrightarrow X$ and the closed immersion $i : Z \hookrightarrow X$ with $U = X \backslash Z$ — satisfy similar adjoint functor relationships as in the case of étale sheaves (see [58, P. 693]). These functors are particularly useful for analyzing the structure of Weil-étale sheaves. For instance, the exact sequence

$$0 \longrightarrow j_! j^* \mathcal{F} \longrightarrow \mathcal{F} \longrightarrow i_* i^* \mathcal{F} \longrightarrow 0$$

remains valid for any Weil-étale sheaf $\mathcal{F}$ on X.

4.1.3 Weil-étale cohomology groups of sheaves

In this subsection we collect several basic properties of Weil–étale cohomology groups for certain sheaves. Throughout we let k be a finite field and X a scheme of finite type over k. In what follows we will mainly be interested in the constant sheaf $\mathbb{Z}$, the extension–by–zero sheaf $j_!\mathbb{Z}$ associated to an open immersion $j : U \hookrightarrow X$, and the Weil–étale sheaf $\mathbb{G}_m$, which is defined as the restriction of the étale sheaf $\mathbb{G}_m$ on $\bar{X}_{\text{ét}}$ to $X_{W\text{ét}}$.

For the constant sheaf $\mathbb{Z}$ on $X_{W\text{ét}}$, Lichtenbaum has proved that the cohomology groups $H^q(X_{W\text{ét}}, \mathbb{Z})$ are finitely generated for all integers $q \geq 0$, are finite for all $q \geq 2$, and vanish for all sufficiently large q (see [58, Thm 3.1]).

Now we compute the extension by zero sheaf $j_!\mathbb{Z}$. Let U be a smooth d-dimensional quasi-projective variety over a finite field k. Since the proof of the following proposition involves certain technical subtleties, we assume the existence of an open dense immersion $j : U \hookrightarrow X$, where X is a smooth projective variety over k. The existence of X is justified by the existence of resolution of singularities in positive characteristic when $d \leq 3$.

Proposition 4.1.9. *Let $d \leq 3$, $j : U \to X$ as mentioned in the above paragraph. Then $H^q(X, j_!\mathbb{Z})$ are independent of the choice of X and j. Moreover, the groups are finitely generated and vanishing for q large enough.*

Proof. See [58, Thm 3.3] □

Remark 4.1.10. *It is well-known that the existence of resolution of singularities for varieties over fields of characteristic zero was proven by H. Hironaka in [47]. However, for varieties of dimension more than 3 over fields of characteristic p, the existence problem is still open. For curves, the problem is relatively straightforward and can be handled via normalization. In dimension $d = 2$, the existence was proven by S. Abhyankar in [1], and for $d = 3$, the case was settled by V. Cossart and O. Piltant in [27].*

It should be noted that in [58], S. Lichtenbaum proved the proposition 4.1.9 only for the case $d \leq 2$. At the time S. Lichtenbaum completed [58], the result of [27] for $d = 3$ had not yet been established. After reviewing the argument, the author of this thesis believes that the proposition should also hold in dimension $d = 3$, in light of the results in [27].

Proposition 4.1.11. *Let X be a geometrically connected smooth curve over a finite field k. Then the cohomology groups $H^q(X_{W\acute{e}t}, \mathbb{G}_m)$ are finitely generated for all q and vanishing for all $q \geq 3$. In particular, when X is projective, we have $H^0(X_{W\acute{e}t}, \mathbb{G}_m) = k^\times, H^1(X_{W\acute{e}t}, \mathbb{G}_m) = \mathrm{Pic}(X), H^2(X_{W\acute{e}t}, \mathbb{G}_m) = \mathbb{Z}$.*

Proof. See ([58, Prop. 3.4]). □

4.1.4 Duality theorems in the derived version

Let U be a smooth geometrically connected curve over a finite field k, equipped with an open dense immersion $j : U \hookrightarrow X$ into a smooth projective curve X over k. Let $\mathcal{F}$ be a sheaf in $\mathbf{T}_{X,W\acute{e}t}$. Notice that X has finite cohomological dimension. Thus by taking an injective (bounded-above) resolution $I^\bullet$ of $\mathcal{F}$, a sufficiently far-out truncation $\tau I^\bullet$ and an injective resolution $J^\bullet$ of $\mathbb{G}_m$, we construct $\mathsf{R}\mathrm{Hom}_X(\mathcal{F}, \mathbb{G}_m) = \mathrm{Hom}_X(\tau I^\bullet, J^\bullet)$. We can also define the derived global sections $\mathsf{R}\Gamma_X(\mathcal{F})$ as the right derived functor of the global section functor $\Gamma(\bar{X}, -)^{W_k}$.

Let $\mathbf{D}$ be the derived category of abelian groups consisting of those complexes with finitely generated homology groups. Applying the functor $\mathsf{R}\Gamma_X(\mathcal{F})$, we obtain a natural morphism $k_{\mathcal{F}} : \mathsf{RHom}_X(\mathcal{F}, \mathbb{G}_m) \to \mathsf{RHom}_{\mathbf{D}}(\mathsf{R}\Gamma_X(\mathcal{F}), \mathsf{R}\Gamma_X(\mathbb{G}_m))$ in $\mathbf{D}$. Moreover, by Proposition 4.1.11, there is a natural morphism $f : \mathsf{R}\Gamma_X(\mathbb{G}_m) \to \mathbb{Z}[-2]$ in $\mathbf{D}$. Then we define $\kappa_{\mathcal{F}} = f \circ k_{\mathcal{F}}$ which is the composition morphism from $\mathsf{RHom}_X(\mathcal{F}, \mathbb{G}_m)$ to $\mathsf{RHom}_X(\mathsf{R}\Gamma_X(\mathcal{F}), \mathbb{Z}[-2])$. The proof of next proposition can be found in [58, Thm 5.1].

Proposition 4.1.12. *Let $\mathcal{F}$ be either $j_!\mathbb{Z}$ or $j_!\mathbb{Z}/n\mathbb{Z}$. Then $\kappa_{\mathcal{F}}$ is an isomorphism.*

Since the six standard functors applies well for Weil-étale sheaves, the functor j^* has the exact left $j_!$ and j^* is exact. Consequently j^* carries a resolution of $\mathbb{G}_{m,X}$ to a resolution of $j^*\mathbb{G}_{m,X} = \mathbb{G}_{m,U}$. By the adjointness of the pair $(j^*, j_!)$, we obtain the following lemma.

Lemma 4.1.13. *Let $\mathcal{F}$ be a Weil-étale sheaf on U. There is a canonical isomorphism in $\mathbf{D}$ between $\mathsf{RHom}_X(j_!\mathcal{F}, \mathbb{G}_{m,X})$ and $\mathsf{RHom}_U(\mathcal{F}, \mathbb{G}_{m,U})$.*

Notice that $\mathsf{R}\Gamma_U(\mathcal{F}) \cong \mathsf{RHom}_U(\mathbb{Z}, \mathcal{F})$ and the functor is $\mathsf{RHom}_{\mathbf{D}}(-, \mathbb{Z}[-2])$ is self-inverse. By combining Proposition 4.1.12 and Lemma 4.1.13, we obtain the following duality theorem.

Proposition 4.1.14. *The following two assertions are right.*

1) $\mathsf{R}\Gamma_U(\mathbb{G}_m)$ *is naturally isomorphic to* $\mathsf{RHom}_{\mathbf{D}}(\mathsf{R}\Gamma_X(j_!\mathbb{Z}), \mathbb{Z}[-2])$.

2) $\mathsf{R}\Gamma_X(j_!\mathbb{Z})$ *is naturally isomorphic to* $\mathsf{RHom}_{\mathbf{D}}(\mathsf{R}\Gamma_U(\mathbb{G}_m), \mathbb{Z}[-2])$.

4.2 Arithmetic of function fields

4.2.1 Application of algebraic results

In this section we describe an application of the algebraic results in Chapters 2 and 3 to the rings and modules occurring in the context of Iwasawa theory. For this, we write $\mathcal{U}(G)$ for the set of open subgroups of a profinite group G.

The Iwasawa algebra of $\mathbb{Z}_p^{\mathbb{N}}$ over a commutative $\mathbb{Z}_p$-algebra $\mathcal{O}$ is the completed group ring

$$\mathcal{O}[[\mathbb{Z}_p^{\mathbb{N}}]] := \varprojlim_{U\in\mathcal{U}(\mathbb{Z}_p^{\mathbb{N}})} \mathcal{O}[\mathbb{Z}_p^{\mathbb{N}}/U],$$

where the limit is taken respect to the natural projection maps. In particular, after fixing a $\mathbb{Z}_p$-basis $\{\gamma_i\}_{i\in\mathbb{N}}$ of $\mathbb{Z}_p^{\mathbb{N}}$, the association $X_i \mapsto \gamma_i - 1$ induces an isomorphism of rings between $\mathcal{O}[[\mathbb{Z}_p^{\mathbb{N}}]]$ and the power series ring

$$\mathcal{R}_{\mathcal{O}} := \varprojlim_{n} \mathcal{R}_{n,\mathcal{O}} \quad \text{with} \quad \mathcal{R}_{n,\mathcal{O}} := \mathcal{O}[[X_1, \dots, X_n]]$$

in commuting indeterminates $\{X_i\}_{i\in\mathbb{N}}$. Here the inverse limit is taken with respect to the (surjective) $\mathbb{Z}_p$-linear ring homomorphisms

$$\rho_{n,\mathcal{O}} : \mathcal{R}_{n,\mathcal{O}} \twoheadrightarrow \mathcal{R}_{n-1,\mathcal{O}}$$

that send X_i to X_i if $1 \le i < n$ and to 0 if $i = n$. For each n we also use the maps

$$\iota_{n,\mathcal{O}} : \mathcal{R}_{n,\mathcal{O}} \hookrightarrow \mathcal{R}_{\mathcal{O}} \quad \text{and} \quad \rho_{\langle n\rangle,\mathcal{O}} : R_{\mathcal{O}} \twoheadrightarrow R_{n,\mathcal{O}},$$

that are respectively the natural inclusion and the (surjective) $\mathcal{O}$-linear ring homomorphism that sends X_i to X_i if $1 \le i \le n$ and to 0 if $i > n$ (so that the pair $(\iota_{n,\mathcal{O}}, \rho_{\langle n\rangle,\mathcal{O}})$ is a retract of rings and, for each $n > 1$, one has $\rho_{n,\mathcal{O}} \circ \rho_{\langle n\rangle,\mathcal{O}} = \rho_{\langle n-1\rangle,\mathcal{O}}$).

In the case $\mathcal{O} = \mathbb{Z}_p$, we abbreviate $\mathcal{R}_{\mathcal{O}}, \mathcal{R}_{n,\mathcal{O}}, \rho_{n,\mathcal{O}}, \rho_{\langle n\rangle,\mathcal{O}}$ and $\iota_{n,\mathcal{O}}$ to $\mathcal{R}, \mathcal{R}_n, \rho_n, \rho_{\langle n\rangle}$ and ι_n respectively. We then also fix a finite abelian group G and consider the group rings

$$\mathcal{A} := \mathcal{R}[G] \quad \text{and} \quad \mathcal{A}_n = \mathcal{R}_n[G],$$

together with the maps $\mathcal{A}_n \to \mathcal{A}_{n-1}, \mathcal{A}_n \to \mathcal{A}$ and $\mathcal{A} \to \mathcal{A}_n$ that are respectively induced by ρ_n, ι_n and $\rho_{\langle n\rangle}$ (and which we continue to denote by the same notation).

We then define a separated decreasing filtration $\mathcal{I}_\bullet = (\mathcal{I}_n)_n$ of $\mathcal{A}$ by setting

$$\mathcal{I}_n := \ker(\rho_{\langle n\rangle})$$

for each n, and we note that $\mathcal{A}$ is $\mathcal{I}_\bullet$-complete.

Now, since the submodule of $\mathcal{I}_n$ that is generated by $\{X_i\}_{i>n}$ is not finitely generated, the ring $\mathcal{A}$ is not Noetherian (cf. Remark 4.2.3 below) and its module theory is complicated. For instance, the example discussed in the proof of Lemma 3.2.1(i) shows that cyclic $\mathcal{A}$-modules need not be $\mathcal{I}_\bullet$-complete (or even pro-finite). Nevertheless, claims (i) and (ii) of the following result ensure that our theory developed in Chapter 2 and Chapter 3 can be applied in this setting.

For each natural number m, we use $\mathcal{O}_m$ to denote $\mathbb{Z}_p[\zeta_m] \subset \mathbb{Q}_p^c$.

Lemma 4.2.1. *For every n the following claims are valid.*

(i) For all natural numbers m, the rings $\mathcal{R}_{\mathcal{O}_m}$ and $\mathcal{R}_{n,\mathcal{O}_m}$ are p-adically complete unique factorisation domains, and hence admissible (in the sense of Definition 2.3.1).

(ii) The ring $\mathcal{A}$ is p-adically complete and compact (in the sense of §3.2.2) and both rings $Q(\mathcal{A})$ and $Q(\mathcal{A}_n)$ are semisimple (as algebras over $Q(\mathcal{R})$

and $Q(\mathcal{R}_n)$ respectively). In addition, an $\mathcal{A}$-module M is finitely-presented, torsion and admissible if it is finitely-presented and torsion as an $\mathcal{R}$-module and, in addition, no height one prime of $\mathcal{R}$ that lies in the support of M contains $|G|$. In particular, if $p \nmid |G|$, then the ring $\mathcal{A}$, and also the ring $\mathcal{A}_n$ for each n, is admissible.

(iii) If $\mathfrak{p}$ is a prime ideal of $\mathcal{A}_n$, then $\iota_n(\mathfrak{p})\mathcal{A}$ is a prime ideal of $\mathcal{A}$.

Proof. Since $\mathcal{O}_m$ is a regular local domain, the first assertion of (i) is classical in the case of $\mathcal{R}_{n,\mathcal{O}_m}$. This result then implies that the ring $\mathcal{R}_{\mathcal{O}_m}$ satisfies the condition $(*)$ of Nishimura [64, Intro.] and hence that it is a unique factorisation domain by [64, Th. 1]. The second assertion of (i) then follows directly from Remark 2.3.2(ii).

To prove (ii) we note that, for each subgroup U in $\mathcal{U}(\mathbb{Z}_p^{\mathbb{N}})$ the ring $\mathbb{Z}_p[(\mathbb{Z}_p^{\mathbb{N}}/U)\times G]$ is finitely generated over $\mathbb{Z}_p$ and hence compact with respect to the canonical p-adic topology. The (inverse limit) ring $\mathbb{Z}_p[[\mathbb{Z}_p^{\mathbb{N}}\times G]]$ is therefore compact with respect to the induced inverse limit topology. This induces a compact topology on $\mathcal{A}$ that is independent of the choice of $\mathbb{Z}_p$-basis $\{\gamma_i\}_{i\in\mathbb{N}}$ of $\mathbb{Z}_p^{\mathbb{N}}$ and such that each ideal $\mathcal{I}_n$ is closed. This proves the first assertion of (ii). In addition, as $\mathcal{R}$ and $\mathcal{R}_n$ are both domains of characteristic zero, and G is finite, the algebras $Q(\mathcal{A})$ and $Q(\mathcal{A}_n)$ are respectively equal to $Q(\mathcal{R})[G]$ and $Q(\mathcal{R}_n)[G]$ and so are semisimple (see the discussion at the paragraph above Proposition 2.3.3).

Next we note that (i) combines with Proposition 2.3.5 (with R and A replaced by $\mathcal{R}$ and $\mathcal{A}$) to imply an $\mathcal{A}$-module M that is finitely-presented and torsion as an $\mathcal{R}$-module is finitely-presented, torsion and admissible as an $\mathcal{A}$-module provided that both $\mathcal{P}_{\mathcal{R}}(M)\subseteq \mathcal{P}_{\mathcal{R}}^{|G|}$ and $R_{\mathfrak{q}}$ is Noetherian for every $\mathfrak{q}\in\mathcal{P}_{\mathcal{R}}(M)$. In addition, since for each divisor m of n, the ring $\mathcal{O}_m\otimes_{\mathbb{Z}_p}\mathcal{R}=\mathcal{R}_{\mathcal{O}_m}$ is a unique factorisation domain, one has $\mathcal{P}_{\mathcal{R}}^{|G|}=\{\mathfrak{q}\in\mathcal{P}_{\mathcal{R}} : |G|\notin\mathfrak{q}\}$ (cf. Example 2.3.4(ii)) and the localisation of $\mathcal{R}$ at each prime in $\mathcal{P}_{\mathcal{R}}$ is a principal ideal domain, and hence Noetherian. This proves the second sentence of (ii). Given this fact, it is clear that if $p \nmid |G|$ then $\mathcal{A}$ is admissible as no prime in $\mathcal{P}_{\mathcal{R}}$ can contain $|G|$. Finally, we recall that the admissibility of each ring $\mathcal{A}_n$ in this case was already observed in Remark 3.1.3

To prove (iii) we note $\mathfrak{p}$ is a (finitely generated) ideal of the (Noetherian) ring $\mathcal{A}_n$, and hence that $\mathfrak{P} := \iota_n(\mathfrak{p})\mathcal{A}$ is a finitely generated ideal of $\mathcal{A}$. Proposition 3.2.2(i) therefore implies that the map $\mu_{\mathcal{A}/\mathfrak{P}}$ is bijective. Since, for $m > n$, the image of the natural map $\mathfrak{P}_{(m)} \to \mathcal{A}_{(m)} = \mathcal{A}_m$ is $\rho_{\langle m\rangle}(\mathfrak{P}) = \mathfrak{p}[[X_{n+1}, \ldots, X_m]]$, these observations combine to give a composite ring isomorphism

$$\mathcal{A}/\mathfrak{P} \xrightarrow{\mu_{\mathcal{A}/\mathfrak{P}}} \varprojlim_{m>n} \left(\mathcal{A}/\mathfrak{P}\right)_{(m)} \cong \varprojlim_{m>n} \mathcal{A}_m/\rho_{\langle m\rangle}(\mathfrak{P}) \cong \varprojlim_{m>n} (\mathcal{A}_n/\mathfrak{p})[[X_{n+1}, \cdots, X_m]].$$

Hence, since each ring $(\mathcal{A}_n/\mathfrak{p})[[X_{n+1}, \cdots, X_m]]$ is a domain, the limit is a domain and so $\mathfrak{P}$ is a prime ideal of $\mathcal{A}$. □

Remark 4.2.2. *Every non-zero prime ideal of $\mathcal{R}$ that is principal has height one (since if a generating element x does not belong to any prime in $\mathcal{P}_{\mathcal{R}}$, then x^{-1} belongs to $\mathcal{R}_{\mathfrak{q}}$ for all $\mathfrak{q}$ in $\mathcal{P}_{\mathcal{R}}$ and hence to $\mathcal{R} = \bigcap_{\mathfrak{q}\in\mathcal{P}_{\mathcal{R}}} \mathcal{R}_{\mathfrak{q}}$). Lemma 4.2.1(iii) (with G trivial) therefore implies that $\iota_n(\mathfrak{p})\mathcal{R}$ belongs to $\mathcal{P}_{\mathcal{R}}$ if $\mathfrak{p}$ belongs to $\mathcal{P}_{\mathcal{R}_n}$. This observation is a special case of a result of Gilmer [42, Th. 3.2] and is also related to the second part of [7, Prop. 2.3].*

Remark 4.2.3. *Since $\mathcal{R}$ is a unique factorisation domain, it is a finite conductor ring in the sense of Glaz [43] (so that every ideal with at most two generators is finitely-presented).*

The following result proves a more concrete version of Proposition 3.2.2(iii) in this case. In particular, it shows that, for a natural class of torsion $\mathcal{A}$-modules, the notion of lower generalised characteristic ideal coincides with the 'pro-characteristic ideal' defined by Bandini et al in [7].

Proposition 4.2.4. *Assume $|G|$ is prime to p. Then the following claims are valid for any quadratically-presented, torsion $\mathcal{A}$-module M.*

(i) For any natural number n for which the $\mathcal{A}_n$-module $M_{(n)}$ is torsion, the $\mathcal{A}_n$-module $(M_{(n+1)})^{X_{n+1}=0}$ is pseudo-null.

(ii) The $\mathcal{A}$-module M identifies with $\varprojlim_n M_{(n)}$ and its pro-characteristic ideal (in the sense of [7, Def. 1.3]) is equal to $\mathrm{char}_{\mathcal{A}}(M)$.

Proof. Since $p \nmid |G|$, there exists a finite set $\{m_i\}_{i\in I}$ of natural numbers and corresponding direct product decompositions $\mathcal{A} = \prod_{i\in I} \mathcal{R}_{\mathcal{O}_{m_i}}$ and $\mathcal{A}_n = \prod_{i\in I} \mathcal{R}_{n,\mathcal{O}_{m_i}}$ (for each n) that are compatible with all transition maps. Hence, in this argument we can, and will, henceforth assume that $\mathcal{A}$ and $\mathcal{A}_n$ respectively represent $\mathcal{R}_{\mathcal{O}_m}$ and $\mathcal{R}_{n,\mathcal{O}_m}$ for some natural number m.

To prove (i) we note $\mathcal{A}_{n+1}$ is Noetherian. Hence, assuming $M_{(n)}$ to be a torsion $\mathcal{A}_n$-module, the equality $(M_{(n+1)})_{(n)} = M_{(n)}$ combines with Nakayama's Lemma to imply $(M_{(n+1)})_{\mathfrak{p}} = (0)$ with $\mathfrak{p} = (X_{n+1}) \in \mathrm{Spec}(\mathcal{A}_{n+1})$ and so $M_{(n+1)}$ is a torsion $\mathcal{A}_{n+1}$-module. In particular, since $M_{(n+1)}$ and $M_{(n)}$ are both quadratically-presented (over $\mathcal{A}_{n+1}$ and $\mathcal{A}_n$ respectively), there are equalities of $\mathcal{A}_n$-ideals

$$\begin{aligned}
\mathrm{char}_{\mathcal{A}_n}\big((M_{(n+1)})^{X_{n+1}=0}\big)\cdot \rho_{n+1}\big(\mathrm{char}_{\mathcal{A}_{n+1}}(M_{(n+1)})\big) &= \mathrm{char}_{\mathcal{A}_n}(M_{(n)}) \\
&= \mathrm{Fit}^0_{\mathcal{A}_n}(M_{(n)}) \\
&= \rho_{n+1}\big(\mathrm{Fit}^0_{\mathcal{A}_{n+1}}(M_{(n+1)})\big) \\
&= \rho_{n+1}\big(\mathrm{char}_{\mathcal{A}_{n+1}}(M_{(n+1)})\big).
\end{aligned} \tag{4.5}$$

Here the second and last equalities follow from Proposition 3.1.2(i)(b) (with G trivial and R taken to be respectively $\mathcal{A}_n$ and $\mathcal{A}_{n+1}$), the first equality follows from Remark 3.1.3 and the general result of [7, Prop. 2.10] (see also [65, Lem. 4]) and the third from a standard property of Fitting ideals under scalar extension.

Next we note that, as $M_{(n)}$ is a quadratically-presented, torsion $\mathcal{A}_n$-module, the ideal $\mathrm{Fit}^0_{\mathcal{A}_n}\big(M_{(n)}\big)$, and hence (by (4.5)) also $\rho_{n+1}\big(\mathrm{char}_{\mathcal{A}_{n+1}}(M_{(n+1)})\big)$, is principal and generated by a non-zero divisor. The equalities (4.5) therefore imply $\mathrm{char}_{\mathcal{A}_n}\big((M_{(n+1)})^{X_{n+1}=0}\big) = \mathcal{A}_n$, and hence that $(M_{(n+1)})^{X_{n+1}=0}$ is a pseudo-null $\mathcal{A}_n$-module, as required to prove (i).

In a similar way, Proposition 3.1.2(i)(b) implies for every n that

$$\mathrm{char}_{\mathcal{A}_n}(M_{(n)}) = \mathrm{Fit}^0_{\mathcal{A}_n}(M_{(n)}) = \rho_{\langle n\rangle}\big(\mathrm{Fit}^0_{\mathcal{A}}(M)\big) = \rho_{\langle n\rangle}\big(\mathrm{char}_{\mathcal{A}}(M)\big).$$

Taking account of Proposition 3.2.2(ii) (and Lemma 4.2.1(ii)), these equalities in turn imply that the pro-characteristic ideal of the $\mathcal{A}$-module $\varprojlim_n M_{(n)}$ is equal to $\mathrm{char}_{\mathcal{A}}(M)$. To complete the proof of (ii), it is now enough to note that the canonical map $M \to \varprojlim_n M_{(n)}$ is bijective as a consequence of Proposition 3.2.2(i) (and the first assertion of Lemma 4.2.1(ii)). □

Remark 4.2.5. *The assumptions used in [7] are more general than those of Proposition 4.2.4. Specifically, the authors of loc. cit. assume only to be given a Krull domain Λ that arises as the inverse limit (over $d \in \mathbb{N}$) of Noetherian Krull domains Λ_d and a Λ-module M arising as the inverse limit of torsion Λ_d-modules M_d. Then, under suitable hypotheses on each Λ_d, they formulate conditions on the modules M_d that are analogous to the conclusion of Proposition 4.2.4(i) and, assuming these conditions to be satisfied, [7, Th. 2.13] provides a well-defined 'pro-characteristics ideal' $\widetilde{\mathrm{Ch}}_\Lambda(M)$ of M. We now assume M is a finitely-presented, torsion Λ-module that is supported on only finitely many primes in $\mathcal{P}_\Lambda$, each of which is finitely generated. Then M is also an admissible Λ-module (cf. Remarks 2.1.2(i) and 2.3.2(i)) and so has a generalised characteristic ideal $\mathrm{char}_\Lambda(M)$ in the sense of Definition 3.1.1. As a possible extension of Proposition 4.2.4 (and Proposition 3.2.2(iii)), it would seem reasonable to expect that in any such case $\mathrm{char}_\Lambda(M)$ should be closely related to $\widetilde{\mathrm{Ch}}_\Lambda(M)$.*

4.2.2 The Weil-étale cohomology group and Stickelberger element

In rest of this chapter, we fix a global function field k of characteristic p and a Galois extension K of k that is ramified at only finitely many places and such that the group $\Gamma := \mathrm{Gal}(K/k)$ is topologically isomorphic to a direct product $\mathbb{Z}_p^{\mathbb{N}} \times G$ for a finite abelian group G. We fix such an isomorphism and, in addition, a finite non-empty set of places Σ of k that contains all places that ramify in K but no place that splits completely in K. For every intermediate field L of K/k we set $\Gamma_L := \mathrm{Gal}(L/k)$ and, if L/k is finite, we write $\mathcal{O}_L^{\Sigma}$ for the subring of L comprising elements that are integral at all places outside those above Σ.

This section aims to introduce the Stickelberger element associated with the special value at 0 of the Dirichlet L-series, as well as the derived complex over which we work to extract arithmetic information. These two objects, representing two aspects of the Iwasawa Main Conjecture, will be the focus of the following section.

For a finite extension F of k in K, the result of [73, Chap. V, Th. 1.2] implies that the sum

$$\theta_F^{\Sigma} := [F:k]^{-1} \sum\nolimits_{\psi \in \mathrm{Hom}(\Gamma_F, \mathbb{Q}_p^{c,\times})} \sum\nolimits_{\gamma \in \Gamma_F} \psi(\gamma^{-1}) L_{\Sigma}(\psi, 0)$$

is a well-defined element of $\mathbb{Z}_p[\Gamma_F]$, where $L_\Sigma(\psi, 0)$ denotes the value at 0 of the Σ-truncated Dirichlet L-series of ψ (here we use that, in terms of the notation of loc. cit., θ_F^{Σ} is equal to $\Theta_\Sigma(1)$ and, as $p = \mathrm{char}(k)$, the integer e is prime to p). In addition, the behaviour of Dirichlet L-series under inflation of characters implies the elements θ_F^{Σ} are compatible with respect to the projection maps $\mathbb{Z}_p[\Gamma_{F'}] \to \mathbb{Z}_p[\Gamma_F]$ for any finite extension F' of k in K with $F \subset F'$ and so, for each extension L of k in K, one obtains a well-defined element of $\mathbb{Z}_p[[\Gamma_L]]$ by setting

$$\theta_L^\Sigma := \varprojlim_{U \in \mathcal{U}(\Gamma_L)} \theta_{L^U}^\Sigma.$$

For each such L, we also set

$$H^1((\mathcal{O}_L^\Sigma)_{W\text{ét}}, \mathbb{Z}_p(1)) := \varprojlim_{U \in \mathcal{U}(\Gamma_L)} \left(\mathbb{Z}_p \otimes_{\mathbb{Z}} H^1((\mathcal{O}_{L^U}^\Sigma)_{W\text{ét}}, \mathbb{G}_m)\right)$$

and both

$$\mathrm{Pic}^0(L)_p := \varprojlim_{U \in \mathcal{U}(\Gamma_L)} (\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathrm{Pic}^0(L^U)) \quad \text{and} \quad \mathrm{Cl}(\mathcal{O}_L^\Sigma)_p := \varprojlim_{U \in \mathcal{U}(\Gamma_L)} (\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathrm{Cl}(\mathcal{O}_{L^U}^\Sigma)),$$

where $(-)_{W\text{ét}}$ denotes the Weil-étale site and $\mathrm{Pic}^0(L^U)$ the degree zero divisor class group of L^U, and the respective limits are with respect to the natural corestriction and norm maps.

We next recall some general facts about Weil-étale cohomology. For a commutative Noetherian ring Λ, we write $\mathsf{D}(\Lambda)$ for the derived category of complexes of Λ-modules and $\mathsf{D}^{\mathrm{perf}}(\Lambda)$ for the full triangulated subcategory of $\mathsf{D}(\Lambda)$ comprising complexes isomorphic to a bounded complex of finitely generated projective Λ-modules.

For a finite extension F of k in K we also write C_F for the unique geometrically irreducible smooth projective curve with function field F and j_F^Σ for the natural open immersion $\mathrm{Spec}(\mathcal{O}_F^\Sigma) \to C_F$. We then define an object of $\mathsf{D}(\mathbb{Z}_p[\Gamma_F])$ by setting

$$D_{F,\Sigma}^\bullet := \mathsf{R}\mathrm{Hom}_{\mathbb{Z}_p}(\mathsf{R}\Gamma((C_F)_{\text{ét}}, j_{F,!}^\Sigma(\mathbb{Z}_p)), \mathbb{Z}_p[-2]).$$

We recall that $D_{F,\Sigma}^\bullet$ belongs to $\mathsf{D}^{\mathrm{perf}}(\mathbb{Z}_p[\Gamma_F])$ (cf. [16, Lem. 3.3]), and also that there exist canonical isomorphisms

$$\begin{aligned} H^1(D_{F,\Sigma}^\bullet) &\cong \mathbb{Z}_p \otimes_{\mathbb{Z}} H^1(\mathsf{R}\mathrm{Hom}_{\mathbb{Z}}(\mathsf{R}\Gamma((C_F)_{W\text{ét}}, j_{F,!}^\Sigma(\mathbb{Z})), \mathbb{Z}[-2])) \\ &\cong \mathbb{Z}_p \otimes_{\mathbb{Z}} H^1((\mathcal{O}_F^\Sigma)_{W\text{ét}}, \mathbb{G}_m) = H^1((\mathcal{O}_F^\Sigma)_{W\text{ét}}, \mathbb{Z}_p(1)). \end{aligned} \tag{4.6}$$

Here the first isomorphism is a consequence of Proposition 4.1.8 and the second of the duality theorem 4.1.14 in Weil-étale cohomology and the equality follows directly from our definition of $H^1((\mathcal{O}_F^\Sigma)_{W\acute{e}t}, \mathbb{Z}_p(1))$.

We next recall (from the proof of [16, Prop. 4.1]) that $D^\bullet_{F,\Sigma}$ is acyclic in degrees greater than one and such that, for each intermediate field F' of F/k, there is exists a canonical projection formula isomorphism $\mathbb{Z}_p[\Gamma_{F'}] \otimes^{\mathsf{L}}_{\mathbb{Z}_p[\Gamma_F]} D^\bullet_{F,\Sigma} \cong D^\bullet_{F',\Sigma}$ in $\mathsf{D}(\mathbb{Z}_p[\Gamma_{F'}])$. These facts combine with (4.6) to imply that the natural corestriction map $H^1((\mathcal{O}_F^\Sigma)_{W\acute{e}t}, \mathbb{G}_m) \to H^1((\mathcal{O}_{F'}^\Sigma)_{W\acute{e}t}, \mathbb{G}_m)$ induces a canonical isomorphism of $\mathbb{Z}_p[\Gamma_{F'}]$-modules

$$\mathbb{Z}_p[\Gamma_{F'}] \otimes_{\mathbb{Z}_p[\Gamma_F]} H^1((\mathcal{O}_F^\Sigma)_{W\acute{e}t}, \mathbb{Z}_p(1)) \cong H^1((\mathcal{O}_{F'}^\Sigma)_{W\acute{e}t}, \mathbb{Z}_p(1)). \tag{4.7}$$

Remark 4.2.6. *Some explicit relations between the complexes $D^\bullet_{F,\Sigma}$ and leading terms of Σ-truncated Artin L-series have already been established elsewhere. In the case of finite abelian extensions F/k, these relations are obtained by the main result of Lai, Tan and Burns in [16] and in the case of arbitrary finite Galois extensions F/k by the main result of Burns and Kakde in [18].*

4.3 The structural result of the Weil-étale cohomology group

In this section, we next fix a $\mathbb{Z}_p$-basis $\{\gamma_i\}_{i\in\mathbb{N}}$ of $\mathbb{Z}_p^{\mathbb{N}}$ (as at the beginning of §4.2.1) and, for each $n \in \mathbb{N}$, write $\Gamma(n)$ for the $\mathbb{Z}_p$-module generated by $\{\gamma_i\}_{i>n}$ and K_n for the fixed field of $\Gamma(n)$ in K (so that Γ_{K_n} is isomorphic to $\mathbb{Z}_p^n \times G$). We also write Γ_v for the decomposition group in Γ of each v in Σ and consider the following condition on K and Σ.

Hypothesis 4.3.1. *There exists a natural number n_0 such that, for every v in Σ, the group $\Gamma(n_0) \cap \Gamma_v$ is not open in Γ_v.*

We note that this hypothesis is satisfied in the setting of the main results of both Anglès et al [3] and Bley and Popescu [12] and hence that the structural aspects of the next result complement these earlier results (for more details see the discussions in Remarks 4.4.2 and 4.4.3 below).

We use the fixed basis $\{\gamma_i\}_{i\in\mathbb{N}}$ of $\mathbb{Z}_p^{\mathbb{N}}$ to identify the completed p-adic group ring $\mathbb{Z}_p[[\Gamma]]$ with the group ring $\mathcal{A} = \mathcal{R}[G]$ of G over the power series ring $\mathcal{R} = \mathbb{Z}_p[[\mathbb{Z}_p^{\mathbb{N}}]]$. In the sequel we shall thereby regard the inverse limit

$$M := H^1((\mathcal{O}_K^{\Sigma})_{W\text{ét}}, \mathbb{Z}_p(1))$$

as an $\mathcal{A}$-module.

Finally, for each n we set $\mathcal{A}_n := \mathcal{R}_n[G] \cong \mathbb{Z}_p[[\Gamma_{K_n}]]$ and $M_{(n)} := \mathcal{A}_n \otimes_{\mathcal{A}} M$.

Theorem 4.3.2 (Iwasawa Main Conjecture)**.** *The $\mathcal{A}$-module M has the following properties.*

(i) M is quadratically-presented and, for every n, the $\mathcal{A}_n$-module $M_{(n)}$ is isomorphic to $H^1((\mathcal{O}_{K_n}^{\Sigma})_{W\text{ét}}, \mathbb{Z}_p(1))$.

In the remainder of the result we assume that K and Σ satisfy Hypothesis 4.3.1.

(ii) M is torsion and $\mathcal{P}_{\mathcal{A}}(M)$ is finite.

(iii) If $|G|$ does not belong to any prime in $\mathcal{P}_{\mathcal{A}}(M)$, then there exists a pseudo-isomorphism of $\mathcal{A}$-modules of the form

$$M \to \bigoplus_{\mathfrak{p}\in\mathcal{P}_{\mathcal{A}}(M)} \bigoplus_{1\le i\le n(\mathfrak{p})} \mathcal{A}/\mathfrak{p}^{e(\mathfrak{p})_i}$$

(for suitable natural numbers $n(\mathfrak{p})$ and $e(\mathfrak{p})_i$). Setting $e(\mathfrak{p})$:=

$\sum_{1\le i\le n(\mathfrak{p})} e(\mathfrak{p})_i$ *for each* $\mathfrak{p}\in\mathcal{P}_A(M)$*, one also has*

$$\prod\nolimits_{\mathfrak{p}\in\mathcal{P}_{\mathcal{A}}(M)}\mathfrak{p}^{e(\mathfrak{p})}\subseteq\bigcap\nolimits_{\mathfrak{q}\in\mathcal{P}_R}\big(\prod\nolimits_{\mathfrak{p}\in\mathcal{P}_{\mathcal{A}}(M)}\mathfrak{p}^{e(\mathfrak{p})}\big)_{\mathfrak{q}}=\mathcal{A}\cdot\theta_K^{\Sigma},\tag{4.8}$$

with equality if and only if $\prod_{\mathfrak{p}\in\mathcal{P}_{\mathcal{A}}(M)}\mathfrak{p}^{e(\mathfrak{p})}$ *is a principal ideal of* $\mathcal{A}$*.*

(iv) If $|G|$ *is prime to* p*, then the inclusion in (4.8) is an equality and, in addition, for every* $n\ge n_0$ *the* $\mathcal{A}_n$*-modules*

$$H^1((\mathcal{O}^{\Sigma}_{K_{n+1}})_{W\text{ét}},\mathbb{Z}_p(1))^{X_{n+1}=0}\quad\textit{and}\quad \mathrm{Cl}(\mathcal{O}^{\Sigma}_{K_{n+1}})_p^{X_{n+1}=0}$$

are both pseudo-null.

The proof of these results will occupy the remainder of this section.

Proof. At the outset we fix an exhaustive separated decreasing filtration $(\Delta_n)_{n\in\mathbb{N}}$ of the subgroup $\mathbb{Z}_p^{\mathbb{N}}$ of Γ by open subgroups. We set $F_n:=K^{\Delta_n}$, write J_n for the kernel of the natural projection map

$$\mathcal{A}\twoheadrightarrow\mathcal{A}_{[n]}:=\mathbb{Z}_p[\Gamma_{F_n}]=\mathbb{Z}_p[\Gamma/\Delta_n]\cong\mathbb{Z}_p[(\mathbb{Z}_p^{\mathbb{N}}/\Delta_n)][G],$$

and for each $\mathcal{A}$-module N, respectively homomorphism of $\mathcal{A}$-modules θ, we set $N_{[n]}:=\mathcal{A}_{[n]}\otimes_{\mathcal{A}}N$ and $\theta_{[n]}:=\mathrm{id}_{\mathcal{A}_{[n]}}\otimes_{\mathcal{A}}\theta$. Then

$$J_\bullet:=(J_n)_{n\in\mathbb{N}}$$

is a separated decreasing filtration with respect to which $\mathcal{A}$ is complete. In addition, the isomorphisms (4.7) with F/F' equal to each F_n/F_{n-1} imply the $\mathcal{A}$-module M is $J_\bullet$-complete and that, for every n, there is a natural isomorphism $M_{[n]}\cong H^1((\mathcal{O}^{\Sigma}_{F_n})_{W\text{ét}},\mathbb{Z}_p(1))$.

Turning now to the proof of Theorem 4.3.2, we first observe the isomorphisms in the second assertion of (i) are directly induced by the descent isomorphisms

(4.7). We then claim that, to prove the quadratic-presentability of M (and hence complete the proof of (i)), it suffices to inductively construct, for every n, an exact commutative diagram of $\mathcal{A}_{[n]}$-modules

$$\begin{array}{ccccccc} \mathcal{A}_{[n]}^d & \xrightarrow{\theta_n} & \mathcal{A}_{[n]}^d & \xrightarrow{\pi_n} & M_{[n]} & \longrightarrow & 0 \\ \tau_n^0 \downarrow & & \tau_n^1 \downarrow & & \tau_n \downarrow & & \\ \mathcal{A}_{[n-1]}^d & \xrightarrow{\theta_{n-1}} & \mathcal{A}_{[n-1]}^d & \xrightarrow{\pi_{n-1}} & M_{[n-1]} & \longrightarrow & 0 \end{array} \tag{4.9}$$

in which the natural number d is independent of n, all maps π_n and τ_n^0 are surjective and τ_n^1 and τ_n are the tautological projections. To justify this reduction we use the fact that Δ_{n-1}/Δ_n is a finite p-group and hence that the kernel of the projection $\mathcal{A}_{[n]} \to \mathcal{A}_{[n-1]}$ is contained in the Jacobson radical of (the finitely generated $\mathbb{Z}_p$-algebra) $\mathcal{A}_{[n]}$. This in turn implies that the natural maps $\mathrm{GL}_d(\mathcal{A}_{[n]}) \to \mathrm{GL}_d(\mathcal{A}_{[n-1]})$ are surjective and therefore, since $\mathcal{A}$ is $J_\bullet$-complete, that the inverse limit of $\mathcal{A}_{[n]}^d$ with respect to the maps τ_n^0 is isomorphic to $\mathcal{A}^d$. Then, since M is also $J_\bullet$-complete (and the inverse limit functor is exact on the category of finitely generated $\mathbb{Z}_p$-modules), by passing to the limit over n of the above diagrams one obtains an exact sequence of $\mathcal{A}$-modules

$$\mathcal{A}^d \xrightarrow{\theta} \mathcal{A}^d \xrightarrow{\pi} M \to 0 \tag{4.10}$$

(with $\theta = \varprojlim_n \theta_n$ and $\pi = \varprojlim_n \pi_n$) which shows directly that M is quadratically-presented.

To complete the proof of (i), we must therefore construct the diagrams (4.9). To do this, we note that F_1 is a finite extension of k and hence that $M_{[1]} \cong H^1((\mathcal{O}_{F_1}^{\Sigma})_{W\acute{e}t}, \mathbb{Z}_p(1))$ is finitely generated over $\mathcal{A}_{[1]}$ (this follows, for example, from (4.6) and the fact $D^{\bullet}_{F_1,\Sigma}$ belongs to $\mathsf{D}^{\mathrm{perf}}(\mathcal{A}_{[1]})$). We can therefore fix a natural number d and a subset $\{m_i\}_{1\le i\le d}$ of M whose image in $M_{[1]}$ generates $M_{[1]}$ over $\mathcal{A}_{[1]}$. For each n, we write $m_{i,n}$ for the projection of m_i to $M_{[n]}$. We then note that, just as above, the kernel of the projection $\mathcal{A}_{[n]} \to \mathcal{A}_{[1]}$ lies in the Jacobson radical of the (Noetherian) ring $\mathcal{A}_{[n]}$, and hence that the tautological isomorphism $\mathcal{A}_{[1]} \otimes_{\mathcal{A}_{[n]}} M_{[n]} \cong M_{[1]}$ combines with Nakayama's Lemma and our choice of elements $\{m_i\}_{1\leq i\leq d}$ to imply $\{m_{i,n}\}_{1\leq i\leq d}$ generates the $\mathcal{A}_{[n]}$-module $M_{[n]}$. We therefore obtain the right hand commutative square in (4.9) by defining π_n (and similarly π_{n-1}) to be the map of $\mathcal{A}_{[n]}$-modules that sends the i-th element in the standard basis of $\mathcal{A}_{[n]}^d$ to $m_{i,n}$.

By following the argument of [16, Prop. 4.1] it now follows that $D^\bullet_{F_n,\Sigma}$ can be represented by a complex of the form $P_n \xrightarrow{\theta_n} \mathcal{A}_{[n]}^d$ in which P_n is a finitely generated projective $\mathcal{A}_{[n]}$-module (placed in degree zero), $\mathrm{im}(\theta_n) = \ker(\pi_n)$ and π_n induces an isomorphism between $\mathrm{coker}(\theta_n)$ and $M_{[n]}$. Then, since $\mathcal{A}_{[n]}$ is a finite product of local rings and the $\mathcal{A}_{[n]}$-equivariant Euler characteristic of $D^\bullet_{F_n,\Sigma}$ vanishes (by Flach [40, Th. 5.1]), the $\mathcal{A}_{[n]}$-module P_n is free of rank d (and so, after changing θ_n if necessary, can be taken to be $\mathcal{A}_{[n]}^d$). In particular, if we choose both of the rows in (4.9) in this way, then they are exact and so the commutativity of the right hand square reduces us to proving the existence of a surjective map τ_n^0 that makes the left hand square commute. To do this we can first choose a morphism of $\mathcal{A}_{[n-1]}$-modules $\tau_n' : (\mathcal{A}_{[n]}^d)_{[n-1]} \to \mathcal{A}_{[n-1]}^d$ for which the associated diagram

$$\begin{array}{ccc} (\mathcal{A}_{[n]}^d)_{[n-1]} & \xrightarrow{(\theta_n)_{[n-1]}} & (\mathcal{A}_{[n]}^d)_{[n-1]} \\ \tau_n' \downarrow & & \cong \downarrow (\tau_n^1)_{[n-1]} \\ \mathcal{A}_{[n-1]}^d & \xrightarrow{\theta_{n-1}} & \mathcal{A}_{[n-1]}^d \end{array}$$

commutes and represents the canonical isomorphism $\mathcal{A}_{[n-1]} \otimes^{\mathsf{L}}_{\mathcal{A}_{[n]}} D^\bullet_{F_n,\Sigma} \cong D^\bullet_{F_{n-1},\Sigma}$. In particular, since the morphism of complexes represented by this diagram is a quasi-isomorphism and $(\tau_n^1)_{[n-1]}$ is bijective, the map τ_n' must also be bijective. The composite map

$$\tau_n^0 : \mathcal{A}_{[n]}^d \twoheadrightarrow (\mathcal{A}_{[n]}^d)_{[n-1]} \xrightarrow{\tau_n'} \mathcal{A}_{[n-1]}^d$$

(in which the first map is the tautological projection) is then surjective and such that the diagram (4.9) commutes. This completes the proof of (i).

In the rest of the argument we assume that K and Σ satisfy Hypothesis 4.3.1.

To prove (ii) we note that, by Proposition 2.3.3(iii)(b), M is a torsion $\mathcal{R}$-module if and only if it is a torsion $\mathcal{A}$-module. The exact sequence (4.10) therefore implies that M is a torsion $\mathcal{R}$-module if and only if $\det(\theta)$ is a non-zero divisor of $\mathcal{A}$. To investigate this condition, we recall that, for each n, K_n denotes $K^{\Gamma(n)}$ and we set $\Gamma_n := \Gamma/\Gamma(n) = \mathrm{Gal}(K_n/k)$ so that $\mathcal{A}_n = \mathbb{Z}_p[[\Gamma_n]]$. We also write $I_\bullet := (I_n)_{n\in\mathbb{N}}$ for the separated decreasing filtration of $\mathcal{A}$ in which each I_n is the kernel of the natural projection map $\rho_{\langle n\rangle} : \mathcal{A} \to \mathcal{A}_n$.

Then, for every $n \geq n_0$, Hypothesis 4.3.1 implies that the decomposition subgroup in Γ_n of every place in Σ is infinite. Hence, for each such n, the results of [16, Prop. 4.1 and Prop. 4.4] combine to imply that $\rho_{\langle n\rangle}(\det(\theta))$ and $\theta^{\Sigma}_{K_n}$ are non-zero divisors of $\mathcal{A}_n$ such that

$$\mathcal{A}_n \cdot \rho_{\langle n\rangle}(\det(\theta)) = \mathcal{A}_n \cdot \theta^{\Sigma}_{K_n}. \tag{4.11}$$

This implies, in particular, that $\det(\theta) = (\rho_{\langle n\rangle}(\det(\theta)))_{n\geq n_0}$ is a non-zero divisor in the ring $\mathcal{A} = \varprojlim_n \mathcal{A}_n = \varprojlim_{n\geq n_0} \mathcal{A}_n$, and so the first assertion of (ii) is proved. In addition, the fact that $\mathcal{P}_{\mathcal{A}}(M)$ is finite follows directly from Lemma 4.2.1(i) and Proposition 2.3.3(iii)(c). This completes the proof of (ii).

To prove (iii), we note first that the results of (i) and (ii) combine with Lemma 4.2.1(ii) to imply, under the stated hypotheses, that M is a finitely-presented, admissible, torsion $\mathcal{A}$-module. From Theorem 2.2.3(b), we can therefore deduce the existence of a pseudo-isomorphism of $\mathcal{A}$-modules of the form

$$M \to \bigoplus_{\mathfrak{p}\in\mathcal{P}_{\mathcal{A}}(M)} \bigoplus_{1\leq i\leq n(\mathfrak{p})} \mathcal{A}/\mathfrak{p}^{e(\mathfrak{p})_i}$$

for suitable natural numbers $n(\mathfrak{p})$ and $e(\mathfrak{p})_i$. Upon setting $e(\mathfrak{p}) := \sum_{1\leq i\leq n(\mathfrak{p})} e(\mathfrak{p})_i$ and combining this pseudo-isomorphism with the explicit definition of the lower generalised characteristic ideal $\mathrm{char}_{\mathcal{A}}(M)$ (and the result of

Proposition 3.1.2(i)(a)) one then obtains an equality

$$\prod\nolimits_{\mathfrak{p}\in\mathcal{P}_{\mathcal{A}}(M)} \mathfrak{p}^{e(\mathfrak{p})} = \mathrm{char}_{\mathcal{A}}(M).$$

Next we note that, as $\rho_{\langle n\rangle}(\det(\theta))$ is a non-zero divisor for each $n \geq n_0$, the equality (4.11) implies the existence for each such n of an element u_n of $\mathcal{A}_n^\times$ with $\rho_{\langle n\rangle}(\det(\theta)) = u_n \cdot \theta^\Sigma_{K_n}$. In particular, the family $u := (u_n)_{n\geq n_0}$ belongs to $\mathcal{A}^\times = \varprojlim_{n\geq n_0} \mathcal{A}_n^\times$ and is such that $\det(\theta) = u \cdot \theta^\Sigma_K$. From the resolution (4.10) one therefore has

$$\mathrm{Fit}^0_{\mathcal{A}}(M) = \mathcal{A}\cdot\det(\theta) = \mathcal{A}\cdot\theta^\Sigma_K.$$

Given the last two displayed equalities, all of the claims in (iii) follow directly from Proposition 3.1.2(i)(b).

To prove (iv) we assume $|G|$ is prime to p and adapt the argument of Proposition 4.2.4. Specifically, in this case every prime in $\mathcal{P}_{\mathcal{A}}$ is principal since $\mathcal{A}$ is a finite direct product of unique factorisation domains. The first assertion of (iv) therefore follows directly from the final assertion of (iii). To prove the remaining assertions in (iv), we note that the resolution (4.10) combines with the isomorphisms in (i) to imply that, for each n, the $\mathcal{A}_n$-module $\mathrm{cok}(\mathrm{id}_{\mathcal{A}_n}\otimes_{\mathcal{A}}\theta) \cong \mathcal{A}_n\otimes_{\mathcal{A}} M = M_{(n)}$ is isomorphic to $H^1((\mathcal{O}^\Sigma_{K_n})_{W\acute{e}t}, \mathbb{Z}_p(1))$.

In particular, if $n \geq n_0$, then the latter module is torsion since it is annihilated by the non-zero divisor $\det(\mathrm{id}_{\mathcal{A}_n}\otimes_{\mathcal{A}}\theta) = \rho_{\langle n\rangle}(\det(\theta))$ of $\mathcal{A}_n$. Given this, the pseudo-nullity of $H^1((\mathcal{O}^\Sigma_{K_{n+1}})_{W\acute{e}t}, \mathbb{Z}_p(1))^{X_{n+1}=0}$ follows directly from the argument of Proposition 4.2.4(i). The $\mathcal{A}_n$-module $\mathrm{Cl}(\mathcal{O}^\Sigma_{K_{n+1}})_p^{X_{n+1}=0}$ is then also pseudo-null since, after taking account of the isomorphisms (4.6), the exact sequence [16, (4)] (with the field K in loc. cit. taken to be K_{n+1}) gives a canonical identification of $\mathrm{Cl}(\mathcal{O}^\Sigma_{K_{n+1}})_p$ with a submodule of $H^1((\mathcal{O}^\Sigma_{K_{n+1}})_{W\acute{e}t}, \mathbb{Z}_p(1))$. $\square$

4.4 Some applications

Theorem 4.3.2 has the following concrete consequence for the $\mathcal{A}$-module $\mathrm{Pic}^0(K)_p$.

Corollary 4.4.1. *Assume K and Σ satisfy Hypothesis 4.3.1. Then $\mathrm{Pic}^0(K)_p$ is a torsion $\mathcal{R}$-module. In addition, if $\mathrm{Pic}^0(K)_p$ is finitely generated over $\mathcal{R}$, then at most one place that ramifies in K has an open decomposition subgroup in Γ and, if such a place v exists, then one has $\Gamma_v = \Gamma$.*

Proof. For each subset Σ' of Σ we write $\epsilon_{\Sigma'}$ for the canonical projection map $\bigoplus_{v\in\Sigma'}\mathbb{Z}_p[[\Gamma/\Gamma_v]] \to \mathbb{Z}_p$. Then, by taking the inverse limit over n of the exact sequences [16, (4)] used above (for the fields K_{n+1}), one obtains an exact sequence of $\mathcal{A}$-modules

$$0 \to \mathrm{Cl}(\mathcal{O}_K^{\Sigma})_p \to M \to \ker(\epsilon_\Sigma) \to 0. \tag{4.12}$$

In a similar way, the corresponding limits of the exact sequences [16, (5) and (6)] combine to give an exact sequence of $\mathcal{A}$-modules

$$\ker(\epsilon_{\Sigma^K_{\mathrm{fin}}}) \to \mathrm{Pic}^0(K)_p \to \mathrm{Cl}(\mathcal{O}_K^{\Sigma})_p \to \mathbb{Z}_p/(n_K) \to 0, \tag{4.13}$$

in which Σ^K_{fin} is the subset of Σ comprising places that have finite residue degree in K/k and n_K is a (possibly zero) integer.

We now assume that Hypothesis 4.3.1 is satisfied. In this case the $\mathcal{A}$-module M is finitely-presented and torsion (by Theorem 4.3.2(i) and (ii)) and the $\mathcal{A}$-module $\ker(\epsilon_{\Sigma^K_{\mathrm{fin}}})$ is torsion. The first of these facts combines with the sequence (4.12) to imply both that the $\mathcal{A}$-module $\mathrm{Cl}(\mathcal{O}_K^{\Sigma})_p$ is torsion and also (by using Proposition 1.7.4, 2) and 3)) that it is finitely generated if and only if the $\mathcal{A}$-module $\ker(\epsilon_\Sigma)$ is finitely-presented. From the sequence (4.13) we can then also deduce that $\mathrm{Pic}^0(K)_p$ is a torsion $\mathcal{A}$-module (and hence a torsion $\mathcal{R}$-module) and also that $\mathrm{Cl}(\mathcal{O}_K^\Sigma)_p$ is finitely generated (over $\mathcal{A}$) if $\mathrm{Pic}^0(K)_p$ is finitely generated over $\mathcal{R}$.

To complete the proof we now argue by contradiction and, for this, the above observations imply it is enough to assume both that $\ker(\epsilon_\Sigma)$ is finitely-presented (over $\mathcal{A}$) and that there are either two places v_1 and v_2 in Σ such that Γ_{v_1} and Γ_{v_2} are open, or at least one place v_1 in Σ for which Γ_{v_1} is open and not equal to Γ. We then define an open subgroup of Γ by setting $\Gamma' := \Gamma_{v_1} \cap \Gamma_{v_2}$ in the first case and $\Gamma' := \Gamma_{v_1}$ in the second case, we set $\mathcal{A}' := \mathbb{Z}_p[[\Gamma']]$ and we write I and I' for the kernels of the respective canonical projection maps $\mathcal{A} \to \mathbb{Z}_p$ and $\mathcal{A}' \to \mathbb{Z}_p$.

Then the definition of Γ' ensures that the $\mathcal{A}'$-module $\ker(\epsilon_\Sigma)$ is both finitely-presented and contains a direct summand that is isomorphic to the trivial module $\mathbb{Z}_p$. This implies (via Proposition 1.7.4, 4)) that $\mathbb{Z}_p$ is finitely-presented as an $\mathcal{A}'$-module and hence, by applying Proposition 1.7.1 to the tautological short exact sequence

$$0 \to I' \to \mathcal{A}' \to \mathbb{Z}_p \to 0,$$

that I' is finitely generated over $\mathcal{A}'$. However, writing d for the order of Γ/Γ', there exists an exact sequence of $\mathcal{A}'$-modules

$$0 \to (I')^d \to I \to \mathbb{Z}_p^{d-1}$$

and so one can deduce that I is finitely generated over $\mathcal{A}'$, and hence also over $\mathcal{R}$. However, this last assertion is easily shown to be false and this contradiction completes the proof of Corollary 4.4.1. □

Remark 4.4.2. *Assume that K is a Carlitz-Hayes cyclotomic extension of k, as considered by Anglès et al in [3]. In this case $\Gamma = \mathbb{Z}_p^{\mathbb{N}}$ (so $\mathcal{A} = \mathcal{R}$) and $\Sigma = \{v\}$ with v a place that is totally ramified in K. Hence $\Gamma_v = \Gamma$ (so that Hypothesis 4.3.1 is clear) and, as v is totally ramified in K, for each $U \in \mathcal{U}(\Gamma)$*

the integers c^U and m^U_Σ that occur in [16, (5)] are both equal to 1 *and so (4.13) is valid with $n_K = 1$. Thus, in this case, the exact sequences (4.12) and (4.13) combine to induce identifications $M = \mathrm{Cl}(\mathcal{O}_K^\Sigma)_p = \mathrm{Pic}^0(K)_p$.*

In addition, since M is quadratically-presented as an $\mathcal{R}$-module (by (4.10)), the results of Proposition 3.1.2(i)(b) (with G trivial and $R = \mathcal{R}$) and Proposition 4.2.4(ii) (with G trivial) imply that the generalised characteristic ideal $char_{\mathcal{R}}(M)$ coincides both with $\mathrm{Fit}^0_{\mathcal{R}}(M)$ and with the pro-characteristic ideal $\widetilde{\mathrm{Ch}}_{\mathcal{R}}(M)$ of M defined in [7]. Given this, one finds that the explicit structural information concerning M that is provided by claims (iii) and (iv) of Theorem 4.3.2 strengthens the main results of [3] concerning $\mathrm{Pic}^0(K)_p$ (see, in particular, [3, Th. 5.2, Rem. 5.3]).

Remark 4.4.3. *Assume that K is a Drinfeld modular tower extension L_∞ of k of the form specified by Bley and Popescu in [12, §2.2]. In this case $\mathcal{A} = \mathcal{R}[G]$ with G isomorphic to $\mathrm{Gal}(H_{\mathfrak{fp}}/k)$ for a 'real' ray class field $H_{\mathfrak{fp}}$ of k relative to a fixed prime ideal $\mathfrak{p}$ and integral ideal $\mathfrak{f}$. The set Σ therefore comprises $\mathfrak{p}$ and the set of prime divisors of $\mathfrak{f}$, and so the validity of Hypothesis 4.3.1 in this case follows from the argument of [12, Prop. 3.22]. We now assume that $p\mathcal{R} \notin \mathcal{P}_{\mathcal{R}}(M)$ if p divides $|G|$. Then the arguments of Proposition 3.1.2(i)(b) and Theorem 4.3.2(iii) combine to imply that the explicit ideal $\prod_{\mathfrak{p}\in\mathcal{P}_{\mathcal{A}}(M)}\mathfrak{p}^{e(\mathfrak{p})}$ that occurs as the first term in (4.8) is contained in $\mathrm{Fit}^0_{\mathcal{A}}(M)$, with equality if and only if it is principal (as occurs automatically if $|G|$ is prime to p). Further, by comparing the sequence (4.12) to the sequences of [12, (24), (25), (26)], and using the fact $\mathcal{A}_{\mathfrak{p}}$ is a discrete valuation ring for $\mathfrak{p} \in \mathcal{P}_{\mathcal{A}}(M)$, one verifies an equality of principal $\mathcal{A}$-ideals*

$$\mathrm{Fit}^0_{\mathcal{A}}(M) = \mathrm{Fit}^0_{\mathcal{A}}(T_p(M_\Sigma^{(\infty)})_\Gamma).$$

Here the $\mathcal{A}$-module $T_p(M_\Sigma^{(\infty)})_\Gamma$ is (quadratically-presented and) defined in [12, §3.3] as an inverse limit $\varprojlim_n T_p(M_\Sigma^{(n)})_\Gamma$ over the p-adic Tate modules of a canonical family of Picard 1*-motives. In particular, as the main result [12,* *Th. 1.3] (with $S = \Sigma$) of loc. cit. concerning Stickelberger elements and divisor class groups is an equality*

$$\mathcal{A} \cdot \theta_K^\Sigma = \mathrm{Fit}^0_{\mathcal{A}}(T_p(M_\Sigma^{(\infty)})_\Gamma),$$

it is strengthened by the explicit structural results obtained in Theorem 4.3.2(iii) and (iv). Finally, we note that if $\mathfrak{p}$ decomposes in the field $H_{\mathfrak{f}\mathfrak{p}}$, then Corollary 4.4.1 implies that $\mathrm{Pic}^0(L_\infty)_p$ cannot be finitely generated as an $\mathcal{R}$-module. This observation implies, in particular, that the non-splitting hypotheses on $\mathfrak{p}$ that are imposed in the results of [12, Th. 3.16 and Th. 3.17] are actually necessary for the stated conclusions to be valid.

Chapter 5

Outlook on the future development

When we establish the theory for $\mathbb{Z}_p^{\mathbb{N}}$-extensions, we find two meaningful questions still waiting for exploring in the future.

Q1: **Is the ring $\mathbb{Z}_p[[\mathbb{Z}_p^{\mathbb{N}}]]$ coherent? Or as a fallback, is the ring n-coherent?**

The definition of n-coherent rings can be found in Definition 6.0.3, and motivation for studying this property is discussed following Theorem 6.0.7. The main difficulty in analyzing this question comes from the structure of the Iwasawa algebra

$$\mathbb{Z}_p[[\mathbb{Z}_p^{\mathbb{N}}]] \cong \varprojlim_n \mathbb{Z}_p[[X_1, \ldots, X_n]].$$

This inverse limit is strictly larger than the I-adic completion of the polynomial ring $\mathbb{Z}_p[X_1, X_2, \ldots]$, where $I = (p, X_1, X_2, \ldots)$. In the I-adic completion each element is represented by a formal power series $\sum_\alpha a_\alpha X^\alpha$ such that, for every integer $d \geq 0$, only finitely many monomials of total degree $\leq d$ have non-zero coefficient. By contrast, in $\mathbb{Z}_p[[\mathbb{Z}_p^{\mathbb{N}}]]$ there exist elements whose components of a fixed degree involve infinitely many variables. For example, the compatible family

$$f_n = X_1 + \cdots + X_n \in \mathbb{Z}_p[[X_1, \ldots, X_n]]$$

defines an element of $\mathbb{Z}_p[[\mathbb{Z}_p^{\mathbb{N}}]]$ which one may heuristically denote by $\sum_{i\geq 1} X_i$. Its degree-1 part has a non-zero coefficient at every variable X_i, so it does not belong to the usual formal power series ring obtained as the I-adic completion of $\mathbb{Z}_p[X_1, X_2, \ldots]$. Currently, we do not have a method for effectively handling such terms.

Q2: **Can we find arithmetic applications for our $\mathbb{Z}_p[[\mathbb{Z}_p^{\mathbb{N}}]]$-theory over number fields?**

Thanks to a valuable comment from Meng Fai Lim, we discovered that the answer to this question is affirmative. A notable example is provided by Mináč, Rogelstad and Tân [60]. Let F be a number field satisfying the following condition.

If p is odd then F contains a primitive p-th root of unity ζ_p. If $p = 2$ then F contains a primitive fourth root ζ_4 of unity.

We define

$$CR(F) = F\left(\sqrt[p^\infty]{F^\times}\right) := \bigcup F\left(\sqrt[p^m]{a}, \zeta_{p^m}\right).$$

The union is taken over all positive integers m and all elements $a \in F^\times$. The field $CR(F)$ is called the p-cyclotomic radical extension of F. Then the following theorem has been proven in [60, Appendix, Thm A.1].

Proposition 5.0.1. *Let F be a field containing μ_{p^∞}. Let I be a set of cardinality of a basis for $F^\times/(F^\times)^p$ over $\mathbb{F}_p$. Then*

$$\mathrm{Gal}(CR(F)/F) \simeq \langle \tau_i, i \in I \mid [\tau_i, \tau_j] = 1, \forall i, j \in I\rangle \simeq \prod_{i\in I} \mathbb{Z}_p.$$

It should be noted that the cyclotomic radical extension is closely related to the false Tate extensions. Therefore, it is meaningful and worthwhile to pursue further study on this topic.

Part II: Non-Noetherian study in integral Iwasawa theory

Chapter 6

A review of integral Iwasawa theory

For a commutative ring A and a prime p, the completed group ring $A[[\mathbb{Z}_p]]$ is defined as the inverse limit $\varprojlim_n A[\mathbb{Z}/(p^n)]$, where the transition morphisms $A[\mathbb{Z}/(p^{n+1})] \to A[\mathbb{Z}/(p^n)]$ are the A-linear group ring maps induced by the natural projections $\mathbb{Z}/(p^{n+1}) \to \mathbb{Z}/(p^n)$.

Arithmetic modules over $\mathbb{Z}[[\mathbb{Z}_p]]$ naturally arise as the inverse limits of families of modules in $\mathbb{Z}_p$-towers of global fields. For example, let K be a number field, K_∞ be the cyclotomic extension of K, and consider the field tower

$$K = K_0 \subset K_1 \subset \cdots \subset K_\infty.$$

One can construct the inverse limit $\varprojlim_i \mathrm{Cl}(K_i)$ where the transition maps are induced by the norm maps. There is a natural action of the complete group ring $\mathbb{Z}[[\mathbb{Z}_p]]$ on $\varprojlim_i \mathrm{Cl}(K_i)$. However, $\mathbb{Z}[[\mathbb{Z}_p]]$ is neither a Noetherian ring nor a compact topological ring. Iwasawa addressed this issue by passing to the pro-p completion of $\varprojlim_i \mathrm{Cl}(K_i)$ and working instead over the associated ring $\mathbb{Z}_p[[\mathbb{Z}_p]]$, which is both Noetherian and compact.

But what is the price of Iwasawa's method? The passage to pro-p completion can result in a loss of significant arithmetic information. For instance, one can only obtain an asymptotic formula estimating the growth of the p-part of the ideal class group along the tower, rather than the growth of the entire class group. Intuitively, current Iwasawa theory—which studies the p-part of the ideal class groups—can be seen as a kind of "local theory." In contrast, the integral Iwasawa theory aims to become a more "global theory," capable of capturing information about the full ideal class group by working over complete group rings $\mathbb{Z}[[G]]$, for certain p-adic Lie groups G.

Many researchers have commented on the benefits and challenges of working over $\mathbb{Z}[[\mathbb{Z}_p]]$ or $\mathbb{Z}_\ell[[\mathbb{Z}_p]]$ for a prime $\ell \neq p$ instead of $\mathbb{Z}_p[[\mathbb{Z}_p]]$, or have made efforts to investigate specific aspects of this issue. For example, Washington proved the following theorem in [78].

Theorem 6.0.1. *Let K be an abelian number field and K_∞ the cyclotomic $\mathbb{Z}_p$-extension of K. Let $\ell \neq p$ be a prime and ℓ^{e_n} be the power of ℓ dividing the class number h_n of the K_n in the field tower. Then e_n is bounded independently of n. In fact, e_n is constant for large n.*

However, to the best of the author's knowledge, no better result is currently known. On the other hand, the proof of the theorem 6.0.1 of Washington is not achieved by studying the properties of $\mathbb{Z}_\ell[[\mathbb{Z}_p]]$. In fact, as Washington points out in [77, §VI], very little is known about the structure of modules over $\mathbb{Z}_\ell[[\mathbb{Z}_p]]$ for $\ell \neq p$. Another well-known contribution concerning $\mathbb{Z}[[\mathbb{Z}_p]]$ was made by Coleman [26, §II]. He proved an analogue of the Weierstrass Preparation Theorem for $\mathbb{Z}[[\mathbb{Z}_p]]$, which plays a crucial role in characterizing certain norm-compatible families of units in abelian fields.

As part of the broader puzzle of the integral Iwasawa theory, the first work, [17], was recently published by David Burns and Alexandre Daoud on the *Nagoya Mathematical Journal*. The aim of this article, and of the subsequent articles in the series, is to develop some foundational aspects of a workable theory of arithmetic $\mathbb{Z}[[\mathbb{Z}_p]]$-modules. This overall approach relies crucially on ring-theoretical results, which in turn depend upon a detailed analysis of the category of 'pro-discrete' $\mathbb{Z}[[\mathbb{Z}_p]]$-modules introduced in [17, §3]. In particular, natural 'pro-discrete' versions of both Nakayama's Lemma and Roiter's Lemma are established. Furthermore, the authors provide several explicit criteria for the finite presentability of pro-discrete modules (see [17, Thm. 3.8, Thm. 3.11]). These results are then applied to give an explicit description of the finitely generated prime spectrum of $\mathbb{Z}[[\mathbb{Z}_p]]$ (see [17, Thm. 4.2, Remark 4.3]), which in turn is used to establish a range of natural ring-theoretic properties of $\mathbb{Z}[[\mathbb{Z}_p]]$. To present the most important of these properties, we first introduce some necessary notions.

Definition 6.0.2. *For a non-negative integer n, one says that an R-module M is finitely n-presented if there exists an exact sequence of R-modules*

$$M_n \to M_{n-1} \to \cdots \to M_0 \to M \to 0$$

in which each M_i is both finitely generated and free.

In particular, M is finitely 0-presented, respectively finitely 1-presented, if and only if it is finitely generated, respectively finitely presented. One also says that M is 'finitely ∞-presented' if it is finitely n-presented for every non-negative n. For example, if R is Noetherian, then every finitely generated module is automatically finitely ∞-presented.

Definition 6.0.3. *For each non-negative integer n, the ring R is then said to be 'n-coherent' if every finitely n-presented R-module is finitely $(n+1)$-presented.*

In addition, a ring R is 0-coherent if and only if every finitely generated module is finitely presented, which is easily seen to be equivalent to R being Noetherian. Similarly, R is 1-coherent if and only if every finitely generated ideal is finitely presented, which is equivalent to R being coherent. This notion is further generalized at the beginning of §7.3.3 to accommodate the non-commutative case. We now introduce a related notion from [28, §1].

Definition 6.0.4. *For each pair of non-negative integers n and d, an integral domain R is called a (n, d)-domain if every finitely n-presented module has projective dimension at most d. R is called a strict (n, d)-domain if it is an (n, d)-domain that is neither an $(n-1, d)$-domain nor an $(n, d-1)$-domain.*

The following definition is taken from [32] and [43].

Definition 6.0.5. *An integral domain is called a finite conductor domain if it has the property that the intersection of any two of its principal ideals is finitely generated.*

It is then straightforward to show that any coherent integral domain is automatically a finite conductor domain, though the converse does not hold. The following definition is taken from [71].

Definition 6.0.6. *A commutative ring R is said to have weak Krull dimension equal to n if n is the maximum integer m for which there exists a chain*

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_m$$

of finitely generated prime ideals of R.

By the definition, it is obvious that for a commutative ring R the weak Krull dimension is less than or equal to its Krull dimension. If it is not possible to calculate the Krull dimension, then the weak Krull dimension becomes an acceptable substitute.

Finally, the ring-theoretical property of $\mathbb{Z}[[\mathbb{Z}_p]]$ that we aim to present holds for all prime numbers p, except for finitely many. We call a prime number p exceptional if it satisfies the following three conditions simultaneously:

1. p is irregular.

2. p satisfies Vandiver's Conjecture.

3. The p-adic λ-invariant of every (odd) isotypic component of the ideal class group of $\mathbb{Q}(e^{2\pi i/p})$ is at least $p-1$.

A probabilistic argument due to Lang [54, Chap. 10 App] suggests there are only finitely many exceptional primes. According to the computations of Hart, Wilson and Ong [46], no exceptional primes exist up to the bound 2^{31}. We are now in a position to state the important property of $\mathbb{Z}[[\mathbb{Z}_p]]$ established by Burns and Daoud [17].

Theorem 6.0.7. *The completed integral group ring* $\mathbb{Z}[[\mathbb{Z}_p]]$ *is not a finite conductor ring. However, it is a* 2*-coherent domain of weak Krull dimension* 2 *and if p is not exceptional then it is also a strict* $(2,2)$*-domain.*

We now explain the underlying significance of the algebraic properties involved in Theorem 6.0.7. The property of coherency can be viewed as a suboptimal substitute for Noetherianness, serving at least to ensure that certain arguments in Iwasawa theory still function properly. For instance, it becomes much easier to compute $\mathrm{Ext}^i_\Lambda(M,\Lambda)$ when M is finitely presented over any unital ring Λ (see [62, V. §4]). If Λ is a Noetherian Iwasawa algebra, then every finitely generated Λ-module is finitely presented. This allows one to leverage the advantages of finite presentability (see [62, Thm. 5.4.13]) to extract arithmetic information from Ext-groups $\mathrm{Ext}^i_\Lambda(M,\Lambda)$ (see [62, Prop. 5.5.10]). Although the integral complete group ring $\mathbb{Z}[[\mathbb{Z}_p]]$ which we want to work with is not Noetherian, if one could show that it is coherent, the above reasoning would still apply. Unfortunately, Burns and Daoud demonstrated that $\mathbb{Z}[[\mathbb{Z}_p]]$ is not a finite conductor ring, and consequently not coherent. However, one saving grace is that $\mathbb{Z}[[\mathbb{Z}_p]]$ is at least 2-coherent. Moreover, Theorem 6.0.7 still yields several favorable results — for example, the fact that $\mathbb{Z}[[\mathbb{Z}_p]]$ is strict $(2,2)$-domain of weak Krull dimension 2 except finitely many primes p. These results which help control the homological dimension properties of $\mathbb{Z}[[\mathbb{Z}_p]]$, remain sufficiently robust — especially when combined with the theory of pro-discrete modules developed in [17]— to support a range of meaningful arithmetic applications.

As far as the author is aware, a series of works following [17] is currently under development, including a $\mathbb{Z}[[\mathbb{Z}_p]]$-version of Weil-étale cohomology theory and arithmetic applications for global function fields and number fields. These developments illustrate the potential power of integral Iwasawa theory, which is poised to become a prominent direction in algebraic number theory.

To extend the study of integral Iwasawa theory to non-commutative settings, the next chapter presents our generalization of the coherency results in [17] from $\mathbb{Z}[[\mathbb{Z}_p]]$ to $\mathbb{Z}[[G]]$, where G belongs to certain classes of non-abelian groups.

Chapter 7

Coherency properties in non-commutative cases

This chapter is based on joint work with David Burns and Yu Kuang. More precisely, it is a slightly modified version of the article [19]. The material is reproduced here with minor changes in notation and with some additional explanations adapted to the context of this thesis.

Following Chase [24], and Bourbaki [13, Chap. 1], a ring is said to be (left, respectively right) 'coherent' if every finitely generated (left, respectively right) ideal is finitely presented. The theory of coherent rings is by now well established (for a comprehensive overview see Glaz's book [44]) and has important applications, particularly in arithmetic geometry.

It is clear that every Noetherian ring is coherent, and it is also known that any flat direct limit of coherent rings is coherent (cf. [loc. cit., Th. 2.3.3]). However, determining whether a given inverse limit of coherent—or even Noetherian—rings remains coherent can be highly nontrivial, and no general results in this direction appear to be known. In this chapter, we examine this problem in the context of completed group algebras.

We recall that, for each commutative ring Λ and profinite group G, the completed group algebra of G over Λ is defined (following Brumer [15]) to be the inverse limit

$$\Lambda[[G]] := \varprojlim_U \Lambda[G/U]$$

in which U runs over open normal subgroups of G and the transition map for $U \subseteq U'$ is the group ring homomorphism $\Lambda[G/U] \to \Lambda[G/U']$ induced by the natural projection $G/U \to G/U'$. Such rings arise naturally in various arithmetic contexts – for instance, when $\mathbb{Z}[[G]]$ acts on inverse limits of modules (such as class groups, Selmer groups, etc.) defined over a tower of fields within a given Galois extension of number fields with Galois group G.

In this chapter, we state and prove two theorems concerning properties related to the coherency of the integral completed group ring $\mathbb{Z}[[G]]$ for two classes of profinite groups G. The proof of the first theorem relies on an analysis of the ring homeomorphisms induced by group characters. In Corollary 7.2.4, we show that a broad class of profinite groups arising in arithmetic contexts fails to be coherent. The proof of the second theorem is based on Nakayama's Lemma (Proposition 7.3.3) for pro-discrete $\mathbb{Z}[[G]]$-modules, together with a divisibility result for Tor-groups (Proposition 7.3.4).

As mentioned in the previous chapter, the aim of this work is to generalize the results of Burns and Daoud [17] and to build the algebraic foundation of non-commutative integral Iwasawa theory.

7.1 Statements of theorems

Our first result, which will be proved in §7.2.1, addresses the question of the coherence of $\mathbb{Z}[[G]]$ under a mild technical assumption on G (see also Remark 7.2.3).

Theorem 7.1.1. *If G has a countable basis of neighborhoods of the identity and a non-torsion Sylow subgroup, then $\mathbb{Z}[[G]]$ is neither left nor right coherent.*

The existence of a non-torsion Sylow subgroup is a very mild condition, and thus the above result applies to most groups that arise naturally in arithmetic (cf. Corollary 7.2.4).

With potential arithmetic applications in mind, it is therefore natural to consider the classification of non-coherent rings. In this context, we focus on the hierarchy of n-coherence conditions (indexed by natural numbers n) introduced by Costa in [28] where 1-coherence coincides with the classical notion of coherence. In particular, we recall that n-coherent rings — whose definition is explicitly reviewed at the beginning of §7.3.3 — possess a range of useful properties, including a relatively well-behaved algebraic K-theory (cf. [36]).

However, despite the weaker nature of these conditions, verifying them for any given n appears to be highly nontrivial — if possible at all — since $\mathbb{Z}[[G]]$ is not a compact topological ring, and in cases where it is not coherent, there are no general methods available for establishing finite generation.

To address these issues, in §7.3.1 we introduce a category of 'pro-discrete' modules over $\mathbb{Z}[[G]]$, and establish a natural analogue of Nakayama's Lemma for this category (see Proposition 7.3.3). By combining this result with well-known theorems of Brumer [15] and Serre [70], we then deduce the following result in §7.3.3.

Theorem 7.1.2. *If G is a compact p-adic analytic group of rank d, then $\mathbb{Z}[[G]]$ is $(d+3)$-coherent.*

Whilst this result is not in all cases best possible (see Remark 7.3.7(ii)), establishing any form of coherency for completed integral group algebras associated with a general class of profinite groups is striking — and, as far as we are aware, without precedent. Moreover, such results enable interesting arithmetic applications. More specifically, we recall that a stronger version of Theorem 7.1.2 was first proved in the special case $G = \mathbb{Z}_p$ by Burns and Daoud in [17], and that several of the techniques developed here generalize those in loc. cit. The results of [17] have already been applied to develop key aspects of an arithmetic integral Iwasawa theory over $\mathbb{Z}[[\mathbb{Z}_p]]$, including new concrete results concerning the structure of ideal class groups. The results of Theorem 7.1.2, as well as the more general Proposition 7.3.3 and Proposition 7.3.4, are expected to similarly contribute to the development of integral Iwasawa theory over broader families of compact p-adic analytic extensions of global fields — a direction we aim to pursue in future work.

7.2 Coherence theorem I

7.2.1 Proof of Theorem 7.1.1

We shall only prove that the stated conditions imply that $\mathbb{Z}[[G]]$ is not left coherent (with a completely analogous argument showing that it is not right coherent).

To do this, we fix a countable basis $\{N_m\}_{m\geq 0}$ of neighbourhoods of the identity of G comprised of open normal subgroups N_m with $N_0 = G$ and $N_{m+1} \subset N_m$ for every m.

We also fix a prime p for which G has a non-torsion Sylow p-subgroup P and an element π of P of infinite order. We set

$$R := \mathbb{Z}[[G]] \quad \text{and} \quad \varpi := \pi - 1 \in R.$$

For each natural number m we define a finite group by setting

$$\Gamma_m := G/N_m.$$

We then write π_m for the image of π in Γ_m and p^{n_m} for the order of π_m (so that $n_0 = 0$). We assume, as we may (after changing the groups $\{N_m\}_m$ if necessary), that $n_{m+1} > n_m$ for every m. We set

$$R_m := \mathbb{Z}[\Gamma_m],\ T_m := \sum_{i=0}^{i=p^{n_m}-1} \pi_m^i \in R_m \quad \text{and} \quad \varpi_m := \pi_m - 1 \in R_m$$

(so that $R_0 = \mathbb{Z}, T_0 = 1$ and $\varpi_0 = 0$). We then define a left R-ideal by setting

$$I(\varpi) := \varprojlim_m R_m\varpi_m \subset \varprojlim_m R_m = R,$$

where the limits are with respect to the natural projection maps $R_m \to R_{m'}$ for $m > m'$.

Finally, we write R^p and R^p_m for the pro-p completions $\mathbb{Z}_p[[G]]$ and $\mathbb{Z}_p[\Gamma_m]$ of R and R_m respectively.

Proposition 7.2.1. *The element ϖ is a right non-zero divisor in R and there exists a canonical short exact sequence of (left) R-modules*

$$0 \to R\varpi \xrightarrow{\subseteq} I(\varpi) \xrightarrow{\phi_\varpi} R^p/(R^p\varpi + R) \to 0$$

(in which ϕ_ϖ is not *induced by the inclusion $I(\varpi) \subset R^p$).*

Proof. We write Λ for either R or R^p, with Λ_m denoting the corresponding ring R_m or R^p_m. Then, in both cases, there exists an exact commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \prod_m \Lambda_m T_m & \xrightarrow{\subseteq} & \prod_m \Lambda_m & \xrightarrow{1\mapsto(\varpi_m)_m} & \prod_m \Lambda_m \varpi_m & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle (1-\rho_m)_m} & & \downarrow{\scriptstyle (1-\rho_m)_m} & & \downarrow{\scriptstyle (1-\rho_m)_m} & & \\
0 & \longrightarrow & \prod_m \Lambda_m T_m & \xrightarrow{\subseteq} & \prod_m \Lambda_m & \xrightarrow{1\mapsto(\varpi_m)_m} & \prod_m \Lambda_m \varpi_m & \longrightarrow & 0
\end{array} \tag{7.1}$$

in which ρ_m denotes the natural projection map $\Lambda_m \to \Lambda_{m-1}$ (and its restrictions to both $\Lambda_m T_m$ and $\Lambda_m\varpi_m$). In particular, since $\rho_m(T_m) = p^{n_m - n_{m-1}} \cdot T_{m-1}$ with $n_m > n_{m-1}$ and $\rho_m(\Lambda_m) = \Lambda_{m-1}$, the Snake Lemma applies to this diagram to give an exact sequence

$$0 = \varprojlim_m \Lambda_m T_m \to \Lambda \xrightarrow{\lambda \mapsto \lambda\varpi} \varprojlim_m \Lambda_m \varpi_m \to \varprojlim_m^1 \Lambda_m T_m \to \varprojlim_m^1 \Lambda_m = 0.$$

This sequence implies ϖ is a right non-zero divisor in Λ and also gives a short exact sequence

$$0 \to \Lambda\varpi \xrightarrow{\subseteq} \varprojlim_m \Lambda_m \varpi_m \to \varprojlim_m^1 \Lambda_m T_m \to 0. \tag{7.2}$$

If $\Lambda = R^p$, then the derived limit $\varprojlim_m^1 \Lambda_m T_m$ vanishes since each module $\Lambda_m T_m$ is finitely generated over $\mathbb{Z}_p$ and hence compact.

To compute $\varprojlim_m^1 R_m T_m$ we write e_m for the idempotent $p^{-n_m} T_m$ of $\mathbb{Q}[\Gamma_m]$ and Q_m for the quotient of $R_m e_m$ by $R_m T_m$ and use the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \prod_m R_m T_m & \xrightarrow{\subseteq} & \prod_m R_m e_m & \longrightarrow & \prod_m Q_m & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle (1-\rho_m)_m} & & \downarrow{\scriptstyle (1-\rho_m)_m} & & \downarrow{\scriptstyle (1-\rho'_m)_m} & & \\ 0 & \longrightarrow & \prod_m R_m T_m & \xrightarrow{\subseteq} & \prod_m R_m e_m & \longrightarrow & \prod_m Q_m & \longrightarrow & 0 \end{array} \tag{7.3}$$

in which each row is the tautological short exact sequence and $\rho'_m : Q_m \to Q_{m-1}$ is induced by ρ_m. Then, since $\rho_{m+1}(e_{m+1}) = e_m$, by applying the Snake Lemma to this diagram one obtains a short exact sequence

$$0 \to \varprojlim_m R_m e_m \to \varprojlim_m Q_m \to \varprojlim_m^1 R_m T_m \to 0. \tag{7.4}$$

In view of the natural isomorphisms of finite abelian p-groups

$$Q_m = R_m e_m/(R_m T_m) = R_m e_m/(p^{n_m} R_m e_m) \cong R_m^p e_m/(p^{n_m} R_m^p e_m) = R_m^p e_m/R_m^p T_m,$$

there are also analogues of the diagrams (7.3) in which each term R_m is replaced by R_m^p. By passing to the limit over these diagrams and noting $\varprojlim_m^1 R_m^p T_m$

vanishes since each module $R^p_m T_m$ is compact, one obtains an identification

$$\varprojlim_m R^p_m e_m = \varprojlim_m Q_m \tag{7.5}$$

and hence a short exact sequence

$$0 \to \varprojlim_m R_m e_m \xrightarrow{\subset} \varprojlim_m R^p_m e_m \to \varprojlim^1_m R_m T_m \to 0. \tag{7.6}$$

In addition, for each m, there exists an exact commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Lambda_{m+1}\varpi_{m+1} & \xrightarrow{\subset} & \Lambda_{m+1} & \xrightarrow{1\mapsto e_{m+1}} & \Lambda_{m+1}e_{m+1} & \longrightarrow & 0, \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \Lambda_m\varpi_m & \xrightarrow{\subset} & \Lambda_m & \longrightarrow & \Lambda_m e_m & \longrightarrow & 0 \end{array}$$

in which each vertical arrow is induced by ρ_{m+1} and so is surjective. In particular, since $R^p\varpi = \varprojlim_m R^p_m \varpi_m$ (as a consequence of (7.2) with $\Lambda = R^p$), by passing to the limit over these diagrams we obtain short exact sequences

$$0 \to I(\varpi) \to R \to \varprojlim_m R_m e_m \to 0 \tag{7.7}$$

$$0 \to R^p\varpi \to R^p \to \varprojlim_m R^p_m e_m \to 0. \tag{7.8}$$

These sequences combine with the sequence (7.6) to induce an identification of the derived limit $\varprojlim^1_m R_m T_m$ with the quotient R-module $R^p/(R^p\varpi + R)$ and then the claimed exact sequence follows directly from (7.2) with $\Lambda = R$. □

In the sequel we fix an element $a \in (\mathbb{Z}_p \setminus \mathbb{Q}) \subset R^p$ and write $Q(a)$ for the R-submodule of $R^p/(R^p\varpi + R)$ generated by the class of a. In the next result we also use the surjective map ϕ_ϖ from Proposition 7.2.1.

Proposition 7.2.2. *The following claims are valid.*

(i) The R-module $Q(a)$ is isomorphic to $R/I(\varpi)$.

(ii) There exists $x_a \in I(\varpi)$ with $\phi_\varpi(x_a) = a$ and such that the R-module Rx_a is free.

Proof. To prove claim (i) it is enough to show that if $r = (r_m)_m$ is any element of $R = \varprojlim_m R_m$ such that, in $R^p = \varprojlim_m R^p_m$, one has $ra \in R^p\varpi + R$, then for every m one has $r_m \in R_m\varpi_m$. However, if $ra \in R^p\varpi + R$, then for every m there exist elements b_m of R^p_m and c_m of R_m such that $ar_m = (ra)_m = b_m\varpi_m + c_m$ and, upon multiplying this equality on the right by T_m we deduce that

$$ar_mT_m = b_m\varpi_mT_m + c_mT_m = c_mT_m.$$

Since $a \notin \mathbb{Q}$, this equality implies $r_mT_m = 0$ and hence that $r_m \in R_m\varpi_m$, as required.

Next we note that, since $Q(a)$ is non-zero (by claim (i)), any pre-image x_a of the class of a under ϕ_ϖ is also non-zero. In particular, if R is a domain (as is the case, by Neumann [63], if G is a torsion-free p-adic analytic pro-p group), then the R-module Rx_a is automatically free. In the general case, however, the proof of claim (ii) requires more effort. To proceed, for each non-negative integer i we write a_i for the unique integer with $0 \le a_i < p^{n_{i+1}-n_i}$ such that

$$a = \sum\nolimits_{i\ge 0} a_ip^{n_i} \in \mathbb{Z}_p.$$

For integers j with $0 \le j \le m$, we then define elements of R_m by setting

$$T_{m,j} := \sum\nolimits_{i=0}^{i=p^{n_j}-1} \pi_m^i \quad \text{and} \quad y_{a,m} := \sum\nolimits_{j=0}^{j=m-1} a_jT_{m,j}$$

(so $T_{m,0} = 1$ and $T_{m,m} = T_m$). It is then easily checked that the element

$$x_a := (\varpi_my_{a,m})_m \in \prod\nolimits_m R_m$$

belongs to $I(\varpi) = \varprojlim_m R_m\varpi_m$ and we aim to verify that this element has the properties stated in claim (ii).

As a first step, an explicit computation of the connecting homomorphism arising from the diagram (7.1) shows that the image in $\varprojlim^1_m \Lambda_m T_m$ of x_a under the map in (7.2) is represented by the element

$$(y_{a,m} - \rho_{m+1}(y_{a,m+1}))_m = (-a_m T_m)_m \in \prod_m R_m T_m. \tag{7.9}$$

In a similar way, an explicit computation of the connecting homomorphism of (7.3) shows that this element of $\varprojlim^1_m \Lambda_m T_m$ is the image under the map in (7.4) of the element of $\varprojlim_m Q_m$ that is represented by

$$\Big((\sum_{j=0}^{m-1} a_j p^{n_j}) e_m \Big)_m \in \prod_m R_m e_m.$$

Then, since for each m one has $a \equiv \sum_{j=0}^{m-1} a_j p^{n_j}$ modulo $p^{n_m}\mathbb{Z}_p$, the latter element corresponds under the identification (7.5) to the element $(ae_m)_m$ of $\varprojlim_m R^p_m e_m$. Hence, under the isomorphism of $\varprojlim^1_m R_m T_m$ with $R^p/(R^p\varpi + R)$ that is induced by the sequences (7.5), (7.7) and (7.8), the element of $\varprojlim^1_m R_m T_m$ represented by (7.9) corresponds to the class of a.

This explicit computation has shown that $\phi_\varpi(x_a) = a$ and so, to complete the proof of claim (ii), it is enough for us to prove that the R-module Rx_a is free. Hence, since $x_a = \varpi \cdot (y_{a,m})_m$ in $\prod_m R_m$ and ϖ is a non-zero divisor of R, it is enough for us to show that, for every m, the element $y_{a,m}$ is a non-zero divisor of R_m. To do this, we fix m and write Δ_m for the subgroup of Γ_m that is generated by π_m. We also write $\bar{\mathbb{Q}}$ for the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$, and note that, since $y_{a,m}$ belongs to $\mathbb{Z}[\Delta_m]$, it is enough to show that the annihilator in $\bar{\mathbb{Q}}[\Delta_m]$ of $y_{a,m}$ vanishes. Then, since the semisimple algebra $\bar{\mathbb{Q}}[\Delta_m]$ decomposes as a product of copies of $\bar{\mathbb{Q}}$, it is enough to show that the image of $y_{a,m}$ in each component of $\bar{\mathbb{Q}}[\Delta_m]$ is non-zero. More precisely, if for each homomorphism $\chi : \Delta_m \to \bar{\mathbb{Q}}^\times$ we write χ_* for the induced ring homomorphism $\bar{\mathbb{Q}}[\Delta_m] \to \bar{\mathbb{Q}}$, then it is enough for us to show that $\chi_*(y_{a,m}) \neq 0$ for every such χ.

If, firstly, χ is trivial, then the sum

$$\chi_*(y_{a,m}) = \sum_{j=0}^{j=m-1} a_j\chi_*(T_{m,j}) = \sum_{j=0}^{j=m-1} a_j p^{n_j}$$

is non-zero since $0 \leq a_j < p^{n_{j+1}-n_j}$ for every j. Then, if χ is non-trivial, and of order p^d say (so $d \leq n_m$), the element $\chi_*(\varpi_m) = \chi(\pi_m) - 1$ is non-zero and

$$\begin{aligned}\chi_*(\varpi_m)\chi_*(y_{a,m}) &= \chi_*((\pi_m - 1)y_{a,m}) \\ &= \chi_*\Big(\sum_{j=0}^{j=m-1} a_j(\pi_m^{p^{n_j}} - 1)\Big) = \sum_{j\in J_\chi} a_j(\chi(\pi_m)^{p^{n_j}} - 1),\end{aligned}$$

where J_χ is the set of integers j with $n_j < d$. It is therefore enough to note that this last sum is non-zero since the elements $\{\chi(\pi_m)^{n_j} - 1\}_{j\in J_\chi}$ are linearly independent over $\mathbb{Q}$ (as $n_j > n_{j'}$ for $j > j'$). □

To prove Theorem 7.1.1 we now fix an element x_a as in Proposition 7.2.2(ii). Then, since each R-module $R\varpi$ and Rx_a is free (the former by the first assertion of Proposition 7.2.1), Schanuel's Lemma [29, (2.24)] applies to the exact sequences

$$0 \to R\varpi \cap Rx_a \xrightarrow{x\mapsto(x,x)} R\varpi \oplus Rx_a \xrightarrow{(y,z)\to y-z} R\varpi + Rx_a \to 0,$$

$$0 \to \ker(\alpha) \to R^k \xrightarrow{\alpha} R\varpi + Rx_a \to 0$$

(for any suitable natural number k and surjective homomorphism of R-modules α) to imply that the (finitely generated) ideal $R\varpi + Rx_a$ of R is finitely presented if and only if the R-module $R\varpi \cap Rx_a$ is finitely generated (see also [44, Cor. 2.1.3]). It is therefore enough for us to show that $R\varpi \cap Rx_a$ is not finitely generated. To do this, we use the composite isomorphism of R-modules

$$Rx_a/(R\varpi \cap Rx_a) \cong (R\varpi + Rx_a)/R\varpi \cong Q_a \cong R/I(\varpi)$$

in which the second isomorphism is induced by ϕ_ϖ (and the exact sequence in Proposition 7.2.1) and the third by Proposition 7.2.2(i). In particular, since the R-module Rx_a is free of rank one, the displayed isomorphism combines with another application of Schanuel's Lemma to imply that $R\varpi \cap Rx_a$ is finitely generated if and only if $I(\varpi)$ is finitely generated. In view of the surjectivity of ϕ_ϖ, it is therefore enough for us to show that the quotient module $R^p/(R^p\varpi + R)$ is not finitely generated over R.

To establish this, we argue by contradiction and so assume that, for some natural number t, the set $\{y_i\}_{1\le i\le t}$ is a set of elements of R^p whose images generate $R^p/(R^p\varpi + R)$ as an R-module. Then, writing $\varepsilon : R^p \to \mathbb{Z}_p$ for the natural projection map, and noting that $\varepsilon(\varpi) = 0$, it follows that $\{\varepsilon(y_i)\}_{1\le i\le t}$ is a finite set of generators of the abelian quotient group $\varepsilon(R^p)/\varepsilon(R) = \mathbb{Z}_p/\mathbb{Z}$ and this is not possible since $\mathbb{Z}_p/\mathbb{Z}$ is uncountable. This completes the proof of Theorem 7.1.1.

Remark 7.2.3. *As a natural weakening of the notion of coherence, a domain is said to be a (left, respectively right) 'finite conductor domain' if the intersection of any two of its principal (left, respectively right) ideals is finitely generated (see Glaz [43], but note that the concept was first considered by Dobbs in [32]). In particular, by showing that $R\varpi \cap Rx_a$ is not finitely generated over R, the above argument implies that, under the conditions of Theorem 7.1.1, $\mathbb{Z}[[G]]$ is not a (left, respectively right) finite conductor domain.*

7.2.2 Examples

The assumed existence of a non-torsion Sylow subgroup rules out profinite groups such as $(\mathbb{Z}/p\mathbb{Z})^{\mathbb{N}}$ for any prime p and $\prod_\ell(\mathbb{Z}/\ell\mathbb{Z})$ where ℓ runs over any infinite set of primes. However, it is satisfied by most of the groups that arise naturally in arithmetic. In particular, Theorem 7.1.1 has concrete consequences such as the following.

Corollary 7.2.4. *Fix a prime p. Then the ring $\mathbb{Z}[[G]]$ is neither left nor right* *coherent in each of the following cases:*

(i) G is a compact p-adic analytic group of positive rank.

(ii) G is the Galois group of an algebraic extension of number fields, or of p-adic fields, that contains a $\mathbb{Z}_\ell$-subextension for any prime ℓ.

(iii) G is a Sylow p-subgroup of the absolute Galois group of a number field.

Proof. To prove claim (i) we recall Lazard [57] has shown that any compact p-adic analytic group is isomorphic to a closed subgroup of $\mathrm{GL}_n(\mathbb{Z}_p)$ for some n. It is then enough to note that, for any infinite subgroup G of $\mathrm{GL}_n(\mathbb{Z}_p)$ the collection $\{G \cap (\mathrm{I}_n + p^m \cdot \mathrm{M}_n(\mathbb{Z}_p))\}_{m\geq 1}$ is a countable basis of neighbourhoods of the identity that comprises open, torsion-free, pro-p subgroups (that are normal in G).

To prove claim (ii) we fix a finite extension K of either $\mathbb{Q}$ or $\mathbb{Q}_p$, an algebraic closure $\bar{K}$ of K and a Galois extension L of K in $\bar{K}$, with $G := \mathrm{Gal}(L/K)$, for which there exists an intermediate field E for which $\Gamma := \mathrm{Gal}(E/K)$ is isomorphic to $\mathbb{Z}_\ell$. Then, for each natural number n, the composite $K(n)$ of all finite extensions K' of K inside L with the property that the absolute value of the discriminant of $K'/\mathbb{Q}$ is at most n is a finite Galois extension of K. In the case of the number fields, respectively p-adic fields, this follows directly from the Hermite-Minkowski Theorem (cf. [61, §III.2]), respectively [53, Prop. 14, II, §5]. The groups $\{\mathrm{Gal}(L/K(n))\}_{n\geq 1}$ then give a countable base of neighbourhoods of the identity of G. Notice that we have a short exact sequence

$$1 \longrightarrow \mathrm{Gal}(L/E) \longrightarrow G \longrightarrow \Gamma \longrightarrow 1.$$

Since $\Gamma \cong \mathbb{Z}_\ell$ is non-torsion, it contains elements of infinite ℓ-power order. Hence G also contains elements of infinite ℓ-power order, and in particular its Sylow ℓ-subgroups are non-torsion. Together with the fact that G has a countable basis of neighbourhoods of the identity (as shown above), this shows that G satisfies the hypotheses of Theorem 7.1.1, and so $\mathbb{Z}[[G]]$ is neither left nor right coherent.

To prove claim (iii) we fix a number field K and a Sylow p-subgroup P of $\mathrm{Gal}(\bar{K}/K)$. It is then enough to note that P has a countable base of neighbourhoods of its identity (inherited from the countable base of $\mathrm{Gal}(\bar{K}/K)$ constructed in claim (ii)) and a subgroup that is a free pro-p group on countably many generators (for a proof of the latter fact, see Bary-Soroker et al [11, §3]).

□

7.3 Coherence theorem II

In this section we continue to use the notation fixed at the beginning of §7.2.1, so that $R = \mathbb{Z}[[G]]$ and $R_n = \mathbb{Z}[\Gamma_n]$ with $\Gamma_n = G/N_n$.

We shall only consider the category of left R-modules (noting that completely analogous arguments prove the same results for the category of right R-modules). In particular, for an R-module M and map ϕ of such modules, and a non-negative integer n, we set

$$M_{(n)} := R_n \otimes_R M, \quad \text{and} \quad \phi_{(n)} := R_n \otimes_R \phi,$$

respectively regarded, in the natural way, as a (left) R_n-module and as a map of (left) R_n-modules.

7.3.1 Nakayama's lemma

Following the approach of Burns and Daoud in [17, §3], we will find it useful to consider the category of R-modules introduced in the following definition.

Definition 7.3.1. *An inverse system $(M_n, \pi_n)_n$ of R-modules indexed by non-negative integers n is said to be a pro-discrete system if, for every n, the action* *of R on M_n factors through R_n and the transition morphism $\pi_n : M_{n+1} \to M_n$ induces an isomorphism of R_n-modules $R_n \otimes_{R_{n+1}} M_{n+1} \cong M_n$. An R-module is then said to be pro-discrete if it is equal to the limit of a pro-discrete system of R-modules.*

Remark 7.3.2. *The ring R is itself a pro-discrete R-module since it is the limit of the inverse system $(R_n, \rho_n)_n$ in which ρ_n is the natural projection map $R_{n+1} \to R_n$ (which induces the canonical identification $R_n \otimes_{R_{n+1}} R_{n+1} \cong R_n$). In addition, any R-module M gives rise to a pro-discrete system $(M_{(n)}, \pi_n)_n$, with π_n the canonical map $M_{(n+1)} \to M_{(n)}$, and hence to a pro-discrete R-module $\varprojlim_n M_{(n)}$. In particular, an R-module M is pro-discrete if the canonical map $M \to \varprojlim_n M_{(n)}$ is bijective. In general, however, finitely presented R-modules need not be pro-discrete and the category of pro-discrete R-modules need not be abelian (cf. [17, Rem. 3.4]).*

In the sequel, for any finitely generated (left) module M over a ring Λ we will also write $\mu_\Lambda(M)$ for the minimal number of generators of M.

The next result establishes a natural analogue of Nakayama's Lemma for the category of pro-discrete R-modules (and thereby generalises aspects of [17, Th. 3.8]).

Proposition 7.3.3. *Assume G is pro-p, fix a pro-discrete system $(M_n, \pi_n)_n$ of R-modules, and write M for the associated pro-discrete R-module $\varprojlim_n M_n$. Then the following claims are valid.*

(i) M is finitely generated (over R) if and only if it contains a finite subset that, for every n, projects under the natural map $M \to M_n$ to give a set of generators of the R_n-module M_n.

(ii) If there exists a natural number d such that $\mu_{R_n}(M_n) \leq d$ for all n, then M is finitely generated and $\mu_R(M) \leq \mu_{\mathbb{Z}}(M_0) + d$.

Proof. To prove claim (i) we assume to be given a natural number m and a subset $Z := \{z_i := (z_{i,n})_n\}_{1 \leq i \leq m}$ of M (so, for all i and n, $z_{i,n} \in M_n$ and $\pi_n(z_{i,n+1}) = z_{i,n}$) such that, for all n, the R_n-module M_n is generated by $\{z_{i,n}\}_{1 \leq i \leq m}$. It is then enough to show Z generates M over R and to do this we consider the exact commutative diagram

$$
\begin{array}{ccccccccc}
 & & & & \ker(\rho^m_{n+1}) & \xrightarrow{\iota'_{n+1}} & \ker(\pi_{n+1}) & & \\
 & & & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \ker(\iota_{n+1}) & \longrightarrow & R^m_{n+1} & \xrightarrow{\iota_{n+1}} & M_{n+1} & \longrightarrow & 0 \\
 & & \theta_n \downarrow & & \rho^m_n \downarrow & & \pi_n \downarrow & & \\
0 & \longrightarrow & \ker(\iota_n) & \longrightarrow & R^m_n & \xrightarrow{\iota_n} & M_n & \longrightarrow & 0.
\end{array}
\tag{7.10}
$$

Here ι_n is the (assumed surjective) map of R_n-modules that sends the i-th element in the standard basis of R^m_n to $z_{i,n}$ (so that the lower right hand square commutes) and θ_n and ι'_{n+1} are the respective restrictions of ρ^m_n and ι_{n+1}.

Write J_{n+1} for the (two-sided) ideal of R_{n+1} generated by $\{h - 1 : h \in N_n/N_{n+1}\}$. Then the map ρ^m_n is surjective, with kernel the submodule J^m_{n+1} of R^m_{n+1}, and the (assumed) bijectivity of $R_n \otimes_{R_{n+1}} \pi_n$ implies $\ker(\pi_n) = J_{n+1} \cdot M_{n+1}$. It follows that ι'_{n+1} is surjective and hence, by applying the Snake Lemma to (7.10), that θ_n is surjective. This last fact then implies (via the Mittag-Leffler criterion) that the derived limit $\varprojlim^1_n \ker(\iota_n)$ with respect to the maps θ_n vanishes. Upon passing to limit over n of the commutative diagrams given by the second and third rows of (7.10), one therefore deduces that the map of R-modules

$$R^m = \varprojlim_n R^m_n \to \varprojlim_n M_n = M$$

that sends the i-th element in the standard basis of R^m to z_i is surjective. It follows that M is generated over R by the set Z, as required.

To prove claim (ii) we note $R_0 = \mathbb{Z}$ and set $\kappa := \mu_{\mathbb{Z}}(M_0) \leq d$. We show first that, for each n, there exists a subset $X_n := \{x_{i,n}\}_{1\leq i\leq\kappa}$ of M_n with the following two properties:

(P1) the R_n-submodule M'_n of M_n generated by X_n has finite, prime-to-p index;

(P2) for each $n' < n$, the natural map $M_n \to M_{n'}$ sends $x_{i,n}$ to $x_{i,n'}$ for every index i and also induces an isomorphism of $R_{n'}$-modules $R_{n'} \otimes_{R_n} M'_n \cong M'_{n'}$.

To establish this we use induction on n. For $n = 0$ the necessary conditions are satisfied by taking X_0 to be any set of generating elements for the (assumed to be finitely generated) abelian group M_0 (so that $M'_0 = M_0$). For the inductive step we fix $n > 0$ and assume that suitable sets X_m have been constructed for each $m < n$. For each index i with $1 \leq i \leq \kappa$ we then fix a pre-image $x_{i,n}$ of $x_{i,n-1}$ under the given map $\pi_{n-1} : M_n \to M_{n-1}$, set $X_n := \{x_{i,n}\}_{1\leq i\leq\kappa}$ and write M'_n for the R_n-submodule of M_n generated by X_n. It is then clear that

$$\mathbb{Z}_p \otimes_{\mathbb{Z}} \pi_{n-1}(M'_n) = \mathbb{Z}_p \otimes_{\mathbb{Z}} M'_{n-1} = \mathbb{Z}_p \otimes_{\mathbb{Z}} M_{n-1} = \mathbb{Z}_p \otimes_{\mathbb{Z}} \pi_{n-1}(M_n),$$

where the second equality is a consequence of (P1) (for $n-1$), and hence that

$$\mathbb{Z}_p \otimes_{\mathbb{Z}} M_n = \mathbb{Z}_p \otimes_{\mathbb{Z}} M'_n + \mathbb{Z}_p \otimes_{\mathbb{Z}} \ker(\pi_{n-1}) = \mathbb{Z}_p \otimes_{\mathbb{Z}} M'_n + J_n \cdot (\mathbb{Z}_p \otimes_{\mathbb{Z}} M_n).$$

Now, since N_{n-1}/N_n is a finite p-group, the ideal J_n belongs to the Jacobson radical of $\mathbb{Z}_p\otimes_{\mathbb{Z}}R_n$ and so the last displayed equality combines with Nakayama's Lemma to imply that $\mathbb{Z}_p \otimes_{\mathbb{Z}} M_n = \mathbb{Z}_p \otimes_{\mathbb{Z}} M'_n$. It follows that the index of M'_n in M_n is finite and prime to p, and hence that (P1) is satisfied. The first property in (P2) is also clear for this construction, and the second property is true provided that the natural composite map

$$R_{n'} \otimes_{R_n} M'_n \to R_{n'} \otimes_{R_n} M_n \cong M_{n'}$$

is injective. However, the kernel of this map is isomorphic to a quotient of the group

$$\mathsf{Tor}_1^{R_n}(R_{n'}, M_n/M'_n) \cong \mathsf{Tor}_1^{\mathbb{Z}[N_{n'}/N_n]}(\mathbb{Z}, M_n/M'_n) \cong H_1(N_{n'}/N_n, M_n/M'_n),$$

and the latter group vanishes since $N_{n'}/N_n$ is a finite p-group whilst the order of M_n/M'_n is prime to p.

For each $n > 0$ we now consider the exact commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \prod_n M'_n & \xrightarrow{(\iota_n)_n} & \prod_n M_n & \longrightarrow & \prod_n Q_n & \longrightarrow & 0 \\ & & \big\downarrow{\scriptstyle (1-\pi'_n)_n} & & \big\downarrow{\scriptstyle (1-\pi_n)_n} & & \big\downarrow{\scriptstyle (1-\pi''_n)_n} & & \\ 0 & \longrightarrow & \prod_n M'_n & \xrightarrow{(\iota_n)_n} & \prod_n M_n & \longrightarrow & \prod_n Q_n & \longrightarrow & 0 \end{array} \tag{7.11}$$

in which $\iota_n : M'_n \to M_n$ is the natural inclusion map, we set $Q_n := \mathrm{cok}(\iota_n)$, π'_n is the map $M'_{n+1} \to M'_n$ obtained by restriction of π_n and π''_n is the map $Q_{n+1} \to Q_n$ induced by π_n. In particular, since the maps π'_n are surjective, the Snake Lemma applies to this diagram to give a short exact sequence of R-modules

$$0 \to M' \to M \to Q \to 0, \tag{7.12}$$

in which we set $M' := \varprojlim_n M'_n$ and $Q := \varprojlim_n Q_n$ (with the respective limits taken with respect to the maps π'_n and π''_n). In addition, the final assertion of property (P2) implies that the inverse system $(M'_n, \pi'_n)_n$ is pro-discrete and so claim (i) implies that the set $\{(x_{i,n})_n\}_{1\le i\le\kappa}$ generates M' over R and hence that

$$\mu_R(M') \le \kappa = \mu_{\mathbb{Z}}(M_0). \tag{7.13}$$

To establish that M is finitely generated and $\mu_R(M) \le \mu_{\mathbb{Z}}(M_0) + d$, we are therefore reduced, via the exact sequence (7.12) and inequality (7.13), to showing that $\mu_R(Q) \le d$.

To prove this we note that, for each n, the diagram (7.11) gives rise to an exact commutative diagram of R_n-modules

$$\begin{array}{ccccccccc} & & (M'_{n+1})_{(n)} & \xrightarrow{(\iota_{n+1})_{(n)}} & (M_{n+1})_{(n)} & \longrightarrow & (Q_{n+1})_{(n)} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle (\pi'_n)_{(n)}} & & \downarrow{\scriptstyle (\pi_n)_{(n)}} & & \downarrow{\scriptstyle (\pi''_n)_{(n)}} & & \\ 0 & \longrightarrow & M'_n & \xrightarrow{\iota_n} & M_n & \longrightarrow & Q_n & \longrightarrow & 0. \end{array}$$

In particular, since the first two vertical maps are bijective (as the systems $(M'_n, \pi'_n)_n$ and $(M_n, \pi_n)_n$ are pro-discrete), the third vertical map is also bijective and so the inverse system $(Q_n, \pi''_n)_n$ is pro-discrete. It follows that Q is a pro-discrete R-module and so claim (i) reduces us to constructing a subset $\tilde{Z}$ of Q such that $|\tilde{Z}| \le d$ and, for every n, the module Q_n is generated over R_n by the image of $\tilde{Z}$.

We shall now inductively construct a suitable set $\tilde{Z}$ and to do this we note that, as Q_n has order prime-to-p, it is naturally a module over the algebra $\mathcal{R}_n := \mathbb{Z}[1/p][\Gamma_n]$. In particular, for each n' with $0 \le n' < n$, the central idempotent

$$e_{n,n'} := |(N_{n'}/N_n)|^{-1} \sum\nolimits_{\gamma \in N_{n'}/N_n} \gamma$$

of $\mathcal{R}_n$ induces an identification of $Q_{n'} \cong R_{n'} \otimes_{R_n} Q_n = \mathcal{R}_{n'} \otimes_{\mathcal{R}_n} Q_n$ with the submodule $e_{n,n'}Q_n$ of Q_n, and hence also a direct sum decomposition of R_n-modules

$$Q_n = (1 - e_{n,n'})Q_n \oplus e_{n,n'}Q_n = (1 - e_{n,n'})Q_n \oplus Q_{n'}. \qquad (7.14)$$

In addition, since each module Q_n is (by its very definition) a quotient of M_n, one has $\mu_{R_n}(Q_n) \le \mu_{R_n}(M_n) \le d$, where the last inequality follows from the stated assumption on M. For each n we can therefore fix a set of generators $\{\tilde{z}'_{i,n}\}_{1 \le i \le d}$ of the R_n-module Q_n. We then set $e_{0,-1} := 0$ and, for each index i, define an element

$$\tilde{z}_{i,n} := \sum_{0 \le a \le n} (1 - e_{a,a-1}) \tilde{z}'_{i,a} \in Q_n$$

(where we use (7.14) to regard each $Q_{n'}$ for $n' < n$ as a submodule of Q_n). Then each family $\tilde{z}_i := \big(\tilde{z}_{i,n}\big)_{n \ge 0}$ belongs to the inverse limit $Q = \varprojlim_n Q_n$. In addition, for every n, the decompositions (7.14) imply that the R_n-module Q_n is generated by the elements $\{\tilde{z}_{i,n}\}_{1 \le i \le d}$, and so the subset $\tilde{Z} := \{\tilde{z}_i\}_{1 \le i \le d}$ of Q has all of the properties that are required to complete the proof of claim (ii). □

7.3.2 Divisibility of Tor-groups

Throughout this subsection we fix a rational prime p. For an abelian group A and natural number m we set $A[m] := \{a \in A : m \cdot a = 0\}$. We also write $A_{\langle p \rangle}$ for the inverse limit $\varprojlim_{m \in \mathbb{N}} A/p^m$ (with respect to the natural projection maps), and use similar notation for homomorphisms. For a ring R, we write $\mathrm{pd}_R(M)$ for the projective dimension of a (left) R-module M. We also recall that, for any natural number n, an R-module M is said to be 'finitely n-presented' if there exists a collection of natural numbers $\{t_i\}_{0 \le i \le n}$ and an exact sequence of R-modules of the form

$$0 \to \ker(\theta_n) \xrightarrow{\iota} R^{t_n} \xrightarrow{\theta_n} R^{t_{n-1}} \cdots \xrightarrow{\theta_1} R^{t_0} \xrightarrow{\theta_0} M \to 0. \tag{7.15}$$

The following technical result will be useful for the proof of Theorem 7.1.2.

Proposition 7.3.4. *Let p be a rational prime and let G be a profinite group and M be a finitely generated $\mathbb{Z}[[G]]$-module with the following properties:*

(i) $M[p] = (0)$.

(ii) *M is finitely n-presented, for some natural number n.*

(iii) $\mathrm{pd}_{\mathbb{Z}_p[[G]]}\big(M_{\langle p \rangle}\big) < n$.

Then, for every $\mathbb{Z}[[G]]$*-module* L *with* $L[p] = (0)$*, and every integer* $a \geq n$*, the higher Tor-group* $\mathsf{Tor}_a^{\mathbb{Z}[[G]]}(L, M)$ *is* p*-divisible.*

Proof. Set $R := \mathbb{Z}[[G]]$ and $\Lambda := R_{\langle p \rangle} = \mathbb{Z}_p[[G]]$. We first make an easy observation about short exact sequences. For this we note that, if M_3 is any R-module with $M_3[p] = (0)$, then a short exact sequence of R-modules $0 \to M_1 \to M_2 \to M_3 \to 0$ gives rise, for each natural number m, to an exact commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_1/p^{m+1} & \longrightarrow & M_2/p^{m+1} & \longrightarrow & M_3/p^{m+1} & \longrightarrow & 0 \\ & & \Big\downarrow{\scriptstyle \varrho_{1,m}} & & \Big\downarrow{\scriptstyle \varrho_{2,m}} & & \Big\downarrow{\scriptstyle \varrho_{3,m}} & & \\ 0 & \longrightarrow & M_1/p^m & \longrightarrow & M_2/p^m & \longrightarrow & M_3/p^m & \longrightarrow & 0, \end{array}$$

in which each map $\varrho_{i,m}$ is the natural projection. Then, since $\varrho_{1,m}$ is surjective, the Mittag-Leffler criterion implies that, upon passing to the limit over m of these sequences, one obtains a short exact sequence of Λ-modules $0 \to M_{1,\langle p \rangle} \to M_{2,\langle p \rangle} \to M_{3,\langle p \rangle} \to 0$.

Turning now to the proof of the stated result, property (ii) allows us to fix an exact sequence of R-modules of the form (7.15). Then, under condition (i), this sequence breaks up into a finite collection of short exact sequences in which no occurring term has an element of order p. Hence, by applying the above observation to each of these short exact sequences, one deduces firstly that for each m the induced sequence

$$0 \to \ker(\theta_n)/p^m \xrightarrow{\iota/p^m} (R/p^m)^{t_n} \xrightarrow{\theta_n} (R/p^m)^{t_{n-1}} \cdots \xrightarrow{\theta_1} (R/p^m)^{t_0} \to M/p^m \to 0 \tag{7.16}$$

is exact and then, upon passing to the limit over m, that the induced sequence of Λ-modules

$$0 \to \ker(\theta_n)_{\langle p \rangle} \xrightarrow{\iota_{\langle p \rangle}} \Lambda^{t_n} \xrightarrow{\theta_{n,\langle p \rangle}} \Lambda^{t_{n-1}} \cdots \xrightarrow{\theta_{1,\langle p \rangle}} \Lambda^{t_0} \to M_{\langle p \rangle} \to 0 \tag{7.17}$$

is also exact. By using this sequence to compute Tor-groups, one obtains an isomorphism

$$\mathsf{Tor}_n^{\Lambda}(L_{\langle p\rangle}, M_{\langle p\rangle}) \cong \frac{\ker\big(L_{\langle p\rangle} \otimes_\Lambda \theta_{n,\langle p\rangle}\big)}{\operatorname{im}\big(L_{\langle p\rangle} \otimes_\Lambda \iota_{\langle p\rangle}\big)}. \tag{7.18}$$

To compute this group, we note that, for each index i, the module $L_{\langle p\rangle} \otimes_\Lambda \Lambda^{t_i}$ identifies with $(L_{\langle p\rangle})^{t_i} = \varprojlim_m ((L/p^m) \otimes_{R/p^m} (R^{t_i}/p^m))$. In particular, since inverse limits are left exact, this observation (with $i = n$ and $i = n-1$) gives an equality

$$\ker\big(L_{\langle p\rangle} \otimes_\Lambda \theta_{n,\langle p\rangle}\big) = \varprojlim_m \ker((L \otimes_R \theta_n)/p^m) = \varprojlim_m \ker((L/p^m) \otimes_{R/p^m} (\theta_n/p^m)),$$

where the limits are taken with respect to the transition maps induced by the projections $(L/p^m)^{t_n} \to (L/p^{m-1})^{t_n}$. In a similar way, one finds that there is a corresponding inclusion

$$\operatorname{im}\big(L_{\langle p\rangle} \otimes_\Lambda \iota_{\langle p\rangle}\big) \subseteq \varprojlim_m \operatorname{im}((L/p^m) \otimes_{R/p^m} \iota_m).$$

The isomorphism (7.18) therefore induces a surjective composite map of Λ-modules

$$\begin{aligned} \mathsf{Tor}_n^{\Lambda}(L_{\langle p\rangle}, M_{\langle p\rangle}) &\twoheadrightarrow \frac{\varprojlim_m \ker((L/p^m) \otimes_{R/p^m} (\theta_n/p^m))}{\varprojlim_m \operatorname{im}((L/p^m) \otimes_{R/p^m} \iota_m)} \\ &\cong \varprojlim_m \frac{\ker((L/p^m) \otimes_{R/p^m} (\theta_n/p^m))}{\operatorname{im}((L/p^m) \otimes_{R/p^m} \iota_m)} \\ &\cong \varprojlim_m \mathsf{Tor}_n^{R/p^m}(L/p^m, M/p^m). \end{aligned} \tag{7.19}$$

Here the first isomorphism follows from the Mittag-Leffler criterion since the projections

$$\operatorname{im}((L/p^m) \otimes_{R/p^m} \iota_m) \to \operatorname{im}((L/p^{m-1}) \otimes_{R/p^{m-1}} \iota_{m-1})$$

are surjective, and the second is obtained by computing the groups $\mathsf{Tor}_n^{R/p^m}(L/p^m, M/p^m)$ via the resolutions (7.16).

Next we note that (since $L[p]$ and $M[p]$ vanish) there are short exact sequences

$$0 \to L \xrightarrow{p^m} L \to L/p^m \to 0 \quad \text{and} \quad 0 \to M \xrightarrow{p^m} M \to M/p^m \to 0$$

which combine to give a composite injective homomorphism of abelian groups

$$\mathsf{Tor}_n^R(L, M)/p^m \hookrightarrow \mathsf{Tor}_n^R(L/p^m, M/p^m) \cong \mathsf{Tor}_n^{R/p^m}(L/p^m, M/p^m). \tag{7.20}$$

Here the isomorphism is induced by the fact that the standard spectral sequence

$$\mathsf{Tor}_b^{R/p^m}\left(L/p^m, \mathsf{Tor}_c^R(M, R/p^m)\right) \Longrightarrow \mathsf{Tor}_{b+c}^{R/p^m}(L/p^m, M/p^m)$$

collapses on its first page since $\mathsf{Tor}_c^R(M, R/p^m)$ vanishes for all $c > 0$ (as $\mathsf{Tor}_1^R(M, R/p^m)$ is isomorphic to $M[p^m]$). After taking the inverse limit over m of the maps (7.20), we deduce from (7.19) that $\mathsf{Tor}_n^R(L, M)_{\langle p \rangle}$ is isomorphic to a subquotient of $\mathsf{Tor}_n^\Lambda(L_{\langle p \rangle}, M_{\langle p \rangle})$.

In particular, since property (iii) implies that $\mathsf{Tor}_n^\Lambda(L_{\langle p \rangle}, M_{\langle p \rangle})$ vanishes, the module $\mathsf{Tor}_n^R(L, M)_{\langle p \rangle}$ must also vanish and so the group $\mathsf{Tor}_n^R(L, M)$ is p-divisible.

This proves the stated claim with $a = n$. To prove the same result for all $a > n$, one can then use an induction on a. The key point for this is that, if $0 \to L' \to F \to L \to 0$ is any short exact sequence of left R-modules in which F is free, then one has $L'[p] = (0)$ and also, since $a - 1 > n - 1 \geq 0$, the natural exact sequence

$$(0) = \mathsf{Tor}_a^R(F, M) \to \mathsf{Tor}_a^R(L, M) \to \mathsf{Tor}_{a-1}^R(L', M) \to \mathsf{Tor}_{a-1}^R(F, M) = (0)$$

implies $\mathsf{Tor}_a^R(L, M)$ is isomorphic to $\mathsf{Tor}_{a-1}^R(L', M)$. □

7.3.3 Proof of Theorem 7.1.2

We henceforth fix a group G as in Theorem 7.1.2, and continue to set $R := \mathbb{Z}[[G]]$. We also now fix natural numbers n and $\{t_i\}_{0\le i\le n}$ and an exact sequence of left R-modules of the form (7.15).

We recall that Costa [28] defines R to be 'left n-coherent' if, for every such sequence, the R-module $\ker(\theta_n)$ is finitely generated. (This property is labeled as 'strong left n-coherence' by Dobbs et al [33], and more conceptual treatments are given by Zhu [81] and Bravo and Pérez [14]). We note, in particular, that R is left 1-coherent if and only if it is left coherent in the classical sense of Chase [24] and Bourbaki [13], and we recall that if R is left n-coherent, then it is automatically left n'-coherent for every $n' > n$.

We start by recording a useful technical result.

Lemma 7.3.5. *If U is an open subgroup of G, then R is left n-coherent if and only if $\mathbb{Z}[[U]]$ is left n-coherent.*

Proof. Since the index of U in G is finite, the functor $\mathbb{Z}[[G]] \otimes_{\mathbb{Z}[[U]]} -$ is flat and a $\mathbb{Z}[[U]]$-module N is finitely generated if and only if the $\mathbb{Z}[[G]]$-module $\mathbb{Z}[[G]] \otimes_{\mathbb{Z}[[U]]} N$ is finitely generated. The stated result is a direct consequence of these facts. □

Following this result (and the observations made in the proof of Corollary 7.2.4(i)), to prove Theorem 7.1.2 it is enough for us to show the following: if G is both pro-p and has no element of order p, and if $n = d+3$ in (7.15), then the R-module $K := \ker(\theta_{d+3})$ is finitely generated. Our verification of this fact will depend crucially on the properties of K that are established in claim (ii) of the next result.

Proposition 7.3.6. *Assume that G is pro-p and has no element of order p.*

(i) The R-module $\mathrm{im}(\theta_{d+3})$ is pro-discrete.

(ii) Set $t = t_{d+3}$ and, for each m, write ϱ^t_m for the natural projection $R^t \to R^t_m$. Then the R-module K is equal to $\varprojlim_m \varrho^t_m(K)$ and is pro-discrete.

Proof. For each natural number a, there exists a commutative diagram of R-modules

$$\begin{array}{ccccccccc}
 & 0 & \longrightarrow & K & \xrightarrow{\iota} & R^t & \xrightarrow{\theta} & M' & \longrightarrow 0 \\
 & & \swarrow & \downarrow{\scriptstyle \varrho^t_{a+1}} & & \downarrow{\scriptstyle \varrho^t_{a+1}} & & \downarrow & \\
K_{(a+1)} & & & & & & & & \\
 & \searrow{\scriptstyle \nu_{a+1}} & & & & & & & \\
 & 0 & \longrightarrow & \varrho^t_{a+1}(K) & \xrightarrow{\iota_{a+1}} & R^t_{a+1} & \xrightarrow{\theta_{(a+1)}} & M'_{(a+1)} & \longrightarrow 0, \\
 & & & \downarrow{\scriptstyle \rho^t_a} & & \downarrow{\scriptstyle \rho^t_a} & & \downarrow & \\
 & 0 & \longrightarrow & \varrho^t_a(K) & \xrightarrow{\iota_a} & R^t_a & \xrightarrow{\theta_{(a)}} & M'_{(a)} & \longrightarrow 0.
\end{array} \tag{7.21}$$

Here we set $\theta = \theta_{d+3}$, $K = \ker(\theta)$, $M' := \mathrm{im}(\theta) = \ker(\theta_{d+2})$, and write ι for the tautological inclusion $K \subseteq R^t$. We also write ρ^t_a for the projection $R^t_{a+1} \to R^t_a$ (so that $\varrho^t_a = \rho^t_a \circ \varrho^t_{a+1}$), ν_{a+1} for the canonical map $K_{(a+1)} \to \varrho^t_{a+1}(K)$ and ι_{a+1} for the inclusion $\varrho^t_{a+1}(K) \subseteq R^t_{a+1}$. In addition, all unlabelled arrows in the diagram are the natural projections. Then, as ν_{a+1} is surjective and $R^t_{a+1} = (R^t)_{(a+1)}$, the commutativity of the diagram implies that the second, and in a similar way third, row is exact. In particular, since $\rho^t_a(\varrho^t_{a+1}(K)) = \varrho^t_a(K)$ for every a, the Mittag-Leffler criterion ensures that, by passing to the inverse limit over a of these diagrams, we obtain an exact commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & K & \xrightarrow{\iota} & R^t & \xrightarrow{\theta} & M' & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \iota'} & & \downarrow{\scriptstyle \cong} & & \downarrow{\scriptstyle \mu} & & \\
0 & \longrightarrow & \varprojlim_a \varrho^t_a(K) & \xrightarrow{\subseteq} & \varprojlim_a R^t_a & \xrightarrow{(\theta_{(a)})_a} & \varprojlim_a M'_{(a)} & \longrightarrow & 0,
\end{array} \tag{7.22}$$

and hence, by applying the Snake Lemma to this diagram, an exact sequence of R-modules

$$0 \to K \xrightarrow{\iota'} \varprojlim_a \varrho_a^t(K) \to M' \xrightarrow{\mu} \varprojlim_a M'_{(a)} \to 0.$$

To simultaneously prove claim (i) and the first assertion of claim (ii), it is thus enough to prove μ is injective. This is, however, a direct consequence of the commutative diagram

$$\begin{array}{ccc} M' & \xrightarrow{\mu'} & R^{t_{d+2}} \\ {\scriptstyle\mu}\downarrow & & \| \\ \varprojlim_a M'_{(a)} & \xrightarrow{(\mu'_{(a)})_a} & \varprojlim_a R_a^{t_{d+2}} \end{array}$$

in which μ' denotes the natural inclusion.

To prove the second assertion of claim (ii) it is then enough to show that the map

$$\kappa_a : R_a \otimes_{R_{a+1}} \varrho_{a+1}^t(K) \to \varrho_a^t(K)$$

that is induced by the surjection ρ_a^t is injective (and hence bijective). For this argument we write Δ for the finite normal subgroup N_a/N_{a+1} of Γ_{a+1} and note that the functor $R_a \otimes_{R_{a+1}} -$ on left R_{a+1}-modules identifies with taking Δ-coinvariants. In particular, the second and third rows of the exact diagram (7.21) give rise to an exact commutative diagram of R_a-modules

$$\begin{array}{ccccccccc} \mathsf{Tor}_1^{R_{a+1}}(R_a, M'_{(a+1)}) & \xrightarrow{\tilde\kappa_a} & \big(\varrho_{a+1}^t(K)\big)_\Delta & \xrightarrow{(\iota_{a+1})_\Delta} & \big(R_{a+1}^t\big)_\Delta & \to & \big(M'_{(a+1)}\big)_\Delta & \to & 0 \\ & & {\scriptstyle\kappa_a}\downarrow & & {\scriptstyle\cong}\downarrow & & \downarrow & & \\ 0 & \to & \varrho_a^t(K) & \xrightarrow{\iota_a} & R_a^t & \to & M'_{(a)} & \to & 0, \end{array}$$

which implies that $\ker(\kappa_a) = \ker((\iota_{a+1})_\Delta) = \mathrm{im}(\tilde\kappa_a)$ is isomorphic to a quotient of the homology group $\mathsf{Tor}_1^{R_{a+1}}(R_a, M'_{(a+1)}) \cong H_1(\Delta, M'_{(a+1)})$. In particular, since the exponent of the latter group divides $|\Delta|$ (which is a finite power of p), the same is true for the group $\ker(\kappa_a)$.

On the other hand, the first row of (7.21) induces an isomorphism of $\ker(\nu_{a+1}) = \ker(\iota_{(a+1)})$ with $\mathsf{Tor}_1^R(R_{a+1}, M')$ and hence gives rise to an exact commutative diagram

$$\begin{array}{ccccccccc} & & \big(\mathsf{Tor}_1^R(R_{a+1}, M')\big)_\Delta & \longrightarrow & \big(K_{(a+1)}\big)_\Delta & \xrightarrow{(\nu_{a+1})_\Delta} & \big(\varrho_{a+1}^t(K)\big)_\Delta & \longrightarrow & 0 \\ & & \downarrow & & \cong\downarrow & & \downarrow{\scriptstyle \kappa_a} & & \\ 0 & \longrightarrow & \mathsf{Tor}_1^R(R_a, M') & \longrightarrow & K_{(a)} & \xrightarrow{\nu_a} & \varrho_a^t(K) & \longrightarrow & 0. \end{array}$$

This diagram implies $\ker(\kappa_a)$ is isomorphic to a quotient of $\mathsf{Tor}_1^R(R_a, M')$. Hence, since the exponent of $\ker(\kappa_a)$ divides $|\Delta|$, to prove κ_a is injective it is enough to show $\mathsf{Tor}_1^R(R_a, M')$, and hence also $\ker(\kappa_a)$, is p-divisible. To prove this we first note that the exact sequence (7.15) (with $n = d+3$) induces an isomorphism between $\mathsf{Tor}_1^R(R_a, M') = \mathsf{Tor}_1^R(R_a, \mathrm{im}(\theta_{d+3}))$ and $\mathsf{Tor}_{d+3}^R(R_a, \mathrm{im}(\theta_1))$.

The key point now is that, since G has no element of order p, its p-cohomological dimension is finite and equal to d (by Serre [70, Cor. (1)]). In particular, by applying a result of Brumer [15, Th. 4.1 with $\Omega = \mathbb{Z}_p$] in this case, it follows that $\mathrm{pd}_\Lambda\big(\mathrm{im}(\theta_1)_{\langle p\rangle}\big) \leq d+1$.

In addition, the sequence (7.15) (with $n = d+3$) implies that the R-module $\mathrm{im}(\theta_1)$ is finitely $(d+2)$-presented. Hence, since neither $\mathrm{im}(\theta_1) \subseteq R^{t_0}$ nor R_a has an element of order p, we may apply Proposition 7.3.4 with $M = \mathrm{im}(\theta_1), L = R_a, n = d+2$ and $a = d+3$ in order to deduce that $\mathsf{Tor}_{d+3}^R(R_a, \mathrm{im}(\theta_1)) \cong \mathsf{Tor}_1^R(R_a, M')$, and hence also $\ker(\kappa_a)$, is p-divisible, as required. □

In view of Proposition 7.3.6(ii), we can now apply Proposition 7.3.3(ii) to the R-module K to deduce it is finitely generated provided that, as m varies, the quantities $\mu_{R_m}\big(\varrho_m^t(K)\big)$ are bounded independently of m. By applying the Forster-Swan Theorem (cf. [29, Th. 41.21]) to each order R_m, the latter condition is then reduced to showing the existence of a natural number c such that, for every m and every prime ideal $\mathfrak{p}$ of $\mathbb{Z}$, one has

$$\mu_{R_{m,\mathfrak{p}}}\big(\varrho^t_m(K)_\mathfrak{p}\big) \leq c.$$

We therefore fix m and first consider $\mu_{R_{m,\mathfrak{p}}}\big(\varrho^t_m(K)_\mathfrak{p}\big)$ for prime ideals $\mathfrak{p} \neq p\mathbb{Z}$. To do this, we fix such a $\mathfrak{p}$ and set $\mathcal{A} := R_{m,\mathfrak{p}} = \mathbb{Z}_\mathfrak{p}[\Gamma_m]$ and $A := \mathbb{Q}_\mathfrak{p}[\Gamma_m]$. Then, since Γ_m is a finite p-group (and so $|\Gamma_m| \notin \mathfrak{p}$), $\mathcal{A}$ is a maximal $\mathbb{Z}_\mathfrak{p}$-order in the finite-dimensional separable $\mathbb{Q}_\mathfrak{p}$-algebra A, and so the results of Auslander and Goldman in [5] imply that $\mathcal{A}$-lattices M and N are isomorphic if and only if the associated A-modules $\mathbb{Q}_\mathfrak{p} \otimes_{\mathbb{Z}_\mathfrak{p}} M$ and $\mathbb{Q}_\mathfrak{p} \otimes_{\mathbb{Z}_\mathfrak{p}} N$ are isomorphic (for details see Reiner [66, Th. (18.10)]). In addition, if we write $\{e_i\}_{i\in I}$ for the full set of (mutually orthogonal) primitive central idempotents of A, then the maximality of $\mathcal{A}$ implies that it decomposes as a direct product $\prod_{i\in I} \mathcal{A}e_i$ of $\mathbb{Z}_\mathfrak{p}$-orders and, for a set of non-negative integers $\{d_i\}_{i\in I}$, there exists an isomorphism of A-modules

$$\mathbb{Q}_\mathfrak{p} \otimes_{\mathbb{Z}_\mathfrak{p}} \varrho^t_m(K)_\mathfrak{p} \cong \bigoplus\nolimits_{i\in I} (Ae_i)^{d_i} \cong \mathbb{Q}_\mathfrak{p} \otimes_{\mathbb{Z}_\mathfrak{p}} \bigoplus\nolimits_{i\in I} (\mathcal{A}e_i)^{d_i}$$

(see, for example, [29, Prop. (3.18)]). It follows that the $\mathcal{A}$-lattice $\varrho^t_m(K)_\mathfrak{p}$ is isomorphic to $\bigoplus_{i\in I}(\mathcal{A}e_i)^{d_i}$ and hence that $\mu_\mathcal{A}\big(\varrho^t_m(K)_\mathfrak{p}\big)$ is the maximum of the set $\{d_i : i \in I\}$. On the other hand, since $\varrho^t_m(K) \subseteq R^t_m$, for each $i \in I$ the $\mathbb{Q}_\mathfrak{p}$-space $(Ae_i)^{d_i} \cong e_i(\mathbb{Q}_\mathfrak{p} \otimes_\mathbb{Z} \varrho^t_m(K))$ is a subspace of $e_i(\mathbb{Q}_\mathfrak{p} \otimes_\mathbb{Z} R^t_m) = (Ae_i)^t$. It follows that $d_i \leq t$ for all $i \in I$, and hence that $\mu_\mathcal{A}\big(\varrho^t_m(K)_\mathfrak{p}\big) \leq t$.

We now compute $\mu_{R_{m,\mathfrak{p}}}\big(\varrho^t_m(K)_\mathfrak{p}\big)$ for the ideal $\mathfrak{p} = p\mathbb{Z}$. In this case, the kernel of the projection $R_{m,\mathfrak{p}} \to R_{0,\mathfrak{p}} = \mathbb{Z}_p$ belongs to the Jacobson radical of $R_{m,\mathfrak{p}}$ and so Nakayama's Lemma combines with the isomorphism $\mathbb{Z}_p \otimes_{R_{m,\mathfrak{p}}} \varrho^t_m(K) \cong \varrho^t_0(K)_\mathfrak{p}$ that is induced by (the argument of) Proposition 7.3.6(ii) to imply that $\mu_{R_{m,\mathfrak{p}}}\big(\varrho^t_m(K)_\mathfrak{p}\big) = \mu_{\mathbb{Z}_p}(\mathbb{Z}_p \otimes_\mathbb{Z} \varrho^t_0(K))$.

Thus, if one takes c to be the maximum of t and $\mu_{\mathbb{Z}_p}(\mathbb{Z}_p \otimes_\mathbb{Z} \varrho^t_0(K))$, then the above argument shows that $\mu_{R_{m,\mathfrak{p}}}\big(\varrho^t_m(K)_{\mathfrak{p}}\big) \leq c$ for every m and every prime ideal $\mathfrak{p}$ of $\mathbb{Z}$. This therefore completes the proof of Theorem 7.1.2.

Remark 7.3.7. *In this remark, we continue to assume G is a compact p-adic analytic group of rank d, and consider the possibility of strengthening Theorem 7.1.2.*

(i) In order to prove, by the same method, R is $(d+2)$-coherent, it would be enough to show, if $n = d+2$ in (7.15), then $\mathrm{pd}_\Lambda\big(\mathrm{im}(\theta_1)_{\langle p\rangle}\big) < d+1$. This condition is satisfied if $\bigcup_{n\in\mathbb{N}} M[p^n]$ has no non-zero p-divisible subgroup (as is the case if M is pro-discrete) since then the induced map $\mathrm{im}(\theta_1)_{\langle p\rangle} \to R^{t_0}_{\langle p\rangle}$ is injective and so [15, Th. 4.1] implies $\mathrm{pd}_\Lambda\big(\mathrm{im}(\theta_1)_{\langle p\rangle}\big) \leq d$. In general, however, establishing injectivity of all the possible maps $\mathrm{im}(\theta_1)_{\langle p\rangle} \to R^{t_0}_{\langle p\rangle}$ is, in effect, equivalent to showing R satisfies a variant of the Artin-Rees property relative to the ideal pR and seems difficult.

(ii) If $d \leq 2$, then an alternative approach (that does not rely on [15] and [70]) can be used to improve Theorem 7.1.2. Specifically, if either $d = 1$, or $d = 2$ and G contains a pro-p meta-procyclic subgroup (in the sense of [31, Chap. 3, Ex. 10]), then a special case of the exact sequence in Proposition 7.2.1 can be used to show directly that, if $n = 2d$ in (7.15), then $\mathsf{Tor}^R_{2d}(R_a, \mathrm{im}(\theta_1))$ is p-divisible, and so (by the above argument) R is $2d$-coherent. This approach underlies the proof of [17, Th. 1.1] (for $G = \mathbb{Z}_p$), but does not apply in all cases since pro-p compact p-adic analytic groups need not have any infinite procyclic normal subgroups (for example, if $m \geq 3$, then results [51, Th. 1 and Th. 3(ii)] of Klingenberg imply all infinite normal subgroups of $\mathrm{SL}_m(\mathbb{Z}_p)$ are open). In fact, by closely analysing the finite-presentability of pro-discrete modules, it is also shown in [17, Th. 1.1 and Prop. 5.2] that $\mathbb{Z}[[\mathbb{Z}_p]]$ has weak Krull dimension 2 (in the sense of Tang [71]) and, for 'most' p, is a $(2,2)$-domain that is neither a $(1,2)$-domain nor a $(2,1)$-domain (in the sense of Costa [28]). However, we do not know the extent, if any, to which such finer structure results generalise.

Bibliography

[1] Shreeram Abhyankar. Local uniformization on algebraic surfaces over ground fields of characteristic $p \neq 0$. *Annals of Mathematics*, 63(3):491–526, 1956.

[2] Frank W. Anderson and Kent R. Fuller. *Rings and Categories of Modules*, volume 13 of *Graduate Texts in Mathematics*. Springer New York, New York, NY, second edition. edition, 1998.

[3] Bruno Anglès, Andrea Bandini, Francesc Bars, and Ignazio Longhi. Iwasawa main conjecture for the Carlitz cyclotomic extension and applications. *Mathematische Annalen*, 376(1):475–523, 2020.

[4] Emil Artin and John Tate. *Class field theory*. Benjamin, New York, 1967.

[5] Maurice Auslander and Oscar Goldman. Maximal orders. *Transactions of the American Mathematical Society*, 97(1):1–24, 1960.

[6] Gorô Azumaya. Corrections and supplementaries to my paper concerning Krull-Remak-Schmidt's theorem. *Nagoya Mathematical Journal*, 1:117–124, 1950.

[7] Andrea Bandini, Francesc Bars, and Ignazio Longhi. Characteristic ideals and Iwasawa theory. *New York Journal of Mathematics*, 20:759–778, 2014.

[8] Andrea Bandini, Francesc Bars, and Ignazio Longhi. Characteristic ideals and Selmer groups. *Journal of Number Theory*, 157:530–546, 2015.

[9] Andrea Bandini, Francesc Bars, Ignazio Longhi, et al. Aspects of Iwasawa

theory over function fields. *t-motives: Hodge structures, transcendence and other motivic aspects*, pages 375–416, 2020.

[10] Andrea Bandini and Edoardo Coscelli. Stickelberger series and main conjecture for function fields. *Publicacions matematiques*, 65(2):459–498, 2021.

[11] Lior Bary-Soroker, Moshe Jarden, and Danny Neftin. The Sylow subgroups of the absolute Galois group Gal $(\mathbb{Q})$. *Advances in Mathematics*, 284:186–212, 2015.

[12] Werner Bley and Cristian D. Popescu. Geometric main conjectures in function fields. *Journal für die reine und angewandte Mathematik (Crelles Journal)*, 2025(818):1–33, 2025.

[13] Nicolas Bourbaki. *Commutative algebra.* Actualités scientifiques et industrielles. Hermann, Paris, 1972.

[14] Daniel Bravo and Marco A. Pérez. Finiteness conditions and cotorsion pairs. *Journal of Pure and Applied Algebra*, 221(6):1249–1267, 2017.

[15] Armand Brumer. Pseudocompact algebras, profinite groups and class formations. *Journal of Algebra*, 4(3):442–470, 1966.

[16] David Burns. Congruences between derivatives of geometric L-functions. *Inventiones mathematicae*, 184(2):221–256, 2011.

[17] David Burns and Alexandre Daoud. On integral Iwasawa theory, I: Preliminaryies on $\mathbb{Z}[[\mathbb{Z}_p]]$. *Nagoya Mathematical Journal*, 2025.

[18] David Burns and Mahesh Kakde. On Weil-étale cohomology and Artin L-series. *submitted for publication.*

[19] David Burns, Yu Kuang, and Dingli Liang. On the coherency of completed group algebras. *Journal of Algebra*, 661:757–777, 2025.

[20] Colin J. Bushnell and Guy Henniart. *The local Langlands conjecture for*

GL(2). Grundlehren der mathematischen Wissenschaften ; 335. Springer, Berlin ;, 2006.

[21] Henri Cartan and Samuel Eilenberg. *Homological algebra*, volume 19. Princeton university press, 1999.

[22] J. W. S. Cassels, A Fröhlich, London Mathematical Society, and International Mathematical Union. *Algebraic number theory : proceedings of an instructional conference*. Academic Press, London, 1967.

[23] Gyu Whan Chang. Rings of formal power series in an infinite set of indeterminates. *Communications in Algebra*, 42(10):4182–4187, 2014.

[24] Stephen U Chase. Direct products of modules. *Transactions of the American Mathematical Society*, 97(3):457–473, 1960.

[25] I. S. Cohen. Commutative rings with restricted minimum condition. *Duke mathematical journal*, 17(1):27–42, 1950.

[26] Robert F. Coleman. On an archimedian characterization of the circular units. *Journal für die reine und angewandte Mathematik*, 356:161–173, 1985.

[27] Vincent Cossart and Olivier Piltant. Resolution of singularities of threefolds in positive characteristic. I.: Reduction to local uniformization on Artin–Schreier and purely inseparable coverings. *Journal of Algebra*, 320(3):1051–1082, 2008.

[28] D.L. Costa. Parameterizing families of non-Noetherian rings. *Communications in Algebra*, 22(10):3997–4011, 1994.

[29] Charles W Curtis and Irving Reiner. *Methods of representation theory: with applications to finite groups and orders*, volume I,II. John Wiley and Sons, 1981.

[30] P. Deligne. Les constantes des equations fonctionnelles des fonctions l. In Pierre Deligne and Willem Kuijk, editors, *Modular Functions of One*

Variable II, pages 501–597, Berlin, Heidelberg, 1973. Springer Berlin Heidelberg.

[31] John D. Dixon. *Analytic pro-p groups.* London Mathematical Society lecture note series ; 157. Cambridge University Press, Cambridge ;, 1991.

[32] David E Dobbs. On going down for simple overrings. *Proceedings of the American Mathematical Society*, 39(3):515–519, 1973.

[33] David E Dobbs, Salah-Eddine Kabbaj, and Najib Mahdou. n-Coherent rings and modules. In *Commutative Ring Theory*, pages 269–282. CRC Press, 2023.

[34] L. van den Dries and Angus Macintyre. The logic of rumely's local-global principle. *Journal für die reine und angewandte Mathematik*, 407:33–56, 1990.

[35] Paul M. Eakin and William J. Heinzer. Some open questions on minimal primes of a Krull domain. *Canadian journal of mathematics*, 20:1261–1264, 1968.

[36] Eugenia Ellis and Rafael Parra. K-theory of n-coherent rings. *Journal of Algebra and Its Applications*, 21(12):2350007, 2022.

[37] Shizuo Endo. On semi-hereditary rings. *Journal of the Mathematical Society of Japan*, 13(2):109–119, 1961.

[38] Antonio J Engler and Alexander Prestel. *Valued fields.* Springer Science & Business Media, 2005.

[39] Fabio Ferri and Henri Johnston. Applications of representation theory and of explicit units to Leopoldt's conjecture. *arXiv preprint*, 2023.

[40] Matthias Flach. Euler characteristics in relative K-groups. *Bulletin of the London Mathematical Society*, 32(3):272–284, 2000.

[41] László Fuchs and Luigi Salce. *Modules over Non-Noetherian Domains*,

volume 84 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2001.

[42] Robert Gilmer. Power series rings over a Krull domain. *Pacific Journal of Mathematics*, 29(3):543–549, 1969.

[43] Sarah Glaz. Finite conductor rings. *Proceedings of the American Mathematical Society*, 129(10):2833–2843, 2001.

[44] Sarah Glaz. *Commutative coherent rings*, volume 1371. Springer, 2006.

[45] Ralph Greenberg. The Iwasawa invariants of Γ-extensions of a fixed number field. *American Journal of Mathematics*, 95(1):204–214, 1973.

[46] William Hart, David Harvey, and Wilson Ong. Irregular primes to two billion. *Mathematics of Computation*, 86(308):3031–3049, 2017.

[47] Heisuke Hironaka. Resolution of singularities of an algebraic variety over a field of characteristic zero: I. *Annals of Mathematics*, 79(1):109–203, 1964.

[48] Irving Kaplansky. Elementary divisors and modules. *Transactions of the American Mathematical Society*, 66(2):464–491, 1949.

[49] Irving Kaplansky. *Fields and rings*. Chicago lectures in mathematics. University of Chicago Press, Chicago ;, 2nd ed edition, 1972.

[50] Nicholas M. Katz and Pierre Deligne. *Groupes de monodromie en géométrie algébrique : (SGA 7II)*. Lecture notes in mathematics ; 340. Springer, Berlin, 1973.

[51] Wilhelm Klingenberg. Lineare Gruppen über lokalen Ringen. *American Journal of Mathematics*, pages 137–153, 1961.

[52] Tsit-Yuen Lam. *Lectures on modules and rings*, volume 189 of *Graduate Texts in Mathematics*. Springer Science & Business Media, 2012.

[53] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer Science & Business Media, 1994.

[54] Serge Lang. *Cyclotomic fields I and II*, volume 121 of *Graduate Texts in Mathematics*. Springer Science & Business Media, 2012.

[55] Max D. Larsen, William J. Lewis, and Thomas S. Shores. Elementary divisor rings and finitely presented modules. *Transactions of the American Mathematical Society*, 187:231–248, 1974.

[56] Max Dean Larsen and Paul Joseph McCarthy. *Multiplicative theory of ideals*. Pure and applied mathematics / Academic Press ; 43. Academic Press, New York ;, 1971.

[57] Michel Lazard. Groupes analytiques p-adiques. *Publications Mathématiques de l'IHÉS*, 26:5–219, 1965.

[58] S. Lichtenbaum. The Weil-étale topology on schemes over finite fields. *Compositio mathematica*, 141(3):689–702, 2005.

[59] Hideyuki Matsumura. *Commutative ring theory*. Cambridge university press, 1989.

[60] Ján Mináč, Michael Rogelstad, and Nguyen Tân. Relations in the maximal pro-p quotients of absolute Galois groups. *Transactions of the American Mathematical Society*, 373(4):2499–2524, 2020.

[61] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften*. Springer Science & Business Media, 2013.

[62] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften*. Springer Science & Business Media, 2013.

[63] Andreas Neumann. Completed group algebras without zero divisors. *Archiv der Mathematik*, 51:496–499, 1988.

[64] Hajime Nishimura. On the unique factorization theorem for formal power series. *Journal of Mathematics of Kyoto University*, 7(2):151–160, 1967.

[65] Bernadette Perrin-Riou. Arithmétique des courbes elliptiques et théorie d'Iwasawa. *Mémoires de la société mathématique de France*, 17:1–130, 1984.

[66] Irving Reiner. *Maximal orders*. L.M.S. monographs ; 5. Academic Press for the London Mathematical Society, London, 1975.

[67] Michael Rosen. Formal Drinfeld modules. *Journal of Number Theory*, 103(2):234–256, 2003.

[68] Michael Rosen. *Number theory in function fields*, volume 210 of *Graduate Texts in Mathematics*. Springer Science & Business Media, 2013.

[69] Joseph J. Rotman. *An introduction to homological algebra*. Pure and applied mathematics. Academic Press, New York ;, 1979.

[70] Jean-Pierre Serre. Sur la dimension cohomologique des groupes profinis. In *Oeuvres-Collected Papers II*, pages 264–271. Springer, 2003.

[71] Gaohua Tang. Weak Krull dimension over commutative rings. In *Advances in Ring Theory*, pages 215–224. World Scientific, 2005.

[72] J. Tate. Number theoretic background. In *Automorphic Forms, Representations and L-Functions*, volume 33.2 of *Proceedings of Symposia in Pure Mathematics*, pages 3–26. American Mathematical Society, Providence, Rhode Island, 1979.

[73] John Torrence Tate, Dominique Bernardi, and Norbert Schappacher. *Les conjectures de Stark sur les fonctions L d'Artin en s=O : notes d'un cours à Orsay [de] John Tate*. Progress in mathematics ; vol. 47. Birkhäuser, Boston, 1984.

[74] John Von Neumann. On regular rings. *Proceedings of the National Academy of Sciences - PNAS*, 22(12):707–713, 1936.

[75] R. B. Warfield. Decomposability of finitely presented modules. *Proceedings of the American Mathematical Society*, 25(1):167–172, 1970.

[76] Robert Warfield. Purity and algebraic compactness for modules. *Pacific Journal of Mathematics*, 28(3):699–719, 1969.

[77] Lawrence C. Washington. Class numbers and $\mathbb{Z}_p$-extensions. *Mathematische Annalen*, 214:177–193, 1975.

[78] Lawrence C. Washington. The non-p-part of the class number in a cyclotomic $\mathbb{Z}_p$-extension. *Inventiones mathematicae*, 49:87–97, 1978.

[79] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer Science & Business Media, 2012.

[80] Andre Weil. Sur la Théorie du Corps de Classes. *Journal of the Mathematical Society of Japan*, 3(1):1 – 35, 1951.

[81] Zhanmin Zhu. On n-coherent rings, n-hereditary rings and n-regular rings. *Bull. Iranian Math. Soc.*, 2011.