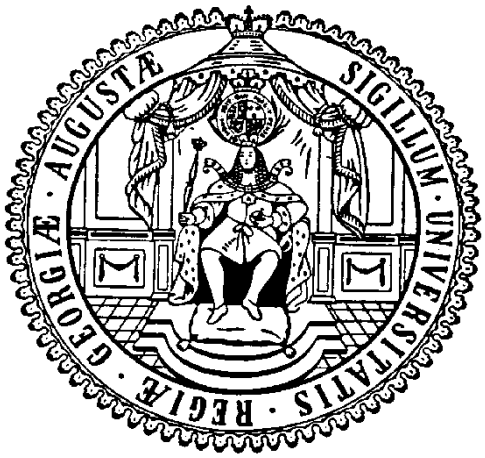
A new approach to the investigation of Iwasawa invariants

Dissertation
zur Erlangung des mathematisch-naturwissenschaftlichen Doktorgrades
"Doctor rerum naturalium"
der Georg-August-Universität Göttingen

im Promotionsprogramm 'Mathematical Sciences'
der Georg-August University School of Science (GAUSS)



vorgelegt von

Sören Kleine

aus Hagen

Göttingen, 2014

Betreuungsausschuss

Prof. Dr. Preda Mihăilescu, Mathematisches Institut

Prof. Dr. Valentin Blomer, Mathematisches Institut

Mitglieder der Prüfungskommission

Referent: Prof. Dr. Preda Mihăilescu, Mathematisches Institut

Koreferent: Prof. Dr. Valentin Blomer, Mathematisches Institut

Weitere Mitglieder der Prüfungskommission:

Prof. Dr. Ina Kersten, Mathematisches Institut

Prof. Dr. Jörg Brüdern, Mathematisches Institut

Prof. Dr. Russell Luke, Institut für Numerische und Angewandte Mathematik

Prof. Dr. Carsten Damm, Institut für Informatik

Tag der mündlichen Prüfung: 16. Dezember 2014

Acknowledgement

I would like to thank the people who contributed to the writing of this thesis. First of all, I am grateful to my supervisor, Prof. Dr. Preda Mihăilescu, for his patient encouragement, his optimism, and for allowing me great latitude for doing my own research.

I also want to thank my second supervisor, Prof. Dr. Valentin Blomer, who has always been available for giving me advice when I needed it. Furthermore, I would like to thank my colleagues for their interest, support and for the good time we shared over the last years. Special thanks are due to Stefan Baur for his help concerning all kinds of IT problems.

Finally, I am deeply indebted to my family for their steady support and understanding. Particularly, my sister made great efforts to check the entire manuscript for orthographical mistakes. Without them, this work would not have been possible.

Introduction

In the 1950s, K. Iwasawa initiated the study of $\mathbb{Z}_p$-extensions, which became an area of extensive research. We will briefly sketch the basic notions of classical Iwasawa theory, thus describing the setting for the investigations done in this thesis. For details, we refer to the rigorous introduction to the subject given in Chapter 1.

Let p denote a fixed prime number. Let K be a number field, i.e., a finite algebraic extension of the field $\mathbb{Q}$ of rational numbers. We consider a sequence of field extensions

$$K_0 := K \subseteq K_1 \subseteq K_2 \subseteq \dots$$

such that for every $n \in \mathbb{N}$, K_n/K is a cyclic extension of degree p^n. Then $\mathbb{K} := \bigcup_{n\geq 0} K_n$ is called a $\mathbb{Z}_p$-*extension* of K. One can show that the $K_n \subseteq \mathbb{K}$, $n \in \mathbb{N}$, are the only intermediate fields in the extension $\mathbb{K}/K$. The name '$\mathbb{Z}_p$-extension' is based on the fact that

$$\mathrm{Gal}(\mathbb{K}/K) \cong \varprojlim \mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_p .$$

Here $\mathbb{Z}_p$ denotes the additive group of p-adic integers.

The most basic example of a $\mathbb{Z}_p$-extension of a fixed number field K arises if we consider the algebraic extension L of K that is generated by all p-power roots of unity. L contains the so-called *cyclotomic* $\mathbb{Z}_p$*-extension of* K. In particular, every number field has at least one $\mathbb{Z}_p$-extension. Typically there exist infinitely many $\mathbb{Z}_p$-extensions of K; in fact the set of $\mathbb{Z}_p$-extensions of K can be finite only is K is totally real.

A basic problem in algebraic number theory is the investigation of the ideal class groups of given number fields. In general, it is a highly non-trivial task to actually determine the structure of these groups, in particular if the degree of the number field becomes large.

Iwasawa showed that in the case of a $\mathbb{Z}_p$-extension, the orders of the p-Sylow subgroups A_n of the ideal class groups of the intermediate fields K_n grow very uniformly. The following famous theorem actually gives a complete asymptotic description of the growth of these groups and therefore contains information about the class numbers of a sequence of number fields having unbounded degrees.

Theorem 0.1 (Iwasawa)**.** *There exist integers μ, λ and ν such that μ, $\lambda \geq 0$ and such that for every sufficiently large n, $|A_n| = p^{e_n}$ with*

$$e_n = \mu \cdot p^n + \lambda \cdot n + \nu .$$

This remarkable result describes the information about the class-numbers p^{e_n} in terms of the so-called *Iwasawa invariants* μ, λ and ν of $\mathbb{K}/K$.

We are therefore naturally lead to the problem of determining, for a given $\mathbb{Z}_p$-extension $\mathbb{K}/K$, the corresponding Iwasawa invariants. After more than 50 years of research, only very few general properties of these invariants are known. For example, Iwasawa conjectured that the μ-invariant of a cyclotomic $\mathbb{Z}_p$-extension $\mathbb{K}/K$ always vanishes. This has been proved for abelian ground fields K, and has also been checked numerically for many other fields, but the general problem is still open.

The present work contains a new approach to the investigation of Iwasawa's invariants. We will be concerned with the study of Iwasawa invariants attached to $\mathbb{Z}_p$-extensions of a fixed number field K. If $\mathcal{E}(K)$ denotes the set of $\mathbb{Z}_p$-extensions of K, then to each $\mathbb{K} \in \mathcal{E}(K)$ is attached a tuple of invariants. We will thus regard the Iwasawa invariants as maps

$$\mu, \lambda, \nu : \mathcal{E}(K) \longrightarrow \mathbb{Z} ,$$

and we want to study properties of these maps.

In his Ph.D. thesis, R. Greenberg defined a topology on the set $\mathcal{E}(K)$ with respect to which $\mathcal{E}(K)$ becomes a compact topological space. This induced new kinds of questions. For example, suppose that $\mathbb{K}, \mathbb{L} \in \mathcal{E}(K)$ are two elements which are 'close' with respect to Greenberg's topology. Does this imply that the values of $\mathbb{K}$ and $\mathbb{L}$ under μ, λ and ν are also close in $\mathbb{Z}$? Greenberg proved some first results in this direction.

Theorem 0.2 (Greenberg)**.** *Let $\mathbb{K}/K$ denote a $\mathbb{Z}_p$-extension such that only finitely many primes of $\mathbb{K}$ divide p. Then μ is* **locally bounded** *around $\mathbb{K}$, i.e., there exist a constant $C \in \mathbb{N}$ and a neighbourhood U of $\mathbb{K}$ such that $\mu(\mathbb{L}/K) \leq C$ for each $\mathbb{L} \in U$.*
If moreover $\mu(\mathbb{K}/K) = 0$, then there exists a neighbourhood U of $\mathbb{K}$ such that $\mu = 0$ on U and such that λ is bounded on U.

In this thesis, we will improve on these results, using a completely different approach. We will define a finer topology that takes care of ramification, and we will be able to prove that with respect to this topology, the following theorem holds.

Theorem 0.3. *Let $\mathbb{K}/K$ denote any $\mathbb{Z}_p$-extension.*

(i) There exists a neighbourhood U of $\mathbb{K}$ such that μ is **locally maximal** *on U, i.e., $\mu(\mathbb{L}/K) \leq \mu(\mathbb{K}/K)$ for every $\mathbb{L} \in U$.*

(ii) There exists a neighbourhood U of $\mathbb{K}$ such that $\lambda(\mathbb{L}/K) \leq \lambda(\mathbb{K}/K)$ for every $\mathbb{L} \in U$ satisfying $\mu(\mathbb{L}/K) = \mu(\mathbb{K}/K)$.

(iii) There exists a neighbourhood U of $\mathbb{K}$ such that $\nu(\mathbb{L}/K) = \nu(\mathbb{K}/K)$ for every $\mathbb{L} \in U$ satisfying $\mu(\mathbb{L}/K) = \mu(\mathbb{K}/K)$ and $\lambda(\mathbb{L}/K) = \lambda(\mathbb{K}/K)$.

This nicely reflects the hierarchy of Iwasawa's invariants: The μ-invariant describes the dominating part of the growth of the $|A_n|$, whereas the ν-invariants contains the finer information. It is one of the main advantages of our method

that we are able to obtain results about λ- and ν-invariants also in the case where the μ-invariant does not vanish.

Based on Greenberg's results, V.A. BABAĬCEV equipped the set $\mathcal{E}(K)$ with the structure of a projective variety, and he used geometric arguments in order to prove that μ is in fact ***globally bounded*** on $\mathcal{E}(K)$. This was also proved independently by P. MONSKY . It is unknown whether the same is true for λ-invariants. We will enhance the methods of Monsky and Babaĭcev and develop necessary and sufficient criteria for the λ-invariants to be globally bounded.

Finally, we consider, more generally, $\mathbb{Z}_p^i$-extensions of K, $i \in \mathbb{N}$, and we show how to generalise the approach used for the study of Iwasawa invariants to this higher-dimensional setting.

We will now briefly give an outline of the contents of the individual chapters of this work.

0.1 Structure of the thesis

Chapter 1. In the first chapter, we will introduce the basic notions and collect some facts concerning $\mathbb{Z}_p$-extensions. In particular, we will point out the main ingredients that are used in the proof of Iwasawa's famous Theorem 0.1. This will include an overview of the theory of finitely generated $\mathbb{Z}_p[[T]]$-modules because the action of the ring $\mathbb{Z}_p[[T]]$ on the ideal class groups is of fundamental importance in this context.

Chapter 2. We will define more structure on the set $\mathcal{E}(K)$ of $\mathbb{Z}_p$-extensions of K. On the one hand, we will describe Greenberg's topology on $\mathcal{E}(K)$. On the other hand, we will depict several ways to turn $\mathcal{E}(K)$ into a projective variety; this contains work of Babaĭcev.

Finally, Chapter 2 also prepares for the study of multiple $\mathbb{Z}_p$-extensions in later chapters. Analogously to the one-dimensional case, the action of power series rings $\mathbb{Z}_p[[T_1, \ldots, T_i]]$ in a suitable number of variables is of particular interest for these investigations. We will therefore collect basic facts about the rings $\mathbb{Z}_p[[T_1, \ldots, T_i]]$ and about modules over these rings.

Chapter 3. Chapter 3 contains the heart of our work, namely, a new approach to the study of Iwasawa's invariants. This method is based on a generalisation of a theorem of T. FUKUDA concerning the stabilisation of certain ranks. We will be able to obtain information about Iwasawa invariants from the values of these ranks. Therefore bounding the Iwasawa invariants reduces to bounding the ranks. While Fukuda's original theorem considers only p-ranks (i.e., uses group-theoretic information), we will extensively exploit the action of $\mathbb{Z}_p[[T]]$ on the class groups and consider also ranks attached to elements of $\mathbb{Z}_p[[T]] \setminus \mathbb{Z}_p$. This essentially strengthens the power of the approach and is one reason why our method works also in the case of non-vanishing μ-invariants (if $\mu \neq 0$, then the corresponding p-ranks get arbitrarily large and therefore are not suitable for the extraction of information about Iwasawa invariants).

Our approach makes it necessary to refine Greenberg's topology in order to

obtain control on ramification. We will therefore study possible configurations of ramification in multiple $\mathbb{Z}_p$-extensions.

We will also study connections between Iwasawa invariants and the phenomenon of capitulation. This is closely related to the investigation of certain cohomology groups of global units.

Chapter 4. In contrast to the method used in Chapter 3, we will describe the approach that has been developed by Greenberg and Babaĭcev, leading to a proof that μ is globally bounded on $\mathcal{E}(K)$ (the method of Chapter 3 in general is not suitable for attacking this kind of question).

We then apply an adapted version of Greenberg's approach to the task of studying λ-invariants, and we develop a criterion for the λ-invariants to be globally bounded. A special case of this criterion was known to P. Monsky, who considered $\mathbb{Z}_p$-extensions contained in a fixed $\mathbb{Z}_p^2$-extension of K.

Chapter 5. In Chapter 5, we turn to the consideration of multiple $\mathbb{Z}_p$-extensions, i.e., we study $\mathbb{Z}_p^i$-extensions of a number field K, $i \in \mathbb{N}$. A. Cuoco and P. Monsky proved a generalisation of Iwasawa's Theorem 0.1 for multiple $\mathbb{Z}_p$-extensions, introducing *generalised Iwasawa invariants*, which are usually denoted by m_0 and l_0. If $i = 1$, then these invariants reduce to the classical μ- and λ-invariant, respectively (there seems to be no canonical generalisation of Iwasawa's ν-invariant).

Analogously to the investigations in Chapter 3, we study the local behaviour of these generalised Iwasawa invariants. We first show how to use Greenberg's and Babaĭcev's approach, described in Chapter 4, in order to reduce the i-dimensional problem to a one-dimensional problem, which then can be studied with the help of the results proved in Chapter 3. This will yield local boundedness results for m_0 and l_0.

In order to obtain stronger results, we then generalise the method used in Chapter 3 to the higher-dimensional setting in order to apply this method directly to $\mathbb{Z}_p^i$-extensions of K. It turns out that this is considerably more difficult than the one-dimensional case. Particularly, the handling of suitable ranks needs much more effort.

We conclude the chapter with some results concerning the special situation of a $\mathbb{Z}_p^2$-extension, culminating in a new proof of Greenberg's Generalised Conjecture for imaginary quadratic number fields whose class number is coprime to p and in which the rational prime p does not split.

0.2 Notation

We will now introduce some notation that will be used throughout the thesis.

Let M be a finite set. Then we denote by $|M|$ the cardinality of M, i.e., the number of elements contained in M.

$\mathbb{N} = \{1, 2, 3, \dots, \}$ denotes the set of natural numbers, and $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$. $\mathbb{Z}$ denotes the ring of integers. $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ denote the fields of rational, real, and complex numbers, respectively.

Throughout the thesis, p will denote a fixed rational prime number (we will

sometimes assume that $p \neq 2$). $\mathbb{F}_p$ denotes the finite field with p elements, and $\mathbb{Z}_p$, respectively, $\mathbb{Q}_p$, denote the ring, respectively, the field, of p-adic integers.

If G denotes a finite abelian p-group, then the *p-rank* of G,

$$\mathrm{rank}_p(G) := \dim_{\mathbb{F}_p}(G/(p \cdot G)) ,$$

is defined to be the dimension of the $\mathbb{F}_p$-vector space $G/(p \cdot G)$. This is the number r of cyclic groups $\mathbb{Z}/p^n\mathbb{Z}$ in the canonical representation

$$G \cong \mathbb{Z}/p^{n_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{n_r}\mathbb{Z}$$

of G. We could also write $\mathrm{rank}_p(G) = v_p(|G/(p \cdot G)|)$, where v_p denotes the usual p-adic valuation on $\mathbb{Z}$ (i.e., if $n = p^v \cdot n' \in \mathbb{Z}$, $p \nmid n'$, then $v_p(n) = v$).

Moreover, the *exponent* of a finite abelian p-group G, written $\exp(G)$, denotes the smallest power p^n, $n \in \mathbb{N}_0$, that annihilates G.

G is called *p-elementary* if $\exp(G) = p$.

Our rings will always be commutative, and we assume that they contain a multiplicative unit element.

If R is a ring, and if $n, m \in \mathbb{N}$, then $\mathrm{Mat}(n, m, R)$ denotes the set of $n \times m$-matrices over R. $\mathrm{GL}_n(R)$ denotes the subset of invertible $n \times n$-matrices. If $A \in \mathrm{Mat}(n, m, R)$ has entries $a_{ij} \in R$, $1 \leq i \leq n$, $1 \leq j \leq m$, then the *transposed* matrix of A is the matrix $B = A^T \in \mathrm{Mat}(m, n, R)$ having entries $b_{ij} := a_{ji}$, $1 \leq i \leq m$, $1 \leq j \leq n$.

Let R be a ring, and let M denote an R-module. Then the *rank* $\mathrm{rank}_R(M)$ *of M over R* denotes the supremum of the natural numbers n such that there exist n R-linearly independent elements in M.

We will be mainly concerned with *number fields*, i.e., finite algebraic extensions K of $\mathbb{Q}$. For each number field K, we denote by $\mathcal{O}_K$ the ring of integral elements of K. The ideal class group of K will be denoted by $\mathrm{Cl}(K)$.

We will usually assume that we have fixed an algebraic closure $\overline{K}$ of K. An important subfield of $\overline{K}$ is the *Hilbert class field* of K, i.e., the maximal abelian unramified extension of K. Since we are mainly interested in the p-divisibility of class numbers, we will usually consider the maximal unramified p-abelian extension $H(K)$ of K.

We will often denote by $\mathcal{I} = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_t\}$ the set of primes of the number field K that divide our fixed rational prime p.

Fix a number field K. If we consider embeddings $\varphi : K \hookrightarrow \mathbb{C}$ of K into the field $\mathbb{C}$ of complex numbers, then we may distinguish between embeddings mapping K into $\mathbb{R} \subseteq \mathbb{C}$ and those mapping K onto a proper imaginary field. Then $r_1(K)$ will denote the number of real embeddings of K, and $r_2(K)$ denotes the number of pairs of complex conjugate embeddings.

A *CM-field* is a totally imaginary quadratic extension K of a totally real number field K^+. This means that $r_2(K^+) = r_1(K) = 0$ and $[K : K^+] = 2$.

Contents

Chapter 1

Iwasawa's theory of $\mathbb{Z}_p$-extensions

In this first chapter, we will introduce the basic objects that are dealt with in classical Iwasawa theory. This subfield of algebraic number theory is concerned with the study of so-called $\mathbb{Z}_p$-extensions of number fields, which will be defined below. The first section collects, in addition to some examples, basic properties of $\mathbb{Z}_p$-extensions that will be used throughout this thesis.

Typical objects of interest will be the ideal class groups of the number fields contained in a given $\mathbb{Z}_p$-extension. IWASAWA discovered that one can obtain deep insight on the growth of these class groups by taking into account the additional structure arising from the action of certain group rings. Therefore the second section will be devoted to a structure theory of groups admitting an action of such group rings.

This general structure theory may be used to obtain a proof of Iwasawa's famous class number formula (Theorem 1.32). In the third section, we will describe the main ideas used in the proof of this result. In particular, we will discuss several versions of Nakayama's Lemma, which will be an indispensable tool for many proofs derived in this work.

1.1 Basic properties of $\mathbb{Z}_p$-extensions

Let K be a number field and let p be a fixed rational prime. A ***$\mathbb{Z}_p$-extension*** of K is a Galois extension K_∞ of K such that the Galois group $\Gamma := \mathrm{Gal}(K_\infty/K)$ is topologically isomorphic to the additive group $\mathbb{Z}_p$ of p-adic integers. In this section we summarise some basic facts about such extensions. For proofs and more details see [Wa 97], Chapter 13.

Proposition 1.1. *For every $n \in \mathbb{N}$, there is a unique field $K_n \subseteq K_\infty$ such that $\mathrm{Gal}(K_n/K) \cong \mathbb{Z}/p^n\mathbb{Z}$. These are the only intermediate fields in K_∞/K.*

This just follows from infinite Galois theory (see [Neu 92], Thm. IV.1.2): the intermediate fields correspond to the closed subgroups of $\Gamma \cong \mathbb{Z}_p$, and the only non-trivial closed subgroups of $\mathbb{Z}_p$ are the groups $p^n\mathbb{Z}_p$, $n \in \mathbb{N}$.

This means that we can think of the extension K_∞/K as the chain of cyclic field extensions of p-power degree

$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \ldots \subseteq K_n \subseteq \ldots \subseteq K_\infty = \bigcup_{n \in \mathbb{N}_0} K_n \, .$$

Lemma 1.2. *A $\mathbb{Z}_p$-extension K_∞/K is unramified outside the primes of K lying above p. In particular, K_∞/K is unramified at infinity, i.e., a $\mathbb{Z}_p$-extension of a totally real field is totally real.*

Proof. see [Wa 97], Proposition 13.2. □

However, the extension K_∞/K cannot be completely unramified, because otherwise the field K_∞ would be contained in the *Hilbert class field* H of K. But class field theory (see [Neu 92], Theorem VI.6.9) implies that the Galois group $\mathrm{Gal}(H/K)$ is isomorphic to the ideal class group of K, which is finite, and therefore K_∞ would have to be a finite extension of K, which gives a contradiction.

More precisely, we have the following proposition:

Proposition 1.3. *Let K_∞/K be a $\mathbb{Z}_p$-extension. Then at least one prime ramifies in K_∞/K. Moreover, there exists some integer $e \geq 0$ such that every prime which ramifies in K_∞/K_e is totally ramified.*

Proof. see [Wa 97], Lemma 13.3. □

It is, however, possible to have K_n/K unramified for some n (see Example 1.6 below).

Up to now, we have described some properties of $\mathbb{Z}_p$-extensions without having shown yet that such extensions do exist. We will now show that every number field K has at least one $\mathbb{Z}_p$-extension. For that purpose, we first review the following easy group-theoretic result.

Lemma 1.4.

(i) *If $p \neq 2$ is a prime and $e \in \mathbb{N}$, then the group $(\mathbb{Z}/p^e\mathbb{Z})^*$ of multiplicatively invertible elements of the ring $\mathbb{Z}/p^e\mathbb{Z}$ is cyclic, and*

$$(\mathbb{Z}/p^e\mathbb{Z})^* \cong \mathbb{Z}/p^{e-1}\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \, .$$

(ii) *If $e \in \mathbb{N}$, then $(\mathbb{Z}/2^e\mathbb{Z})^*$ is cyclic if and only if $e \in \{1, 2\}$. For $e \geq 3$ we have $(\mathbb{Z}/2^e\mathbb{Z})^* \cong \mathbb{Z}/2^{e-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

Proof. See [Rib 01], 3.(J) and 3.(K). □

Example 1.5. Let p be an odd prime, let ζ_p be a primitive p-th root of unity, and consider the field $K = K_0 := \mathbb{Q}(\zeta_p)$. The fields $K_n := \mathbb{Q}(\zeta_{p^{n+1}})$, $n \in \mathbb{N}$, (where $\zeta_{p^{n+1}}$ denotes a primitive p^{n+1}-th root of unity contained in a fixed algebraic closure $\overline{K}$ of K, respectively) are cyclic over $\mathbb{Q}$ with Galois groups $\mathrm{Gal}(K_n/\mathbb{Q}) \cong (\mathbb{Z}/p^{n+1}\mathbb{Z})^*$. Moreover, each K_n is abelian over $K = K_0$, and

$\mathrm{Gal}(K_n/K) \cong \mathbb{Z}/p^n\mathbb{Z}$ is cyclic of order p^n for all n (compare Lemma 1.4, (i)). Therefore

$$K_\infty := \bigcup_{n\geq 1} K_n = \bigcup_{n\geq 1} \mathbb{Q}(\zeta_{p^{n+1}})$$

is a $\mathbb{Z}_p$-extension of $K = \mathbb{Q}(\zeta_p)$. We call it the ***cyclotomic $\mathbb{Z}_p$-extension of*** K.

Now let K be an arbitrary number field; let p be a prime, let

$$q := \begin{cases} p & : p \text{ is odd} \\ 4 & : p = 2 \end{cases} .$$

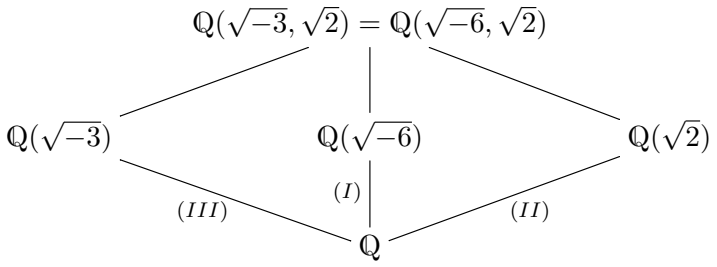
For any $n \in \mathbb{N}$ (in the case $p = 2$, we have to assume that $n > 1$), there is a unique subfield $\mathbb{B}_n$ of $\mathbb{Q}(\zeta_{qp^n})$ which is cyclic of degree p^n over $\mathbb{Q}$ (using the isomorphism from Lemma 1.4, (i), respectively, (ii), define $\mathbb{B}_n$ to be the subfield of $\mathbb{Q}(\zeta_{qp^n})$ fixed by the $\mathbb{Z}/(p-1)\mathbb{Z}$-part, respectively, the $\mathbb{Z}/2\mathbb{Z}$-part, of the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_{qp^n})/\mathbb{Q})$). We define $\mathbb{B}_\infty := \bigcup_{n\geq 1} \mathbb{B}_n$ and $K_\infty := K \cdot \mathbb{B}_\infty$. Then K_∞/K is a $\mathbb{Z}_p$-extension. Indeed, let $L := K \cap \mathbb{B}_\infty$. Then $[L : \mathbb{Q}]$ is a finite power of p, and L is cyclic over $\mathbb{Q}$. Therefore $L = \mathbb{B}_e$ for some $e \geq 0$ by the uniqueness of the $\mathbb{B}_n$. (We have to pay attention to the case $p = 2$: There are *three* cyclic extensions Q_1, Q_2 and Q_3 of degree 2 over $\mathbb{Q}$ that are contained in $\mathbb{Q}(\zeta_8)$ (see Example 1.6 below), and exactly one of them serves as the first step in our $\mathbb{Z}_p$-extension).

Moreover, there are group isomorphisms

$$\begin{aligned} \mathrm{Gal}(K_\infty/K) &= \mathrm{Gal}(K \cdot \mathbb{B}_\infty/K) \cong \mathrm{Gal}(\mathbb{B}_\infty/(K \cap \mathbb{B}_\infty = \mathbb{B}_e)) \\ &\cong p^e\,\mathbb{Z}_p \cong \mathbb{Z}_p\,. \end{aligned}$$

K_∞ is called the ***cyclotomic $\mathbb{Z}_p$-extension of*** K.

Example 1.6. We will now show that it is possible that in a $\mathbb{Z}_p$-extension K_∞/K, K_n/K is unramified for some n (compare Proposition 1.3); the following example is put as an exercise in [Wa 97]. Let $p = 2$. There are exactly three quadratic subfields of $\mathbb{Q}(\zeta_8)$, namely $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i)$ and $\mathbb{Q}(i\sqrt{2})$. Since $\mathbb{Q}(i)/Q$ and $\mathbb{Q}(i\sqrt{2})/\mathbb{Q}$ are ramified at infinity, Lemma 1.2 shows that $\mathbb{Q}(\sqrt{2})$ is the first step of the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}$. More generally, if K is a number field and $\sqrt{2} \notin K$, then $K(\sqrt{2})/K$ is the first step of the cyclotomic $\mathbb{Z}_2$-extension of K. Now consider $K := \mathbb{Q}(\sqrt{-6})$. We show that $K_1 := \mathbb{Q}(\sqrt{-6}, \sqrt{2})$ is unramified over K. In order to see this we consider the following diagram of fields.



We have the following ramification indices in the labelled subextensions (here we denote by $e_p = e_p(M/L)$ the ramification index of the prime p of L in the extension M/L):
(I) $e_2 = e_3 = 2$, all $p \notin \{2, 3\}$ are unramified
(II) $e_2 = 2$, all odd primes are unramified
(III) $e_3 = 2$, all primes $p \neq 3$ are unramified.
We see this by computing the discriminants of these quadratic subfields (a rational prime $p \in \mathbb{Q}$ ramifies in a number field if and only if it divides the absolute discriminant of that field): $\delta_{\mathbb{Q}(\sqrt{2})} = 4 \cdot 2 = 8$, $\delta_{\mathbb{Q}(\sqrt{-6})} = 4 \cdot (-6) = -24$ and $\delta_{\mathbb{Q}(\sqrt{-3})} = -3$ (note that $-3 \equiv 1 \bmod 4$).
By looking at (III), we see that

$$e_2(K_1/\mathbb{Q}) \ \leq \ 2 \ \stackrel{(I)}{=} \ e_2(K/\mathbb{Q}) \ ,$$

and therefore $e_{\mathfrak{p}_2}(K_1/K) = 1$ for the unique prime $\mathfrak{p}_2$ of K lying above 2. Analogously,

$$e_3(K_1/\mathbb{Q}) \ \stackrel{(II)}{\leq} \ 2 \ \stackrel{(I)}{=} \ e_3(K/\mathbb{Q}) \ ,$$

and so $e_{\mathfrak{p}_3}(K_1/K) = 1$ for the unique prime $\mathfrak{p}_3$ of K lying above 3. This shows that K_1/K is unramified, since obviously no prime different from 2 and 3 is ramified in $K_1/\mathbb{Q}$.

Every number field K has at least one $\mathbb{Z}_p$-extension, namely the cyclotomic one, as defined above. We will now give an estimate for the number of $\mathbb{Z}_p$-extensions of K. Two $\mathbb{Z}_p$-extensions L_1/K and L_2/K are called ***independent*** if $L_1 \cap L_2 = K$.

First, we introduce some notation. Let E denote the group of units of (the ring of integers $\mathcal{O}_K$ of) K. Let $\mathcal{I} := \{\mathfrak{p} \subseteq \mathcal{O}_K \ : \ \mathfrak{p} \,|\, (p)\}$ be the set of primes of K lying above p. Define $E_1 := \{\varepsilon \in E \mid \varepsilon \equiv 1 \mod \mathfrak{p} \ \forall\, \mathfrak{p} \in \mathcal{I}\}$. For every $\mathfrak{p} \in \mathcal{I}$ we consider the completion $K_\mathfrak{p}$ of K with respect to the non-archimedean absolute value induced by the prime $\mathfrak{p}$. Let $U_{1,\mathfrak{p}} \subseteq K_\mathfrak{p}$ denote the local units congruent to 1 modulo $\mathfrak{p}$. Then we have a diagonal embedding

$$E_1 \ \longrightarrow \ U_1 \ := \ \prod_{\mathfrak{p} \in \mathcal{I}} U_{1,\mathfrak{p}} \ , \quad \varepsilon \ \mapsto \ (\varepsilon, \ldots, \varepsilon) \ .$$

If $\mathrm{N}(\mathfrak{p})$ denotes the norm of the prime $\mathfrak{p}$, i.e., the number of elements in the residue class field $\mathcal{O}_K/\mathfrak{p}$, then $\varepsilon^{\mathrm{N}(\mathfrak{p})-1} \in U_{1,\mathfrak{p}}$ for any $\varepsilon \in E$. Therefore E_1 is a subgroup of E of finite index, and thus a free abelian group of rank $r = r_1 + r_2 - 1$, where r_1 denotes the number of real embeddings of the number field K and r_2 denotes the number of pairs of complex conjugate embeddings (by Dirichlet's Unit Theorem).

Let $\overline{E_1}$ be the closure of $E_1 \hookrightarrow U_1$ with respect to the product topology on U_1. U_1 is a $\mathbb{Z}_p$-module via $x \cdot u := u^x$ ($x \in \mathbb{Z}_p$, $u \in U_1$), and so the closure $\overline{E_1}$ is also a $\mathbb{Z}_p$-module. It has rank $r_1 + r_2 - 1 - \delta$ for some $\delta = \delta(K) \geq 0$ which is called the ***Leopoldt defect*** of K. ***Leopoldt's Conjecture*** predicts that $\delta = 0$ for every number field K, which has been proved by A. Brumer in [Br 67] for

abelian number fields (so the Leopoldt defect measures the extent to which the conjecture fails).

The following theorem gives an estimate for the number of independent $\mathbb{Z}_p$-extensions of K:

Theorem 1.7. *With the above notation, let d denote the number of independent $\mathbb{Z}_p$-extensions of K. Then $d = r_2 + 1 + \delta$. Therefore*

$$r_2 + 1 \ \leq \ d \ \leq \ 2r_2 + r_1 \ = \ [K : \mathbb{Q}] \ .$$

The proof via class field theory (cf. [Wa 97], pp. 266-269) also shows the following result ([Wa 97], Corollary 13.6):

Lemma 1.8. *Let H be the Hilbert class field of K and let F be the maximal abelian extension of K which is unramified outside primes lying above p. Then there exists a group homomorphism*

$$\mathrm{Gal}(F/H) \ \simeq \ (\prod_{\mathfrak{p} \in \mathcal{I}} U_{\mathfrak{p}})/\overline{E}$$

with finite kernel and cokernel, where $U_{\mathfrak{p}}$ denotes the unit group of the completion $K_{\mathfrak{p}}$, respectively, and $\overline{E}$ is the closure of the group of global units E (embedded in $(\prod_{\mathfrak{p} \in \mathcal{I}} U_{\mathfrak{p}})$ diagonally).

In Chapter 3, we will prove a generalisation of this lemma (compare Lemma 3.28).

1.2 Group rings and Λ-modules

Group rings play an important role in the study of algebraic number fields. For example, suppose that we are interested in the ideal class group $\mathrm{Cl}(K)$ of a number field K which is galois over $\mathbb{Q}$. The group $G := \mathrm{Gal}(K/\mathbb{Q})$ acts on $\mathrm{Cl}(K)$. If we take R to be an appropriate coefficient ring which, too, operates on $\mathrm{Cl}(K)$ (e.g., $R = \mathbb{Z}$), then the group ring $R[G]$ acts on $\mathrm{Cl}(K)$. Now if we have knowledge about the structure of $R[G]$-modules in general, then these results in particular hold for $\mathrm{Cl}(K)$ (viewed as a $R[G]$-module). This approach sometimes delivers a deeper insight into the structure of $\mathrm{Cl}(K)$ or other objects related to K which can be equipped with the structure of a $R[G]$-module.

In our situation, we will usually have $R = \mathbb{Z}_p$. More generally, let $R = \mathcal{O}$ denote a unique factorisation domain that is a local ring with unique maximal ideal $\mathfrak{p}$. Assume further that $\mathcal{O}$ is complete with respect to the $\mathfrak{p}$-adic topology (note that $\mathbb{Z}_p$ fills into this pattern, by [Neu 92], Theorems II.2.3 and II.2.4). Let K be a number field, let K_∞/K be a $\mathbb{Z}_p$-extension with Galois group $\Gamma \cong \mathbb{Z}_p$, and let $\gamma \in \Gamma$ be a fixed topological generator, i.e., the cyclic subgroup generated by γ is dense in Γ with regard to the topology on Γ induced by the p-adic topology on $\mathbb{Z}_p$. This will be the case if, for example, γ corresponds to $1 \in \mathbb{Z}_p$ under the above isomorphism. We will write Γ multiplicatively. Since the only nontrivial closed subgroups of $\mathbb{Z}_p$ are of the form $p^n \mathbb{Z}_p$ for some $n \in \mathbb{N}_0$, the nontrivial closed subgroups of Γ are given by Γ^{p^n}, $n \in \mathbb{N}_0$. If we

define $\Gamma_n := \Gamma/\Gamma^{p^n}$, then Γ_n is a cyclic group of order p^n generated by the coset $\overline{\gamma}$ of γ modulo Γ^{p^n}. It corresponds to the Galois group of the subextension K_n/K (compare Proposition 1.1).

We consider the group rings $\mathcal{O}[\Gamma_n]$, $n \geq 0$. If, for example, $\mathcal{O} = \mathbb{Z}_p$, then $\mathcal{O}[\Gamma_n]$ acts on the p-Sylow parts of the class groups $\mathrm{Cl}(K_n)$, respectively. We would like to define an analogous group ring which acts on arithmetic objects attached to the extension K_∞ itself. It turns out that instead of using the group ring $\mathcal{O}[\Gamma]$ it is much better to consider the so-called ***profinite group ring*** or ***completed group ring*** $\mathcal{O}[[\Gamma]]$ of Γ which is kind of a compactification of $\mathcal{O}[\Gamma]$ and will be defined now.

If $m \geq n \geq 0$ then $\Gamma^{p^m} \subseteq \Gamma^{p^n}$, so there is a canonical surjection $\Gamma_m \twoheadrightarrow \Gamma_n$ which induces a map $\phi_{m,n} : \mathcal{O}[\Gamma_m] \longrightarrow \mathcal{O}[\Gamma_n]$. We define $\mathcal{O}[[\Gamma]]$ to be the inverse limit of the group rings $\mathcal{O}[\Gamma_n]$ with respect to the maps $\phi_{m,n}$. Since any element $\alpha \in \mathcal{O}[\Gamma]$ canonically induces a sequence of elements $\alpha_n \in \mathcal{O}[\Gamma_n]$ such that $\phi_{m,n}(\alpha_m) = \alpha_n \; \forall\, m \geq n \geq 0$, we have an embedding $\mathcal{O}[\Gamma] \hookrightarrow \mathcal{O}[[\Gamma]]$. Note that $\mathcal{O}[[\Gamma]]$ is somewhat 'bigger' than $\mathcal{O}[\Gamma]$ (it contains certain 'infinite' sums of elements of Γ). $\mathcal{O}[[\Gamma]]$ is a compact $\mathcal{O}$-module with respect to the topology induced by the projective limit of the topologies on the $\mathcal{O}[\Gamma_n]$.

At any finite level n we have an isomorphism

$$\mathcal{O}[\Gamma_n] \;\cong\; \mathcal{O}[T]/((1+T)^{p^n} - 1)$$

induced by

$$\gamma \mod \Gamma^{p^n} \;\mapsto\; 1+T \mod ((1+T)^{p^n} - 1)$$

(since $\overline{\gamma^{p^n}} \mapsto \overline{1}$, this map is well-defined; one can easily see that it is onto and one-to-one). If $m \geq n \geq 0$, then $(1+T)^{p^n} - 1$ divides $(1+T)^{p^m} - 1$, so there is a natural map $\theta_{m,n} : \mathcal{O}[T]/((1+T)^{p^m} - 1) \longrightarrow \mathcal{O}[T]/((1+T)^{p^n} - 1)$ corresponding to the map $\phi_{m,n} : \mathcal{O}[\Gamma_m] \longrightarrow \mathcal{O}[\Gamma_n]$ defined above. We obtain

$$\mathcal{O}[[\Gamma]] \;\cong\; \varprojlim_n \mathcal{O}[T]/((1+T)^{p^n} - 1)\;,$$

where the inverse limit on the right-hand side is taken with respect to the maps $\theta_{m,n}$.

The following theorem is fundamental for the understanding of the profinite group ring $\mathcal{O}[[\Gamma]]$.

Theorem 1.9. *Let $\mathcal{O}[[T]]$ denote the ring of formal power series in one variable with coefficients in $\mathcal{O}$. Then $\mathcal{O}[[\Gamma]] \cong \mathcal{O}[[T]]$ as $\mathcal{O}$-algebras, the isomorphism being induced by $\gamma \mapsto 1+T$.*

The proof (see, for example, [Wa 97], pp. 114-117) is based on the following auxiliary results which are important on their own.

Lemma 1.10 (Division Lemma). *Let $\mathcal{O}$ be a local ring with maximal ideal $\mathfrak{p}$ that is Hausdorff and complete with regard to the $\mathfrak{p}$-adic topology. Let*

$$f \;=\; \sum_{i=0}^{\infty} a_i T_i \in \mathcal{O}[[T]]\;,$$

and assume that $n := \inf(\{i \mid a_i \notin \mathfrak{p}\})$ *is finite (*n *is called the* **reduced degree** *of* f*). Then every* $g \in \mathcal{O}[[T]]$ *may be uniquely written as*

$$g \;=\; qf + r \;,$$

with $q \in \mathcal{O}[[T]]$*, and where* $r \in \mathcal{O}[T]$ *is a polynomial of degree at most* $n-1$*. In particular,* $\mathcal{O}[[T]]/(f)$ *is a free* $\mathcal{O}$*-module of rank* n *having basis*

$$\{\, T^i \mod f \mid 0 \leq i \leq n-1\} \;.$$

Proof. See [Bou 89], Chapter 7, §3, Proposition 5. □

We will now define an important class of elements in $\mathcal{O}[T]$ to which we can apply the Division Lemma.

Definition 1.11. Let $\mathcal{O}$ be a local ring with maximal ideal $\mathfrak{p}$. A polynomial $F \in \mathcal{O}[T]$ is called ***distinguished*** (or a ***Weierstraß polynomial***) if it is of the form $F(T) = T^n + a_{n-1}T^{n-1} + \ldots + a_0$ with $a_i \in \mathfrak{p}$ for all $0 \leq i \leq n-1$.

Remarks 1.12.

(1) In particular, a distinguished polynomial $F(T)$ is not constant (since $n \geq 1$). If $\mathcal{O}$ is a principal ideal domain, then $F(T)$ is almost an Eisenstein polynomial: if $a_0 \notin \mathfrak{p}^2$, then $F(T)$ will be irreducible.

(2) The polynomials $\omega_n(T) := (1+T)^{p^n} - 1$, $n \geq 0$, which played an important role above (and will do later on), are distinguished in $\mathbb{Z}_p[T]$.

Lemma 1.13. *Let* $\mathcal{O}$ *be as in Lemma 1.10, let* $F(T) \in \mathcal{O}[T]$ *be a distinguished polynomial. Then we have an* $\mathcal{O}$*-module isomorphism*

$$\mathcal{O}[T]/(F(T)\cdot\mathcal{O}[T]) \;\xrightarrow{\sim}\; \mathcal{O}[[T]]/(F(T)\cdot\mathcal{O}[[T]]) \;.$$

Proof. The injection $\mathcal{O}[T] \hookrightarrow \mathcal{O}[[T]]$ induces a well-defined map

$$\varphi :\; \mathcal{O}[T]/(F(T)\cdot\mathcal{O}[T]) \;\longrightarrow\; \mathcal{O}[[T]]/(F(T)\cdot\mathcal{O}[[T]]) \;.$$

Let n be the degree of $F(T)$ (which is the same as the reduced degree because $F(T)$ is distinguished). By the Division Lemma, each coset of the quotient on the right hand side may be uniquely represented by an element $r \in \mathcal{O}[T]$ of degree less than n. Therefore the map φ actually has to be a bijection.

□

Finally, we come to the main result used in the proof of Theorem 1.9.

Theorem 1.14 (**Weierstraß Preparation Theorem**)**.** *Let* $\mathcal{O}$ *denote a local ring with maximal ideal* $\mathfrak{p}$*, and assume that* $\mathcal{O}$ *is Hausdorff and complete with respect to the* $\mathfrak{p}$*-adic topology. Let furthermore* $f = a_0 + a_1T + \ldots \in \mathcal{O}[[T]]$ *be a series such that there exists a coefficient of* f *that is not contained in* $\mathfrak{p}$ *(in particular,* $f \neq 0$*). Let* s *denote the reduced degree of* f*, as defined in Lemma 1.10.*
Then we may uniquely write

$$f = U \cdot F \;,$$

where $U \in (\mathcal{O}[[T]])^*$ is a unit, and where $F = F(T) \in \mathcal{O}[T]$ is a distinguished polynomial of degree s, as in Definition 1.11. (If $s = 0$, then $f = U$ is a unit.) In particular, if $\mathcal{O}$ is a principal ideal domain, then we may choose a generator π of $\mathfrak{p}$, and every non-zero element $f \in \mathcal{O}[[T]]$ may be uniquely written as

$$f(T) = \pi^\mu \cdot U(T) \cdot F(T) \ ,$$

where $0 \leq \mu \in \mathbb{Z}$ denotes the largest integer such that π^μ divides f, and with U and F as above.

Proof. See [Bou 89], Chapter 7, §3, Proposition 6. □

We now specialise to the case $\mathcal{O} = \mathbb{Z}_p$. Let $\Lambda := \mathbb{Z}_p[[T]]$.

Definition 1.15. The profinite group ring $\mathbb{Z}_p[[\Gamma]] \cong \Lambda$ is called the ***Iwasawa algebra***. Every compact Λ-module is called an ***Iwasawa module***.

The isomorphism $\mathbb{Z}_p[[\Gamma]] \cong \Lambda$ given in Theorem 1.9 depends on the choice of the topological generator γ of Γ. In the following we will identify $\mathbb{Z}_p[[\Gamma]]$ with Λ, using a *fixed* topological generator γ.

We will now state some basic properties of the ring Λ which build the foundation of a couple of results concerning the structure of finitely generated Λ-modules. This culminates in an important structure theorem which afterwards will be applied to some specific Λ-modules which are of arithmetic interest.

Proposition 1.16. *Λ is a unique factorisation domain whose irreducible elements are the rational prime p and the irreducible distinguished polynomials. The units of Λ are the power series with constant term in $\mathbb{Z}_p^*$.*

Proof. The first statement is a consequence of Theorem 1.14. The last assertion follows from a general fact: if R is any domain, then the units in $R[[T]]$ are those power series whose constant term is a unit in R (see [Rib 01], pp. 345f.). □

Lemma 1.17.

(i) Let $f, g \in \Lambda$ be relatively prime. Then the ideal (f, g) is of finite index in Λ.

(ii) Let $f \in \Lambda$ with $f \notin \Lambda^*$. Then $\Lambda/(f)$ is infinite.

Proof. See [Wa 97], Lemmas 13.7 and 13.10. □

Proposition 1.18.

(i) The prime ideals of Λ are (0), (p), (p, T) and the ideals $(F(T))$ generated by irreducible distinguished polynomials $F(T)$.

(ii) Λ is a local ring with unique maximal ideal $\mathfrak{m} = (p, T)$.

(iii) Λ is a Noetherian ring.

Proof. See [Wa 97], Proposition 13.9 for (i) and (ii). For (iii), we can use Chapter 4, Corollary 9.6 in [La 93] which states that if A is a Noetherian ring, then the ring $A[[T]]$ is Noetherian, too (inductively, this is also true for the ring of power series in more than one variable). □

We will now describe the above-mentioned structure theorem for (finitely generated) Λ-modules. We will classify these modules up to *pseudo-isomorphism*.

Definition 1.19. Two Λ-modules M and M' are called ***pseudo-isomorphic*** (written $M \sim M'$) if there exists a Λ-module homomorphism $\varphi : M \longrightarrow M'$ with finite kernel and cokernel. In other words, $M \sim M'$ if there is an exact sequence of Λ-modules

$$0 \longrightarrow A \longrightarrow M \xrightarrow{\varphi} M' \longrightarrow B \longrightarrow 0$$

with A and B finite.

Remarks 1.20.

(1) In general, $M \sim M'$ does *not* imply $M' \sim M$. For example, $(p, T) \sim \Lambda$, because the inclusion $(p, T) \hookrightarrow \Lambda$ has finite cokernel by Lemma 1.17, (i). On the other hand, we cannot have $\Lambda \sim (p, T)$ (the following argument is due to [Wa 97], p. 272): Suppose that $\varphi : \Lambda \longrightarrow (p, T)$ is a Λ-module-homomorphism. Let $f(T) \in (p, T)$ be the image of $1 \in \Lambda$. Then

$$\varphi(\Lambda) \subseteq (f(T)) \subseteq (p, T) .$$

But $\Lambda/(f(T))$ is infinite (Lemma 1.17, (ii)), whereas $\Lambda/(p, T)$ is finite, again by Lemma 1.17, (i). Therefore the cokernel of φ has to be infinite.

(2) It can be shown (compare Remarks 2.22, (1)) that if M and M' are finitely generated over Λ and Λ-torsion, then

$$M \sim M' \quad \Longleftrightarrow \quad M' \sim M \quad .$$

(3) The composition of two pseudo-isomorphisms is again a pseudo-isomorphism. Indeed, let $f : M \longrightarrow M'$ and $g : M' \longrightarrow M''$ denote pseudo-isomorphisms. Then $|\ker(g \circ f)| \leq |\ker(g)| \cdot |\ker(f)|$, since f and g are homomorphisms.
Furthermore, it is easy to see that $|\mathrm{coker}(g \circ f)| \leq |\mathrm{coker}(f)| \cdot |\mathrm{coker}(g)|$.
Therefore $g \circ f$ is a pseudo-isomorphism.

Example 1.21. Let $f, g \in \Lambda$ be relatively prime. Then

$$\Lambda/(fg) \sim \Lambda/(f) \oplus \Lambda/(g) \quad \text{and} \quad \Lambda/(f) \oplus \Lambda/(g) \sim \Lambda/(fg) .$$

Proof. See [Wa 97], Lemma 13.8. We will generalise this result in Chapter 5 (compare Proposition 5.43). □

Remark 1.22. If f and g are relatively prime non-units, then there cannot exist a Λ-module isomorphism

$$\varphi : \Lambda/(f) \oplus \Lambda/(g) \xrightarrow{\sim} \Lambda/(fg) .$$

Proof. We assume that

$$\varphi : \Lambda/(f) \oplus \Lambda/(g) \longrightarrow \Lambda/(fg)$$

denotes a Λ-module homomorphism, and we will show that φ cannot be an isomorphism. Indeed, let $a_1, a_2 \in \Lambda$ denote representatives of the classes $\varphi((\overline{1},\overline{0}))$, respectively, $\varphi((\overline{0},\overline{1}))$ in $\Lambda/(fg)$. Since

$$f \cdot \varphi((\overline{1},\overline{0})) \;=\; \varphi((\overline{f},\overline{0})) \;=\; \varphi((\overline{0},\overline{0})) \;=\; \overline{0}$$

and

$$g \cdot \varphi((\overline{0},\overline{1})) \;=\; \varphi((\overline{0},\overline{g})) \;=\; \varphi((\overline{0},\overline{0})) \;=\; \overline{0}\,,$$

it follows that $f \cdot a_1 \in (fg)$ and $g \cdot a_2 \in (fg)$. Since Λ is a unique factorisation domain, we may conclude that g divides a_1 and that f divides a_2.

This means that every image

$$\varphi((\overline{x},\overline{y})) \;=\; x \cdot \varphi((\overline{1},\overline{0})) + y \cdot \varphi((\overline{0},\overline{1}))\,, \quad x, y \in \Lambda\,,$$

is the coset in $\Lambda/(fg)$ of an element contained in the ideal (f,g). But $1 \notin (f,g)$, since f and g are non-units and therefore are contained in the maximal ideal $\mathfrak{m} = (p,T)$ of Λ. We therefore see that φ cannot be surjective. □

Definition 1.23. A Λ-module E is called ***elementary*** if E is of the form

$$E \;=\; \Lambda^r \oplus \left(\bigoplus_{i=1}^{s} \Lambda/(p^{n_i})\right) \oplus \left(\bigoplus_{j=1}^{t} \Lambda/(f_j(T)^{l_j})\right)\,,$$

where $r, s, t \in \mathbb{N}_0$, $n_i, l_j \in \mathbb{N}$ for all i, j, and where the $f_j(T)$ are irreducible distinguished polynomials in $\mathbb{Z}_p[T]$.

Theorem 1.24 (Structure theorem for finitely generated Λ-modules). *Let M be a finitely generated Λ-module. Then M is pseudo-isomorphic to an elementary Λ-module E. E is uniquely determined by X (up to permutation of the summands).*

Proof. See [Wa 97], Theorem 13.12 and Corollary 15.19. □

Corollary 1.25. *Let X, Y denote finitely generated Λ-modules.*

(i) If Y is pseudo-isomorphic to X, then the elementary Λ-modules E_X and E_Y attached to X and Y are equal (up to permutation of the summands).

(ii) If $Y \subseteq X$ denotes a submodule such that X/Y is finite, then the same conclusion holds.

Proof. (i) Suppose that $\varphi_X : X \longrightarrow E_X$, $\varphi_Y : Y \longrightarrow E_Y$ and $\psi : Y \longrightarrow X$ are pseudo-isomorphisms. Then $\varphi_X \circ \psi : Y \longrightarrow E_X$ is a pseudo-isomorphism (compare Remarks 1.20, (3)). Therefore $E_X = E_Y$ by the uniqueness statement of Theorem 1.24.

(ii) This is a special case of (i), since under the assumptions stated in the corollary, the embedding $\psi : Y \hookrightarrow X$ is a pseudo-isomorphism.

□

In this thesis, we will be mainly concerned with elementary torsion Λ-modules; we will sometimes simply speak of *elementary Λ-modules*.

For each $n \in \mathbb{N}_0$, consider the distinguished polynomial

$$\nu_n(T) := \frac{(1+T)^{p^n}-1}{T} = \frac{\omega_n(T)}{T}$$

(see Remarks 1.12, (2)) which via the isomorphism described in Theorem 1.9 corresponds to the element $1+\gamma+\gamma^2+\ldots+\gamma^{p^n-1} \in \mathbb{Z}_p[[\Gamma]]$.

For integers $n, e \in \mathbb{N}_0$ with $n \geq e$, we define

$$\nu_{(n,e)} := \frac{\nu_n}{\nu_e} = \frac{(1+T)^{p^n}-1}{(1+T)^{p^e}-1} = 1+(1+T)^{p^e}+(1+T)^{2p^e}+\ldots+(1+T)^{p^n-p^e}.$$

Lemma 1.26. *The polynomials $\nu_{(n,e)}(T) \in \mathbb{Z}_p[T]$ are distinguished whenever $n > e$ (and $\nu_{(e,e)} = 1$).*

This follows from the following useful properties of distinguished polynomials:

Proposition 1.27.

(i) *The product of two distinguished polynomials is again distinguished.*

(ii) *Suppose that $f(T) \in \mathbb{Z}_p[T]$ denotes a distinguished polynomial, let $g \in \Lambda$ be arbitrary. If f divides g in Λ, then in fact $\frac{g}{f} \in \mathbb{Z}_p[T]$.*

(iii) *If the quotient of two distinguished polynomials is a polynomial, then it is distinguished or the constant polynomial 1.*

(iv) *Let $f(T) \in \mathbb{Z}_p[T] \subseteq \Lambda$ be a distinguished polynomial. Then $f(T)$ is irreducible in $\mathbb{Z}_p[T]$ if and only if it is irreducible in Λ.*

Proof. (i) This is obvious from the definitions.

(ii) This may be deduced from the Weierstraß Preparation Theorem 1.14 (see [Wa 97], Lemma 7.5).

(iii) Let f, g, h denote polynomials with $f \cdot g = h$, and suppose that g and h are distinguished. Then $f(T)$ has leading coefficient 1. Therefore if f is not constant and not distinguished, then $f(T) = u(T) \cdot \tilde{f}(T)$ with a distinguished polynomial $\tilde{f}(T)$ and a unit $u(T) \in \Lambda^*$, by Theorem 1.14. But then $h(T) = g(T) \cdot \tilde{f}(T) \cdot u(T)$ with $g(T) \cdot \tilde{f}(T)$ distinguished by (i). Therefore $u = 1$ by the uniqueness in 1.14, i.e., $f = \tilde{f}$.
Note that if $f(T) = \frac{h(T)}{g(T)}$ is constant, then it has to equal 1, since $g(T)$ and $h(T)$ have leading coefficients 1.

(iv) Let us first assume that f was reducible in Λ. Then $f = g \cdot h$ for suitable $g, h \in \Lambda \setminus \Lambda^*$. Using the Weierstraß Preparation Theorem 1.14, we may write

$$g = p^{n_1} \cdot \tilde{g} \cdot u_1 \quad \text{and} \quad h = h^{n_2} \cdot \tilde{h} \cdot u_2$$

with $u_1, u_2 \in \Lambda^*$ and $\tilde{g}(T), \tilde{h}(T) \in \mathbb{Z}_p[T]$ distinguished; note that in fact $n_1 = n_2 = 0$, since f is distinguished and therefore its leading coefficient is equal to 1. Now $u_1 = \frac{g}{\tilde{g}}$ and $u_2 = \frac{h}{\tilde{h}}$ are polynomials (see (ii)), and in fact $u_1 \cdot u_2 = \frac{f}{\tilde{g} \cdot \tilde{h}} = 1$ by (iii), since it is contained in Λ^* and therefore cannot

be distinguished. So $f(T) = \tilde{g}(T) \cdot \tilde{h}(T)$. Since $g, h \notin \Lambda^*$, we may conclude that $\tilde{g}, \tilde{h} \neq 1$, and therefore $\tilde{g}, \tilde{h} \notin (\mathbb{Z}_p[T])^* = \mathbb{Z}_p^*$, as being distinguished polynomials. Thus f is reducible in $\mathbb{Z}_p[T]$.
Assume now to the contrary that there exist polynomials $g(T), h(T)$ in $\mathbb{Z}_p[T] \setminus \mathbb{Z}_p^*$ such that $f(T) = g(T) \cdot h(T)$. Since $\mathbb{Z}_p[T] \subseteq \Lambda$, it will be sufficient to show that $g(T)$ and $h(T)$ both are not contained in Λ^*. It is easy to see that they cannot simultaneously lie in Λ^*, since the product of their constant coefficients (which belong to $\mathbb{Z}_p^*$ if and only if $g(T)$ or $h(T)$ are invertible in Λ, respectively) has to yield the constant coefficient of $f(T)$, which is divisible by p, since f is distinguished. Moreover, the product of their leading terms equals 1, and therefore we may assume that

$$g(T) = T^k + c_{k-1} \cdot T^{k-1} + \ldots + c_0 \quad \text{and} \quad h(T) = T^l + a_{l-1} \cdot T^{l-1} + \ldots + a_0$$

with

$$p \mid a_0 \qquad \text{and} \qquad p \nmid c_0 \, .$$

Now

$$\begin{aligned} g(T) \cdot h(T) &= a_0 c_0 + T \cdot (a_0 c_1 + a_1 c_0) + T^2 \cdot (a_0 c_2 + a_1 c_1 + a_2 c_0) + \ldots \\ &= f(T) \equiv T^{l+k} \mod p \, , \end{aligned}$$

and therefore

$$0 \equiv a_0 c_1 + a_1 c_0 \equiv a_1 c_0 \mod p \, ,$$

so $p \mid a_1$, since $p \nmid c_0$. Then, considering the coefficients of T^2, we get

$$0 \equiv a_0 c_2 + a_1 c_1 + a_2 c_0 \equiv a_2 c_0 \mod p \, ,$$

so $p \mid a_2$, and so on. Inductively, we obtain that $h(T) \in \mathbb{Z}_p[T]$ is distinguished. But as we have seen in (iii), this means that the quotient $g(T) = \frac{f(T)}{h(T)}$ either is distinguished (contradicting the fact that $p \nmid c_0$) or equals 1 (and therefore is contained in $\mathbb{Z}_p^*$, again contrary to our assumptions). This shows that $g(T), h(T) \notin \Lambda^*$, so $f(T)$ is reducible in Λ.

□

The following proposition will become very important in the next section.

Proposition 1.28. *Let*

$$E = \Lambda^r \oplus \left(\bigoplus_{i=1}^{s} \Lambda/(p^{n_i}) \right) \oplus \left(\bigoplus_{j=1}^{t} \Lambda/(f_j(T)^{l_j}) \right)$$

be an elementary Λ-module as defined in Definition 1.23.
Let $\mu := \sum_{i=1}^{s} n_i$ *and* $\lambda := \sum_{j=1}^{t} l_j \cdot \deg(f_j)$.

(i) *If $E/(\nu_{(n,e)} \cdot E)$ is finite for some fixed $e \geq 0$ and all $n \geq e$, then $r = 0$ and there exist constants n_0 and ν (which depend on E and e, but are independent of n) such that*

$$|E/(\nu_{(n,e)} \cdot E)| = p^{\mu \cdot p^n + \lambda \cdot n + \nu} \quad \text{for all } n > n_0 \, .$$

(ii) *Assume that $r = 0$. Then $\mu = 0 \iff$ the p-rank of $(E/(\nu_{(n,e)} \cdot E))$ is bounded as $n \to \infty$.*

Proof. See [Wa 97], Proposition 13.19 and Lemma 13.20. □

Definition 1.29. Let X be a finitely generated torsion Λ-module. By Theorem 1.24 and Proposition 1.28 we can attach to X (via the corresponding elementary Λ-module E) two integers $\lambda = \lambda(X)$ and $\mu = \mu(X)$ and a polynomial

$$F_X := \prod_{j=1}^{t} f_j(T)^{l_j} \, ,$$

the product of the polynomials occurring in the representation of E.
Then $\lambda = \deg(F_X)$ and μ are called the ***Iwasawa invariants*** of the Λ-module X and F_X is called the ***characteristic polynomial*** of X (it will be explained below where this name comes from; see Proposition 1.31, (ii)).

Remark 1.30. If X is a $\mathbb{Z}_p[[\Gamma]]$-module and therefore bears a Λ-module structure via Theorem 1.9, then the characteristic polynomial of X depends on the choice of the topological generator γ of Γ which induces the isomorphism in 1.9. However, the invariants λ and μ are independent of γ (compare [NSW 08], Remark 1 on p. 292).

We will conclude our discussion of Λ-modules by describing some of the properties of the Iwasawa invariants.

Let X be a finitely generated torsion Λ-module. For every $n \in \mathbb{N}_0$, we let

$$X[p^n] := \{x \in X \mid p^n \cdot x = 0\} \, ,$$

and we define

$$X^\circ := \bigcup_{n \geq 0} X[p^n]$$

to be the $\mathbb{Z}_p$-torsion submodule of X. Then the quotient module X/X° is a finitely generated torsion Λ-module which by construction is torsion-free as a $\mathbb{Z}_p$-module.

Let $f(T) \in \Lambda$ denote a non-zero annihilator of X. We write $f = p^r \cdot g$ for some $g \in \Lambda$ coprime to p. Then g annihilates X/X°. By the Weierstraß Preparation Theorem 1.14, g is associated to a distinguished polynomial $\tilde{g} \in \mathbb{Z}_p[T]$. Then $\Lambda/(g)$ is isomorphic to a free $\mathbb{Z}_p$-module of rank $\deg(\tilde{g})$, by the Division Lemma 1.10 (compare Lemma 1.13). If X/X° is generated as a Λ-module by s elements, then X/X° is isomorphic to a quotient of $(\Lambda/(g))^s$. Therefore X/X° is a free $\mathbb{Z}_p$-module of finite rank.

Recall that

$$X \sim \bigoplus_{i=1}^{s} \Lambda/(p^{n_i}) \oplus \bigoplus_{j=1}^{t} \Lambda/(f_j(T)^{l_j})$$

with irreducible distinguished polynomials $f_j(T) \in \mathbb{Z}_p[T]$.

If we let

$$V := X \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \,,$$

then it is easy to see that

$$V \cong \bigoplus_{j=1}^{t} \mathbb{Q}_p[T]/(f_j(T)^{l_j})$$

as $\mathbb{Q}_p$-vector spaces: First, we have

$$\mathbb{Z}_p[[T]]/(f_j(T)^{l_j}) \cong \mathbb{Z}_p[T]/(f_j(T)^{l_j})$$

for every j (see Lemma 1.13). Moreover, $\mathbb{Z}_p[T] \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong \mathbb{Q}_p[T]$. Finally, the tensoring $\cdot \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ eliminates the $\mathbb{Z}_p$-torsion part.

Note that

$$\dim_{\mathbb{Q}_p}(V) = \lambda(X) \,,$$

since the dimension of $\mathbb{Q}_p[T]/(f_j(T)^{l_j})$ is equal to $l_j \cdot \deg(f_j)$, respectively.

Multiplication by T induces an endomorphism on the $\mathbb{Q}_p$-vector space

$$\mathbb{Q}_p[T]/(f_j(T)^{l_j})$$

with characteristic polynomial $f_j(T)^{l_j}$, respectively. Therefore the characteristic polynomial F_X of X as defined via Theorem 1.24 and Proposition 1.28 is the characteristic polynomial for the operation of T on the $\mathbb{Q}_p$-vector space $V = X \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$.

We summarise our results, together with some facts about the Iwasawa invariant $\mu(X)$ which are immediately clear from the definitions:

Proposition 1.31. *Let X be a finitely generated torsion Λ-module with Iwasawa invariants $\lambda(X)$ and $\mu(X)$, and let F_X be the characteristic polynomial of X, as introduced in Definition 1.29. Let X° be the $\mathbb{Z}_p$-torsion submodule of X.*

(i) *X° is a Λ-submodule of X. There is a finite integer $t \in \mathbb{N}_0$ such that $p^t \cdot X^\circ = \{0\}$. X/X° is a free $\mathbb{Z}_p$-module of finite rank.*

(ii) *$V := X \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is a $\mathbb{Q}_p$-vector space of dimension $\lambda(X)$. F_X is the characteristic polynomial of the endomorphism on V induced by multiplication by T.*

(iii) *X is finitely generated as a $\mathbb{Z}_p$-module if and only if $\mu(X) = 0$. Moreover, we have*

$$\mu(X) = 0 \iff X^\circ \text{ is finite} \iff X/pX \text{ is finite} \,.$$

(iv) *$\lambda(X) = 0 \iff p^s \cdot X = \{0\}$ for some $s \geq 0$.*

Proof. Most of the assertions are clear from the above.

(i) If $x \in X$ is a $\mathbb{Z}_p$-torsion element and $f \in \Lambda$, then clearly also $f \cdot x$ is annihilated by the same element of $\mathbb{Z}_p$ (because $\Lambda \supseteq \mathbb{Z}_p$ is commutative), and so X° is a Λ-module. Since Λ is Noetherian, X° has to be finitely generated, and therefore there exists a $t \geq 0$ such that $X^\circ = X[p^t]$.

(ii) This has been explained above.

(iii) First, X° is finite if and only if E° is finite, where E denotes the elementary Λ-module attached to X. Now E° is finite if and only if $\mu(X) = 0$ (recall that $\Lambda/(f_j(T)^{l_j})$ is $\mathbb{Z}_p$-free for each j by Lemma 1.10).
Moreover, X is finitely generated as a $\mathbb{Z}_p$-module if and only if E is finitely generated as $\mathbb{Z}_p$-module, which is the case if and only if $\mu(X) = 0$ (note that $\Lambda/(p) \cong (\mathbb{Z}/p\mathbb{Z})[[T]]$ is not finitely generated over $\mathbb{Z}_p$). Finally, X is finitely generated as $\mathbb{Z}_p$-module if and only if X/pX is finite.

(iv) Let $\varphi : X \xrightarrow{\sim} E$ denote a pseudo-isomorphism. Then the kernel of φ is finite, and therefore $\ker(\varphi) \subseteq X^\circ$. If $\lambda(X) = 0$, then there exists a finite integer s with $p^s \cdot X = \{0\}$ (e.g., choose $s = \mu(X) + t$, where t has been defined in (i)). But if $\lambda(X) \neq 0$, then E contains a nontrivial $\mathbb{Z}_p$-free submodule by the Division Lemma 1.10. Since the cokernel of φ is finite, this proves the proposition.

□

1.3 Iwasawa's Theorem on the asymptotic growth of class numbers in $\mathbb{Z}_p$-extensions

In this section we will show how to use the general theory developed above for the study of arithmetic properties of $\mathbb{Z}_p$-extensions. The main result will be the following fundamental theorem due to K. Iwasawa.

Theorem 1.32. *Let K_∞/K be a $\mathbb{Z}_p$-extension of the number field K. Let A_n denote the p-Sylow part of the ideal class group of the intermediate field K_n, respectively. Let p^{e_n} be the exact power of p dividing the class number of K_n, i.e., $|A_n| = p^{e_n}$. Then there exist rational integers $\lambda \geq 0$, $\mu \geq 0$ and ν, independent of n, and an integer $n_0 = n_0(K_\infty/K) \in \mathbb{N}$ such that for every $n \geq n_0$, we have*

$$e_n = \mu p^n + \lambda n + \nu \ .$$

The constants μ, λ and ν are called the **Iwasawa invariants** *of K_∞/K.*

Therefore, for sufficiently large n, the growth of the p-primary parts of the class numbers of the fields K_n splits into a linear part (described by λ), a portion proportional to the degree p^n of the subextension K_n/K, with factor μ, and a constant part, described by ν.

The detailed proof of the theorem is given, for example, in [Wa 97], pp. 277-285. We will describe here the main ideas the proof is based on; this will give us the opportunity to introduce some objects and notions that will be important in later chapters.

Let $\mathrm{Gal}(K_\infty/K) =: \Gamma \cong \mathbb{Z}_p$, and let γ be a fixed topological generator of Γ. For every $n \geq 0$, let $L_n = H(K_n)$ be the maximal unramified abelian

p-extension of K_n (i.e., L_n is the 'p-part' of the Hilbert class field of K_n). Then, by class field theory, $X_n := \mathrm{Gal}(L_n/K_n)$ is isomorphic to the p-Sylow group $A_n \subseteq \mathrm{Cl}(K_n)$. Let $L := \bigcup_{n\geq 0} L_n$ and $X := \mathrm{Gal}(L/K_\infty)$; note that $K_\infty = \bigcup_{n\geq 0} K_n \subseteq L$, since $K_n \subseteq L_n$ for every n.

L_n is galois over K for each n. Indeed, suppose that

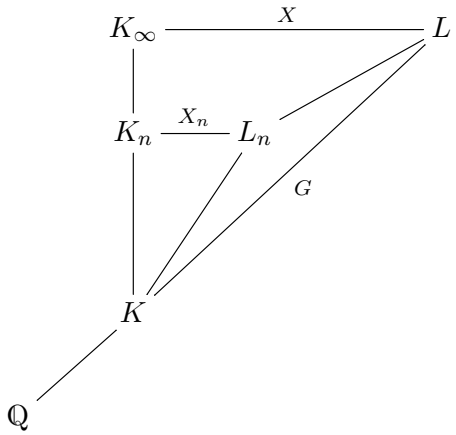
$$\sigma : L_n \longrightarrow \sigma(L_n) \subseteq \mathbb{C}$$

is a homomorphism that fixes K. Since K_n is galois over K, it follows that $\sigma(K_n) = K_n$, and

$$\mathrm{Gal}(\sigma(L_n)/K_n) \cong \mathrm{Gal}(L_n/K_n)$$

is an abelian p-group. Now $\sigma(L_n)/K_n$ is unramified because L_n/K_n is unramified, and therefore $\sigma(L_n) \subseteq L_n$ by the maximality of L_n. Since this holds for every such homomorphism (in particular, it holds for σ^{-1}), we have $\sigma(L_n) = L_n$, i.e., L_n is galois over K for each n.

Therefore L/K is galois, too, because $L = \bigcup_{n\geq 0} L_n$. Let $G := \mathrm{Gal}(L/K)$. Then we have the following diagram:



Proposition 1.33. *$L = \bigcup_{n\geq 0} L_n$ is the maximal p-abelian unramified extension of K_∞.*

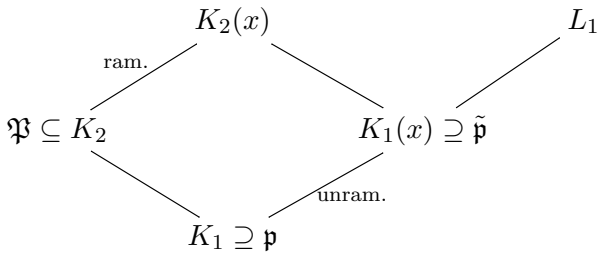
Proof. Let H be the maximal p-abelian unramified extension of K_∞. We want to show that $L = H$.

We will apply the following general fact.

Proposition 1.34. *Let K_2/K_1 be a p-abelian field extension, let L_1 and L_2 denote the maximal p-abelian unramified extensions of K_1 and K_2, respectively. Then $L_1 \subseteq L_2$.*

Proof. Suppose that $L_1 \not\subseteq L_2$. Then there exists an element $x \in L_1$ such that $x \notin L_2$ and $[K_2(x) : K_2] = p$. Since $K_2(x)/K_2$ is p-abelian, there exists a prime $\mathfrak{P}$ of K_2 that ramifies in $K_2(x)$. Let $\mathfrak{p} := \mathfrak{P} \cap K_1$, and let $\tilde{\mathfrak{p}}$ be a prime of $K_1(x)$

lying above $\mathfrak{p}$. We have the following diagram of fields:



If $I \subseteq \mathrm{Gal}(K_2/K_1)$ denotes the inertia subgroup of the prime $\mathfrak{p}$, then we let $K_1' := K_2^I$ denote the subfield fixed by I. $\mathfrak{p}$ is unramified in K_1' and in $K_1(x) \subseteq L_1$, and therefore $\mathfrak{p}$ is unramified in $K_1'(x) = K_1' \cdot K_1(x)$.

Let $\mathfrak{p}' := \mathfrak{P} \cap K_1'$. Then $\mathfrak{p}'$ is totally ramified in K_2/K_1'. Therefore $\mathfrak{P}$ is the unique prime of K_2 dividing $\mathfrak{p}'$, and there exists a unique prime $\overline{\mathfrak{P}}$ of $K_2(x)$ lying above $\mathfrak{p}'$. Moreover, the residue class fields $\mathcal{O}_{K_2(x)}/\overline{\mathfrak{P}}$ and $\mathcal{O}_{K_2}/\mathfrak{P}$ both are isomorphic to $\mathcal{O}_{K_1'}/\mathfrak{p}'$.

But this means that $\mathfrak{p}'$ has to ramify in the extension $K_1'(x)/K_1'$, since it cannot be split or inert (note that $\mathcal{O}_{K_2(x)}/\overline{\mathfrak{P}} \cong \mathcal{O}_{K_1'}/\mathfrak{p}'$ is a field extension of $\mathcal{O}_{K_1'(x)}/\tilde{\mathfrak{p}'}$, where $\tilde{\mathfrak{p}'}$ denotes the corresponding prime in $K_1'(x)$).

This contradicts the fact that $\mathfrak{p}'$ is unramified in $K_1'(x)$. □

Now we return to the proof of Proposition 1.33. Proposition 1.34 implies that $L = \bigcup_{n \geq 0} L_n$ is contained in H, because each K_n is a subfield of K_∞.

Suppose that $L \subsetneq H$, and let $x \in H$, $x \notin L$, generate an extension of degree p over K_∞. Then $x \notin L_n$ for every $n \in \mathbb{N}_0$. Proposition 1.3 shows that there exists an integer $e \geq 0$ such that all primes which ramify in K_∞/K_e are totally ramified. Fix some $m \geq e$. We have the following diagram of fields.

$$\begin{array}{ccc} K_\infty & \text{——} & K_\infty(x) \\ | & & | \\ K_m & \text{——} & K_m(x) \end{array}$$

Since $K_m(x)$ is a finite extension of K_m, the intersection $K_\infty \cap K_m(x)$ is equal to K_{m+k} for some $k \in \mathbb{N}_0$. Replacing m by $m+k$, we may assume that in fact $K_m(x) \cap K_\infty = K_m$, so that $\mathrm{Gal}(K_m(x)/K_m) \cong \mathrm{Gal}(K_\infty(x)/K_\infty)$ is cyclic of order p.

By assumption, there exists a prime $\mathfrak{p}$ of K_m ramifying in $K_m(x)/K_m$, whereas the extension $K_\infty(x)/K_\infty$ is unramified. If $\mathfrak{p}$ was unramified also in K_∞/K_m, it would have to be unramified in $K_\infty(x)/K_m$. Since $m \geq e$, we may therefore assume that $\mathfrak{p}$ is totally ramified in K_∞/K_m.

Now we consider the extension $K_\infty(x)/K_m(x)$. Since $K_\infty \cap K_m(x) = K_m$, we have

$$\mathrm{Gal}(K_\infty(x)/K_m(x)) \;\cong\; \mathrm{Gal}(K_\infty/K_m) \;\cong\; \mathbb{Z}_p \;.$$

If $\tilde{\mathfrak{p}} \subseteq K_m(x)$ denotes the prime above $\mathfrak{p}$, then there exists some $k \in \mathbb{N}$ such that $\tilde{\mathfrak{p}}$ is unramified in $K_{m+k}(x)/K_m(x)$, and totally ramified in $K_\infty(x)/K_{m+k}(x)$. Since $[K_\infty(x) : K_\infty] = p$, we actually have $k = 1$.

Since this holds for every prime $\mathfrak{p}$ of K_m ramifying in $K_m(x)$, we may conclude that the extension $K_{m+1}(x)/K_{m+1}$ is unramified, and thus $x \in L_{m+1}$. Indeed, if some prime $\mathfrak{P}$ of K_{m+1} was ramified in $K_{m+1}(x)$, we would again conclude that $\mathfrak{P}$ was ramified in K_∞, and thus already ramified in K_{m+1}/K_m. But then $\mathfrak{p} := \mathfrak{P} \cap K_m$ was totally ramified in $K_{m+1}(x)/K_m$, and therefore also in $K_m(x)/K_m$. By the above, the prime $\tilde{\mathfrak{P}}$ of $K_{m+1}(x)$ dividing $\mathfrak{P}$ was totally ramified in $K_\infty(x)/K_{m+1}(x)$, and unramified in $K_{m+1}(x)/K_m(x)$, yielding a contradiction. □

We want to provide $X = \mathrm{Gal}(L/K_\infty)$ with the structure of a Γ-module, hence of a Λ-module, in order to apply the results of the last section. Let us first assume that the following condition is satisfied:

Assumption 1.35. *All primes which ramify in K_∞/K are totally ramified.*

By Proposition 1.3, there exists an integer $e \geq 0$ such that this may be arranged by replacing K by K_e. Under the assumption, $K_{n+1} \cap L_n = K_n$ for every n (since L_n/K_n is unramified), and therefore

$$X_n \;=\; \mathrm{Gal}(L_n/K_n) \;\cong\; \mathrm{Gal}(L_nK_{n+1}/K_{n+1})\,.$$

Since $L_n \cdot K_{n+1} \subseteq L_{n+1}$, we obtain a surjective map

$$\mathrm{Gal}(L_{n+1}/K_{n+1}) \;=\; X_{n+1} \longrightarrow\!\!\!\!\!\rightarrow X_n$$

induced by restriction (one can show that this map corresponds to the norm map $A_{n+1} \longrightarrow A_n$ on the corresponding ideal class groups, see page 400 of [Wa 97] or [Neu 92], Theorem IV.6.4). Since $X_n \cong \mathrm{Gal}(L_nK_\infty/K_\infty)$ for every n, because $K_\infty \cap L_n = K_n$, it follows that

$$X \;=\; \mathrm{Gal}(L/K_\infty) \;\cong\; \varprojlim_n \mathrm{Gal}(L_nK_\infty/K_\infty) \;\cong\; \varprojlim X_n \;\cong\; \varprojlim A_n \;=:\; A\,.$$

Now we make each X_n into a $\mathbb{Z}_p[\Gamma_n]$-module, respectively, where $\Gamma_n = \Gamma/\Gamma^{p^n}$ can be identified with $\mathrm{Gal}(K_n/K)$. Let $x \in X_n$, and extend a given $\alpha \in \Gamma_n$ to $\tilde{\alpha} \in \mathrm{Gal}(L_n/K)$ (recall that L_n is galois over K, as mentioned above). Then we define

$$\alpha \cdot x := \tilde{\alpha} \circ x \circ \tilde{\alpha}^{-1}\,,$$

where $\circ$ denotes composition in $\mathrm{Gal}(L_n/K)$. Since $\mathrm{Gal}(L_n/K_n)$ is abelian, $\alpha \cdot x$ is well-defined, i.e., does not depend on the choice of the extension $\tilde{\alpha}$ of α. Using this construction, we can define a $\mathbb{Z}_p[\Gamma_n]$-module structure on X_n. By considering an element $x \in X \cong \varprojlim X_n$ as a sequence $(x_0, x_1, \ldots)$ of elements $x_i \in X_i$, it can be shown that X becomes a module over $\varprojlim \mathbb{Z}_p[\Gamma_n] \cong \Lambda$, letting $\mathbb{Z}_p[\Gamma_n]$ act on the n-th component, respectively.

In order to be able to apply Theorem 1.24, we want to show now that the Λ-module X is finitely generated. For this purpose we define some important submodules of X – still under the above assumption. By Lemma 1.2, there are only finitely many prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ which ramify in K_∞/K. For $i = 1, \ldots, s$, let $\widetilde{\mathfrak{p}_i}$ be a fixed prime of L lying above $\mathfrak{p}_i$, and let

$$I_i \subseteq G = \mathrm{Gal}(L/K)$$

be its inertia group, respectively.

Since L/K_∞ is unramified by definition of L, $I_i \cap X = \{1\}$ for all i. Therefore we have an injection

$$I_i \hookrightarrow G/X \;\cong\; \Gamma \;=\; \mathrm{Gal}(K_\infty/K) \;\;.$$

Since $\mathfrak{p}_i$ ramifies totally in K_∞/K by our assumption, the map $I_i \hookrightarrow \Gamma$ has to be also surjective and therefore is a bijection. The pre-image $\sigma_i \in I_i$ of the fixed topological generator γ of Γ then yields a topological generator of I_i. Moreover, using the exact sequence of groups

$$0 \longrightarrow X \longrightarrow G \longrightarrow G/X \longrightarrow 0 \;,$$

the isomorphism $G/X \cong I_1$ implies that G is isomorphic to the semi-direct product $X \rtimes I_1$. It follows that $I_i \subseteq G = X \rtimes I_1$, and therefore $\sigma_i = a_i \cdot \sigma_1$ for some $a_i \in X$, $i = 1, \ldots, s$ (note that we can take $a_1 = 1$).

$G = \mathrm{Gal}(L/K)$ forms a profinite topological group with respect to the Krull topology, see [Neu 92], § IV.1. The action of Λ on $X \subseteq G$ as defined above is continuous, and $X \subseteq G$ forms a closed subgroup. In fact, X is compact as being the inverse limit of finite groups (compare [Neu 92], Theorem IV.2.3), because the topology induced by the inverse limit coincides with the Krull topology on $X \subseteq G$. This means that X is an Iwasawa module in the sense of Definition 1.15.

Lemma 1.36. *Under the above assumption, the following hold:*

(i) If G' denotes the closure of the commutator subgroup of G, then $G' = T \cdot X$.

(ii) Let Y_0 be the $\mathbb{Z}_p$-submodule of X generated by $\{a_i \mid 2 \leq i \leq s\}$ and by $T \cdot X$. For each $n \in \mathbb{N}$, let $Y_n = \nu_n \cdot Y_0$ ($\nu_n \in \mathbb{Z}_p[T]$ is defined in Section 1.2). Then $X_n \cong X/Y_n$ for every $n \geq 0$.

Proof. See Lemmas 13.14 and 13.15 in [Wa 97]. □

Note that Y_0 in fact is a Λ-module, since $T \cdot Y_0 \subseteq T \cdot X \subseteq Y_0$. Therefore each Y_n denotes a Λ-submodule of X.

Recalling that $X = \mathrm{Gal}(L/K_\infty) = \varprojlim \mathrm{Gal}(K_\infty \cdot L_n/K_\infty)$, we will now prove the following important characterisation of the $Y_n \subseteq X$:

Lemma 1.37. *For each $n \in \mathbb{N}_0$, we let $\tilde{X}_n := \mathrm{Gal}(K_\infty \cdot L_n/K_\infty)$. Then, under Assumption 1.35,*

$$Y_n \;=\; \ker(\mathrm{pr}_n : X \longrightarrow \tilde{X}_n)$$

for each $n \geq 0$.

Proof. We let $\tilde{Y}_n := \ker(\mathrm{pr}_n : X \longrightarrow \tilde{X}_n)$, and we will show that $\tilde{Y}_n = Y_n$ for each n. The proof will occupy three steps.

1. *Let $n \geq 0$ be arbitrary, but fixed. Then an element $y \in X = \mathrm{Gal}(L/K_\infty)$ is contained in $\tilde{Y}_n$ if and only if $y|_{(K_\infty \cdot L_n)} = 1$.*

Proof. Since $L = \bigcup_{n\geq 0} L_n = \bigcup_n K_\infty \cdot L_n$ and $\tilde{X}_n = \mathrm{Gal}((K_\infty \cdot L_n)/K_\infty)$, we have, as mentioned above, $X = \varprojlim \tilde{X}_n$. Therefore we can represent each element $y \in X$ by a coherent sequence $(y_0, y_1, \ldots)$ with

$$\mathrm{pr}_i(y) \;=\; y|_{(K_\infty \cdot L_i)} \;=\; y_i \in \tilde{X}_i$$

for all i and $y_i|_{(K_\infty \cdot L_j)} = y_j$ for $i \geq j$. The statement now is obvious.

□

2. *We have* $\tilde{Y_0} = Y_0$.

Proof. By Lemma 1.2, there are only finitely many prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ which ramify in K_∞/K. For $i = 1, \ldots, s$, let $\widetilde{\mathfrak{p}_i}$ be a fixed prime of L lying above $\mathfrak{p}_i$, and let $I_i \subseteq G = \mathrm{Gal}(L/K)$ be its inertia group, respectively. We have seen above that each I_i is isomorphic to Γ. Let σ_i be a topological generator of I_i, respectively. Then we have chosen elements $a_2, \ldots, a_s \in X$ such that $\sigma_i = a_i \cdot \sigma_1 \in X \cdot I_1 = G$, $i = 2, \ldots, s$.
Since L_0 by definition is the maximal abelian unramified p-extension of K, and since L/K is a pro-p-extension, it follows that L_0 is the maximal abelian unramified subextension of L/K. Therefore $\mathrm{Gal}(L/L_0) \subseteq \mathrm{Gal}(L/K) = G$ is the closed subgroup generated by the commutator subgroup of G together with all the inertia subgroups I_i, $1 \leq i \leq s$.
This means that $\mathrm{Gal}(L/L_0)$ is the closure of the subgroup of G generated by G', I_1 and the elements $a_2, \ldots, a_s$. Therefore

$$\begin{aligned} \mathrm{Gal}(L_0/K) \;&\cong\; \mathrm{Gal}(L/K)/\mathrm{Gal}(L/L_0) \;=\; G/\mathrm{Gal}(L/L_0) \\ &=\; X \cdot I_1 \,/\, \overline{<G', I_1, a_2, \ldots, a_s>} \;\cong\; X/<T \cdot X, a_2, \ldots, a_s>_{\mathbb{Z}_p} , \end{aligned}$$

since Lemma 1.36, (i) implies that $G' = T \cdot X$. But $X = \mathrm{Gal}(L/K_\infty)$, so that we may conclude that

$$\begin{aligned} X/\mathrm{Gal}(L/(K_\infty \cdot L_0)) \;&\cong\; \mathrm{Gal}(K_\infty \cdot L_0)/K_\infty) \\ &\cong\; \mathrm{Gal}(L_0/K) \\ &\cong\; X/<T \cdot X, a_2, \ldots, a_s>_{\mathbb{Z}_p} . \end{aligned}$$

The second isomorphism uses the fact that $K_\infty \cap L_0 = K$, which follows from Assumption 1.35.
Therefore the elements of X fixing $K_\infty \cdot L_0$ are those contained in

$$Y_0 \;=\; <T \cdot X, a_2, \ldots, a_s>_{\mathbb{Z}_p} .$$

By the first part of the proof, it follows that $\tilde{Y_0} = Y_0$, as claimed. □

3. *Now consider an arbitrary* $n \geq 0$. *Then* $\tilde{Y_n} = Y_n$.

Proof. This can be proved analogously to the second step. Simply replace the ground field K by K_n. Then L_n corresponds to the fields L_0, and the topological generators σ_i, $i = 1, \ldots, s$, of the inertia groups are replaced by their p^n-th powers. Note that the replacement does not change L and X.

In [Wa 97], p. 280, it is shown that $\sigma_i^{p^n} = (\nu_{(n,0)} \cdot a_i) \cdot \sigma_1^{p^n}$ (i.e., the a_i are replaced by $\nu_{(n,0)} \cdot a_i$, respectively), and that $T \cdot X$ has to be replaced by $(\nu_{(n,0)} \cdot T) \cdot X$. But therefore, by the argument used in step 2, $\nu_{(n,0)} \cdot Y_0 = Y_n$ is the subgroup of X fixing $K_\infty \cdot L_n$, and so $\tilde{Y_n} = Y_n$ by step 1. □

□

Remark 1.38. In order to get rid of Assumption 1.35, we recall that for an arbitrary $\mathbb{Z}_p$-extension K_∞/K, Proposition 1.3 shows that there exists an integer $e \geq 0$ such that the above lemmas apply to the $\mathbb{Z}_p$-extension K_∞/K_e. Note that $X = \mathrm{Gal}(L/K_\infty)$ does not depend on the ground field K. In particular, if we let Y_e be the analogue of Y_0 for the base field K replaced by K_e, then the results of Lemmas 1.36 and 1.37 may be transferred to the general case, being valid for all $n \geq e$.

Lemma 1.39. *Let K_∞/K be an arbitrary $\mathbb{Z}_p$-extension. Then $X = \mathrm{Gal}(L/K_\infty)$ is a finitely generated Λ-module which is sometimes called the* **Greenberg module** *of K_∞/K, and there exist an integer $e \geq 0$ and a Λ-submodule $Y_e \subseteq X$, such that*

$$X_n \;\cong\; X/(\nu_{(n,e)} \cdot Y_e) \quad \textit{for all } n \geq e,$$

where the $\nu_{(n,e)}$ are defined in Section 1.2. In particular, by Proposition 1.28, (i), X is a torsion Λ-module.

Proof. See [Wa 97], Lemmas 13.17 and 13.18. As in Remark 1.38, we let Y_e be the analogue of Y_0 for the base field K_e instead of K. Since $\nu_{(n,e)} = \frac{\nu_n}{\nu_e}$ by definition and therefore $\nu_{(n,e)} \cdot Y_e = Y_n$, the lemma follows because the replacement $\nu_n \mapsto \nu_{(n,e)}$ corresponds to the change of the ground fields $K \mapsto K_e$ (see [Wa 97] for details). □

An important ingredient in the proof of the first assertion of Lemma 1.39 (Lemma 13.17 in [Wa 97]) is *Nakayama's Lemma*. Since it is a very useful tool, we give several versions of this statement:

Lemma 1.40 (Nakayama's Lemma I)**.** *Let A be a ring. Let $\mathfrak{A} \subseteq A$ be an ideal which is contained in every maximal ideal of A, and let E be a finitely generated A-module.*
If $\mathfrak{A} \cdot E = E$, then $E = \{0\}$.

Proof. See [La 93], Chapter X, Lemma 4.1. □

Now we consider local rings.

Lemma 1.41 (Nakayama's Lemma II)**.** *Let A be a local ring with maximal ideal $\mathfrak{m}$, let E be a finitely generated A-module, and let F be a submodule of E. If $E = F + \mathfrak{m} \cdot E$, then $E = F$.*

Proof. See [La 93], Chapter X, Lemma 4.2. □

The next version shows how to replace the condition that E is finitely generated over A by a topological assumption on E.

Lemma 1.42 (Nakayama's Lemma III)**.** *Let A be a local ring with maximal ideal $\mathfrak{m}$. Suppose that A is complete with respect to the $\mathfrak{m}$-adic topology. Let E be a compact A-module.*

(i) If $\mathfrak{m} \cdot E = E$, then $E = \{0\}$.

(ii) Suppose that A is compact. Let $x_1, \ldots, x_n \in E$ be elements such that $\overline{x_1}, \ldots, \overline{x_n}$ generate $E/\mathfrak{m}E$ over $A/\mathfrak{m}A$. Then $x_1, \ldots, x_n$ generate E as an A-module.

Proof. See [La 90], page 126. □

We conclude with a special case of Nakayama's Lemma which will be the version that we will apply most frequently.

Corollary 1.43 (Nakayama's Lemma for Λ-modules)**.** *Let X be a compact Λ-module. Let $\mathfrak{m} := (p, T) \subseteq \Lambda$. Then*

$$X \text{ is finitely generated over } \Lambda \iff X/(\mathfrak{m} \cdot X) \text{ is finite} \quad .$$

If $\overline{x}_1, \ldots, \overline{x}_n$ are generators of $X/(\mathfrak{m} \cdot X)$ over $\Lambda/\mathfrak{m} \cong \mathbb{Z}/p\mathbb{Z}$, then any set of lifts $x_1, \ldots, x_n \in X$ generates X as a Λ-module. In particular,

$$X/(\mathfrak{m} \cdot X) = \{0\} \iff X = \{0\} \; .$$

Proof. This follows from Lemmas 1.42 and 1.17, (i) together with Proposition 1.18, (ii) (see [Wa 97], Lemma 13.16). Note that $\Lambda = \mathbb{Z}_p[[T]]$ is complete with respect to the $\mathfrak{m}$-adic topology and compact (compare Proposition 2.17, (i) and (iii)). □

We can now finish the sketch of the proof of Theorem 1.32. We have shown that

$$X \;\cong\; \varprojlim_n X_n \;\cong\; \varprojlim_n A_n =: A$$

is a finitely generated torsion Λ-module, and that $X/(\nu_{(n,e)} \cdot Y_e) \cong X_n$ is finite for all $n \geq e$. By Theorem 1.24, we have an exact sequence

$$0 \longrightarrow M_1 \longrightarrow X \longrightarrow E \longrightarrow M_2 \longrightarrow 0$$

where M_1 and M_2 are finite Λ-modules and E is as in Proposition 1.28, and similarly for Y_e (since $X/Y_e \cong X_e$ is finite, we have $Y_e \sim X$ in view of Corollary 1.25, (ii)). The theorem now follows from a topological argument which relates the orders $|E/(\nu_{(n,e)} \cdot E)|$ and $|X_n| = |X/Y_e| \cdot |Y_e/(\nu_{(n,e)} \cdot Y_e)|$ (see [Wa 97], pp. 284-285), together with an explicit computation of $|E/(\nu_{(n,e)} \cdot E)|$ (compare Proposition 1.28, (i)).

The following observation, proved in a special case by J. Sands in [Sa 91], will be used in Chapter 3.

Proposition 1.44. *Let K_∞/K be a $\mathbb{Z}_p$-extension. For every pair of integers (n,m) with $n > m$, we consider the distinguished polynomial*

$$\nu_{(n,m)} \;=\; \frac{(T+1)^{p^n}-1}{(T+1)^{p^m}-1} \in \mathbb{Z}_p[T]\;.$$

If $n > m \geq e = e(K_\infty/K)$, then $\nu_{(n,m)}$ is coprime to the characteristic polynomial $F_X(T)$ of X.

Proof. Assume that we are given an integer $n > e$. Fix a topological generator γ of $\mathrm{Gal}(K_\infty/K)$ and an isomorphism $\mathbb{Z}_p[[\mathrm{Gal}(K_\infty/K)]] \cong \mathbb{Z}_p[[T]] = \Lambda$. Then we have a pseudo-isomorphism of Λ-modules $E_X \xrightarrow{\sim} X$ for some suitable elementary Λ-module E_X. Let $F_X(T)$ denote the characteristic polynomial of X (compare Definition 1.29). $F_X(T)$ depends on the coice of γ, but the following proof will work for every choice of γ.

We give an adaption of (part of) the proof of Lemma 2.1 in [Sa 91], where $e = 0$ is assumed. We will show that for every $n > e$, $F_X(T)$ is coprime to the polynomial $\nu_{(n,e)}$. This obviously proves the proposition, since $\nu_{(n,m)} \mid \nu_{(n,e)}$ for $n > m \geq e$.

Recall that there exist Λ-submodules $Y_n \subseteq X$, $n \geq e$, such that we have $Y_n = \nu_{(n,e)} \cdot Y_e$ and

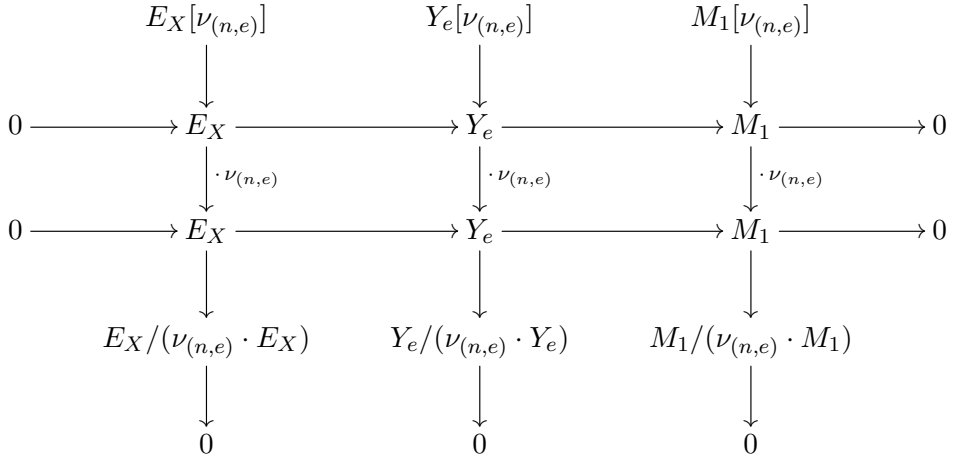
$$X_n \;\cong\; X/(\nu_{(n,e)} \cdot Y_e)$$

for every $n \geq e$ (see Lemma 1.39). In particular, $X/Y_e \cong X_e$ is finite, and therefore the elementary Λ-modules attached to the finitely generated torsion Λ-modules X and Y_e are equal, i.e., we also have a pseudo-isomorphism $E_X \xrightarrow{\sim} Y_e$ (compare Corollary 1.25, (ii)).

Since E_X does not contain any non-trivial finite Λ-submodules, this map actually is an injection, i.e., we have an exact sequence

$$0 \longrightarrow E_X \longrightarrow Y_e \longrightarrow M_1 \longrightarrow 0$$

of Λ-modules, with M_1 finite. We obtain the following commutative diagram.



Here, for any Λ-module N, we define $N[\nu_{(n,e)}] := \{n \in N \mid \nu_{(n,e)} \cdot n = 0\}$. The Snake Lemma yields a long exact sequence

$$0 \longrightarrow E_X[\nu_{(n,e)}] \longrightarrow Y_e[\nu_{(n,e)}] \longrightarrow M_1[\nu_{(n,e)}] \longrightarrow E_X/(\nu_{(n,e)} \cdot E_X) \longrightarrow Y_e/(\nu_{(n,e)} \cdot Y_e) \longrightarrow M_1/(\nu_{(n,e)} \cdot M_1) \longrightarrow 0 \, .$$

Since both $Y_e/(\nu_{(n,e)} \cdot Y_e) \subseteq X/(\nu_{(n,e)} \cdot Y_e) = X/Y_n \cong X_n$ and $M_1[\nu_{(n,e)}] \subseteq M_1$ are finite, it follows that $E_X/(\nu_{(n,e)} \cdot E_X)$ is finite, and therefore $\nu_{(n,e)}$ is coprime to $F_X(T)$, using Lemma 1.17, (i) and (ii). □

We will conclude the chapter by mentioning some well-known properties of the Iwasawa invariants μ and λ attached to a given $\mathbb{Z}_p$-extension.

Proposition 1.45. *Let K_∞/K be a $\mathbb{Z}_p$-extension with Iwasawa invariants λ, μ and ν. Let $A = \varprojlim A_n$ be defined as above.*

(i) $\mu = 0 \iff \operatorname{rank}_p(A_n)$ *is bounded as* $n \to \infty$.

(ii) Suppose that $\mu = 0$. Then $A \cong \mathbb{Z}_p^\lambda \oplus F$ as $\mathbb{Z}_p$-modules, where F is a finite p-group (this is not *an isomorphism of Λ-modules).*

Proof. This follows from Proposition 1.28, (ii) and Proposition 1.31; see [Wa 97], Propositions 13.23 and 13.25, respectively. □

Chapter 2

Multiple $\mathbb{Z}_p$-extensions

In the first chapter, we introduced the notion of $\mathbb{Z}_p$-extensions, together with the related arithmetic objects that we want to study. We have seen in Sections 1.2 and 1.3 that these objects admit a natural action of the ring $\Lambda := \mathbb{Z}_p[[T]]$ of formal power series in one variable over $\mathbb{Z}_p$.

In the following chapters, we will pursue two aims:

- find relations between the arithmetic invariants of distinct $\mathbb{Z}_p$-extensions which are in some sense 'similar' (this will be the main subject in Chapters 3 and 4), and
- generalise the theory developed so far to the study of $\mathbb{Z}_p^i$-extensions of a number field K, $i \in \mathbb{N}$ (to be performed in Chapter 5).

The current chapter wants to prepare in both directions:

- In the first, respectively, the third section, we define more algebraic structure on the set $\mathcal{E}(K)$ of all $\mathbb{Z}_p$-extensions of K. More precisely, in the first section, we show how to view $\mathcal{E}(K)$ as a projective variety. This will be used in Chapter 4. In the third section, we define *Greenberg's topology* on $\mathcal{E}(K)$, which will be fundamental throughout this work.
- The second section is devoted to a study of general profinite group rings that will naturally come up in the study of multiple $\mathbb{Z}_p$-extensions. It will be shown that these are closely connected to rings $\Lambda_i := \mathbb{Z}_p[[T_1, \dots, T_i]]$ of formal power series in several variables over $\mathbb{Z}_p$. In particular, we describe a theory of finitely generated Λ_i-modules, which can be seen as a generalisation of the study of Λ-modules in Section 1.2.

2.1 An approach using projective geometry

Let K be a number field. If d denotes the number of independent $\mathbb{Z}_p$-extensions of K, then $r_2(K) + 1 \leq d \leq [K : \mathbb{Q}]$ (see Theorem 1.7). In this chapter, we want to study the composite $\mathbb{K}$ of these d $\mathbb{Z}_p$-extensions. Note that $\mathbb{K}$ contains every $\mathbb{Z}_p$-extension of K: If L/K was a $\mathbb{Z}_p$-extension not contained in $\mathbb{K}$, then $L \cap \mathbb{K} = L_n$ for some $n \in \mathbb{N}$, where L_n denotes the n-th intermediate field of L/K, i.e., $[L_n : K] = p^n$. Therefore $[L : (L \cap \mathbb{K})] = \infty$. Now let $M_p(K)$ denote the maximal p-abelian p-ramified (i.e., unramified outside p) extension of K.

Using class field theory, one can show that we have a homomorphism

$$f : \mathrm{Gal}(M_p(K)/\mathbb{K}) \longrightarrow \mathbb{Z}_p^d$$

having finite kernel and cokernel, see [La 90], Chapter 5, Theorems 5.1 and 5.2 (this is based on Lemma 1.8). It follows that $[M_p(K) : \mathbb{K}] < \infty$ (recall that $\mathbb{K} \subseteq M_p(K)$ by Lemma 1.2). But since, again by Lemma 1.2, $L \subseteq M_p(K)$, it is then impossible to have $[L : (L \cap \mathbb{K})] = \infty$.

For the rest of this chapter (and the following parts of the text) we will usually assume that $d \geq 2$. Otherwise there would exist only one single $\mathbb{Z}_p$-extension of K, and this would have to be the cyclotomic one as defined in Section 1 of Chapter 1. Note that $d \geq 2$ if K is not totally real.

$\mathbb{K}$ is a Galois extension of K, and we have $G := \mathrm{Gal}(\mathbb{K}/K) \cong \mathbb{Z}_p^d$. Let $\sigma_1, \sigma_2, \ldots, \sigma_d$ be fixed topological generators of G. We let $\mathcal{E}(K)$ denote the set of all $\mathbb{Z}_p$-extensions of K. More generally, we define $\mathcal{E}^i(K)$, $1 \leq i \leq d$, to be the sets consisting of all $\mathbb{Z}_p^i$-extensions of K, respectively. Then $\mathcal{E}(K) = \mathcal{E}^1(K)$. By viewing the fields contained in $\mathcal{E}^i(K)$ as fixed fields of $\mathbb{K}$ under appropriate subgroups of $G = \mathrm{Gal}(\mathbb{K}/K)$, we will be able to give $\mathcal{E}(K)$ the structure of a certain projective variety. The underlying projective space is defined as follows.

Definition 2.1. For $n \in \mathbb{N}_0$ define

$$\mathbb{P}^n(\mathbb{Z}_p) := \{(a_0, \ldots, a_n)^T \in \mathbb{Z}_p^{n+1} \mid \text{not all } a_i \text{ are divisible by } p\}/\sim ,$$

where $(a_0, a_1, \ldots, a_n)^T \sim (b_0, b_1, \ldots, b_n)^T \ :\Longleftrightarrow\ \exists\, t \in \mathbb{Z}_p^* : b_i = t \cdot a_i$ for every $i = 0, \ldots, n$.

We usually write elements of $\mathbb{P}^n(\mathbb{Z}_p)$ as $(a_0 : \ldots : a_n)$.

Remark 2.2. $\mathbb{P}^n(\mathbb{Z}_p) \cong \mathbb{P}^n(\mathbb{Q}_p)$, *where the latter is the usual n-dimensional projective space over the field $\mathbb{Q}_p$.*

Proof. Every $0 \neq x \in \mathbb{Q}_p$ can be written as $x = p^{-k} \cdot y$ with $k \in \mathbb{N}_0$ and $y \in \mathbb{Z}_p$. Since $\frac{1}{p} \in \mathbb{Q}_p^* = \mathbb{Q}_p \setminus \{0\}$, we can uniquely represent every tuple $(x_0, \ldots, x_n)^T \in \mathbb{Q}_p^{n+1} \setminus \{(\underline{0})\}$ by an element $(y_0, \ldots y_n)^T \in \mathbb{Z}_p^{n+1}$ such that $p \nmid y_i$ for at least one i: just define $y_i = t \cdot x_i$, where $t = p^k$ is an appropriate power of p.

Furthermore, the equivalence relations on $\mathbb{P}^n(\mathbb{Z}_p)$ and $\mathbb{P}^n(\mathbb{Q}_p)$ coincide: Let us first assume that we have $(a_0, \ldots, a_n)^T \sim (b_0, \ldots, b_n)^T$ in $\mathbb{P}^n(\mathbb{Q}_p)$. This means that $b_i = t \cdot a_i$ for all i with an element $t \in \mathbb{Q}_p^*$. Now we choose representatives of $(a_0, \ldots, a_n)^T$ and $(b_0, \ldots, b_n)^T$ in the way described above: For the indices i with $a_i \neq 0$ (at least one such i does exist) write $a_i = p^{l_i} \cdot u_i$ with $u_i \in \mathbb{Z}_p^*$ and $l_i \in \mathbb{Z}$. Let $l := \min_i(l_i)$ and consider $a_i' := p^{-l} \cdot a_i$. Then $(a_0, \ldots, a_n)^T \sim (a_0', \ldots, a_n')^T$ in $\mathbb{P}^n(\mathbb{Q}_p)$, $a_i' \in \mathbb{Z}_p$ for all i and $a_i' \in \mathbb{Z}_p^*$ for all i with $l = l_i$, so we get an element in $\mathbb{P}^n(\mathbb{Z}_p)$ which under the equivalence relation in $\mathbb{P}^n(\mathbb{Q}_p)$ corresponds to our given tuple $(a_0, \ldots, a_n)^T$. We analogously choose a representative $(b_0', \ldots, b_n')^T \sim (b_0, \ldots, b_n)^T$.

If $t \in \mathbb{Q}_p^*$ denotes an element such that $b_i' = t \cdot a_i'$ for all i, then t cannot be divisible by p because of our choice of the a_i' and b_i' (at least one b_i' is not

divisible by p). Since $a'_i = t^{-1} \cdot b'_i$, it also follows that t cannot be divisible by p^{-1}, and therefore $t \in \mathbb{Z}_p^*$.

If, on the other hand, the classes of $(a_0, \ldots, a_n)^T$, $(b_0, \ldots, b_n)^T \in \mathbb{Q}_p^{n+1}$ are equivalent in $\mathbb{P}^n(\mathbb{Z}_p)$, represented by $(a'_0, \ldots, a'_n)^T$, $(b'_0, \ldots, b'_n)^T \in \mathbb{Z}_p^{n+1}$, then $a'_i = t \cdot b'_i$ for some $t \in \mathbb{Z}_p^* \subseteq \mathbb{Q}_p^*$ and every $i = 0, \ldots, n$, and therefore $a_i = p^s \cdot t \cdot b_i$ for some $s \in \mathbb{Z}$ and every i. Since $p^s \cdot t \in \mathbb{Q}_p^*$, we may conclude that $(a_0, \ldots, a_n)^T \sim (b_0, \ldots, b_n)^T$ in $\mathbb{P}^n(\mathbb{Q}_p)$. □

Proposition 2.3. *There is a bijection $\mathcal{E}^{d-1}(K) \longleftrightarrow \mathbb{P}^{d-1}(\mathbb{Z}_p)$. In particular, if $d = 2$, then $\mathcal{E}(K) \xrightarrow{\sim} \mathbb{P}(\mathbb{Z}_p)$.*

Proof. Let $G = \mathrm{Gal}(\mathbb{K}/K) = <\sigma_1, \ldots, \sigma_d>_{\mathbb{Z}_p}$, as above. By infinite Galois theory, there is a bijective correspondence between the subfields $L \subseteq \mathbb{K}$ having $\mathrm{Gal}(\mathbb{K}/L) \cong \mathbb{Z}_p$ and the (closed) subgroups H of G isomorphic to $\mathbb{Z}_p$, mapping H to its fixed field $L = \mathbb{K}^H$. Since G is abelian, each such L is galois over K and

$$\mathrm{Gal}(L/K) \;\cong\; G/H \;\cong\; \mathbb{Z}_p^{d-1} \;\oplus\; \text{finite torsion}\,,$$

using the fact that the ring $\mathbb{Z}_p$ is a principal ideal domain. If the topological generator $g := \sigma_1^{a_1} \cdot \ldots \cdot \sigma_d^{a_d} \in G$ of H satisfies $g = y^p$ for some element $y \in G$, then G/H contains an element $\overline{y}$ of finite order p.

If, on the other hand, g has been chosen such that $g \notin G^p$, then $G/H \cong \mathbb{Z}_p^{d-1}$ is torsion-free because of the Principal Divisor Theorem.

This shows that every element $(a_1 : \ldots : a_d) \in \mathbb{P}^{d-1}(\mathbb{Z}_p)$ defines a $\mathbb{Z}_p^{d-1}$-extension of K by considering the field fixed by the subgroup

$$H \;:=\; <\sigma_1^{a_1} \cdot \ldots \cdot \sigma_d^{a_d}>_{\mathbb{Z}_p} \;\subseteq\; G\,.$$

If we take a unit $u \in \mathbb{Z}_p^*$ and consider the group H' generated by the element $\sigma_1^{ua_1} \cdot \ldots \cdot \sigma_d^{ua_d}$, then certainly $H = H'$. This means that the group H is independent of the choice of the representative of $(a_1 : \ldots : a_d) \in \mathbb{P}^{d-1}(\mathbb{Z}_p)$, and so we obtain a well-defined and obviously injective map

$$\psi :\; \mathbb{P}^{d-1}(\mathbb{Z}_p) \longrightarrow \mathcal{E}^{d-1}(K)\,.$$

If, on the other hand, L/K is a $\mathbb{Z}_p^{d-1}$-extension, then $\mathrm{Gal}(\mathbb{K}/L) \cong \mathbb{Z}_p$, which can be seen as follows. First, $\mathrm{Gal}(\mathbb{K}/L)$ has to be a closed subgroup of $\mathbb{Z}_p^d$ and therefore is isomorphic to $\prod_{i=1}^{d'} p^{n_i}\mathbb{Z}_p$, $d' \leq d$, $n_i \in \mathbb{N}_0$ for every i. The rank of the quotient

$$\mathrm{Gal}(L/K) \;\cong\; \mathrm{Gal}(\mathbb{K}/K)/\mathrm{Gal}(\mathbb{K}/L)$$

then is equal to $d - d'$, and therefore $d' = 1$. Moreover, $\mathbb{Z}_p/p^{n_i}\mathbb{Z}_p \cong \mathbb{Z}/p^{n_i}\mathbb{Z}$ is finite and non-trivial for every $n_i > 0$, and thus $n_1 = 0$, because $\mathrm{Gal}(L/K)$ has to be torsion-free.

But then $\mathrm{Gal}(\mathbb{K}/L) = <g>_{\mathbb{Z}_p}$ is generated topologically by an element $g = a_1^{\sigma_1} \cdot \ldots \cdot \sigma_d^{a_d}$, and $p \nmid a_i$ for at least one i, by the above. This means that L is the image of $(a_1, \ldots, a_d) \in \mathbb{P}^{d-1}(\mathbb{Z}_p)$ under the above map ψ, which is therefore seen to be surjective. □

Now consider $\mathbb{Z}_p^{d-2}$-extensions of K:

$$\begin{array}{c} \mathbb{K} \\ \Big| \; G \supseteq H \cong \mathbb{Z}_p^2 \\ L \\ \Big| \; G/H \cong \mathbb{Z}_p^{d-2} \\ K \end{array}$$

Then the subgroup $H \subseteq G$ corresponding to $\mathrm{Gal}(\mathbb{K}/L) \cong \mathbb{Z}_p^2$ is topologically generated by two elements $g = \sigma_1^{a_1} \cdot \ldots \cdot \sigma_d^{a_d}$ and $g_2 = \sigma_1^{b_1} \cdot \ldots \cdot \sigma_d^{b_d}$. The above proof of the proposition shows that the tuples $(a_1, \ldots, a_d)$ and $(b_1, \ldots, b_d)$ give rise to elements in $\mathbb{P}^{d-1}(\mathbb{Z}_p)$. We will identify the tuples with their classes in $\mathbb{P}^{d-1}(\mathbb{Z}_p)$. Since $< g >_{\mathbb{Z}_p} \neq < g_2 >_{\mathbb{Z}_p}$, we have $(a_1 : \ldots : a_d) \neq (b_1 : \ldots : b_d)$ in $\mathbb{P}^{d-1}(\mathbb{Z}_p)$.

The situation here is more involved. First note that the subgroup $H \subseteq G$ may also be generated by, for example, g and $g \cdot g_2$ (corresponding to the classes $(a_1 : \ldots : a_d)$ and $(a_1 + b_1 : \ldots : a_d + b_d)$ in $\mathbb{P}^{d-1}(\mathbb{Z}_p)$), and therefore we will not get a well-defined map

$$\mathcal{E}^{d-2}(K) \longrightarrow \{\text{subsets } M \subseteq \mathbb{P}^{d-1}(\mathbb{Z}_p) \text{ with } |M| = 2\} \; ,$$

since the subset M corresponding to H is not unique.

Moreover, not every subset $M \subseteq \mathbb{P}^{d-1}(\mathbb{Z}_p)$ of order 2 yields a subgroup $H \subseteq G$ such that $G/H \cong \mathbb{Z}_p^{d-2}$ is $\mathbb{Z}_p$-free.

We would like to more generally obtain a description of $\mathcal{E}^{d-i}(K)$ for arbitrary $1 \leq i \leq d-1$. This needs even more work because not every subset M of $\mathbb{P}^{d-1}(K)$ of order i gives rise to a subgroup of G isomorphic to $\mathbb{Z}_p^i$.

Each element $x \in \mathbb{P}^{d-1}(K)$ is represented by a tuple $(a_1, \ldots, a_d)^T \in \mathbb{Z}_p^d$ such that at least one a_i is not divisible by p. If we consider the map

$$\tilde{\psi} : \mathbb{P}^{d-1}(\mathbb{Z}_p) \longrightarrow \{ \text{ subgroups } H \subseteq G \text{ isomorphic to } \mathbb{Z}_p \} \; ,$$

defined by $\tilde{\psi}(x) = < \sigma_1^{a_1} \cdot \ldots \cdot \sigma_d^{a_d} >_{\mathbb{Z}_p}$, then we have seen in the proof of Proposition 2.3 that $\tilde{\psi}$ is well-defined and injective.

Now let $y_1, \ldots, y_i \in \mathbb{Q}_p^d$ denote $\mathbb{Q}_p$-linearly independent elements. For every y_j, $j = 1, \ldots, i$, there exists a unique power p^{n_j} of p such that $p^{n_j} \cdot y_j \in \mathbb{Z}_p^d$ has at least one entry which is not divisible by p. Let $x_j := p^{n_j} \cdot y_j$, $j = 1, \ldots, i$, so that each x_j gives rise to a class in $\mathbb{P}^{d-1}(\mathbb{Z}_p)$. Let $H := < g_1, \ldots, g_i >_{\mathbb{Z}_p}$ be the subgroup of G generated by the elements $g_j := \sigma_1^{(x_j)_1} \cdot \ldots \cdot \sigma_d^{(x_j)_d}$. We want to show that $H \cong \mathbb{Z}_p^i$. Assume that $H \ncong \mathbb{Z}_p^i$, i.e., suppose that there exists a relation between the g_j. Then we have an equation of the form $\prod_j g_j^{e_j} = \prod_k g_k^{f_k}$ for suitable elements $e_j, f_k \in \mathbb{Z}_p$, $1 \leq j, k \leq i$. This can be rewritten as $1 = \prod_j g_j^{z_j}$ (setting $z_j = f_j - e_j \in \mathbb{Z}_p$). But this means that

$$1 \; = \; \prod_{j=1}^{i} (\sigma_1^{(x_j)_1} \cdot \ldots \cdot \sigma_d^{(x_j)_d})^{z_j} \; = \; \prod_{k=1}^{d} \sigma_k^{\sum_j z_j \cdot (x_j)_k} \; ,$$

and since the σ_k are multiplicatively independent, it follows that

$$0 \;=\; \sum_{j=1}^{i} z_j \cdot (x_j)_k$$

for every $1 \leq k \leq d$, and therefore the elements $x_j = ((x_j)_1, \ldots, (x_j)_d)^T$ are linearly dependent over $\mathbb{Z}_p$, so that $y_1, \ldots, y_i$ are linearly dependent over $\mathbb{Q}_p$, yielding a contradiction.

This proves that every set $\{y_1, \ldots, y_i\} \subseteq \mathbb{Q}_p^i$ of linearly independent elements defines a subset $M = \{x_1, \ldots, x_i\} \subseteq \mathbb{P}^{d-1}(\mathbb{Z}_p)$ that corresponds to a subgroup $H \cong \mathbb{Z}_p^i$ of G.

Now consider a set $M \subseteq \mathbb{P}^{d-1}(\mathbb{Z}_p)$ of order i that consists of *projectively independent* elements $\overline{x}_1, \ldots, \overline{x}_i$, i.e., one and therefore every set of representatives

$$x_1, \ldots, x_i \;\in\; \mathbb{Z}_p^d \subseteq \mathbb{Q}_p^d$$

of $\overline{x}_1, \ldots, \overline{x}_i$ is $\mathbb{Q}_p$-linearly independent. By the above, M defines a subgroup $H \subseteq G$ isomorphic to $\mathbb{Z}_p^i$.

If $x'_1, \ldots, x'_i \in \mathbb{Z}_p^d$ are representatives of certain classes $\overline{x}'_1, \ldots, \overline{x}'_i$ in $\mathbb{P}^{d-1}(\mathbb{Z}_p)$ such that $x_1, \ldots, x_i$ can be transformed into $x'_1, \ldots, x'_i$ by a linear transformation in $\mathrm{GL}_i(\mathbb{Z}_p)$, then the corresponding subgroups H and H' of G are equal: Let us write $x'_j = \sum_{k=1}^{i} a_{kj} \cdot x_k$ for every $j = 1, \ldots, i$ and suitable elements $a_{kj} \in \mathbb{Z}_p$ such that the matrix $A = (a_{kj})$ is contained in $\mathrm{GL}_i(\mathbb{Z}_p)$. Then the image of each $\overline{x}'_j \in \mathbb{P}^{d-1}(\mathbb{Z}_p)$ under $\tilde{\psi}$ is a subgroup of H. On the other hand, every x_j is a $\mathbb{Z}_p$-linear combination of the x'_k, and therefore also $H \subseteq H'$.

It is easy to see that the converse is also true: If the elements $x_1, \ldots, x_i$ and $x'_1, \ldots, x'_i \in \mathbb{Z}_p^d$ define the same subgroup $H = H'$ of G, then every x_j is a $\mathbb{Z}_p$-linear combination of the x'_k, and vice versa.

This proves that for every $1 \leq i \leq d-1$, we obtain a well-defined map

$$\Psi_i : \tilde{M}^i(\mathbb{P}^{d-1}(\mathbb{Z}_p)) \longrightarrow \{ \text{ subgroups } H \subseteq G \text{ isomorphic to } \mathbb{Z}_p^i \} \;,$$

where

$$\tilde{M}^i(\mathbb{P}^{d-1}(\mathbb{Z}_p)) \;:=\; \Big\{ M = \{\overline{x}_1, \ldots, \overline{x}_i\} \subseteq \mathbb{P}^{d-1}(\mathbb{Z}_p) \mid \overline{x}_1, \ldots, \overline{x}_i \text{ are projectively independent} \Big\} \;/\; \sim ,$$

with $\{\overline{x}_1, \ldots, \overline{x}_i\} \sim \{\overline{x}'_1, \ldots, \overline{x}'_i\}$ if and only if two (arbitrarily chosen) sets of representatives differ by a transformation in $\mathrm{GL}_i(\mathbb{Z}_p)$. Moreover, we have already seen above that the maps Ψ_i are injective. Let J_i denote the image of Ψ_i, respectively.

Proposition 2.4. *For every $1 \leq i \leq d-1$, we have an injection*

$$\mathcal{E}^{d-i}(K) \hookrightarrow J_i \;.$$

Proof. Let $L \in \mathcal{E}^{d-i}(K)$ denote an arbitrary $\mathbb{Z}_p^{d-i}$-extension of K. Then $L \subseteq \mathbb{K}$ is the fixed field of a subgroup $H \subseteq G = \mathrm{Gal}(\mathbb{K}/K)$ isomorphic to $\mathbb{Z}_p^i$. We will show that $H \subseteq J_i$. Let $g_1, \ldots, g_i$ denote topological generators of H. Having fixed a set of generators $\sigma_1, \ldots, \sigma_d$ of G, we write $g_j = \sigma_1^{(x_j)_1} \cdot \ldots \cdot \sigma_d^{(x_j)_d}$, $j = 1, \ldots, i$, with elements $x_j = ((x_j)_1, \ldots, (x_j)_d)^T \in \mathbb{Z}_p^d$, respectively. Since $G/H \cong \mathrm{Gal}(L/K)$ is torsion-free, each x_j contains at least one entry that is not divisible by p, and $< g_j >_{\mathbb{Z}_p} = \tilde{\psi}(\overline{x}_j)$, where $\overline{x}_j \in \mathbb{P}^{d-1}(\mathbb{Z}_p)$ denotes the class of x_j, respectively.

We claim that $x_1, \ldots, x_i \in \mathbb{Z}_p^d \subseteq \mathbb{Q}_p^d$ span a $\mathbb{Q}_p$-vector space of dimension i. Assume, to the contrary, that they are $\mathbb{Q}_p$-linearly dependent. Then there exist elements $z_1, \ldots, z_i \in \mathbb{Q}_p$ such that

$$0 = \sum_{j=1}^{i} z_j \cdot (x_j)_k$$

for every $1 \leq k \leq d$. By multiplying these equations by an appropriate power of p, we may in fact assume that the z_j are contained in $\mathbb{Z}_p$. But then

$$1 \;=\; \prod_{k=1}^{d} \sigma_k^{\sum_j z_j \cdot (x_j)_k} = \prod_{j=1}^{i} (\sigma_1^{(x_j)_1} \cdot \ldots \cdot \sigma_d^{(x_j)_d})^{z_j} = \prod_{j=1}^{i} g_j^{z_j} \;,$$

contradicting the fact that $g_1, \ldots, g_i$ form a basis of $H \cong \mathbb{Z}_p^i$ and therefore must be multiplicatively independent.

This shows that the span $V \subseteq \mathbb{Q}_p^d$ of $x_1, \ldots, x_i$ has dimension i, and therefore $\overline{x}_1, \ldots, \overline{x}_i$ are projectively independent. Thus, the unique subgroup $H \subseteq G$ corresponding to L is contained in J_i. □

We may therefore embed $\mathcal{E}^{d-i}(K)$ into $\tilde{M}^i(\mathbb{P}^{d-1}(\mathbb{Z}_p))$, which can be regarded as a projective variety.

In the above, we described $\mathbb{Z}_p^j$-extensions of K in terms of the subgroups of $\mathrm{Gal}(\mathbb{K}/K)$ fixing them. As we have seen, this description in general gets rather complicated. In Chapter 4, we will use a more practicable way to regard the sets $\mathcal{E}^j(K)$ as projective varieties, which has been used by V.A. Babaĭcev in course of his study of μ-invariants (see [Ba 81] and [Ba 82]).

The basic idea is to describe the elements $L \in \mathcal{E}^j(K)$ via the restriction maps

$$\mathrm{Gal}(\mathbb{K}/K) \;\longrightarrow\; \mathrm{Gal}(L/K) \;.$$

We will start with the most important case, $j = 1$. Let

$$\varepsilon(\mathbb{Z}_p^d) \;:=\; \{\pi : \mathbb{Z}_p^d \twoheadrightarrow \mathbb{Z}_p\}$$

denote the set of all surjective $\mathbb{Z}_p$-module homomorphisms (i.e., continuous group homomorphisms) from $\mathbb{Z}_p^d$ to $\mathbb{Z}_p$.

Proposition 2.5 (Babaĭcev)**.** *There is a bijection*

$$\varphi : \varepsilon(\mathbb{Z}_p^d) \;\xrightarrow{\sim}\; \mathbb{P}^{d-1}(\mathbb{Z}_p) \;.$$

Proof. The map φ is defined as follows: Let $\gamma_1, \ldots, \gamma_d$ denote a fixed system of topological generators of $\mathbb{Z}_p^d$, and let δ be a generator of $\mathbb{Z}_p$. Then every element $\pi \in \varepsilon(\mathbb{Z}_p^d)$ is uniquely determined by the values

$$\pi(\gamma_i) \;=\; \delta^{a_i} \;, \quad a_i \in \mathbb{Z}_p \;, \quad 1 \leq i \leq d \;,$$

i.e., π is uniquely characterised by the tuple $(a_1, \ldots, a_d)^T \in \mathbb{Z}_p^d$.

Furthermore, since each $\pi \in \varepsilon(\mathbb{Z}_p^d)$ is surjective, at least one of the a_i has to be contained in $\mathbb{Z}_p^*$, which means that p does not divide a_i. Now if δ' denotes a different generator of $\mathbb{Z}_p$, then

$$\delta' = \delta^u \;, \quad u \in \mathbb{Z}_p^* \;,$$

and therefore, when considered with regard to the new generator δ', π is described by the tuple $(a_1 \cdot u, \ldots, a_d \cdot u)^T \in \mathbb{Z}_p^d$, which is equivalent to $(a_1, \ldots, a_d)^T$ in $\mathbb{P}^{d-1}(\mathbb{Z}_p)$. Therefore the equivalence relation in $\mathbb{P}^{d-1}(\mathbb{Z}_p)$ corresponds to the possibility of choosing a different topological generator of $\mathbb{Z}_p$; if we fix a generator δ of $\mathbb{Z}_p$, then there is a unique representative $(a_1, \ldots, a_d)^T \in \mathbb{Z}_p^d$ of the class in $\mathbb{P}^{d-1}(\mathbb{Z}_p)$ corresponding to the homomorphism π.

It is then obvious that the map

$$\varphi : \pi \mapsto (a_1 : \ldots : a_d)$$

defines a well-defined bijection between $\varepsilon(\mathbb{Z}_p^d)$ and $\mathbb{P}^{d-1}(\mathbb{Z}_p)$, since for fixed topological generator δ of $\mathbb{Z}_p$, the tuples $(a_1, \ldots, a_d)^T$ and $(a'_1, \ldots, a'_d)^T$ representing two classes in $\mathbb{P}^{d-1}(\mathbb{Z}_p)$ that correspond to homomorphisms

$$\pi, \pi' : \mathbb{Z}_p^d \longrightarrow \mathbb{Z}_p \;,$$

respectively, are equal if and only if $\pi = \pi'$.

Furthermore, it is obvious that every tuple $(a_1, \ldots, a_d)^T \in \mathbb{Z}_p^d$ with $p \nmid a_i$ for at least one index $i \in \{1, \ldots, d\}$ gives rise to a surjective homomorphism $\pi : \mathbb{Z}_p^d \longrightarrow \mathbb{Z}_p$. □

Remarks 2.6.

(1) One may ask for the reason of considering this bijection to $\mathbb{P}^{d-1}(\mathbb{Z}_p)$ instead of simply fixing a topological generator of $\mathbb{Z}_p$ and looking at the induced map

$$\varepsilon(\mathbb{Z}_p^d) \;\longrightarrow\; \{(a_1, \ldots, a_d)^T \in \mathbb{Z}_p^d \mid \; p \nmid a_i \text{ for at least one } i \;\} \;.$$

It will turn out to be important to have the freedom of changing the generator of $\mathbb{Z}_p$, as we will see in the next lemma.

(2) We introduce a topology on $\varepsilon(\mathbb{Z}_p^d)$ by using the canonical topology on $\mathbb{P}^{d-1}(\mathbb{Z}_p)$, induced by the p-adic topology on $\mathbb{Z}_p$: A basis of the neighbourhoods of an element $(a_1, \ldots, a_d)^T \in \mathbb{Z}_p^d$ representing a class in $\mathbb{P}^{d-1}(\mathbb{Z}_p)$ is given by the sets of the form

$$U_{(n_1,\ldots,n_d)}(a_1, \ldots, a_d) \;=\; \{(b_1, \ldots, b_d)^T \in \mathbb{Z}_p^d \mid a_i - b_i \in (p)^{n_i}, i = 1, \ldots, d\}$$

with $(n_1, \ldots, n_d)^T \in \mathbb{N}^d$. Note that $p \nmid b_i$ if $p \nmid a_i$ and $a_i - b_i \in (p)^{n_i}$, $n_i \in \mathbb{N}$.

Using the isomorphism $\mathrm{Gal}(\mathbb{K}/K) \cong \mathbb{Z}_p^d$, we may identify $\varepsilon(\mathbb{Z}_p^d)$ and

$$\varepsilon(\mathrm{Gal}(\mathbb{K}/K)) \;:=\; \{\pi : \mathrm{Gal}(\mathbb{K}/K) \twoheadrightarrow \mathbb{Z}_p\} \; .$$

Lemma 2.7. *There exists a bijection*

$$\mathcal{E}(K) \xrightarrow{\sim} \varepsilon(\mathrm{Gal}(\mathbb{K}/K)) \; .$$

Proof. We define two maps

$$\varphi_1 : \mathcal{E}(K) \longrightarrow \varepsilon(\mathrm{Gal}(\mathbb{K}/K)) \quad \text{and} \quad \varphi_2 : \varepsilon(\mathrm{Gal}(\mathbb{K}/K)) \longrightarrow \mathcal{E}(K)$$

and show that they are inverse to each other.

- Let $L \in \mathcal{E}(K)$. We define $\varphi_1(L) : \mathbb{Z}_p^d \longrightarrow \mathbb{Z}_p$ to be the surjective homomorphism induced by the canonical restriction map, identifying $\mathrm{Gal}(L/K)$ with $\mathbb{Z}_p$. The class of π in $\varepsilon(\mathrm{Gal}(\mathbb{K}/K)) \xrightarrow{\sim} \mathbb{P}^{d-1}(\mathbb{Z}_p)$ does not depend on the choice of a topological generator of the quotient $\mathrm{Gal}(L/K)$. This is important for getting a well-defined map, since there is no distinguished generator of $\mathrm{Gal}(L/K)$ (compare Remarks 2.6, (1)).
- Let $\pi : \mathbb{Z}_p^d \twoheadrightarrow \mathbb{Z}_p$ be a $\mathbb{Z}_p$-module homomorphism, let

  $$H \;:=\; \ker(\pi) \;\subseteq\; G \;:=\; \mathbb{Z}_p^d \;\cong\; \mathrm{Gal}(\mathbb{K}/K) \; .$$

  Then H is a free $\mathbb{Z}_p$-module of rank $d-1$, and $G/H \cong \mathbb{Z}_p$ is torsion-free, so the fixed field $\varphi_2(\pi) := \mathbb{K}^H$ is a $\mathbb{Z}_p$-extension of K (note that $H \subseteq G$ is a closed subgroup, since π is a continuous homomorphism).
- We now want to prove that φ_1 and φ_2 are inverse to each other.
- $\varphi_2(\varphi_1(L)) = L$: By definition, $\varphi_1(L)(\sigma) = \sigma|_L$ for every $\sigma \in \mathrm{Gal}(\mathbb{K}/K)$. In particular, $\varphi_1(L)(\sigma) = 1$ if and only if $\sigma|_L = 1$, i.e., if and only if $\sigma \in \mathrm{Gal}(\mathbb{K}/L)$. This shows that the fixed field $\varphi_2(\varphi_1(L))$ is equal to L.
- $\varphi_1(\varphi_2(\pi)) = \pi$: $\varphi_2(\pi)$ is the subfield of $\mathbb{K}$ fixed by the kernel of π. For every $\sigma \in \mathrm{Gal}(\mathbb{K}/K) \cong \mathbb{Z}_p^d$, $\varphi_1(\varphi_2(\pi)) = \sigma|_{\varphi_2(\pi)}$ is the restriction of σ to $\varphi_2(\pi)$. Choose generators $\gamma_1, \ldots, \gamma_d$ of $\mathbb{Z}_p^d$ such that $\gamma_1, \ldots, \gamma_{d-1}$ generate the kernel of π (compare Remark 4.8 in Chapter 4; note that this is allowed because the definitions of φ_1 and φ_2 do not depend on the choice of generators of $\mathrm{Gal}(\mathbb{K}/K) \cong \mathbb{Z}_p^d$). Then $\varphi_2(\pi)$ is fixed by $\gamma_1, \ldots, \gamma_{d-1}$, so that in particular,

  $$\varphi_1(\varphi_2(\pi))(\gamma_i) \;=\; \gamma_i|_{\varphi_2(\pi)} \;=\; 1 \qquad 1 \leq i \leq d-1 \; .$$

  Furthermore, γ_d has to generate $\mathrm{Gal}(\varphi_2(\pi)/K) \cong \mathbb{Z}_p$, because the restriction map $\mathrm{Gal}(\mathbb{K}/K) \twoheadrightarrow \mathrm{Gal}(\varphi_2(\pi)/K)$ is surjective. If δ denotes any topological generator of $\mathrm{Gal}(\varphi_2(\pi)/K)$, then we have

  $$\varphi_1(\varphi_2(\pi))(\gamma_d) \;=\; \gamma_d|_{\varphi_2(\pi)} \;=\; \delta^a$$

  for some $a \in \mathbb{Z}_p^*$. This means that $\varphi_1(\varphi_2(\pi)) = \pi$ in $\varepsilon(\mathrm{Gal}(\mathbb{K}/K))$, since every tuple $(0, \ldots, 0, a)^T$, $a \in \mathbb{Z}_p^*$, is equivalent to $(0, \ldots, 0, 1)^T$ in $\mathbb{P}^{d-1}(\mathbb{Z}_p) \cong \varepsilon(\mathbb{Z}_p^d)$.

□

Remark 2.8. In Proposition 2.3, we have seen that there is a bijection

$$\mathbb{P}^{d-1}(\mathbb{Z}_p) \xrightarrow{\sim} \mathcal{E}^{d-1}(K) \ ,$$

where $\mathcal{E}^{d-1}(K)$ denotes the set of $\mathbb{Z}_p^{d-1}$-extensions of K. We obtained a $\mathbb{Z}_p^{d-1}$-extension M of K corresponding to the element $(a_1 : \ldots : a_d) \in \mathbb{P}^{d-1}(\mathbb{Z}_p)$ by considering the subfield of $\mathbb{K}$ that is fixed by $<\gamma_1^{a_1} \cdot \ldots \cdot \gamma_d^{a_d}> \cong \mathbb{Z}_p$.
On the other hand, each $(a_1 : \ldots : a_d) \in \mathbb{P}^{d-1}(\mathbb{Z}_p)$ corresponds to some homomorphism $\pi \in \varepsilon(\mathrm{Gal}(\mathbb{K}/K))$, by Proposition 2.5, and therefore yields a $\mathbb{Z}_p$-extension L of K via Lemma 2.7.
This yields a bijective correspondence

$$\mathcal{E}(K) \xrightarrow{\sim} \mathcal{E}^{d-1}(K) \ .$$

The pairs

$$(L, M) \in \mathcal{E}(K) \times \mathcal{E}^{d-1}(K)$$

defined by this bijection are kind of *dual* pairs of extensions of K:
Suppose that a pair (L, M) is given; let $\pi : \mathbb{Z}_p^d \longrightarrow \mathbb{Z}_p$ denote the homomorphism that induces this pair. If we choose the topological generators of $\mathrm{Gal}(\mathbb{K}/K) \cong \mathbb{Z}_p^d$ such that the tuple $(a_1, \ldots, a_d)$ describing the corresponding homomorphism π has the form $(0, \ldots, 0, 1)$ (this is always possible, compare Remark 4.8, and does not affect the pair (L, M)), then $M \subseteq \mathbb{K}$ is the fixed field of $<\gamma_d>$, and the $\mathbb{Z}_p$-extension L/K is the unique extension such that the restriction map $\mathrm{Gal}(\mathbb{K}/K) \twoheadrightarrow \mathrm{Gal}(L/K)$ is given by the homomorphism π that maps $\gamma_i \mapsto 1$ for $i < d$, while γ_d is mapped to a generator of $\mathrm{Gal}(L/K)$. Therefore, L is fixed by the subgroup of $\mathrm{Gal}(\mathbb{K}/K)$ generated by $\gamma_1, \ldots, \gamma_{d-1}$. But this means that we have

$$L \cap M \ = \ K \quad \text{ and } \quad L \cdot M \ = \ \mathbb{K} \ .$$

More generally, for every $n \in \mathbb{N}$ and $0 \leq m \leq n-1$, we let ε_n^m denote the set of all surjective $\mathbb{Z}_p$-module homomorphisms

$$\pi : \mathbb{Z}_p^{n+1} \ \twoheadrightarrow \ \mathbb{Z}_p^{m+1} \ .$$

In particular, $\varepsilon_{d-1}^0 = \varepsilon(\mathbb{Z}_p^d)$ is the set that we have studied above.

Let us fix n and m. Choose topological generators $\gamma_0, \ldots, \gamma_n$ of $\mathbb{Z}_p^{n+1}$ and $\delta_0, \ldots, \delta_m$ of $\mathbb{Z}_p^{m+1}$, respectively. Then every $\pi \in \varepsilon_n^m$ is uniquely determined by the values

$$\pi(\gamma_i) \ = \ \prod_{j=0}^{m} \delta_j^{a_{ij}} \quad , \quad 0 \leq i \leq n \ , \quad \text{with } a_{ij} \in \mathbb{Z}_p \ \text{ for every } i \text{ and } j \quad .$$

If we define $A := (a_{ij}) \in \mathrm{Mat}_{(n+1)\times(m+1)}(\mathbb{Z}_p)$, then we may write this as $\pi((\underline{\gamma})) = A \cdot (\underline{\delta})$, where $(\underline{\gamma}) = (\gamma_0, \ldots, \gamma_n)^T$ and $(\underline{\delta}) = (\delta_0, \ldots, \delta_m)^T$ are column vectors. Choosing a different set of topological generators of $\mathbb{Z}_p^{m+1}$ corresponds to multiplying A from the right by a matrix in $\mathrm{GL}_{m+1}(\mathbb{Z}_p)$. Therefore π determines A only up to multiplication by a matrix in $\mathrm{GL}_{m+1}(\mathbb{Z}_p)$.

Let $A_0, \ldots, A_{N-1}$, $N = \binom{n+1}{m+1}$, denote the minors of A of order $m+1$. Using the map

$$\psi \,:\, A \mapsto (A_0 : \cdots : A_{N-1}) \,,$$

we may embed ε_n^m into the projective space $\mathbb{P}^N(\mathbb{Z}_p)$: First note that this is well-defined. Indeed, if we change A to $A \cdot B$, with $B \in \mathrm{GL}_{m+1}(\mathbb{Z}_p)$, corresponding to a different choice of topological generators of $\mathbb{Z}_p^{m+1}$, then $(A_0 : \cdots : A_{N-1})$ changes to $(A_0 \cdot \det(B) : \cdots : A_{N-1} \cdot \det(B))$, which is the same element in $\mathbb{P}^N(\mathbb{Z}_p)$.

Moreover, the map ψ is injective, which can be seen as follows. Suppose that two matrices $A, B \in \mathrm{Mat}_{(n+1)\times(m+1)}(\mathbb{Z}_p)$ are mapped to the same element $(c_0 : \ldots : c_{N-1}) \in \mathbb{P}^{N-1}(\mathbb{Z}_p)$. Then there exists some $t \in \mathbb{Z}_p^*$ such that $A_i = t \cdot B_i$ for every $0 \leq i \leq N-1$, where $B_0, \ldots, B_{N-1}$ denote the corresponding minors of B.

Suppose that the generators $\gamma_0, \ldots, \gamma_n$ of $\mathbb{Z}_p^{n+1}$ have been chosen such that A corresponds to the map

$$\pi \,:\, \gamma_i \mapsto \begin{cases} \delta_i & : \, i \leq m \\ 1 & : \, i > m \,. \end{cases}$$

Then $\psi(A) = (1 : 0 : \ldots : 0)$, $\psi(B) = (t^{-1} : 0 : \ldots : 0)$, and therefore B describes the same homomorphism π with regard to the basis $\{\delta_0^t, \delta_1, \ldots, \delta_m\}$ of $\mathbb{Z}_p^{m+1}$. This shows that $\psi : \varepsilon_n^m \longrightarrow \mathbb{P}^N(\mathbb{Z}_p)$ is injective.

Moreover, since $m < n$ and therefore $\det(A) = 0$, the image of ψ forms a subvariety of $\mathbb{P}^N(\mathbb{Z}_p)$ (i.e., closed with respect to the Zariski topology). In particular, by identifying ε_n^m with its image, we can view ε_n^m as a compact projective variety.

The *Grassmanian varieties* ε_n^m will be used in Section 4.2.2.

2.2 Group rings and power series

As we have seen in Chapter 1, the complete group ring $\mathbb{Z}_p[[\Gamma]] \cong \Lambda$ plays a fundamental role in the study of the arithmetic properties of $\mathbb{Z}_p$-extensions K_∞/K. We want to generalise the construction given in Section 1.2 in order to be able to apply it to multiple $\mathbb{Z}_p$-extensions. Therefore we give the following very general definition.

Definition 2.9. Let G be a profinite group, i.e., a compact Hausdorff topological group such that there exists a system of neighbourhoods of the neutral element containing only normal subgroups. Let $\mathcal{O}$ be a local ring with unique maximal ideal $\mathfrak{p}$ that is Hausdorff and complete with respect to the $\mathfrak{p}$-adic topology. We furthermore assume that $\mathcal{O}$ is compact. Then we define the ***completed group ring of*** G ***over*** $\mathcal{O}$ to be the topological inverse limit

$$\mathcal{O}[[G]] := \varprojlim_U \mathcal{O}[G/U]$$

of the group rings $\mathcal{O}[G/U]$, where U runs through all the open normal subgroups of G.

Remarks 2.10.

(1) Let $U \subseteq G$ be an open subgroup. Then we can write G as the union of pairwise disjoint cosets modulo U, i.e. $G = \bigcup_i \sigma_i \cdot U$, where σ_i runs through a system of representatives of G/U. Since G is compact and all the $\sigma_i \cdot U$ are open, we can conclude that U is of finite index in G. Therefore every $\mathcal{O}[G/U]$ is the group ring of a finite group over $\mathcal{O}$.

(2) For any profinite topological group G, we have an isomorphism (algebraically and topologically) $G \cong \varprojlim G/U$, where U runs through the open normal subgroups of G (see [Neu 92], Theorem IV.2.8).
Here the projective limit is taken according to the canonical projection mappings induced by inclusions (i.e., the open normal subgroups of G are ordered partially by inclusion; if $U_i \supseteq U_j$, then we consider the maps

$$f_{i,j} : G/U_j \longrightarrow G/U_i$$

between finite groups). This projective system also induces the inverse limit $\varprojlim \mathcal{O}[G/U]$.

(3) The open normal subgroups of $\mathbb{Z}_p$ are exactly the groups $p^n\mathbb{Z}_p$ with $n \in \mathbb{N}_0$ ($\{0\}$ is not open since $\mathbb{Z}_p/(0)$ has infinite order). Therefore Definition 2.9 is a direct generalisation of the definition of $\mathcal{O}[[\Gamma]]$ given in Section 1.2.

In the following, we will prove a generalisation of Theorem 1.9 for multiple $\mathbb{Z}_p$-extensions. We therefore will have to deal with rings of formal power series in several variables and coefficients in $\mathcal{O}$. Before stating the theorem, we will collect some properties of such rings. This makes use of the following concepts.

In what follows, let $\mathcal{O}$ denote an arbitrary ring. For any prime ideal $\mathfrak{p} \subseteq \mathcal{O}$, we can consider the localisation $\mathcal{O}_\mathfrak{p}$. If $\mathcal{O}$ is a domain, then each $\mathcal{O}_\mathfrak{p}$ is a subring of the quotient field of $\mathcal{O}$.

Definition 2.11. The ***height*** of $\mathfrak{p}$ is defined to be $\mathrm{ht}(\mathfrak{p}) := \dim(\mathcal{O}_\mathfrak{p})$, where dim means the ***Krull dimension*** of the ring $\mathcal{O}_\mathfrak{p}$, i.e., the maximal length n of a chain of prime ideals

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_n$$

in $\mathcal{O}_\mathfrak{p}$. This corresponds to the maximal length of a chain of prime ideals in $\mathcal{O}$ descending from $\mathfrak{p}$.
Be aware of the numbering which takes care of the trivial ideal $\{0\}$, which is prime if $\mathcal{O}_\mathfrak{p}$ is a domain.
Let $\mathrm{P}(\mathcal{O})$ denote the set of prime ideals $\mathfrak{p} \subseteq \mathcal{O}$ of height 1.

Definition 2.12. Let now $\mathcal{O}$ be a local ring with maximal ideal $\mathfrak{m}$.

(1) Let $I \subseteq \mathcal{O}$ be an ideal. Then we call I an ***ideal of definition*** of $\mathcal{O}$ if there exists an integer $\nu > 0$ such that $\mathfrak{m}^\nu \subseteq I \subseteq \mathfrak{m}$.

(2) Let d be the Krull dimension of $\mathcal{O}$ as defined in Definition 2.11. If I is an ideal of definition of $\mathcal{O}$ that is generated by d elements $x_1, \ldots, x_d$, then we say that $\{x_1, \ldots, x_d\}$ is a ***system of parameters*** of $\mathcal{O}$.

(3) If there is a system of parameters that generates the maximal ideal $\mathfrak{m}$, then we say that $\mathcal{O}$ is a ***regular local ring***.

(4) An arbitrary (not necessarily local) Noetherian ring $\mathcal{O}$ is called ***regular*** if for every prime ideal $\mathfrak{p} \subseteq \mathcal{O}$, the localisation $\mathcal{O}_\mathfrak{p}$ is a regular local ring.

Definition 2.13. Let $\mathcal{O}$ be a domain with quotient field K. Then $\mathcal{O}$ is called ***completely integrally closed*** if the following condition holds:
If $x \in K$ is such that there exists a finitely generated $\mathcal{O}$-submodule of K containing every power x^n, $n \in \mathbb{N}$, then $x \in \mathcal{O}$.

Proposition 2.14. *Let $\mathcal{O}$ be a domain.*
(i) If $\mathcal{O}$ is completely integrally closed, then $\mathcal{O}$ is integrally closed.
(ii) If $\mathcal{O}$ is Noetherian, then the converse of (i) holds.
(iii) If $\mathcal{O}$ is completely integrally closed, then $\mathcal{O}[X]$ and $\mathcal{O}[[X]]$ are completely integrally closed.

Proof. (i) and (ii): See [Bou 89], Chapter V, §1, no. 1 and no. 4..
(iii): See [Bou 89], Chapter V, §1, no.4, Proposition 14. □

Lemma 2.15. *Let $\mathcal{O}$ denote a regular factorial local ring with maximal ideal $\mathfrak{m}$. Suppose that $\mathcal{O}$ is Hausdorff and complete with respect to the $\mathfrak{m}$-adic topology, and that the residue field $\mathcal{O}/\mathfrak{m}$ is finite. Let $d \in \mathbb{N}$. Then the rings of formal power series in d variables over $\mathcal{O}$ have the following properties:*
(i) $\mathcal{O}[[T_1, \ldots, T_d]]$ is a local ring with maximal ideal

$$\mathfrak{M}_d \;=\; \mathfrak{m} + (T_1, \ldots, T_d)\ .$$

It is Hausdorff and complete with respect to the $\mathfrak{M}_d$-adic topology.
(ii) $\mathcal{O}[[T_1, \ldots, T_d]]$ is a compact topological group.
(iii) $\mathcal{O}[[T_1, \ldots, T_d]]$ is a unique factorisation domain.
(iv) If $\mathcal{O}$ is Noetherian, then also $\mathcal{O}[[T_1, \ldots, T_d]]$ is Noetherian.
(v) If $\mathcal{O}$ is Noetherian and integrally closed, then also $\mathcal{O}[[T_1, \ldots, T_d]]$ is integrally closed.
(vi) If $\mathcal{O}$ is Noetherian and integrally closed, then we have

$$\mathcal{O}[[T_1, \ldots, T_d]] \;=\; \bigcap_{\mathfrak{p} \,\in\, \mathrm{P}(\mathcal{O}[[T_1, \ldots, T_d]])} ((\mathcal{O}[[T_1, \ldots, T_d]])_\mathfrak{p})\ .$$

Proof. (i) It is a general fact that for a local ring A, the ring $A[[T_1, \ldots, T_d]]$ of formal power series in a finite number of variables is local, too (see [Bou 89], Chapter II, §3, no. 1). Furthermore, using the corollary of Proposition 6 in [Bou 89], Chapter III, §2, no. 6, we inductively obtain that the maximal ideal $\mathfrak{M}_d$ of $\mathcal{O}[[T_1, \ldots, T_d]]$ is generated by $\mathfrak{m}$ and $T_1, \ldots, T_d$, and that $\mathcal{O}[[T_1, \ldots, T_d]]$ is Hausdorff and complete with respect to the $\mathfrak{M}_d$-adic topology.
(ii) Since $\mathcal{O}[[T_1, \ldots, T_d]]$ is Hausdorff and complete with respect to the $\mathfrak{M}_d$-adic topology, $\mathcal{O}[[T_1, \ldots, T_d]]$ may be canonically identified with the inverse limit of the finite discrete quotients $(\mathcal{O}[[T_1, \ldots, T_d]])/\mathfrak{M}_d^i$, $i \in \mathbb{N}$, see [Bou 89], Chapter III, §2, no. 6. This limit is compact (see [Neu 92], Theorem IV.2.3).

(iii) Since $\mathcal{O}$ is a regular local ring, Theorem 19.5 of [Mat 86] implies that $\mathcal{O}[[T_1, \ldots, T_d]]$ is regular, too. By a theorem of AUSLANDER and BUCHSBAUM (see Theorem 20.3 in [Mat 86]), every regular local ring is a unique factorisation domain.

(iv) If A denotes any Noetherian domain, then also $A[[T_1, \ldots, T_d]]$ is Noetherian, see [Bou 89], Chapter III, §2, no. 10, Corollary 6.

(v) Since $\mathcal{O}$ is Noetherian and integrally closed, it is completely integrally closed by Proposition 2.14, (ii). The assertion follows inductively by using (iii) and, finally, (i) of the same proposition.

(vi) This is an immediate consequence of (iv) and (v), which together imply that $\mathcal{O}[[T_1, \ldots, T_d]]$ is a so-called *Krull domain*, see [Bou 89], Corollary 1 to Lemma 1 in Chapter VII, §1, no. 3. The statement then follows from Theorem 4 in [Bou 89], Chapter VII, §1, no. 6.

□

We now specialise to the case $\mathcal{O} = \mathbb{Z}_p$ (this will be enough for our purposes).

Definition 2.16. For any $d \in \mathbb{N}$ let $\Lambda_d := \mathbb{Z}_p[[T_1, \ldots, T_d]]$ denote the ring of formal power series in d variables having coefficients in $\mathbb{Z}_p$. In particular, $\Lambda_1 = \Lambda$ is the ring studied in Chapter 1.

Lemma 2.15 yields the following properties of the rings Λ_d.

Proposition 2.17.

(i) *Λ_d is a local ring with unique maximal ideal given by $\mathfrak{M}_d = (p, T_1, \ldots, T_d)$. It is Hausdorff and complete with respect to the $\mathfrak{M}_d$-adic topology.*

(ii) *Λ_d is regular with Krull dimension equal to $d + 1$.*

(iii) *Λ_d is a compact topological group.*

(iv) *Λ_d is a unique factorisation domain.*

(v) *Λ_d is Noetherian and integrally closed.*

(vi) *We have*

$$\Lambda_d \;=\; \bigcap_{\mathfrak{p} \in \mathrm{P}(\Lambda_d)} ((\Lambda_d)_{\mathfrak{p}}) \; .$$

Proof. Everything except (ii) follows immediately from Lemma 2.15. Since the ring $\mathbb{Z}_p$ is a Dedekind domain and therefore any prime ideal $\mathfrak{p} \neq (0)$ is maximal, the Krull dimension of $\mathbb{Z}_p$ is equal to 1. Since $\mathfrak{m} = (p)$ is the maximal ideal of the local ring $\mathbb{Z}_p$, we know that $\{p\}$ is a system of parameters of $\mathbb{Z}_p$. Therefore $\mathbb{Z}_p$ is a regular local ring (compare Definition 2.12, (3)). By Theorem 19.5 of [Mat 86], the ring of formal power series over a regular ring again is regular. Using Theorem 15.4 in [Mat 86], we can compute the Krull dimension of Λ_d as follows:

$$\dim(\mathbb{Z}_p[[T_1, \ldots, T_d]]) \;=\; \dim \mathbb{Z}_p + d \;=\; d + 1 \; .$$

□

We now come to the generalisation of Theorem 1.9 announced above. Let K and $\mathbb{K}$ be as in Section 2.1, and write $G = \mathrm{Gal}(\mathbb{K}/K) = <\sigma_1, \ldots, \sigma_d>_{\mathbb{Z}_p}$ with fixed topological generators $\sigma_1, \ldots, \sigma_d$.

Theorem 2.18. *$\mathbb{Z}_p[[G]] \cong \Lambda_d$, the isomorphism of $\mathbb{Z}_p$-algebras (and homeomorphism of topological groups) being induced by $\sigma_i \mapsto 1 + T_i$, $i = 1, \ldots, d$.*

Proof. The case $d = 1$ is covered by Theorem 1.9. We now let $d \in \mathbb{N}$ be arbitrary.

For every integer $n \in \mathbb{N}_0$, we consider the subgroup $G^{p^n} \subseteq G$ generated by the elements $\sigma_1^{p^n}, \ldots, \sigma_d^{p^n}$, and we let G_n denote the quotient group

$$G/G^{p^n} \cong (\mathbb{Z}/p^n\mathbb{Z})^d ,$$

respectively. Then it is easy to see that $\mathbb{Z}_p[[G]]$ is algebraically and topologically isomorphic to the projective limit $\varprojlim \mathbb{Z}_p[G_n]$, where the limit is taken with respect to the projections $\pi_{n,m} : G_n \longrightarrow G_m$, $n \geq m$, that are induced by the inclusions $G^{p^n} \subseteq G^{p^m}$, respectively:

Indeed, by [Neu 92], Theorem IV.2.8, G is isomorphic to the projective limit $\varprojlim G/U$, where U runs over the open normal subgroups of G; since $G \cong \mathbb{Z}_p^d$, these are isomorphic to $\prod_{j=1}^{d} p^{n_j}\mathbb{Z}_p$, $n_j \in \mathbb{N}_0$ for every $j = 1, \ldots, d$, and therefore every such U contains some G^{p^n}. But then we have $\varprojlim G/U \cong \varprojlim G_n$ and $\mathbb{Z}_p[[G]] \cong \varprojlim \mathbb{Z}_p[G_n]$.

For every fixed integer n, there exists an isomorphism

$$\mathbb{Z}_p[G_n] \xrightarrow{\sim} \mathbb{Z}_p[T_1, \ldots, T_d]/I_n ,$$

where the ideal $I_n \subseteq \mathbb{Z}_p[T_1, \ldots, T_d]$ is generated by the elements $(T_1+1)^{p^n} - 1$, $\ldots$, $(T_d+1)^{p^n} - 1$. Here the isomorphism is induced by mapping each generator $\sigma_i \in G_n = G/G^{p^n} \cong (\mathbb{Z}/p^n\mathbb{Z})^d$ to the polynomial $(T_i + 1)^{p^n} - 1$, respectively.

We therefore have to show that

$$\mathbb{Z}_p[[T_1, \ldots, T_d]] \cong \varprojlim \mathbb{Z}_p[T_1, \ldots, T_d]/\left((T_1 + 1)^{p^n} - 1, \ldots, (T_d + 1)^{p^n} - 1\right) .$$

By Proposition 2.17, (iii), $\Lambda_d = \mathbb{Z}_p[[T_1, \ldots, T_d]]$ is a compact topological group. The canonical projections $\Lambda_d \longrightarrow \Lambda_d/I_n$, $n \in \mathbb{N}$, define a continuous homomorphism $\varphi : \Lambda_d \longrightarrow \varprojlim \Lambda_d/I_n$. Let $\mathfrak{M}_d := (p, T_1, \ldots, T_d)$ denote the maximal ideal of Λ_d. Since

$$\bigcap_{n\geq 0} I_n \subseteq \bigcap_{n\geq 0} \mathfrak{M}_d^n = \{0\} ,$$

the map φ is injective.

Let $(\overline{f}_n)_{n\geq 0} \in \varprojlim \Lambda_d/I_n$ denote an arbitrary element; we will show that there exists a pre-image $f \in \Lambda_d$ under φ: For each n, we choose a representative $f_n \in \Lambda_d$ of $\overline{f}_n \in \Lambda_d/I_n$. Since Λ_d is complete with respect to the $\mathfrak{M}_d$-adic topology (see Proposition 2.17, (i)), and since $I_n \subseteq \mathfrak{M}_d^n$ for every n, there exists an element $f \in \Lambda_d$ such that $f \in \bigcap_{n\geq 0} \overline{f}_n = \bigcap_{n\geq 0} f_n \cdot I_n$ (note that for every $j \geq i$, we have $f_j \equiv f_i \bmod I_i$). But then $\varphi(f) = (\overline{f}_n)_n$, and therefore φ is an isomorphism.

Furthermore, every quotient

$$\Lambda_d/I_n \cong \mathbb{Z}_p[T_1,\ldots,T_d]/I_n \cong \mathbb{Z}_p^{d\cdot p^n}$$

is profinite, and therefore also the limit $\varprojlim \Lambda_d/I_n$ is a profinite group (compare Lemma 1.2.6, (c) in [FJ 08]), and in particular Hausdorff. Since Λ_d is compact, it follows that $\varphi : \Lambda_d \longrightarrow \varprojlim \Lambda_d/I_n$ is a homeomorphism (see [Os 92], Corollary 2.4.9).

□

We will conclude this section by giving an overview of the theory of Λ_d-modules (analogously to the theory of Λ-modules described in Section 1.2, which culminated in the Structure Theorem 1.24 – see Theorem 2.23 below).

Definition 2.19. A finitely generated Λ_d-module M is called ***pseudo-null*** if $M_{\mathfrak{p}} = \{0\}$ for all prime ideals $\mathfrak{p} \subseteq \Lambda_d$ of height ≤ 1.

Remarks 2.20.

(1) A pseudo-null Λ_d-module M is Λ_d-torsion.

(2) M is pseudo-null if and only if it satisfies the following equivalent condition: If $\mathfrak{p}$ is a prime ideal with $\mathrm{Ann}(M) \subseteq \mathfrak{p}$, then $\mathrm{ht}(\mathfrak{p}) \geq 2$. Here

$$\mathrm{Ann}(M) = \{x \in \Lambda_d \mid x \cdot M = \{0\}\}$$

denotes the annihilator ideal of M.

(3) If M is pseudo-null, then (2) implies that M is annihilated by two relatively prime elements of Λ_d.
In fact, if $J := \mathrm{Ann}(M)$, and if $0 \neq g \in J$ is arbitrary, then there exists an element $h \in J$ coprime to g:
Let $0 \neq g \in J$ be arbitrary, and write $g = \prod_{i=1}^{r} p_i^{e_i}$, with irreducible elements p_i in the unique factorisation domain Λ_d (compare Proposition 2.17, (iv)). For every $i = 1,\ldots,r$, there exists an element $h_i \in J$ such that $p_i \nmid h_i$, since otherwise, J would be contained in the prime ideal $(p_i) \subseteq \Lambda_d$ of height one. Without loss of generality, we may assume that $p_j \mid h_i$ for every $j \neq i$. Then g is coprime to $h := h_1 + \ldots + h_r \in J$.

(4) A $\Lambda_1 = \Lambda$-module is pseudo-null if and only if it is finite.

Proof. See the remarks after Definition 5.1.4 in [NSW 08]; for (4) we use that $\Lambda_1 = \Lambda$ is a 2-dimensional, Noetherian, integrally closed local domain with finite residue field $\mathbb{Z}_p[[T]]/(p,T) \cong \mathbb{Z}/p\mathbb{Z}$; compare Proposition 2.17, (i), (iv) and (v). □

Definition 2.21. A homomorphism $f : M \longrightarrow N$ of finitely generated Λ_d-modules is called a ***pseudo-isomorphism*** if the kernel and cokernel of f are pseudo-null Λ_d-modules. Equivalently, this is the case if we have an exact sequence

$$0 \longrightarrow M_1 \longrightarrow M \xrightarrow{f} N \longrightarrow M_2 \longrightarrow 0$$

with pseudo-null Λ_d-modules M_1 and M_2. We write $M \sim N$ if there is such a pseudo-isomorphism.

Remarks 2.22.
(1) In general, $M \sim N$ does not imply $N \sim M$ (compare Remarks 1.20, (1) for an example in the case $d = 1$). But if M and N are finitely generated torsion Λ_d-modules, then $M \sim N$ if and only if $N \sim M$, see the remarks on page 271 of [NSW 08].
(2) In view of Remarks 2.20, (4), the notion of pseudo-isomorphic Λ_1-modules introduced here coincides with the definition given in Chapter 1 (see Definition 1.19).

Theorem 2.23 (**Structure Theorem**). *Let M be a finitely generated Λ_d-module. Then there exist an integer $s \in \mathbb{N}_0$, finitely many prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ of Λ_d of height one, integers $n_i \in \mathbb{N}$, $i = 1, \ldots, s$, and a pseudo-isomorphism*

$$f : M \longrightarrow F_{\Lambda_d}(M) \oplus \bigoplus_{i=1}^{s} \Lambda_d/\mathfrak{p}_i^{n_i} ,$$

where $F_{\Lambda_d}(M)$ denotes the maximal torsion-free quotient of M. The prime ideals $\mathfrak{p}_i$ and the numbers n_i are uniquely determined by M.
For $d = 1$, we can replace the module $F_{\Lambda_d}(M)$ by a free Λ-module, i.e., there exists an integer $r \in \mathbb{N}_0$ such that we have a pseudo-isomorphism

$$f : M \longrightarrow \Lambda^r \oplus \bigoplus_{i=1}^{s} \Lambda_d/\mathfrak{p}_i^{n_i} .$$

Proof. By [NSW 08], Proposition 5.1.7, we have a pseudo-isomorphism

$$f : M \longrightarrow F_{\Lambda_d}(M) \oplus \bigoplus_{i=1}^{s} \Lambda_d/\mathfrak{p}_i^{n_i} .$$

For $d = 1$, compare Theorem 1.24 or see [NSW 08], Propositions 5.1.8 and 5.1.9. □

Definition 2.24. A Λ_d-module of the form $E = \bigoplus_{i=1}^{s} \Lambda_d/\mathfrak{p}_i^{n_i}$ is called an ***elementary*** (torsion) Λ_d-module.

Remarks 2.25.
(1) The prime ideals $\mathfrak{p}_i \subseteq \Lambda_d$ of height one are principal ideals $\mathfrak{p}_i = (g_i)$ generated by irreducible elements $g_i \in \Lambda_d$, respectively. Indeed, let $0 \neq x$ be contained in a prime ideal $\mathfrak{p} \subseteq \Lambda_d$ of height one. We write x as a product of irreducible elements in the unique factorisation domain Λ_d. Since $\mathfrak{p}$ is a prime ideal, at least one irreducible divisor g of x has to be contained in $\mathfrak{p}$. But then $(g) \subseteq \Lambda_d$ is a prime ideal contained in $\mathfrak{p}$, and therefore $(g) = \mathfrak{p}$, because $\mathfrak{p}$ is of height one.
(2) If E denotes an elementary Λ_d-module, then E does not contain any non-trivial pseudo-null submodules.

Proof. Write $E = \bigoplus_{i=1}^{s} \Lambda_d/(g_i^{n_i})$, where the $g_i \in \Lambda_d$ denote suitable irreducible elements. If $0 \neq x = x_1 + \ldots + x_s \in E$, then an element $h \in \Lambda_d$

annihilates x if and only if $\prod_{i=1}^{s} g_i^{k_i}$ divides h, where $k_i \leq n_i$ denotes the smallest integer such that $g_i^{k_i} \cdot x_i = 0$ in $\Lambda_d/(g_i^{n_i})$, respectively. Here we are using the fact that Λ_d is a unique factorisation domain. In particular, the annihilator ideal of x is contained in the principal ideal $(\prod g_i^{k_i})$.
Now suppose that $N \subseteq E$ denotes a non-trivial submodule. Since Λ_d is Noetherian (see Proposition 2.17, (v)), N is finitely generated over Λ_d. The annihilator ideal of each of the generators $b_1, \ldots, b_l$ of N is, by the above, contained in a principal ideal $(\prod g_i^{k_i^{(j)}})$, $1 \leq j \leq l$. If

$$m_i := \max_j k_i^{(j)} \leq n_i \ , \quad 1 \leq i \leq s \ ,$$

then the annihilator ideal of N is contained in the intersection $(\prod g_i^{m_i}) \subseteq \Lambda_d$ of the annihilators of the b_j. Note that $m_i > 0$ for at least one i, since N is non-trivial. The claim now follows from Remarks 2.20, (2). □

(3) Let A denote a finitely generated torsion Λ_d-module with corresponding elementary Λ_d-module E_A, let $\varphi : A \longrightarrow E_A$ denote a pseudo-isomorphism. If M_1, respectively, M_2, denote the pseudo-null kernel and cokernel of φ, then we have an exact sequence

$$0 \longrightarrow M_1 \longrightarrow A \longrightarrow E_A \longrightarrow M_2 \longrightarrow 0 \ .$$

In this situation, M_1 may be seen as the maximal pseudo-null submodule of A. Indeed, if $x \in A$ generates a pseudo-null submodule of A, i.e., the annihilator ideal of x contains two relatively prime elements, then also the annihilator ideal of the submodule of E_A generated by $\varphi(x)$ contains two relatively prime elements. By (2), it follows that $x \in M_1 = \ker(\varphi)$. On the other hand, M_1 is pseudo-null by definition.

2.3 Greenberg's topology

As above, let K be a number field. In his article [Gr 73], R. Greenberg introduced a topology on the set $\mathcal{E}(K)$ of $\mathbb{Z}_p$-extensions of K, in the following way. For $L \in \mathcal{E}(K)$ and $n \in \mathbb{N}_0$, define

$$\mathcal{E}(L,n) := \{L' \in \mathcal{E}(K) \mid [L \cap L' : K] \geq p^n\} \ .$$

This means that $\mathcal{E}(L,n)$ consists of all $\mathbb{Z}_p$-extensions of K which coincide with L up to level n. If we denote by M_k the k-th intermediate field of an element $M \in \mathcal{E}(K)$, respectively, then

$$\mathcal{E}(L,n) = \{L' \in \mathcal{E}(K) \mid (L')_n = L_n\} \ .$$

It is possible to take the sets $\mathcal{E}(L,n)$, $n \in \mathbb{N}_0$, as a base of neighbourhoods of $L \in \mathcal{E}(K)$ (getting smaller while n grows), inducing a topology on $\mathcal{E}(K)$: We have to show that the intersection of two such sets again is of the same shape. So let L^1, L^2 be two $\mathbb{Z}_p$-extensions of K, and let $n_1, n_2 \in \mathbb{N}$. Without loss of generality, we may assume that $n_1 \leq n_2$. Now there are two cases to consider.

If $L^1 \cap L^2 \not\supseteq (L^1)_{n_1}$, i.e., $L^2 \notin \mathcal{E}(L^1, n_1)$, then $\mathcal{E}(L^1, n_1) \cap \mathcal{E}(L^2, n_2) = \emptyset$. But otherwise $\mathcal{E}(L^1, n_1) \cap \mathcal{E}(L^2, n_2) = \mathcal{E}(L^2, n_2)$, since then $(L^1)_{n_1} = (L^2)_{n_1}$.

We also immediately see that with respect to this topology, $\mathcal{E}(K)$ is Hausdorff.

Lemma 2.26. *With regard to Greenberg's topology, $\mathcal{E}(K)$ is compact.*

Proof. Greenberg's proof given in [Gr 73] uses the sets $\mathcal{E}(n)$ containing all cyclic extensions of degree p^n over K which are contained in some $\mathbb{Z}_p$-extension of K. These sets are finite by Theorem 1.7 (we will give a detailed and elementary proof below). For $m \geq n$, there is a map

$$\varphi_{m,n} : \mathcal{E}(m) \longrightarrow \mathcal{E}(n)$$

defined by mapping each element of $\mathcal{E}(m)$ to its unique subfield of degree p^n over K.

We consider the inverse limit $\varprojlim \mathcal{E}(n)$ with respect to the maps $\varphi_{m,n}$. The finite sets $\mathcal{E}(n)$ are equipped with the discrete topology. Then $\mathcal{E}(K) \cong \varprojlim \mathcal{E}(n)$ algebraically and topologically, which follows from the definition of Greenberg's topology. In particular, $\mathcal{E}(K)$ is compact (see [Neu 92], Theorem IV.2.3).

We want to give a more detailed proof which seems to be more descriptive. The main idea is to use the fact that a metric space X is compact if and only if every sequence $(x_n)_{n \in \mathbb{N}}$ in X contains a convergent subsequence (see [Os 92], Theorem 2.4.5). In order to make $\mathcal{E}(K)$ into a metric space, we define, for two arbitrary $\mathbb{Z}_p$-extensions $L^1, L^2 \in \mathcal{E}(K)$,

$$d(L^1, L^2) := \begin{cases} 0 & : \ L^1 = L^2 \\ p^{-n(L^1, L^2)} & : \ \text{otherwise} \end{cases},$$

where $n(L^1, L^2)$ is defined to be the greatest integer $m \in \mathbb{N}$ such that we have $L^1 \in \mathcal{E}(L^2, m)$; $n(L^1, L^2)$ is a finite number whenever $L^1 \neq L^2$. One easily checks that the function

$$d : \mathcal{E}(K) \times \mathcal{E}(K) \longrightarrow \mathbb{R}_{\geq 0}$$

defines a metric on $\mathcal{E}(K)$.

Now suppose that we have a sequence $(L^{(n)})_{n \in \mathbb{N}}$ of $\mathbb{Z}_p$-extensions of K. For the purpose of illustration, let us first assume that $d = 2$, i.e., that there exist exactly two independent $\mathbb{Z}_p$-extensions M^1 and M^2 of K. Consider the field extension $L^{(1)}/K$ and set $L := L^{(1)}$.

By Proposition 1.1, for every $i \geq 0$ there exists a unique subfield $L_i \subseteq L$ which is cyclic of degree p^i over K. We want to prove the following fact: If $i \geq 0$ and L_i are given, then there exist exactly $p + 1$ possible choices for the level L_{i+1} contained in a $\mathbb{Z}_p$-extension $L \subseteq \mathbb{K} = M^1 \cdot M^2$ of K.

Since $\mathrm{Gal}((M^1 \cdot M^2)/K) \cong \mathbb{Z}_p^2$ is torsion-free, it suffices to count cyclic extensions of degree p^{i+1} over K that contain L_i.

Suppose first that $i = 0$. Then $L_{i+1} = L_1$ is contained in the composite $(M^1)_1 \cdot (M^2)_1$. Note that $G_1 := \mathrm{Gal}(((M^1)_1 \cdot (M^2)_1)/K) \cong (\mathbb{Z}/p\mathbb{Z})^2$, and

that we are counting the number of subgroups of order p. If $\sigma \in G_1$ and $a \in \{1, \ldots, p-1\}$, then σ and σ^a generate the same subgroup of G_1. We therefore in fact look for a set of representatives for certain distinct orbits of the action of $(\mathbb{Z}/p\mathbb{Z})^*$ on G_1 given by $(a, \sigma) \mapsto \sigma^a$.

If $\sigma_1, \sigma_2 \in G_1$ denote generators of the rank two abelian group G_1, then a set of representatives for the elements of order p is given by the elements

$$\sigma_1\ ,\ \sigma_1 \cdot \sigma_2\ ,\ \sigma_1 \cdot \sigma_2^2\ ,\ \ldots\ ,\ \sigma_1 \cdot \sigma_2^{(p-1)}\ ,\ \sigma_2\ ,$$

proving that there exist exactly $p+1$ subgroups of G_1 of order p.

Now let $i \geq 0$ be arbitrary, and let

$$G_{i+1} := \mathrm{Gal}(((M^1)_{i+1} \cdot (M^2)_{i+1})/K) \cong (\mathbb{Z}/p^{i+1}\mathbb{Z})^2$$

be generated by elements σ_1 and σ_2. Since $L_{i+1} \subseteq (M^1)_{i+1} \cdot (M^2)_{i+1}$, we are now looking for cyclic subgroups H of G_{i+1} of order p^{i+1}, because these are exactly the subgroups of G_{i+1} such that the quotient G_{i+1}/H is cyclic of order p^{i+1}. Moreover, the image of H under the canonical projection

$$\pi : G_{i+1} \longrightarrow G_{i+1}/(G_{i+1})^{p^i}$$

shall be equal to a given cyclic subgroup $\tilde{H}$ of order p^i. This latter condition encodes the fact that L_{i+1} shall contain the given field $L_i \subseteq (M^1)_i \cdot (M^2)_i$, using the fact that

$$G_{i+1}/(G_{i+1})^{p^i} \cong \mathrm{Gal}(((M^1)_i \cdot (M^2)_i)/K)\ .$$

If $\sigma \in G_{i+1}$ denotes a generator of H, then this means that we want the image $\pi(\sigma)$ to be a generator $\tilde{\sigma}$ of $\tilde{H}$. Any other pre-image of $\tilde{\sigma}$ differs from σ by an element $\tau \in (G_{i+1})^{p^i}$. If $a \in (\mathbb{Z}/p^{i+1}\mathbb{Z})^*$, then $\sigma\tau$ and $\sigma^a\tau^a$ generate the same subgroup of G_{i+1}. Therefore the distinct cyclic subgroups $H \subseteq G_{i+1}$ of order p^{i+1} which are mapped to $\tilde{H}$ are generated by elements $\sigma\tau$, where τ is one of the elements

$$\sigma_1^{p^i}\ ,\ \sigma_1^{p^i} \cdot \sigma_2^{p^i}\ ,\ \sigma_1^{p^i} \cdot \sigma_2^{2p^i}\ ,\ \ldots\ ,\ \sigma_1^{p^i} \cdot \sigma_2^{(p-1)p^i}\ ,\ \sigma_2^{p^i}\ .$$

Again, this yields exactly $p+1$ distinct possibilities.

Now let us return to the general case of arbitrary $d \geq 2$. As above, we can think of $L^{(1)} = L = \bigcup_{i \geq 0} L_i$ as being build up step by step. Analogously to the case $d = 2$ one can show that, for any fixed $i \geq 0$, there are only finitely many possible fields contained in $\mathbb{K}$ that can be taken into consideration for the field L_{i+1} as an extension of L_i of degree p.

Indeed, let us fix a set of pairwise independent $\mathbb{Z}_p$-extensions $M^1, \ldots, M^d$ of K. For every $i \geq 0$, we have

$$L_{i+1} \subseteq (M^1)_{i+1} \cdot \ldots \cdot (M^d)_{i+1}\ ,$$

and therefore we are looking for the number of certain subgroups H of

$$G_{i+1} := \mathrm{Gal}(((M^1)_{i+1} \cdot \ldots \cdot (M^d)_{i+1})/K) \cong (\mathbb{Z}/p^{i+1}\mathbb{Z})^d$$

of rank $d-1$ and order $(p^{i+1})^{d-1}$, since these are the subgroups H yielding quotients G_{i+1}/H which are cyclic of order p^{i+1}.

Moreover, we want the image of H under the projection

$$\pi : G_{i+1} \longrightarrow G_{i+1}/(G_{i+1})^{p^i}$$

to equal a given rank $d-1$ subgroup

$$\tilde{H} \subseteq G_{i+1}/(G_{i+1})^{p^i} \cong \mathrm{Gal}((M^1)_i \cdot \ldots \cdot (M^d)_i)$$

of order $(p^i)^{d-1}$, since L_{i+1} shall contain the field $L_i \subseteq (M^1)_i \cdot \ldots \cdot (M^d)_i$.

If $g_1, \ldots, g_{d-1}$ generate such a subgroup H, and if $\tau_1, \ldots, \tau_{d-1} \in (G_{i+1})^{p^i}$ are arbitrary, then also the subgroup of G_{i+1} generated by $g_1\tau_1, \ldots, g_{d-1}\tau_{d-1}$ is a solution to our problem. Moreover, if $a_1, \ldots, a_{d-1} \in (\mathbb{Z}/p^{i+1}\mathbb{Z})^*$, then we have an equality of (multiplicatively written) subgroups

$$< g_1\tau_1, \ldots, g_{d-1}\tau_{d-1} > \; = \; < g_1^{a_1}\tau_1^{a_1}, \ldots, g_{d-1}^{a_{d-1}}\tau_{d-1}^{a_{d-1}} > \; .$$

Let $\sigma_1, \ldots, \sigma_d$ denote fixed generators of G_{i+1}. Then the above shows that the distinct subgroups H of G_{i+1} we are looking for are parameterised by tuples $(\tau_1, \ldots, \tau_{d-1})$, where each τ_i is contained in the set of elements of the form

$$\sigma_1^{u_1 \cdot p^i} \cdot \ldots \cdot \sigma_d^{u_d \cdot p^i} \; ,$$

where $(u_1, \ldots, u_d) \in (\mathbb{Z}/p\mathbb{Z})^d$ are considered modulo the action of $(\mathbb{Z}/p\mathbb{Z})^*$ defined by $a \cdot (u_1, \ldots, u_d) := (au_1, \ldots, au_d)$.

This shows that there exists a bound $r_d < \infty$ for the number of possible choices for H which is independent of i (e.g., $r_d < p^{d(d-1)}$).

Now we fix generators $\gamma_1, \ldots, \gamma_d$ of $\mathrm{Gal}(\mathbb{K}/K)$. On each level i, this induces a set of generators of G_{i+1} (namely, the restrictions of $\gamma_1, \ldots, \gamma_d$, respectively), and thus an ordering of the set of subgroups $H \subseteq G_{i+1}$ we are looking for. Indeed, on each level we choose the subgroup $H \subseteq G_{i+1}$ which solves our problem and comes first concerning a lexicographical order of the exponents $(a_1, \ldots, a_d)$ of the elements $g = \gamma_1^{a_1} \cdot \ldots \cdot \gamma_d^{a_d}$ generating H. Then we order the subgroups $H \subseteq G_{i+1}$ of interest via the corresponding tuples $(\tau_1, \ldots, \tau_{d-1})$.

Therefore we can describe the process of building up L_i out of $L_0 = K$ in terms of a sequence $\{a_1, \ldots, a_i\}$ of integers satisfying $1 \leq a_j \leq r_d$ for all j. This means that the field $L^{(1)} = L$ is uniquely represented by the sequence $\{a_j\}_{j \in \mathbb{N}}$ of integers. One can easily see that this gives a bijective correspondence between the $\mathbb{Z}_p$-extensions of K and the sequences $\{a_j\}_{j \in \mathbb{N}}$ with $a_j \in \{1, \ldots, r_d\}$ for all j.

Therefore our given sequence $(L^{(n)})_{n \in \mathbb{N}}$ of $\mathbb{Z}_p$-extensions can be represented by a sequence of sequences $\{\{a_j^{(n)}\}_{j \in \mathbb{N}}\}_{n \in \mathbb{N}}$ with $1 \leq a_j^{(n)} \leq r_d$ for every j and n. Consider the sequence $\{a_1^{(n)}\}_{n \in \mathbb{N}}$ of the first terms of these sequences (representing the subfields $L_1^{(n)}$ of degree p over K of the fields in our sequence $(L^{(n)})_{n \in \mathbb{N}}$, repectively). Since r_d is finite, there has to be an integer $k_1 \in \{1, \ldots, r_d\}$ such that $a_1^{(n)} = k_1$ for infinitely many n. By restricting to a subsequence we may assume that $a_1^{(n)} = k_1$ for all n. Now consider the second terms $\{a_2^{(n)}\}_{n \in \mathbb{N}}$. By the

same argument, there has to be a $k_2 \in \{1, \ldots, r_d\}$ such that $a_2^{(n)} = k_2$ infinitely often. Via induction, for any $N \in \mathbb{N}$ we obtain a subsequence $\{(a_j^{(n,N)})_{j\in\mathbb{N}}\}_{n\in\mathbb{N}}$ such that there exist integers $(k_j)_{j\leq N}$, $k_j \in \{1, \ldots, r_d\}$ for every j, such that $a_j^{(n,N)} = k_j$ for all n and $1 \leq j \leq N$. Letting $N \to \infty$, we obtain a sequence $(k_j)_{j\in\mathbb{N}}$ which defines a $\mathbb{Z}_p$-extension $\tilde{L}$ of K, using the above bijective correspondence.

By definition of Greenberg's topology on $\mathcal{E}(K)$, a sequence $(L^{(n)})_{n\in\mathbb{N}}$ of elements in $\mathcal{E}(K)$ converges to some $M \in \mathcal{E}(K)$ if and only if the sequence of numbers $m_n := \max\{i \in \mathbb{N} : L^{(n)} \in \mathcal{E}(M, i)\}$ tends to infinity. But by construction of $\tilde{L}$ we have shown that for any $N \in \mathbb{N}$ we are able to choose a subsequence $(L^{(n,N)})_{n\in\mathbb{N}}$ of $(L^{(n)})_n$ such that for every n, $L^{(n,N)} \in \mathcal{E}(\tilde{L}, N)$. This exactly means that we inductively get a subsequence of $(L^{(n)})_n$ converging to $\tilde{L}$, proving that $\mathcal{E}(K)$ is compact. □

Having defined Greenberg's topology on the set $\mathcal{E}(K)$, some natural questions arise. For example, by Theorem 1.32, every $\mathbb{Z}_p$-extension L of K is attached its Iwasawa invariants λ, μ and $\nu \in \mathbb{Z}$. Now suppose that we are given a $\mathbb{Z}_p$-extension $L' \in \mathcal{E}(K)$ which is 'close' to L in the sense that $L' \in \mathcal{E}(L, n)$ for some large n. Is there then a connection between the Iwasawa invariants of L and L', i.e., are they related and perhaps also close together?

In his article [Gr 73], Greenberg proved some first results in this direction. Roughly speaking, under some assumptions which he had to put on the $\mathbb{Z}_p$-extension L/K whose neighbourhood is studied, Greenberg proved that μ is locally bounded and that λ is locally bounded on the subset of all $\mathbb{Z}_p$-extensions of K having $\mu = 0$:

Theorem 2.27. *Let L be a $\mathbb{Z}_p$-extension of K such that only finitely many prime ideals of L lie above p. Then there exist integers n_0 and $c \in \mathbb{N}$ such that $\mu(L'/K) < c$ for any $L' \in \mathcal{E}(L, n_0)$, i.e., μ is locally bounded.*

Theorem 2.28. *Let L be a $\mathbb{Z}_p$-extension of K such that only finitely many primes of L lie above p. Assume further that $\mu(L/K) = 0$. Then there exist $n_0, c \in \mathbb{N}$ such that $\mu(L'/K) = 0$ and $\lambda(L'/K) < c$ for any $L' \in \mathcal{E}(L, n_0)$, i.e., λ is locally bounded.*

As an application, Greenberg deduced some global boundedness results:

Theorem 2.29. *Let K be a number field which contains only one prime dividing p. Then there exists a constant c such that $\mu(L/K) < c$ for any $\mathbb{Z}_p$-extension of K.*

Theorem 2.30. *Let K be a number field which contains only one prime dividing p. Assume that $\mu(L/K) = 0$ for* every *$L \in \mathcal{E}(K)$. Then there exists a constant c such that $\lambda(L/K) < c$ for any $\mathbb{Z}_p$-extension of K.*

Proof. These four theorems are Theorems 4-7 in [Gr 73]. □

In the next chapter, we will further investigate local properties of Iwasawa's invariants, obtaining finer results.

Chapter 3

Local behaviour of Iwasawa invariants

Let K be a fixed number field. In this chapter, we will study the local behaviour of the Iwasawa invariants attached to $\mathbb{Z}_p$-extensions of K. This means that we will regard these invariants as functions on the topological space $\mathcal{E}(K)$ of all $\mathbb{Z}_p$-extensions of K, and we will ask whether the invariants related to $\mathbb{Z}_p$-extensions of K that are close in the sense of Greenberg's topology (see Section 2.3) are also close together.

We will obtain finer results than the theorems proved by Greenberg in [Gr 73] (compare Theorems 2.27-2.30), using a theory of stabilisation of certain ranks. Starting point of our method is a theorem of T. Fukuda. The first section extracts and formalises the main ingredients of this theorem. This will be used in order to generalise Fukuda's method, making it applicable in a much broader context. In fact, while Fukuda's original theorem mainly uses group-theoretic arguments, we will focus on the action of $\Lambda = \mathbb{Z}_p[[T]]$ on the arithemtic objects of interest.

It turns out that the main obstruction to the application of our method is the need to control the ramification in the corresponding $\mathbb{Z}_p$-extensions. In the second section, we will introduce a modified topology on the set $\mathcal{E}(K)$ which will be adequate for our method.

Section 3.3 presents the main results of this chapter, improving Greenberg's theorems. Theorem 3.57 may be regarded as our most important result concerning Iwasawa invariants of $\mathbb{Z}_p$-extensions.

In Sections 3.4 and 3.5, we use a different approach to obtain results about Iwasawa's invariants. More precisely, we introduce the concept of capitulation and link it to the study of Iwasawa invariants. The capitulation is strongly connected with cohomology groups of units, as will be described in the last section. This will yield a new proof of a part of Theorem 3.57.

3.1 Fukuda's Theorem and Fukuda modules

Our main method is based on a theorem of T. Fukuda (see Theorem 3.1 below). In this section, we will define a general class of objects which share the

necessary properties to make an analogon of Fukuda's Theorem hold for them. We will give examples of classes of natural objects satisfying these properties. In particular, this will enable us to apply an analogon of Fukuda's Theorem in a very general setting.

If L/K denotes a $\mathbb{Z}_p$-extension, then we denote by L_n, $n \in \mathbb{N}_0$, the intermediate field of degree p^n over K, respectively, and we let $A_n^{(L)}$ denote the p-Sylow subgroup of the ideal class group of L_n, respectively.

In his article [Fu 94], Fukuda proves the following theorem, which will be our starting point for the comparison of Iwasawa invariants of elements of $\mathcal{E}(K)$:

Theorem 3.1 (Fukuda)**.** *Let L/K be a $\mathbb{Z}_p$-extension. For any $n \geq 0$, let $A_n := A_n^{(L)}$. Let $e = e(L/K) \geq 0$ be defined as in Proposition 1.3: Any prime of K which ramifies in L/K is totally ramified in L/L_e. Then the following holds:*

(i) If there exists an integer $n \geq e$ such that $|A_{n+1}| = |A_n|$, i.e., A_{n+1} and A_n are p-groups of the same cardinality, then $|A_m| = |A_n|$ for all $m \geq n$. In particular, we then have $\mu(L/K) = 0$ and $\lambda(L/K) = 0$.

(ii) If there exists an integer $n \geq e$ such that $\operatorname{rank}_p(A_n) = \operatorname{rank}_p(A_{n+1})$, then $\operatorname{rank}_p(A_m) = \operatorname{rank}_p(A_n)$ for all $m \geq n$. In particular, $\mu(L/K) = 0$ (compare Proposition 1.45, (i)).

We want to immediately give a quick hint on how to obtain results concerning the local behaviour of Iwasawa invariants by applying Fukuda's Theorem.

Theorem 3.2. *Assume that there exists only one prime of K lying above p.*

(i) The subset of $\mathcal{E}(K)$ consisting of all $\mathbb{Z}_p$-extensions L of K with Iwasawa invariants $\mu(L/K) = \lambda(L/K) = 0$ is open with respect to Greenberg's topology. The invariant ν is locally constant on that subset.

(ii) The subset of $\mathcal{E}(K)$ consisting of all $\mathbb{Z}_p$-extensions L of K for which $\mu(L/K) = 0$ is open.

Proof. (i) Let L/K be a $\mathbb{Z}_p$-extension with $\lambda(L/K) = \mu(L/K) = 0$. Then there exists an integer $n_0 \in \mathbb{N}$ such that

$$|A_m^{(L)}| = |A_{n_0}^{(L)}| = p^{\nu(L/K)} < \infty$$

for every $m \geq n_0$ (see Theorem 1.32). We may assume that $n_0 > e$, where $e = e(L/K)$ is the integer defined in Proposition 1.3. Since, by assumption, there is exactly one prime $\mathfrak{P}$ of K lying above p, and since the maximal abelian unramified extension of K is of finite degree over K, Lemma 1.2 shows that every $\mathbb{Z}_p$-extension M/K is ramified at the prime $\mathfrak{P}$, and unramified outside $\mathfrak{P}$. Now define

$$U := \mathcal{E}(L, n_0 + 1) = \{M \in \mathcal{E}(K) \mid [M \cap L : K] \geq p^{n_0+1}\} .$$

Let $M \in U$. We know that $\mathfrak{P}$ ramifies in L_{e+1}/L_e and therefore in M_{e+1}/M_e, since $n_0 > e$. Now assume that $\mathfrak{P}$ is not totally ramified in the abelian extension M/M_e, and let M_j denote its inertia subfield. Then $M_j \neq M_e$, and in particular $M_{e+1} \subseteq M_j$, since this is the unique subfield

of M of degree p over M_e. But this contradicts the fact that $\mathfrak{P}$ is ramified in M_{e+1}/M_e, proving that $\mathfrak{P}$ is totally ramified in M/M_e. In particular,

$$e(M/K) \;=\; e(L/K) \;<\; n_0\;.$$

Furthermore, for $M \in U$ we have $|A_{n_0+1}^{(M)}| = |A_{n_0+1}^{(L)}| = |A_{n_0}^{(L)}| = |A_{n_0}^{(M)}|$, where $A_m^{(M)}$ denotes the p-Sylow subgroup of the ideal class group of the intermediate field $M_m \subseteq M$, respectively. Using Fukuda's Theorem 3.1, (i), we conclude that $|A_m^{(M)}| = |A_{n_0}^{(M)}|$ for any $m \geq n_0$, i.e.,

$$\mu(M/K) \;=\; \lambda(M/K) \;=\; 0\;.$$

Furthermore, if we consider n large enough to make the formula in Theorem 1.32 be valid for $|A_n^{(L)}|$ and $|A_n^{(M)}|$, respectively, then we see that

$$p^{\nu(M/K)} \;=\; |A_n^{(M)}| \;=\; |A_n^{(L)}| \;=\; p^{\nu(L/K)}\;,$$

which means that ν is locally constant on U.

(ii) Let L/K be a $\mathbb{Z}_p$-extension satisfying $\mu(L/K) = 0$. Then there exists an integer $r \in \mathbb{N}$ such that $\mathrm{rank}_p(A_n^{(L)}) \leq r < \infty$ for every $n \geq 0$ (see Proposition 1.45, (i)).
Using class field theory, one can show that the norm maps

$$N_{m,n} : A_m^{(L)} \longrightarrow A_n^{(L)}$$

induced by the algebraic norms between the fields L_m and L_n are surjective for $m \geq n \geq e = e(L/K)$ (see the Lemma in Chapter 3, §4, of [La 90]; compare also the proof of Corollary 3.9). Actually, class field theory shows that the norm maps $N_{m,n} : \mathrm{Cl}(L_m) \longrightarrow \mathrm{Cl}(L_n)$ between the full class groups of L_m and L_n are surjective, but this immediately carries over to the restrictions on the p-Sylow subgroups. In particular we have

$$\mathrm{rank}_p(A_m^{(L)}) \;\geq\; \mathrm{rank}_p(A_n^{(L)})$$

whenever $m \geq n \geq e$. Therefore the p-ranks have to stabilise, i.e., there exists an integer $n_0 \in \mathbb{N}$ such that $\mathrm{rank}_p(A_{n_0+1}^{(L)}) = \mathrm{rank}_p(A_{n_0}^{(L)})$.
We may assume that $n_0 > e$. Now we define $U := \mathcal{E}(L, n_0 + 1)$, and the assertion follows analogously to the proof of (i), using Fukuda's Theorem 3.1, (ii).

□

There are some natural questions arising from this theorem. For example, are the invariants λ or ν locally constant on the subset of $\mathcal{E}(K)$ defined in (ii)? Can we get rid of the assumption that only one prime of K divides p?

We will study two different approaches to strengthen Theorem 3.2: The restriction to fields K with exactly one prime lying above p arose from the fact that the statements of Fukuda's Theorem 3.1 require the indices n to be greater than the number $e = e(L/K)$ attached to the $\mathbb{Z}_p$-extension L/K under consideration. This means that we could not simply apply Theorem 3.1 to the

$\mathbb{Z}_p$-extensions contained in a fixed neighbourhood U of L without having control on the respective e's. If, for example, the $e(M/K)$, $M \in U$, were unbounded, then Theorem 3.1 would not apply to those $M \in U$ having 'too large' e (e.g., $U = \mathcal{E}(L, n)$ and $e(M/K) > n$). We are therefore looking for conditions that help us to locally bound the $e(M/K)$. As we have seen in the proof of Theorem 3.2, the assumption that only one prime of K lies above p is sufficient to ensure that e even is locally constant. We will deal with the problem of finding appropriate conditions in the case of arbitrary K in the next section. As one can imagine in view of the definition of e, this subject is closely related to the study of ramification inside Greenberg neighbourhoods.

In the current section, we want to further investigate Fukuda's Theorem. We will try to determine the key properties of the groups A_n that make the theorem work in order to get able to apply it in more general settings – with the hope of getting further results concerning the local behaviour of μ, λ and ν-invariants.

In Chapter 1, we have studied $A = \varprojlim A_n$, where the projective limit is taken with respect to the norm maps induced by the algebraic norms

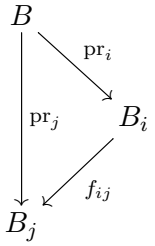
$$N_{m,n} : L_m \longrightarrow L_n,\ m \geq n\ .$$

We have seen that A can in a natural way be equipped with the structure of a Λ-module, where $\Lambda = \mathbb{Z}_p[[T]]$. We now want to define a class of Λ-modules for which the analogue of Fukuda's Theorem holds.

For this purpose, we review the basic notions concerning projective limits that will occur in our investigations (compare [Neu 92], §IV.2). Suppose that we are given a family of Λ-modules $(B_n)_{n\in\mathbb{N}_0}$ together with Λ-module homomorphisms $f_{ij} : B_i \longrightarrow B_j$, $i \geq j$, satisfying $f_{ii} = \mathrm{id}_{B_i}$ for all i and $f_{ik} = f_{jk} \circ f_{ij}$ whenever $i \geq j \geq k$ (a so-called *projective system*). Then we let

$$B\ :=\ \{(b_i)_{i\in\mathbb{N}_0} : f_{ij}(b_i) = b_j\ \forall\, i \geq j\}\ \subseteq\ \prod_{i\in\mathbb{N}_0} B_i\ .$$

$B = \varprojlim_n B_n$ is a projective limit of the B_n. By definition, the f_{ij} commutate with the canonical projections $\mathrm{pr}_n : B \longrightarrow B_n$, i.e., $f_{ij} \circ \mathrm{pr}_i = \mathrm{pr}_j$ for all $i \geq j$, and so all the diagrams



are commutative.

Definition 3.3. Let $B = \varprojlim B_n$ be a projective limit of Λ-modules. We assume that each B_n is a finite abelian p-group, $n \in \mathbb{N}_0$.
Suppose that B further has the following properties. Assume that there exists an integer $e \geq 0$ such that:

(1) For every $n \geq e$, the n-th projection pr_n is surjective. In particular, for any $i \geq j \geq e$, the maps $f_{ij} : B_i \longrightarrow B_j$ are surjective.
(2) For $n \in \mathbb{N}_0$ we define $Y_n := \mathrm{Ker}\{\mathrm{pr}_n : B \longrightarrow B_n\}$. Then for every $n \geq e$, there exists an element $\nu_{(n+1,n)}$ contained in the maximal ideal $\mathfrak{m} = (p, T)$ of $\Lambda = \mathbb{Z}_p[[T]]$ such that

$$Y_{n+1} = \nu_{(n+1,n)} \cdot Y_n$$

(note that Y_n is a Λ-submodule of B as being the kernel of the Λ-module homomorphism pr_n). In particular, we have

$$\boxed{Y_m = \nu_{(m,n)} \cdot Y_n} \tag{F}$$

for any $m > n \geq e$, with $\nu_{(m,n)} := \nu_{(m,m-1)} \cdot \nu_{(m-1,m-2)} \cdot \ldots \cdot \nu_{(n+1,n)} \in \mathfrak{m}^{m-n}$.

If all these properties are satisfied, then we say that B is a ***Fukuda module***, and we call e the ***index barrier*** of B.

Remark 3.4. In Chapter 5, we will study Iwasawa invariants of multiple $\mathbb{Z}_p$-extensions. The ideal class groups of the corresponding intermediate fields admit actions of power series rings $\Lambda_d = \mathbb{Z}_p[[T_1, \ldots, T_d]]$ in several variables. In particular, we will need a notion of Fukuda-Λ_d-modules. Actually, we will develop a theory of Fukuda modules over a broad class of local rings, compare Definition 5.24.

Proposition 3.5. *Every Fukuda module is finitely generated as a Λ-module.*

Proof. Since B_n is finite for any $n \geq 0$, and therefore compact with regard to the discrete topology, $B = \varprojlim B_n$ is compact (see [Neu 92], Theorem IV.2.3). Therefore, by Nakayama's Lemma (Corollary 1.43), B is finitely generated as a Λ-module if and only if $B/(\mathfrak{m} \cdot B)$ is finite, where $\mathfrak{m} = (p, T)$ denotes the maximal ideal of Λ.

Let e denote the index barrier of B. Since $B/Y_e \cong B_e$ is finite, it suffices to show that Y_e is finitely generated, i.e., that $Y_e/(\mathfrak{m} \cdot Y_e)$ is finite (note that Y_e again is compact because it is the kernel of the continuous homomorphism pr_e). Using the Property (F), we see that

$$|Y_e/(\mathfrak{m} \cdot Y_e)| \leq |Y_e/(\underbrace{\nu_{(e+1,e)}}_{\in \mathfrak{m}} \cdot Y_e)| \overset{(F)}{=} |Y_e/Y_{e+1}| \leq |B/Y_{e+1}| = |B_{e+1}|$$

is finite, as claimed. □

We will now see that an analogon of Fukuda's Theorem 3.1 holds for arbitrary Fukuda modules.

Theorem 3.6. *Let $B = \varprojlim B_n$ be a Fukuda module with index barrier e.*
(i) If there exists an integer $n \geq e$ such that $|B_{n+1}| = |B_n|$, then $|B_m| = |B_n|$ for every $m \geq n$ and in fact $|B| = |B_n| < \infty$.
(ii) If there exists an integer $n \geq e$ such that $\mathrm{rank}_p(B_{n+1}) = \mathrm{rank}_p(B_n)$, then $\mathrm{rank}_p(B_m) = \mathrm{rank}_p(B_n) = \mathrm{rank}_p(B)$ for every $m \geq n$.

Proof. We can repeat literally FUKUDA's proof of Theorem 3.1 (see [Fu 94]).

(i) Since $n \geq e$, the map $f_{n+1,n} : B_{n+1} \longrightarrow B_n$ is surjective. The assumption $|B_n| = |B_{n+1}|$ then implies that $f_{n+1,n}$ is in fact a bijection. Therefore, by looking at the diagram

$$\begin{array}{ccc} B_{n+1} & \xrightarrow{\sim} & B/Y_{n+1} \\ {\scriptstyle f_{n+1,n}}\downarrow & & \\ B_n & \xrightarrow{\sim} & B/Y_n \end{array}$$

and using the fact that $B/Y_{n+1} = B/\nu_{(n+1,n)} \cdot Y_n$ for some $\nu_{(n+1,n)} \in (p,T)$ by the Fukuda property (F), we see that there is a bijection

$$B/\nu_{(n+1,n)} \cdot Y_n \xrightarrow{\sim} B/Y_n \ .$$

Now $\nu_{(n+1,n)} \cdot Y_n \subseteq Y_n$, since Y_n is a Λ-module. Since both quotients are finite, we can conclude that $\nu_{(n+1,n)} \cdot Y_n = Y_n$.
We want to apply Nakayama's Lemma (Corollary 1.43). $B = \varprojlim B_n$ is compact as being the inverse limit of finite groups (see [Neu 92], Theorem IV.2.3). This shows that the kernel Y_n of the continuous map

$$\mathrm{pr}_n : B \longrightarrow B_n$$

also is a compact Λ-module. Therefore Nakayama's Lemma implies that $Y_n/(\mathfrak{m} \cdot Y_n) = \{0\}$ if and only if $Y_n = \{0\}$. Since $\nu_{(n+1,n)} \in \mathfrak{m}$, the equality $\nu_{(n+1,n)} \cdot Y_n = Y_n$ shows that $|Y_n/(\mathfrak{m} \cdot Y_n)| \leq |Y_n/(\nu_{(n+1,n)} \cdot Y_n)| = 1$, and thus $Y_n = \{0\}$.
Therefore $Y_m = \nu_{(m,n)} \cdot Y_n = \{0\}$ for every $m \geq n$, where we let

$$\nu_{(m,n)} := \nu_{(m,m-1)} \cdot \nu_{(m-1,m-2)} \cdot \ldots \cdot \nu_{(n+1,n)} \in (p,T) \subseteq \Lambda \ ,$$

$m > n$, and $\nu_{(m,m)} := 1$. This means that

$$|B_m| \ = \ |B/Y_m| \ = \ |B| \ = \ |B/Y_n| \ = \ |B_n|$$

for every $m \geq n$.

(ii) If $\mathrm{rank}_p(B_{n+1}) = \mathrm{rank}_p(B_n)$, then $B_n/p \cdot B_n$ and $B_{n+1}/p \cdot B_{n+1}$ are $\mathbb{F}_p$-vector spaces of the same dimension and therefore are isomorphic (as vector spaces). Therefore, the Λ-module isomorphisms

$$B_{n+1} \ \cong \ B/Y_{n+1} \ \overset{(\mathrm{F})}{=} \ B/(\nu_{(n+1,n)} \cdot Y_n)$$

and $B_n \cong B/Y_n$ imply that

$$B/(Y_n + pB) \ \cong \ B/(\nu_{(n+1,n)} \cdot Y_n + pB) \ ,$$

as $\mathbb{F}_p$-vector spaces. Since $\nu_{(n+1,n)} \cdot Y_n + pB \subseteq Y_n + pB$, and as both quotients are finite, it follows that $\nu_{(n+1,n)} \cdot Y_n + pB = Y_n + pB$.

Now define $Z := (Y_n + pB)/pB$. Since $\nu_{(n+1,n)} \cdot pB = p \cdot \nu_{(n+1,n)} B \subseteq pB$, we can conclude that

$$\nu_{(n+1,n)} \cdot Z \;=\; (\nu_{(n+1,n)} \cdot Y_n + pB)/pB \;=\; Z \;,$$

by the above. Z is a compact Λ-module, and so Nakayama's Lemma shows that $Z = \{0\}$, i.e., $Y_n \subseteq p \cdot B$. Letting $\nu_{(m,n)}$ be defined as in (i) and using Property (F), we obtain

$$Y_m \;=\; \nu_{(m,n)} \cdot Y_n \;\subseteq\; \nu_{m,n} \cdot pB \;\subseteq\; pB \qquad (\star)$$

for every $m \geq n$, and therefore, for these m,

$$\begin{aligned} \mathrm{rank}_p(B_m) \;=\; \mathrm{rank}_p(B/Y_m) \;&=\; \dim_{\mathbb{F}_p}(B/(Y_m + pB)) \\ &\overset{(\star)}{=}\; \dim_{\mathbb{F}_p}(B/pB) \;=\; \mathrm{rank}_p(B) \;. \end{aligned}$$

□

Consider a $\mathbb{Z}_p$-extension K_∞/K with intermediate fields K_n, $n \geq 0$, and p-Sylow class groups A_n, respectively. Fukuda's Theorem 3.1 shows that Theorem 3.6 holds for the projective limit $A = \varprojlim A_n$. We will now prove that indeed A is a Fukuda module. In particular, this implies that Theorem 3.1 is a special case of Theorem 3.6.

Recall the notion of the *Greenberg module* $X = \mathrm{Gal}(L/K_\infty)$ attached to K_∞/K, where L denotes the maximal p-abelian unramified extension of K_∞ (compare Proposition 1.33 and Lemma 1.39).

Proposition 3.7. *The Greenberg module X attached to K_∞/K is a Fukuda module with index barrier $e = e(K_\infty/K)$ (the integer defined in Proposition 1.3).*

Proof. If L_n denotes the maximal unramified p-abelian extension of K_n, $n \in \mathbb{N}_0$, then

$$X \;=\; \varprojlim \underbrace{\mathrm{Gal}((L_n \cdot K_\infty)/K_\infty)}_{=:\,\tilde{X}_n} \;,$$

where the projective limit is taken with respect to the restriction maps.

Since at least one prime is totally ramified in the extension K_∞/K_e, we see that the restrictions $\tilde{X}_m \longrightarrow \tilde{X}_n$ are surjective for each $m \geq n \geq e$, because

$$\mathrm{Gal}((L_n \cdot K_\infty)/K_\infty) \;\cong\; \mathrm{Gal}(L_n/K_n)$$

and $K_m \cap L_n = K_n$ for each $m \geq n \geq e$. By the same reasons, the projections $\mathrm{pr}_n : X \longrightarrow \tilde{X}_n$ are surjective for $n \geq e$.

It therefore remains to show that $X = \varprojlim \tilde{X}_n$ satisfies Property (F). Letting $Y_n := \mathrm{Ker}\{\mathrm{pr}_n : X \longrightarrow \tilde{X}_n\}$, $n \in \mathbb{N}_0$, this means that we have to show that $Y_{n+1} = \nu_{(n+1,n)} \cdot Y_n$ for each $n \geq e$ and suitable elements $\nu_{(n+1,n)} \in \mathfrak{m} = (p, T)$, respectively.

We will in fact see that this property holds with respect to the polynomials $\nu_{(n+1,n)}(T) \in \mathbb{Z}_p[T]$ defined in Section 1.2:

$$\nu_{(n+1,n)} = \frac{(1+T)^{p^{n+1}} - 1}{(1+T)^{p^n} - 1} = (1+T)^{p^{n+1}-p^n} + \ldots + (1+T)^{p^n} + 1 \; .$$

Note that Proposition 1.27, (iii) implies that the $\nu_{(n+1,n)}(T)$ are distinguished polynomials for every $n \geq 0$, and therefore $\nu_{(n+1,n)}(T) \in (p, T)$.

Now we recall that we have seen in Lemma 1.37 an equivalent characterisation of the Y_n. Namely, Y_e is generated by $T \cdot X$ and the $\mathbb{Z}_p$-span of certain elements $a_2, \ldots, a_s$ describing the ramification in K_∞/K_e. Moreover, $Y_n = \nu_{(n,e)} \cdot Y_e$ for every $n \geq e$.

Note that Lemma 1.37 was proved only in the case $e = 0$. However, we may treat the case of arbitrary $e(K_\infty/K)$ by replacing K by K_e (this does not affect $\varprojlim \tilde{X}_n = X = \mathrm{Gal}(L/K_\infty)$), compare Remark 1.38 and Lemma 1.39.

We may obtain the desired statement via induction: First of all, we have $Y_{e+1} = \nu_{(e+1,e)} \cdot Y_e$. Suppose now that $Y_{n+1} = \nu_{(n+1,n)} \cdot Y_n$ holds for every $n \leq k$, for some fixed $k \geq e$. Then

$$\begin{aligned} Y_{k+2} &= \nu_{(k+2,e)} \cdot Y_e \\ &= \nu_{(k+2,k+1)} \cdot \nu_{(k+1,e)} \cdot Y_e \\ &= \nu_{(k+2,k+1)} \cdot Y_{k+1} \; , \end{aligned}$$

using the induction hypothesis and the fact that $\nu_{(k+2,e)} = \nu_{(k+2,k+1)} \cdot \nu_{(k+1,e)}$. □

Lemma 3.8 (Isomorphisms of Fukuda modules)**.** *Let $A = \varprojlim A_n$ be a Fukuda module with index barrier $e = e(A)$, let $\varphi : A \longrightarrow B$ be a Λ-module isomorphism, $B = \varprojlim B_n$. Assume that φ is induced by Λ-module isomorphisms $\varphi_n : A_n \xrightarrow{\sim} B_n$ such that the diagrams*

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ {\scriptstyle \mathrm{pr}_n}\downarrow & & \downarrow{\scriptstyle \mathrm{pr}_n} \\ A_n & \xrightarrow{\varphi_n} & B_n \end{array} \qquad (\star)$$

are commutative for all $n \geq e$.
Then $B = \varphi(A)$ is a Fukuda module with index barrier e.

Proof. First of all, B is an inverse limit $B = \varprojlim B_n$, taken with respect to the maps

$$f_{ij}^B : B_i \longrightarrow B_j \; , \quad x_i \longmapsto \varphi_j(f_{ij}(\varphi_i^{-1}(x_i))) \; , \; i \geq j \; ,$$

where $f_{ij} : A_i \longrightarrow A_j$ denote the maps corresponding to the projective system of $A = \varprojlim A_n$. The f_{ij}^B are well-defined because φ_i and φ_j are isomorphisms, and they are surjective Λ-module homomorphisms for $j \geq e$ as being the composition of surjective homomorphisms.

If $a = (a_n)_n \in A = \varprojlim A_n$, then $b := (\varphi_n(a_n))_n \in \varprojlim B_n$, because

$$f_{ij}^B(b_i) \;=\; f_{ij}^B(\varphi_i(a_i)) \;=\; \varphi_j(f_{ij}(a_i)) \;=\; \varphi_j(a_j) \;=\; b_j \;.$$

Because of the assumptions $(\star)$, the projections $\mathrm{pr}_n : B \longrightarrow B_n$ are surjective whenever $n \geq e$.

It therefore remains to show that B has the Fukuda Property (F). Let Y_n^A, respectively, Y_n^B, denote the kernels of the projections $\mathrm{pr}_n : A \longrightarrow A_n$ and $\mathrm{pr}_n : B \longrightarrow B_n$, respectively. Then we know that for every $n \geq e$, there exists an element $\nu_{(n+1,n)} \in (p, T) \subseteq \Lambda$ such that $Y_{n+1}^A = \nu_{(n+1,n)} \cdot Y_n^A$.

We will show that

$$Y_n^B \;=\; \varphi(Y_n^A)$$

for every $n \geq e$. Let $a \in Y_n^A$, $b := \varphi(a)$. Then $0 = \mathrm{pr}_n(a)$ and therefore

$$0 \;=\; \varphi_n(\mathrm{pr}_n(a)) \;\overset{(\star)}{=}\; \mathrm{pr}_n(\varphi(a)) \;=\; \mathrm{pr}_n(b) \;.$$

If, on the other hand, $b \in Y_n^B$, then we choose a pre-image $a \in A$ of b under the isomorphism φ. Then

$$0 \;=\; \mathrm{pr}_n(b) \;=\; \mathrm{pr}_n(\varphi(a)) \;\overset{(\star)}{=}\; \varphi_n(\mathrm{pr}_n(a)) \,,$$

and thus $0 = \mathrm{pr}_n(a)$, since φ_n is an isomorphism, by assumption. This shows that $a \in Y_n^A$ and $b \in \varphi(Y_n^A)$.

It is now obvious that

$$\begin{aligned} Y_{n+1}^B \;&=\; \varphi(Y_{n+1}^A) \;=\; \varphi(\nu_{(n+1,n)} \cdot Y_n^A) \\ &=\; \nu_{(n+1,n)} \cdot \varphi(Y_n^A) \;=\; \nu_{(n+1,n)} \cdot Y_n^B \end{aligned}$$

for every $n \geq e$.

□

Corollary 3.9. *Let K_∞/K be a $\mathbb{Z}_p$-extension. Then $A = \varprojlim A_n$ is a Fukuda module with index barrier $e = e(K_\infty/K)$.*

Proof. Proposition 3.7 implies that $X = \varprojlim \underbrace{\mathrm{Gal}((L_n \cdot K_\infty)/K_\infty)}_{=:\,\tilde{X}_n}$ is a Fukuda module with index barrier e. We now proceed in two steps:

First, we use Lemma 3.8 in order to transfer the Fukuda property from X to

$$\varprojlim \underbrace{\mathrm{Gal}(L_n/K_n)}_{=:\,X_n} \;.$$

Then we apply Lemma 3.8 again in order to prove the statement.

The isomorphisms $\psi_n : \tilde{X}_n \xrightarrow{\sim} X_n$, $n \geq e$, satisfy the $(\star)$-condition from Lemma 3.8, since both the ψ_n and the pr_n are in fact induced by restriction maps. Therefore Lemma 3.8 implies that $\varprojlim_{n \geq 0} X_n$ is a Fukuda module with index barrier e.

Now we come to the second step. For any finite level K_n/K, we have the Artin isomorphism $\varphi_n : A_n \longrightarrow X_n$ from class field theory (see, for example, [Neu 92], Theorem VI.6.9). On the level of ideals, φ_n satisfies the following property. If I is an ideal of the ring of integers $\mathcal{O}(K_n)$ of K_n, then for any $\sigma \in \mathrm{Gal}(K_n/K)$ we have $\varphi_n(\sigma(I)) = \sigma \cdot \varphi_n(I) \cdot \sigma^{-1}$ (see [Rib 01], 25.(B)). But this exactly means that $\varphi_n : A_n \longrightarrow X_n$ is a Λ-module homomorphism, since the action of $\mathbb{Z}_p[[\mathrm{Gal}(K_\infty/K)]] \cong \Lambda$ on X_n is given by conjugation, see Section 1.3.

Class field theory furthermore implies that for any $i \geq j \geq 0$, we have a commutative diagram

$$\begin{array}{ccc} A_i & \xrightarrow{\varphi_i} & X_i \\ {\scriptstyle f_{ij}}\downarrow & & \downarrow{\scriptstyle g_{ij}} \\ A_j & \xrightarrow{\varphi_j} & X_j \end{array}$$

where the f_{ij} are induced by the algebraic norms $N_{K_i|K_j}$, and the g_{ij} are given by restriction (see [Neu 92], Theorem IV.6.4). This shows that the $\varphi_n : A_n \longrightarrow X_n$ induce a Λ-module isomorphism $\varphi : A \longrightarrow X$ such that the diagrams $(\star)$ in Lemma 3.8 are commutative for all n. Therefore the assertion follows from Lemma 3.8, using the inverse isomorphism $\varphi^{-1} : X \longrightarrow A$.

□

The following lemma is a very useful tool for the construction of new Fukuda modules.

Lemma 3.10 (Quotients of Fukuda modules)**.** *Let $A = \varprojlim A_n$ be a Fukuda module with index barrier $e = e(A)$, let $M = \varprojlim M_n \subseteq A$ be a submodule, i.e., we have Λ-submodules $M_n \subseteq A_n$, $n \geq 0$, and the inverse limit is taken with respect to the mappings $f_{ij} : A_i \longrightarrow A_j$, $i \geq j$, restricted to M_i.*
In particular, we assume that the projections $\mathrm{pr}_n : M \longrightarrow M_n$ are surjective for every $n \geq e$ (and so $f_{ij}(M_i) = M_j$, $j \geq e$).

Then the Λ-module $A/M := \varprojlim A_n/M_n$ (i.e., we take quotients componentwise) is a Fukuda module with index barrier e.

Proof. The factor groups A_n/M_n are finite abelian p-groups and Λ-modules. The maps $f_{ij} : A_i \longrightarrow A_j$ induce mappings

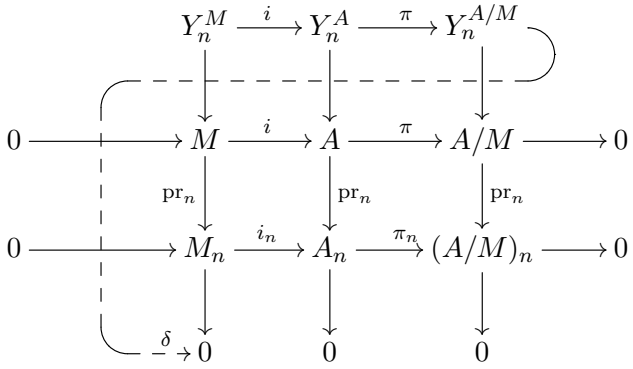
$$\overline{f}_{ij} : A_i/M_i \longrightarrow A_j/M_j\ , \quad \overline{x}_i = x_i + M_i \mapsto f_{ij}(x_i) + M_j\ , \quad i \geq j\ .$$

These are well-defined because $f_{ij}(M_i) \subseteq M_j$, and they are easily seen to be surjective for $j \geq e$. Indeed, let $\overline{x}_j \in (A/M)_j = A_j/M_j$ be arbitrary. Choose a representative $x_j \in A_j$. By the surjectivity of f_{ij}, there is an element $x_i \in A_i$ with $f_{ij}(x_i) = x_j$. But then $\overline{f}_{ij}(\overline{x}_i) = \overline{x}_j$.

Moreover, $((A_n/M_n)_n, \overline{f}_{ij})$ is a projective system, and we can consider a corresponding inverse limit $A/M = \varprojlim A_n/M_n \subseteq \prod_n A_n/M_n$.

We want to show now that the so-defined Λ-module satisfies Property (F). Along the way, we will obtain the surjectivity of the projections of A/M. For every $n \geq 0$, let us denote by Y_n^A, respectively, $Y_n^{A/M}$, the kernel of the n-th

projection $\mathrm{pr}_n : A \longrightarrow A_n$, respectively, $\mathrm{pr}_n : A/M \longrightarrow (A/M)_n = A_n/M_n$. By assumption, we know that for every $n \geq e$, $Y_{n+1}^A = \nu_{(n+1,n)} \cdot Y_n^A$ for some element $\nu_{(n+1,n)} \in (p, T) \subseteq \Lambda$. We will show that $Y_{n+1}^{A/M} = \nu_{(n+1,n)} \cdot Y_n^{A/M}$. In order to do so, we fix $n \geq e$, and we consider the following diagram:



First of all, the two rows in the middle obviously are exact. Furthermore, the corresponding two rectangles are commutative. In particular, the projections $\mathrm{pr}_n : A/M \longrightarrow (A/M)_n$ have to be surjective for $n \geq e$. But then also the two upper rectangles do commutate: It is obvious that $i(Y_n^M) \subseteq Y_n^A$. Moreover, if $x \in Y_n^A \subseteq A$, then by the above

$$\mathrm{pr}_n(\pi(x)) \;=\; \pi_n(\mathrm{pr}_n(x)) \;=\; \pi_n(0) \;=\; 0\,,$$

and therefore $\pi(Y_n^A) \subseteq Y_n^{A/M}$.

We are now in the position to apply the *Snake Lemma* (see, for example, [Os 92], Lemma 5.28) which tells us that there is a Λ-module homomorphism, as suggested in the above picture,

$$\delta : Y_n^{A/M} \longrightarrow \mathrm{Coker}(\mathrm{pr}_n : M \longrightarrow M_n) \;=\; \{0\}\,,$$

such that $Y_n^A \xrightarrow{\pi} Y_n^{A/M} \xrightarrow{\delta} 0$ is exact. This means that, for any $n \geq e$, we have

$$\pi(Y_n^A) = Y_n^{A/M}\,. \qquad (\star)$$

But then

$$Y_{n+1}^{A/M} \overset{(\star)}{=} \pi(Y_{n+1}^A) \overset{(\mathrm{F})}{=} \pi(\nu_{(n+1,n)} \cdot Y_n^A) \;=\; \nu_{(n+1,n)} \cdot \pi(Y_n^A) \overset{(\star)}{=} \nu_{(n+1,n)} \cdot Y_n^{A/M}$$

for any $n \geq e$. □

Example 3.11.

(1) Let K_∞/K be a $\mathbb{Z}_p$-extension with Galois group $\Gamma \cong \mathbb{Z}_p$; let γ be a topological generator of Γ. Assume that every prime of K dividing p ramifies in K_∞/K (this condition is satisfied, for example, by the cyclotomic $\mathbb{Z}_p$-extension of K, as we will prove in Lemma 3.18, (ii)). For every $n \geq 0$, let A_n be the p-Sylow subgroup of the ideal class group of K_n, and let $D_n \subseteq A_n$ denote the subgroup generated by the classes that contain an

ideal all of whose prime factors lie above p. Using Lemma 1.2, we see that D_n in particular contains all classes of ramified ideals. Each D_n actually is a Λ-submodule of A_n, respectively. Indeed, if I is an ideal of K_n all of whose prime factors lie above p, then this is certainly also true for $\gamma(I)$, i.e., $\gamma(D_n) \subseteq D_n$ and therefore $\Lambda \cdot D_n \subseteq D_n$.
Take the projective limit $A = \varprojlim A_n$ with respect to the norm maps

$$f_{ij} : A_i \longrightarrow A_j\,, \quad i \geq j\,.$$

Then $f_{ij}(D_i) = D_j$ whenever $i \geq j \geq e = e(K_\infty/K)$:
On the one hand, it is clear that $f_{ij}(D_i) \subseteq D_j$, since the norms map ideals above p to ideals above p. On the other hand, let $x \in D_j$, and let J be an ideal of the class x such that $J = \prod_{k=1}^{r} \mathfrak{P}_k^{e_k}$ with $e_k \in \mathbb{Z}$ and $\mathfrak{P}_k \mid (p)$ for every k. Since every prime dividing p ramifies in K_i/K_j, $i \geq j \geq e$, we have $f_{ij}(\mathfrak{Q}_k) = \mathfrak{P}_k$ for every $k = 1, \ldots, r$, where $\mathfrak{Q}_k$ denotes the unique prime of K_i dividing $\mathfrak{P}_k$, respectively (i.e., $\mathfrak{P}_k \cdot \mathcal{O}_{K_i} = \mathfrak{Q}_k^{p^{i-j}}$). Letting $I := \prod_{k=1}^{r} \mathfrak{Q}_k^{e_k}$, we may conclude that the class y of I belongs to D_i, and $f_{ij}(y) = x$.
Now we consider the projective limit $D = \varprojlim D_n$ with respect to the f_{ij}. Let $A'_n := A_n/D_n$, $n \geq 0$. Using Corollary 3.9 and Lemma 3.10, we conclude that $A' := \varprojlim A'_n = A/D$ is a Fukuda module. In particular, Theorem 3.6 holds for A', a fact which has been proved for the cyclotomic $\mathbb{Z}_p$-extension K_∞ of K by Mizusawa in [Miz 10], Proposition 3.
Note that for every $n \geq 0$, $A'_n \cong \mathrm{Gal}(H'(K_n)/K_n)$, where $H'(K_n)$ denotes the maximal p-abelian unramified extension of K_n in which every prime ideal of K_n lying above p splits completely. This is the subfield of $H(K_n)$ fixed by the image $\varphi(D_n) \subseteq \mathrm{Gal}(H(K_n)/K_n)$, where φ denotes the Artin isomorphism; it is a general fact that unramified primes $\mathfrak{P}$ split completely in $H(K_n)$ if and only if $\varphi(\mathfrak{P})$ is trivial, see [Rib 01], 25.(A).

(2) More generally, let $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ denote a finite set of primes of K. Let $S' \supseteq S$ denote the union of S with the set of primes of K dividing p. Suppose that K_∞/K denotes a $\mathbb{Z}_p$-extension such that every prime $\mathfrak{p} \in S'$ is only finitely decomposed in K_∞/K, i.e., for each $\mathfrak{p} \in S'$, there exist only finitely many primes of K_∞ lying above $\mathfrak{p}$. Note that this is equivalent to the decomposition group $Z_\mathfrak{p}(K_\infty/K)$ of $\mathfrak{p}$ in K_∞/K being non-trivial, because every non-trivial closed subgroup of $\mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$ will be of finite index. Therefore $Z_\mathfrak{p}(K_\infty/K) = \mathrm{Gal}(K_\infty/K_{n_\mathfrak{p}})$ for some $n_\mathfrak{p} \in \mathbb{N}$, respectively. Let $n_0 := \max_{\mathfrak{p} \in S'} n_\mathfrak{p}$.
For example, it is known that no prime of K splits completely in the cyclotomic $\mathbb{Z}_p$-extension of K (see [Wa 97], Exercise 13.2, (a)).
For every $n \geq n_0$, we let $D_n^S \subseteq A_n$ denote the subgroup generated by the prime ideals of K_n lying above some $\mathfrak{p}_i \in S$, respectively. Then $A_n^S := A_n/D_n^S$ is called the (p-primary subgroup of the) *S-class group* of K_n, respectively. We let $A^S := \varprojlim A_n^S$, where the projective limit is taken with respect to the norm maps $f_{ij} : A_i \longrightarrow A_j$, which satisfy $f_{ij}(D_i^S) \subseteq D_j^S$ for every $i \geq j$.

In [Fe 86], L. FEDERER proved that A^S is a Fukuda module (compare Theorems 3.2, 3.5 and 4.7 in [Fe 86]). We therefore can apply Theorem 3.6 in order to deduce information about the Iwasawa invariants that are attached to this finitely generated Λ-torsion module via Proposition 1.28. (In fact, Federer only considered the case of the cylotomic $\mathbb{Z}_p$-extension of K. Her proofs, however, are valid for any $\mathbb{Z}_p$-extension of K in which every prime $\mathfrak{p} \in S'$ is finitely decomposed.)

Note that under Artin's isomorphism, A_n^S corresponds to the Galois group of the maximal p-abelian unramified extension of K_n in which every prime of K_n dividing some $\mathfrak{p}_i \in S$ is completely decomposed.

(3) Even more generally, the work of FEDERER in [Fe 86] shows that under the assumptions of (2), we could consider *R-generalised S-class groups* ${}^R A_n^S$, where R denotes a set of primes of K, containing all the infinite primes, such that $R \cap S' = \emptyset$. Here ${}^R A_n^S$, $n \geq n_0$, is defined as follows: Let ${}^R A_n$ denote the p-primary subgroup of the ray class group of K_n with modulus $\prod_{\mathfrak{p} \in R} \mathfrak{p} =: \mathfrak{m}$, respectively. This means that we consider the group of fractional ideals of K_n that are coprime to $\mathfrak{m}$, and we divide out principal ideals (α) such that $\alpha \equiv 1 \mod \mathfrak{m}$. At the infinite primes, this means that α has to be totally positive, i.e., for every real infinite prime $\mathfrak{p}$ of K_n, $\alpha > 0$ in $(K_n)_\mathfrak{p} \cong \mathbb{R}$.

We then let ${}^R D_n^S$ denote the subgroup of ${}^R A_n$ generated by the primes dividing some $\mathfrak{p}_i \in S$, and we define ${}^R A_n^S := {}^R A_n / {}^R D_n^S$. By Artin's map, ${}^R A_n^S$ is isomorphic to the Galois group $\mathrm{Gal}(N_n/K_n)$, where N_n denotes the maximal abelian p-extension of K_n which is unramified outside R and in which every prime of S is completely decomposed.

Federer proved in [Fe 86] that ${}^R A^S := \varprojlim {}^R A_n^S$ is a Fukuda module, where the limit is taken with respect to the induced norm maps.

(4) Using Federer's approach, one has to assume that no prime of S' (and in particular no prime dividing p) is totally split in K_∞/K. Using instead the method of (1) (i.e., Corollary 3.9 and Lemma 3.10), we may consider sets S of primes such that every $\mathfrak{p} \in S$ is either ramified or completely decomposed in the $\mathbb{Z}_p$-extension K_∞/K, because this condition is equivalent to the fact that for some fixed $e \in \mathbb{N}_0$, arbitrary $i \geq j \geq e$ and every prime $\mathfrak{P}_j$ of K_j dividing some of the primes of S, there exists a prime $\mathfrak{Q}_i$ of K_i such that $f_{ij}(\mathfrak{Q}_i) = \mathfrak{P}_j$.

(Note that Corollary 3.9 may be generalised in order to prove that for every $\mathbb{Z}_p$-extension K_∞/K and for a set R of primes which does not contain any prime ideal dividing p, ${}^R A = \varprojlim {}^R A_n$ is a Fukuda module.)

Lemma 3.12 (Complementable Fukuda-submodules)**.** *Let $A = \varprojlim A_n$ be a Fukuda module with index barrier $e = e(A)$. Let $B = \varprojlim B_n$ be a Λ-submodule that is a direct summand of A (sometimes also called* **Λ-complement** *of A), i.e. assume that for any $n \in \mathbb{N}_0$, $B_n \subseteq A_n$ is a Λ-submodule such that there exists a Λ-submodule C_n of A_n with $B_n \oplus C_n = A_n$ and such that $f_{ij}(B_i) \subseteq B_j$ and $f_{ij}(C_i) \subseteq C_j$ for every $i \geq j$, where f_{ij}, as usual, are the maps in the projective limit $A = \varprojlim A_n$.*

Then B and C are Fukuda modules with index barrier e.

Proof. Let $j \geq e$. By assumption, we have $f_{ij}(B_i) \subseteq B_j$ and $f_{ij}(C_i) \subseteq C_j$ for any $i \geq j$. But then $f_{ij} : B_i \longrightarrow B_j$ and $f_{ij} : C_i \longrightarrow C_j$ have to be surjective, because $f_{ij} : A_i \longrightarrow A_j$ is surjective. Furthermore, $\mathrm{pr}_n(B) = B_n$ and $\mathrm{pr}_n(C) = C_n$ for every $n \geq e$ by construction, since $\mathrm{pr}_n(A) = A_n = B_n \oplus C_n$ (direct sum) for those n.

As in the proof of Lemma 3.10, we denote by Y_n^B the kernel of the n-th projection $\mathrm{pr}_n : B \longrightarrow B_n$, in contrast to Y_n^A, Y_n^C, etc. It remains to show that $Y_{n+1}^B = \nu_{(n+1,n)} \cdot Y_n^B$ for some $\nu_{(n+1,n)} \in (p, T) \subseteq \Lambda$, $n \geq e$.

Let $n \geq e$ be arbitrary, but fixed. We know by assumption that we have $Y_{n+1}^A = \nu_{(n+1,n)} \cdot Y_n^A$ for some $\nu_{(n+1,n)} \in (p, T)$. But $Y_m^B = Y_m^A \cap B$ for every m and therefore

$$\nu_{(n+1,n)} \cdot Y_n^B \ \subseteq \ \nu_{(n+1,n)} \cdot Y_n^A \cap B \ = \ Y_{n+1}^A \cap B \ = \ Y_{n+1}^B$$

for every n (this argument works for *any* submodule of A). It therefore suffices to prove the other inclusion. Let $x \in Y_{n+1}^B = Y_{n+1}^A \cap B$, $x = \nu_{(n+1,n)} \cdot y$ for some $y \in Y_n^A$, i.e., $x = (x_i)_{i \in \mathbb{N}_0}$ and $y = (y_i)_{i \in \mathbb{N}_0}$ satisfy $\nu_{(n+1,n)} \cdot y_i = x_i \in B_i$ for every $i \geq 0$. Since B_i and C_i are Λ-modules, it follows that $y_i = y_i^{(1)} + y_i^{(2)}$ with $y_i^{(1)} \in B_i$, $y_i^{(2)} \in C_i$ and $\nu_{(n+1,n)} \cdot y_i^{(2)} = 0$ for every i. But then we can replace y_i by $y_i^{(1)}$ for every i, since $f_{ij}(y_i^{(1)}) = y_j^{(1)}$ for each $i \geq j$. We obtain an element $\tilde{y} \in B \cap Y_n^A = Y_n^B$ such that $x = \nu_{(n+1,n)} \cdot \tilde{y} \in \nu_{(n+1,n)} \cdot Y_n^B$. This shows that B is a Fukuda module with index barrier $e = e(A)$. By interchanging the roles of B and C, one can show analogously that C is a Fukuda submodule of A. □

Remarks 3.13.

(1) The following example shows that arbitrary, not Λ-complementable, submodules of Fukuda modules in general will not inherit the Fukuda property with the same index barrier:
Let $A = \varprojlim A_n$ be a Fukuda module with index barrier e, and let $k \in \mathbb{N}_0$ be such that $|A_{e+1}| = p^k$. We consider the submodule $B := p^k \cdot A \subseteq A$, i.e., we let $B_n := p^k \cdot A_n$ for each n. Then we have $B_{e+1} = \{0\}$, since p^k annihilates A_{e+1}, and therefore we conclude that $B_e = f_{e+1,e}(\{0\}) = \{0\}$.
Now assume that B is a Fukuda module with index barrier e. Then Theorem 3.6 implies that $B_m = \{0\}$ for every $m \geq e$. But this means that p^k annihilates A_i for every $i \geq e$. Now there are certainly Fukuda modules that are not $\mathbb{Z}_p$-torsion modules. For example, Proposition 3.7 shows that for any $\mathbb{Z}_p$-extension K_∞/K, the Greenberg module $X = \mathrm{Gal}(L/K_\infty)$ is a Fukuda module. But there exist $\mathbb{Z}_p$-extensions whose λ-invariant (see Theorem 1.32) is different from zero, and this exactly means that we cannot have $p^k \cdot X = 0$ for any $k \in \mathbb{N}_0$ (see Proposition 1.31, (iv)). For example, if p splits completely in $K/\mathbb{Q}$ and if K_∞ denotes the cyclotomic $\mathbb{Z}_p$-extension of K, then $\lambda(K_\infty/K) \geq r_2(K)$ (compare [Gr 76], p. 266).
We will see in Example 3.15 a Fukuda submodule of the limit $A = \varprojlim A_n$ of class groups in a $\mathbb{Z}_p$-extension.

(2) Since the map $A \longmapsto p^k \cdot A$ is a Λ-module homomorphism, the above example also shows that, in general, homomorphic images of Fukuda modules will

not necessarily be Fukuda modules again. The inheritance of the Fukuda property is not even true for isomorphisms, as we will see in Example 3.14, (2). We therefore have to put additional assumptions on the isomorphism, as in Lemma 3.8.

Example 3.14.

(1) Let L/K be a $\mathbb{Z}_p$-extension. Assume that $k \subseteq K$ is a subfield such that K/k is normal with finite abelian Galois group $\Delta = \mathrm{Gal}(K/k)$. Let furthermore $\Gamma = \mathrm{Gal}(L/K) \cong \mathbb{Z}_p$, and assume that L is galois over k with Galois group $\mathrm{Gal}(L/k) \cong \Gamma \times \Delta$. Let us further assume that $|\Delta|$ is coprime to p.
Let $H(L)$ denote the maximal p-abelian unramified extension of L. Then Δ acts on the Greenberg module $X = \mathrm{Gal}(H(L)/L)$, as in Section 1.3 (in fact, $\mathrm{Gal}(L/k)$ acts on X). Since $X \cong A = \varprojlim A_n$ via Artin's isomorphism, this defines an action of Δ on A.
Let $\hat{\Delta}$ denote the group of characters $\chi : \Delta \longrightarrow \overline{\mathbb{Q}}_p^*$ into a fixed algebraic closure of $\mathbb{Q}_p$. For each $\chi \in \hat{\Delta}$, one defines the idempotent

$$\varepsilon_\chi := \frac{1}{|\Delta|} \cdot \sum_{\sigma \in \Delta} \chi(\sigma) \cdot \sigma^{-1} \in \mathcal{O}_\mathfrak{p}[\Delta] \, .$$

Here we note that $\frac{1}{|\Delta|} \in \mathbb{Z}_p$, since we assume that $p \nmid |\Delta|$, and the values $\chi(\sigma)$ are contained in the ring $\mathcal{O}_\mathfrak{p} := \mathbb{Z}_p(\zeta_f)$ of integral elements of a cyclotomic extension $\mathbb{Q}_p(\zeta_f) \subseteq \overline{\mathbb{Q}}_p$, $f = |\Delta|$ (note that $\mathbb{Z}_p$ only contains roots of unity of order dividing $p-1$). The idempotents satisfy the relations

$$\varepsilon_\chi \cdot \varepsilon_\psi = \begin{cases} \varepsilon_\chi & : \chi = \psi \\ 0 & : \chi \neq \psi \end{cases} \quad , \quad \sum_{\chi \in \hat{\Delta}} \varepsilon_\chi = 1 \quad \text{and} \quad \varepsilon_\chi \cdot \sigma = \chi(\sigma) \cdot \varepsilon_\chi$$

for every $\sigma \in \Delta$ (compare [Wa 97], p. 100).
Now let $\chi \in \hat{\Delta}$ denote any fixed character. For every

$$g \in G_f := \mathrm{Gal}(\mathbb{Q}_p(\zeta_f)/\mathbb{Q}_p) \, ,$$

the map χ^g defined by $\chi^g(\sigma) := g(\chi(\sigma))$ is also a homomorphism from Δ to $\mathcal{O}_\mathfrak{p}$; in other words, G_f acts on $\hat{\Delta}$. If $G_f \cdot \chi$ denotes the orbit of $\chi \in \hat{\Delta}$ under the action of G_f, then

$$\sum_{\tau \in G_f \cdot \chi} \tau(\sigma) \ \in \mathbb{Z}_p$$

for every $\sigma \in \Delta$ (note that we are actually taking the trace to $\mathbb{Q}_p$ here).
Let $\hat{\Delta}_1, \ldots, \hat{\Delta}_s$ denote the distinct orbits of the action of G_f on $\hat{\Delta}$.
The elements

$$\varepsilon_i := \frac{1}{|\Delta|} \sum_{\sigma \in \Delta} \left(\sum_{\chi \in \hat{\Delta}_i} \chi(\sigma) \right) \cdot \sigma^{-1} \in \mathbb{Z}_p[\Delta] \, , \quad 1 \leq i \leq s \, ,$$

denote the *orthogonal idempotents* of the group ring $\mathbb{Z}_p[\Delta]$ (compare [Wa 97], p. 339).

Since A is a $\mathbb{Z}_p[\Delta]$-module, and as the sum over the pairwise different idempotents $\varepsilon_1, \ldots, \varepsilon_s$ is still equal to 1, we have a canonical decomposition

$$A = \bigoplus_{i=1}^{s} \varepsilon_i \cdot A$$

of Λ-modules, coming from a decomposition into eigenspaces (the action of each $\sigma \in \Delta$ yields a $\mathbb{Z}_p$-linear map on A, and $\varepsilon_i \cdot A$ is the eigenspace with eigenvalue $\mathrm{Tr}_{\mathbb{Q}_p(\zeta_f)/\mathbb{Q}_p}(\chi(\sigma))$, $\chi \in \Delta_i$ arbitrary).
Every module $\varepsilon_i \cdot A$ is a finitely generated torsion Λ-module, and Proposition 1.28 yields invariants $\mu_i, \lambda_i, \nu_i \in \mathbb{Z}$ attached to $\varepsilon_i \cdot A$, respectively. In particular, the Iwasawa invariants μ, λ, ν of L/K satisfy

$$\mu = \sum_{i=1}^{s} \mu_i \ , \quad \lambda = \sum_{i=1}^{s} \lambda_i \quad \text{and} \quad \nu = \sum_{i=1}^{s} \nu_i \ .$$

In this situation, Lemma 3.12 implies that each $\varepsilon_i \cdot A$ is a Fukuda module having the same index barrier as A. Indeed, it suffices to show that the decomposition

$$A = \bigoplus_{k=1}^{s} \varepsilon_k \cdot A$$

is compatible with the norm maps $f_{ij} : A_i \longrightarrow A_j$ for every $i \geq j$, i.e., that $f_{ij}(\varepsilon_k \cdot A_i) \subseteq \varepsilon_k \cdot A_j$.
Now an application of the norm f_{ij} on A_i may be identified with the action of the element $\sum_{\sigma \in \mathrm{Gal}(L_i/L_j)} \sigma$ of the group ring $\mathbb{Z}_p[\mathrm{Gal}(L_i/L_j)]$, respectively.
Since $\mathrm{Gal}(L/k) \cong \mathrm{Gal}(L/K) \times \Delta$ is abelian by assumption, we see that $\mathrm{Gal}(L_i/k) \cong \mathrm{Gal}(L_i/K) \times \Delta$ for every i, and therefore the group ring elements $f_{ij} \in \mathbb{Z}_p[\mathrm{Gal}(L_i/L_j)] \subseteq \mathbb{Z}_p[\mathrm{Gal}(L_i/K)]$ and $\varepsilon_k \in \mathbb{Z}_p[\Delta]$ commute, i.e.,

$$f_{ij}(\varepsilon_k \cdot A_i) = \varepsilon_k \cdot f_{ij}(A_i) \subseteq \varepsilon_k \cdot A_j$$

for every $k \in \{1, \ldots, s\}$, $i \geq j \geq 0$. This shows that we may apply Lemma 3.12.

(2) For the sake of simplicity, we will for the moment assume that $p \neq 2$. Let K denote a *CM-field*, i.e., a totally imaginary quadratic extension of a totally real number field $k := K^+$. If L denotes the cyclotomic $\mathbb{Z}_p$-extension of K, then L, K and k satisfy the condition from example (1), i.e.,

$$\mathrm{Gal}(L/k) \cong \Gamma \times \Delta \ ,$$

where $\Delta := \mathrm{Gal}(K/K^+)$ is generated by the complex conjugation map j.
According to the above general example, we have a canonical decomposition

$$A = A^+ \oplus A^-$$

of Λ-modules, where $A = \varprojlim A_n^{(L)}$,

$$A^+ = \varepsilon_{\chi_0} \cdot A = (\frac{1}{2}(1 + j)) \cdot A$$

corresponds to the trivial character $\chi_0 \in \hat{\Delta}$, and

$$A^- = \varepsilon_{\chi^-} \cdot A = (\frac{1}{2}(1-j)) \cdot A$$

corresponds to the nontrivial character of $\hat{\Delta}$.
Proposition 13.28 in [Wa 97] shows that the Fukuda module A^- does not contain any non-trivial finite Λ-submodules. Now suppose that $K/\mathbb{Q}$ is abelian, and that every prime of $k = K^+$ dividing p is split in K/k. It is known that in this case,

- $\mu(L/K) = 0$ (compare [FW 79]), and
- $\lambda^-(L/K) := \lambda(A^-) \geq g$, where $g \geq 1$ denotes the number of primes of K^+ dividing p (see Section 2 of [Gr 73(2)]).

Since $\mu^-(L/K) := \mu(A^-) \leq \mu(L/K) = 0$, and as A^- does not contain any non-trivial finite submodules, Proposition 1.31, (i) and (iii) imply that A^- is a finitely generated free $\mathbb{Z}_p$-module. In particular, multiplication by p is an injective Λ-module homomorphism on A^-.
Moreover, if $e = e(L/K)$ denotes the index barrier of A, and if $k \in \mathbb{N}_0$ is large enough to ensure that $p^k \cdot A^-_{e+1} = \{0\}$, then the isomorphic image $p^k \cdot A^-$ of A^- cannot be a Fukuda module with index barrier e, because $\lambda(A^-) \geq 1$ and therefore $p^k \cdot A^- \neq \{0\}$ (see Remarks 3.13, (1)). This shows that isomorphic images of Fukuda modules will not automatically inherit the Fukuda property (compare Remarks 3.13, (2)).

We will conclude the current section with an important example of a Fukuda submodule of the projective limit of ideal class groups $A = \varprojlim A_n^{(L)}$ attached to a $\mathbb{Z}_p$-extension L/K.

Example 3.15. Let L/K denote a $\mathbb{Z}_p$-extension, let $A = \varprojlim A_n^{(L)}$ be defined as usual. Since A is a finitely generated torsion Λ-module, Theorem 1.24 implies that there exists an exact sequence

$$0 \longrightarrow M_1 \longrightarrow A \xrightarrow{\varphi} E_A \longrightarrow M_2 \longrightarrow 0$$

of Λ-modules, where E_A denotes an elementary Λ-module in the sense of Definition 1.23, and where M_1 and M_2 are finite Λ-modules. In other words, there exists a Λ-pseudo-isomorphism $\varphi : A \longrightarrow E_A$ with kernel M_1 and cokernel M_2. We want to show that $M_1 \subseteq A$ is a Fukuda submodule with index barrier $e := e(A) = e(L/K)$.
For each $n \in \mathbb{N}_0$, we define $(M_1)_n := \mathrm{pr}_n(M_1)$, where $\mathrm{pr}_n : A \longrightarrow A_n^{(L)}$ denote the canonical projections. Then each $(M_1)_n \subseteq A_n^{(L)}$ is a Λ-submodule. If $f_{ij} : A_i^{(L)} \longrightarrow A_j^{(L)}$, $i \geq j$, denote the norm maps, then $f_{ij}((M_1)_i) = (M_1)_j$ for each $i \geq j$, since $f_{ij} \circ \mathrm{pr}_i = \mathrm{pr}_j$ for every $i \geq j$.
It therefore remains to prove Property (F). Let $n \geq e$ be arbitrary, let $Y_n^{M_1}$, respectively, Y_n^A, denote the kernels of the projections $\mathrm{pr}_n : M_1 \longrightarrow (M_1)_n$, respectively, $\mathrm{pr}_n : A \longrightarrow A_n$.
Then $Y_n^{M_1} = Y_n^A \cap M_1$ and therefore

$$\nu_{(n+1,n)} \cdot Y_n^{M_1} \subseteq \nu_{(n+1,n)} \cdot Y_n^A \cap M_1 = Y_{n+1}^A \cap M_1 = Y_{n+1}^{M_1} .$$

We want to prove the converse.
Let $x \in Y_{n+1}^{M_1}$ be arbitrary. Since

$$Y_{n+1}^{M_1} \;=\; Y_{n+1}^{A} \cap M_1 \;=\; \nu_{(n+1,n)} \cdot Y_n^A \cap M_1 \;,$$

we may write $x = \nu_{(n+1,n)} \cdot y$ for some element $y \in Y_n^A$, and we want to prove that $y \in M_1 = \ker(\varphi)$. Since $x \in M_1$, we have

$$0 \;=\; \varphi(x) \;=\; \varphi(\nu_{(n+1,n)} \cdot y) \;=\; \nu_{(n+1,n)} \cdot \varphi(y) \;.$$

If X denotes the Greenberg module attached to the $\mathbb{Z}_p$-extension L/K, then we have shown in Proposition 1.44 that $\nu_{(n+1,n)}$ is coprime to the characteristic polynomial of X for every $n \geq e$. But $X \cong A$, and therefore the elementary Λ-modules attached to X and A are equal by Corollary 1.25, (i), implying that multiplication by $\nu_{(n+1,n)}$ is injective on E_A (recall that Λ is a unique factorisation domain). Therefore $0 = \varphi(y)$, i.e., $y \in M_1$, as claimed.

3.2 Ramification and Greenberg's topology

In this section, we want to investigate an important drawback which limits the strength of Fukuda's Theorem 3.1 and of its generalisation, Theorem 3.6: The statements of these theorems only hold for n being large enough, i.e., greater than the index barrier e, which in the classical case of ideal class groups in $\mathbb{Z}_p$-extensions (Theorem 3.1) is given by the ramification describing integer defined in Proposition 1.3.

We therefore want to study the local behaviour of the function

$$e : \; \mathcal{E}(K) \longrightarrow \mathbb{N}_0 \;, \quad L \mapsto e(L/K) \;,$$

where K is a fixed number field. More precisely, we will investigate the values $e(L/K)$, where L ranges over certain open or closed neighbourhoods in the sense of Greenberg's topology (compare Section 2.3). In particular, we will look for subsets of $\mathcal{E}(K)$ restricted to which the e invariant remains bounded.

It turns out that one can modify Greenberg's topology in order to obtain a topology with respect to which e is locally bounded. This topology will take care of ramification. At the end of the section, we will study in some detail which sets of primes of K typically occur as ramification sets of $\mathbb{Z}_p$-extensions of K, looking at the example of a *CM-field* K in which p is totally split.

We start with the following already known facts.

Lemma 3.16. *Let L/K be a $\mathbb{Z}_p$-extension.*

(i) Let $e = e(L/K)$, and let $L' \in \mathcal{E}(K)$ be such that $L \cap L' \supseteq L_{e+1}$. Then every prime of K that ramifies in L also ramifies in L'.

(ii) If there is only one prime of K lying above p, then e is locally constant, i.e., for any $L \in \mathcal{E}(K)$ there exists an open neighbourhood $L \in U \subseteq \mathcal{E}(K)$ such that $e(L'/K) = e(L/K)$ for every $L' \in U$.

Proof. We have shown these two statements in course of the proof of Theorem 3.2, (i). □

We introduce some notation.

Definition 3.17. Let $\mathcal{I} := \{\mathfrak{p}_1, \ldots, \mathfrak{p}_t\}$ be the set of all prime ideals of K lying above p. For any $\mathbb{Z}_p$-extension L of K, let $\mathcal{P}(L)$ denote the subset of $\mathcal{I}$ consisting of the primes that ramify in L/K. Define $\mathcal{E}^{\mathcal{I}}(K)$ to be the set of all $\mathbb{Z}_p$-extensions L of K satisfying $\mathcal{P}(L) = \mathcal{I}$. For any subset $\emptyset \neq I \subsetneqq \mathcal{I}$, let $\mathcal{E}^I(K) := \{L \in \mathcal{E}(K) \mid \mathcal{P}(L) = I\}$, and let $\tilde{\mathcal{E}}^I(K) \subseteq \mathcal{E}(K)$ denote the set of all $L \in \mathcal{E}(K)$ satisfying $\mathcal{P}(L) \subseteq I$.

Now we are able to generalise the above lemma:

Lemma 3.18. *The following assertions are stated with respect to Greenberg's topology on $\mathcal{E}(K)$.*

(i) $\mathcal{E}^{\mathcal{I}}(K) \subseteq \mathcal{E}(K)$ *is open.* $e|_{\mathcal{E}^{\mathcal{I}}(K)}$ *is locally constant.*

(ii) Let K_∞/K denote the cyclotomic $\mathbb{Z}_p$-extension of K (see Example 1.5). Then $K_\infty \in \mathcal{E}^{\mathcal{I}}(K)$. In particular, $\mathcal{E}^{\mathcal{I}}(K) \neq \emptyset$ for every number field K.

(iii) The set $\mathcal{E}^{\mathcal{I}}(K)$ is dense in $\mathcal{E}(K)$. The sets $\tilde{\mathcal{E}}^I(K)$ and $\mathcal{E}^I(K)$, $I \neq \mathcal{I}$, contain no nontrivial open subsets.

(iv) Fix some $I \subseteq \mathcal{I}$. Then e is bounded on every closed subset $V \subseteq \mathcal{E}^I(K)$.

(v) Let $\emptyset \neq I \subseteq \mathcal{I}$ be fixed. The set $\tilde{\mathcal{E}}^I(K)$ is closed and therefore compact. The set $\mathcal{E}^I(K)$ is closed if and only if $\mathcal{E}^I(K) = \emptyset$ or $\tilde{\mathcal{E}}^I(K) \setminus \mathcal{E}^I(K) = \emptyset$.

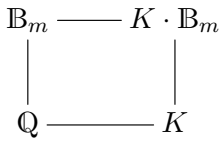
(vi) For any $L \in \mathcal{E}(K)$ there exists an open neighbourhood U of L such that e is constant on $U \cap \tilde{\mathcal{E}}^{\mathcal{P}(L)}(K)$.
Fix some $\emptyset \neq I \subseteq \mathcal{I}$.
If $\tilde{\mathcal{E}}^I(K) \setminus \mathcal{E}^I(K) = \emptyset$, then $e|_{\mathcal{E}^I(K)} = e|_{\tilde{\mathcal{E}}^I(K)}$ is globally bounded.
If $\tilde{\mathcal{E}}^I(K) \setminus \mathcal{E}^I(K) \neq \emptyset$ (and $\mathcal{E}^I(K) \neq \emptyset$), then $e|_{\mathcal{E}^I(K)}$ and therefore also $e|_{\tilde{\mathcal{E}}^I(K)}$ is unbounded and $e|_{\tilde{\mathcal{E}}^I(K)}$ in general is not locally constant: For $L \in \tilde{\mathcal{E}}^I(K)$, the existence of an open neighbourhood U of L such that $e|_{U \cap \tilde{\mathcal{E}}^I(K)}$ is constant is equivalent to the condition that $\mathcal{P}(L) = I$.

Proof. (i) Let $L \in \mathcal{E}^{\mathcal{I}}(K)$. Then every prime ideal of K lying above p ramifies in L. Let $U := \mathcal{E}(L, e(L/K) + 1)$. Then $\mathcal{P}(M) = \mathcal{I}$ for every $M \in U$ by Lemma 3.16, (i). Therefore $U \subseteq \mathcal{E}^{\mathcal{I}}(K)$, i.e., $\mathcal{E}^{\mathcal{I}}(K)$ is open. Furthermore, $e(M/K) = e(L/K)$ for every $M \in U$ (compare the proof of Theorem 3.2, (i)), and therefore $e|_U$ is constant, proving (i). Note that this generalises the statement of Lemma 3.16, (ii), and will be strengthened further in (vi).

(ii) Let K_∞ be the cyclotomic $\mathbb{Z}_p$-extension of K. We want to show that every prime ideal of K dividing p ramifies in K_∞/K. By definition of K_∞ (see Example 1.5), we have $K_\infty = \bigcup_{n \geq 0} K_n$ with $K_n = K \cdot \mathbb{B}_{f+n}$. Here $\mathbb{B}_f = K \cap \mathbb{B}_\infty$, where $\mathbb{B}_\infty$ denotes the union of the unique cyclic subfields $\mathbb{B}_m \subseteq \mathbb{Q}(\zeta_{p^{m+1}})$ of degree p^m over $\mathbb{Q}$, respectively (with slight modifications in the case $p = 2$), as described in Example 1.5. In particular, p is totally ramified in $\mathbb{B}_m/\mathbb{Q}$ for every m.
Now choose any $m \in \mathbb{N}$ such that $[\mathbb{B}_m : \mathbb{Q}] = p^m > [K : \mathbb{Q}]$. Let $\mathfrak{p}$ be a prime of K lying above p, and consider the field $\mathbb{B}_m \cdot K$, which is a non-trivial Galois extension of K with cyclic Galois group

$$\mathrm{Gal}((\mathbb{B}_m \cdot K)/K) \cong \mathrm{Gal}(\mathbb{B}_m/\mathbb{B}_f) .$$

We have the following diagram of fields.



Now we choose a prime $\mathfrak{P}$ in $K \cdot \mathbb{B}_m$ lying above $\mathfrak{p}$; let $\mathfrak{p}' := \mathfrak{P} \cap \mathcal{O}_{B_m}$. Since p is totally ramified in $\mathbb{B}_m/\mathbb{Q}$, the ramification index $e_p(\mathbb{B}_m/\mathbb{Q})$ equals p^m. In particular, $(\mathfrak{p}')^{p^m}$ divides (p) in the ring of integers of $\mathbb{B}_m$, and therefore at least $\mathfrak{P}^{p^m}$ divides (p) in the ring of integers of $K \cdot \mathbb{B}_m$. But since $e_{\mathfrak{p}|p}(K/\mathbb{Q}) \leq [K : \mathbb{Q}] < p^m$, it then follows that $\mathfrak{p}$ has to ramify in $(K \cdot \mathbb{B}_m)/K$. Since $\mathfrak{p}$ was arbitrary, the assertion follows.

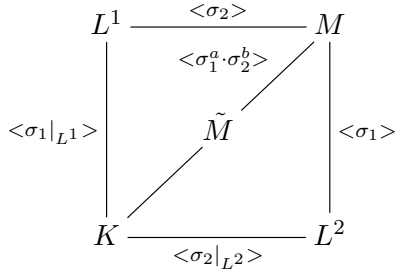
(iii) Let $L \in \mathcal{E}(K)$ be such that $\mathcal{P}(L) \subsetneqq \mathcal{I}$. The idea is to show that there exist $\mathbb{Z}_p$-extensions of K contained in the composite of L with the cyclotomic $\mathbb{Z}_p$-extension K_∞ of K that are arbitrarily close to L and belong to $\mathcal{E}^{\mathcal{I}}(K)$. For this purpose, let $n \in \mathbb{N}$ be arbitrary, and consider

$$\mathcal{E}(L, n) = \{M \in \mathcal{E}(K) \mid M \cap L \supseteq L_n\} .$$

We make use of the following basic lemma:

Lemma 3.19. *Let L^1, L^2 be different $\mathbb{Z}_p$-extensions of K, and let us write $I_1 := \mathcal{P}(L^1)$ and $I_2 := \mathcal{P}(L^2)$. Let $M := L^1 \cdot L^2$.*

(i) Suppose that $L^1 \cap L^2 = K$. Let σ_1, σ_2 denote topological generators of $\mathrm{Gal}(M/K)$ such that $\mathrm{Gal}(L^i/K)$ is generated topologically by the restriction $\sigma_i|_{L^i}$, respectively. Then we consider $\mathbb{Z}_p$-extensions $\tilde{M}$ of K contained in M:



We can write $\mathrm{Gal}(\tilde{M}/K) \cong \mathrm{Gal}(M/K)/ < \sigma_1^a \cdot \sigma_2^b >$ for suitable elements $a, b \in \mathbb{Z}_p$, and we know that one of them is a p-adic unit (see Proposition 2.3). In this situation, the following holds:
If $p^k \parallel a$ and $p^l \parallel b$, then $\tilde{M} \cap L^1 = (L^1)_k$ and $\tilde{M} \cap L^2 = (L^2)_l$. Here $(L^i)_j$, as usual, denotes the j-th intermediate field of L^i/K, respectively.

(ii) $\mathcal{P}(\tilde{M}) = I_1 \cup I_2$ for all but at most $|I_1 \cap I_2|$ $\mathbb{Z}_p$-extensions $\tilde{M} \subseteq M$. In the exceptional $\mathbb{Z}_p$-extensions, we could have $\mathfrak{p}$ unramified for some $\mathfrak{p} \in I_1 \cap I_2$; for every such $\mathfrak{p}$, at most one such $\mathbb{Z}_p$-extension exists.

Proof. (i) Define k and l by the properties $p^k \parallel a$ (i.e., $p^k \mid a$ and $p^{k+1} \nmid a$ in $\mathbb{Z}_p$) and $p^l \parallel b$, respectively. Since $\mathrm{Gal}(\tilde{M}/K) \cong \mathbb{Z}_p$ contains no

p-torsion elements, $k = 0$ or $l = 0$ (compare the proof of Proposition 2.3). Without loss of generality, we may assume that $l = 0$. Write $a = p^k \cdot u$, $u \in \mathbb{Z}_p^*$. Then

$$<\sigma_1^a \cdot \sigma_2^b>_{\mathbb{Z}_p} \;=\; <\sigma_1^{p^k} \cdot \sigma_2^{u^{-1}b}>_{\mathbb{Z}_p} \;,$$

and therefore, letting $b' := u^{-1} \cdot b \in \mathbb{Z}_p^*$,

$$\mathrm{Gal}(\tilde{M}/K) \;\cong\; <\sigma_1, \sigma_2> \,/\, <\sigma_1^{p^k} \cdot \sigma_2^{b'}> \,,$$

i.e., $\sigma_1^{p^k} = \sigma_2^{-b'}$ in $\mathrm{Gal}(\tilde{M}/K)$.
The intersection $\tilde{M} \cap L^1$ is uniquely determined by the subgroup H of $\mathrm{Gal}(M/K)$ fixing it. Since

$$H \;=\; <\sigma_1^{p^k} \cdot \sigma_2^{b'}, \sigma_2> \;=\; <\sigma_1^{p^k}, \sigma_2> \,,$$

it follows that $\tilde{M} \cap L^1 = (L^1)_k$.
Furthermore, $b \in \mathbb{Z}_p^*$ because $l = 0$, and thus we can write

$$<\sigma_1^a \cdot \sigma_2^b>_{\mathbb{Z}_p} = <\sigma_1^{ab^{-1}} \cdot \sigma_2>_{\mathbb{Z}_p} \quad .$$

Therefore $\sigma_1^{-ab^{-1}} = \sigma_2$ in $\mathrm{Gal}(\tilde{M}/K)$, which implies that σ_2 acts trivially on $\tilde{M} \cap L^2$, and therefore $\tilde{M} \cap L^2 \subseteq M^{<\sigma_2, \sigma_1>} = K$.

(ii) Let us first consider a prime $\mathfrak{p} \in \mathcal{I}$ such that $\mathfrak{p} \in I_1$, $\mathfrak{p} \notin I_2$, i.e., $\mathfrak{p}$ ramifies in L^1, but not in L^2. Let

$$T \;:=\; \mathrm{T}_{\mathfrak{p}}(M/K) \;\subseteq\; \mathrm{Gal}(M/K) \;\cong\; \mathbb{Z}_p^2$$

denote the inertia subgroup of $\mathfrak{p}$ in M/K. Then the $\mathbb{Z}_p$-rank of T is greater or equal to 1, since $\mathfrak{p}$ is totally ramified in $L^1/(L^1)_{e(L^1/K)}$. Indeed, if $\mathrm{rank}_{\mathbb{Z}_p}(T)$ was zero, then T would have to be trivial, since it is a closed subgroup of $\mathrm{Gal}(M/K)$, and the only finite closed subgroup of $\mathbb{Z}_p^2$ is $\{0\}$; but then $\mathfrak{p}$ was unramified in M/K.
On the other hand, $\mathfrak{p} \notin \mathcal{P}(L^2)$ implies that $L^2 \subseteq M^T$, and therefore $\mathrm{rank}_{\mathbb{Z}_p}(T) \leq 1$, i.e., $\mathrm{rank}_{\mathbb{Z}_p}(T) = 1$.
Now let $\tilde{M} \subseteq M$ denote a $\mathbb{Z}_p$-extension of K such that $L^1 \neq \tilde{M} \neq L^2$. Then $\mathfrak{p}$ cannot be unramified in $\tilde{M}$, since otherwise $\tilde{M} \cdot L^2 \subseteq M^T$, and as $\mathrm{Gal}(\tilde{M} \cdot L^2/K)$ is isomorphic to (a subgroup of finite index in) $\mathbb{Z}_p^2$, we would conclude that $\mathrm{rank}_{\mathbb{Z}_p}(T) = 0$, yielding a contradiction. Therefore $\mathfrak{p} \in \mathcal{P}(\tilde{M})$.
By a symmetric argument, it follows that $\mathfrak{p} \in \mathcal{P}(\tilde{M})$ for every prime $\mathfrak{p} \in I_2 \setminus I_1$. Let us look now at the primes $\mathfrak{p} \in I_1 \cap I_2$. If $\mathfrak{p} \notin \mathcal{P}(\tilde{M})$, then $\tilde{M} \subseteq M^T$. Therefore, for any such $\mathfrak{p}$, at most one $\mathbb{Z}_p$-extension $\tilde{M}$ with $\mathfrak{p} \notin \mathcal{P}(\tilde{M})$ does exist, since otherwise, its inertia group would satisfy $\mathrm{rank}_{\mathbb{Z}_p}(T) = 0$, which would contradict the fact that $\mathfrak{p}$ is ramified in L^1 and L^2. The assertion follows.

□

Now we return to the proof of (iii). We apply the above lemma with $L^1 := L$ and $L^2 := K_\infty$, the cyclotomic $\mathbb{Z}_p$-extension of K. Let $n \in \mathbb{N}$ be arbitrary. Since there exist only finitely many $\mathbb{Z}_p$-extensions $\tilde{M}$ of K contained in $L \cdot K_\infty$ that satisfy $\mathcal{P}(\tilde{M}) \subsetneqq \mathcal{I} = \mathcal{P}(L) \cup \mathcal{P}(K_\infty)$, by Lemma 3.19, (ii), we can choose $\tilde{M} \in \mathcal{E}(L,n)$ such that $\mathcal{P}(\tilde{M}) = \mathcal{I}$, i.e., $\tilde{M} \in \mathcal{E}^{\mathcal{I}}(K)$.

Now assume that $U \subseteq \mathcal{E}^I(K)$ or $U \subseteq \tilde{\mathcal{E}}^I(K)$, $I \subsetneqq \mathcal{I}$, is non-trivial and open. Let $L \in U$ be a $\mathbb{Z}_p$-extension of K such that $\mathcal{E}(L,n) \in U$ for some $n \in \mathbb{N}$. Since $\mathcal{E}(L,n) \cap \mathcal{E}^{\mathcal{I}}(K) \neq \emptyset$, because $\mathcal{E}^{\mathcal{I}}(K) \subseteq \mathcal{E}(K)$ is dense, this gives a contradiction because $\mathcal{E}^{\mathcal{I}}(K)$ and $\mathcal{E}^I(K)$ (respectively, $\mathcal{E}^{\mathcal{I}}(K)$ and $\tilde{\mathcal{E}}^I(K)$) are disjoint by definition.

(iv) If $e|_V$ was unbounded, we could choose a sequence $(M^{(n)})_{n\in\mathbb{N}_0}$ of elements in $V \subseteq \mathcal{E}^I(K)$ with unbounded $e(M^{(n)}/K)$. Since V is closed and therefore compact, the sequence $(M^{(n)})_{n\geq 0}$ would contain a subsequence converging to a field $M \in V \subseteq \mathcal{E}^I(K)$. Without loss of generality, we may assume that the $M^{(n)}$ themselves converge to M and that $(M^{(n)} \cap M) \supseteq M_n$ for every $n \geq 0$. But then, for every $n \geq e(M/K)+1$, each prime of I would ramify in $(M^{(n)})_{e(M/K)+1}/K$, and in particular,

$$e(M^{(n)}/K) \,=\, e(M/K) \,<\, \infty$$

for these n. This contradicts the unboundedness of the $e(M^{(n)}/K)$.

(v) Let $\emptyset \neq I \subseteq \mathcal{I}$, and consider a sequence $(M^{(i)})_{i\geq 0}$ of elements in $\tilde{\mathcal{E}}^I(K)$. Since $\mathcal{E}(K)$ is compact, there exists a convergent subsequence $M^{n(i)} \longrightarrow M$ for a suitable $M \in \mathcal{E}(K)$. Without loss of generality, we may assume that the $M^{(i)}$ themselves converge to M. We want to show that $M \in \tilde{\mathcal{E}}^I(K)$, i.e., that $\mathcal{P}(M) \subseteq I$.

Since $M^{(i)} \longrightarrow M$, we may assume that $(M^{(i)} \cap M) \supseteq M_i$ for every $i \geq 0$. But then, for $i \geq e(M/K)+1$, every element of $\mathcal{P}(M)$ has to ramify in $M^{(i)}/K$, i.e.,

$$\mathcal{P}(M) \subseteq \mathcal{P}(M^{(i)}) \subseteq I \;,$$

and therefore $M \in \tilde{\mathcal{E}}^I(K)$.

Now consider the set $\mathcal{E}^I(K)$. Without loss of generality, we may assume that it is not empty. If $\tilde{\mathcal{E}}^I(K) \setminus \mathcal{E}^I(K) = \emptyset$, then $\mathcal{E}^I(K) = \tilde{\mathcal{E}}^I(K)$ is closed by the above.

Now assume that there exists a $\mathbb{Z}_p$-extension N of K such that $\mathcal{P}(N) \subsetneqq I$. Then we can construct a sequence $N^{(i)} \longrightarrow N$ such that $\mathcal{P}(N^{(i)}) = I$ for every i by considering appropriate $\mathbb{Z}_p$-extensions of K contained in the composite of N with an element $M \in \mathcal{E}^I(K)$, and using Lemma 3.19, as in the proof of (iii). Thus $N^{(i)} \in \mathcal{E}^I(K)$ for every i, but $N \notin \mathcal{E}^I(K)$. Therefore $\mathcal{E}^I(K)$ is not closed in this case.

(vi) Let L be an arbitrary $\mathbb{Z}_p$-extension of K. Then Lemma 3.16 implies that $\mathcal{P}(M) = \mathcal{P}(L)$ and $e(M/K) = e(L/K)$ for every

$$M \,\in\, \mathcal{E}(L, e(L/K)+1) \,\cap\, \tilde{\mathcal{E}}^{\mathcal{P}(L)}(K) \;.$$

We fix a subset $\emptyset \neq I \subseteq \mathcal{I}$. If $\tilde{\mathcal{E}}^I(K) \setminus \mathcal{E}^I(K) = \emptyset$, then $\mathcal{E}^I(K) = \tilde{\mathcal{E}}^I(K)$ is closed by (v). It follows that $e|_{\mathcal{E}^I(K)}$ is globally bounded, using (iv).

Now let $L \in \tilde{\mathcal{E}}^I(K)$ be a $\mathbb{Z}_p$-extension of K such that $\mathcal{P}(L) \subsetneqq I$. Assume that there exists an integer $n \in \mathbb{N}$ such that e is bounded by a constant $E \in \mathbb{N}$ on $\mathcal{E}(L,n) \cap \tilde{\mathcal{E}}^I(K)$. Define $m' := \max(n, E+1)$. Then we choose $M \in \mathcal{E}^I(K)$ and make use of Lemma 3.19, applied to $L^1 := L$ and $L^2 := M$, in order to obtain a $\mathbb{Z}_p$-extension $\tilde{M}$ of K contained in $L \cdot M$ such that $\tilde{M} \in \mathcal{E}(L,m')$ and $\mathcal{P}(\tilde{M}) = \mathcal{P}(L) \cup \mathcal{P}(M) = \mathcal{P}(M) = I$. In particular, since $\mathcal{P}(L) \subsetneqq I$ and $(\tilde{M})_i = L_i$ for every $i \leq E+1$, we must have $e(\tilde{M}/K) \geq E+1$. But $\tilde{M} \in \mathcal{E}(L,n) \cap \tilde{\mathcal{E}}^I(K)$, proving that e cannot be locally bounded, and in particular cannot be locally constant. Moreover, this shows that $e|_{\mathcal{E}^I(K)}$ is unbounded if $\tilde{\mathcal{E}}^I(K) \setminus \mathcal{E}^I(K) \neq \emptyset$ and $\mathcal{E}^I(K) \neq \emptyset$.
If, on the other hand, $L \in \tilde{\mathcal{E}}^I(K)$ satisfies $\mathcal{P}(L) = I$, then we have seen above that $e|_{\tilde{\mathcal{E}}^I(K)}$ is locally constant around L.

□

Remarks 3.20.

(1) There are two general principles which can be learned from the proofs of the preceding lemmas:

- If we consider a sequence $(M^{(n)})_{n\geq 0}$ of $\mathbb{Z}_p$-extensions converging to an extension M, then the set of primes ramifying in the limit M can be strictly smaller than the $\mathcal{P}(M^{(n)})$ (compare the proofs of Lemma 3.18, (iii) and (v)). On the other hand, every $\mathfrak{p} \in \mathcal{P}(M)$ has to ramify also in the $M^{(n)}$ for n being large enough.
- If we consider a Greenberg open neighbourhood $\mathcal{E}(L,n)$ of a $\mathbb{Z}_p$-extension L of K, then the set of primes ramifying in an arbitrary extension $M \in \mathcal{E}(L,n)$ can be larger than $\mathcal{P}(L)$, since in general, it is possible that $e(M/K) > n$, so that there can exist primes that have not yet started ramifying in $M_n = L_n$.
  If $n > e(L/K)$, then we have at least $\mathcal{P}(L) \subseteq \mathcal{P}(M)$ by Lemma 3.16, (i), whereas for $n \leq e(L/K)$, we can only say that the $\mathfrak{p}_i \in \mathcal{P}(L)$ that have already started ramifying in L_n/K will also belong to $\mathcal{P}(M)$ (it is plausible that for small n we do not have much information about M, since then $\mathcal{E}(L,n)$ is quite coarse).

(2) Both cases mentioned in Lemma 3.18, (vi) do occur: Consider the special case $I = \mathcal{I}$. First of all, it is clear that $\mathcal{E}^{\mathcal{I}}(K) = \mathcal{E}(K)$ if there is only one prime of K lying above p. But there are also a lot of fields K such that there exist $\mathbb{Z}_p$-extensions L/K in which some of the primes $\mathfrak{p}_i \in \mathcal{I}$ above p are unramified. We will now give an example.

Example 3.21. Consider a number field K. Then

$$[K:\mathbb{Q}] \;=\; \sum_{\mathfrak{p}\,|\,(p)} [K_{\mathfrak{p}} : \mathbb{Q}_p]$$

(see [Neu 92], Corollary II.8.4), where $K_{\mathfrak{p}}$ denotes the completion of K with respect to the non-archimedean absolute value induced by the prime $\mathfrak{p}$, respectively. For any finite extension $K_{\mathfrak{p}}$ of $\mathbb{Q}_p$, we have

$$K_{\mathfrak{p}}^* \;\cong\; \mathbb{Z} \oplus \mathbb{Z}/(p-1)\mathbb{Z} \oplus \mathbb{Z}/p^a\mathbb{Z} \oplus \mathbb{Z}_p^d\,,$$

where $d = [K_\mathfrak{p} : \mathbb{Q}_p]$, and where $a \geq 0$ is the greatest integer k such that $K_\mathfrak{p}$ contains a primitive p^k-th root of unity (compare [Neu 92], Theorem II.5.7).
Now let us assume that p splits completely in $K/\mathbb{Q}$. Then the above degree formula implies that $[K_\mathfrak{p} : \mathbb{Q}_p] = 1$ for every $\mathfrak{p}$ dividing p. This means that $K_\mathfrak{p} = \mathbb{Q}_p$ for all $\mathfrak{p}$. Therefore, we have $d = 1$ and $a = 0$ in the decomposition of $K_\mathfrak{p}^*$, since $\mathbb{Q}_p$ does not contain any p-power root of unity (see [Gou 97], Prop. 3.4.2). This means that for every $\mathfrak{p} \mid p$,

$$K_\mathfrak{p}^* \;\cong\; \mathbb{Z} \oplus \mathbb{Z}/(p-1)\mathbb{Z} \oplus \mathbb{Z}_p \;\cong\; \mathbb{Z} \oplus U(K_\mathfrak{p}) \;,$$

where $U(K_\mathfrak{p}) := \{x \in K_\mathfrak{p} \;:\; |x|_\mathfrak{p} \leq 1\}$. Here $|\,.\,|_\mathfrak{p}$ denotes the absolute value induced by $\mathfrak{p}$. We have thus shown that the $\mathbb{Z}_p$-rank of (the pro-p-part of) $U(K_\mathfrak{p})$ is equal to 1 for every $\mathfrak{p} \mid p$.
Now let L/K be a $\mathbb{Z}_p^d$-extension, $d \geq 1$. For every prime $\mathfrak{p} \mid p$ of K, we consider the abelian extension $L_{\overline{\mathfrak{p}}}/K_\mathfrak{p}$, where $K_\mathfrak{p}$, as above, denotes the completion of K with respect to the absolute value induced by $\mathfrak{p}$, $\overline{\mathfrak{p}}$ is any prime of L lying above $\mathfrak{p}$ and $L_{\overline{\mathfrak{p}}} = \bigcup_i L_{i,\mathfrak{p}_i}$ is the union of the completions of the finite subextensions $L_i \subseteq L$ of K with respect to the primes $\mathfrak{p}_i := \overline{\mathfrak{p}} \cap L_i$, respectively.
If $\mathrm{T}_{\overline{\mathfrak{p}}|\mathfrak{p}}(L/K)$ denotes the inertia subgroup of $\overline{\mathfrak{p}}$ over K, then we have an isomorphism $\mathrm{T}_{\overline{\mathfrak{p}}|\mathfrak{p}}(L/K) \;\cong\; \mathrm{T}(L_{\overline{\mathfrak{p}}}/K_\mathfrak{p})$ (see [Neu 92], Theorem II.9.6). Here $\mathrm{T}(L_{\overline{\mathfrak{p}}}/K_\mathfrak{p})$ denotes the inertia group of the Galois extension $L_{\overline{\mathfrak{p}}}/K_\mathfrak{p}$ of the local field $K_\mathfrak{p}$ in the sense of valuation theory: Let $v_\mathfrak{p}$ denote the normalised valuation induced by $\mathfrak{p}$, i.e., if $x \in K^*$ and $(x) = \mathfrak{p}^i \cdot \mathfrak{A}$ with $i \in \mathbb{Z}$ and $\mathfrak{A} \not\subseteq \mathfrak{p}$, then $v_p(x) = i$. Then $K_\mathfrak{p}$ is complete with regard to $v_\mathfrak{p}$, and there exists a unique extension w of $v_\mathfrak{p}$ to $L_{\overline{\mathfrak{p}}}$. We define the decomposition group

$$\mathrm{Z}(L_{\overline{\mathfrak{p}}}/K_\mathfrak{p}) := \{\sigma \in \mathrm{Gal}(L_{\overline{\mathfrak{p}}}/K_\mathfrak{p}) \mid w \circ \sigma = w\}$$

and the inertia subgroup

$$\mathrm{T}(L_{\overline{\mathfrak{p}}}/K_\mathfrak{p}) := \{\sigma \in \mathrm{Z}(L_{\overline{\mathfrak{p}}}/K_\mathfrak{p}) \mid \sigma(x) \equiv x \bmod \overline{\mathfrak{p}} \;\; \forall\, x \in L_{\overline{\mathfrak{p}}} \text{ with } w(x) \geq 0\,\} \;.$$

Now local class field theory (see [Wa 97], p. 403) implies that $\mathrm{T}(L_{\overline{\mathfrak{p}}}/K_\mathfrak{p})$ is isomorphic to a quotient of $U(K_\mathfrak{p})$ (we have to divide out the intersection of the norms $N_{L_{i,\mathfrak{p}_i}/K_\mathfrak{p}}(U(L_{i,\mathfrak{p}_i}))$ of all finite subextensions of $L_{\overline{\mathfrak{p}}}/K_\mathfrak{p}$). By the choice of K, the $\mathbb{Z}_p$-rank of $U(K_\mathfrak{p})$ is equal to 1, and so $\mathrm{rank}_{\mathbb{Z}_p}(\mathrm{T}_{\overline{\mathfrak{p}}|\mathfrak{p}}(L/K)) \leq 1$ for every $\overline{\mathfrak{p}} \mid \mathfrak{p}$.
In particular, if L/K denotes the composite of all $\mathbb{Z}_p$-extensions of K (see Section 2.1), then $\mathrm{Gal}(L/K) \cong \mathbb{Z}_p^d$ with $d \geq r_2(K) + 1$ (see Theorem 1.7). If we assume that $r_2(K) \geq 1$, i.e., that K is not totally real, then $d \geq 2$.
For every prime $\mathfrak{p}_i$ of K lying above p, the $\mathbb{Z}_p$-rank of the inertia group

$$\mathrm{T}_i \;:=\; \mathrm{T}_{\overline{\mathfrak{p}}_i|\mathfrak{p}_i}(L/K)$$

of any prime $\overline{\mathfrak{p}}_i$ of L dividing $\mathfrak{p}_i$ is less than or equal to 1, by the above. Therefore, letting $\tilde{M}^{(i)} := L^{\mathrm{T}_i}$ be the corresponding fixed field, we conclude that $\mathrm{rank}_{\mathbb{Z}_p}(\mathrm{Gal}(\tilde{M}^{(i)}/K)) \geq d-1 \geq 1$. This proves that there exists a $\mathbb{Z}_p$-extension $M^{(i)} \subseteq \tilde{M}^{(i)}$ of K in which $\mathfrak{p}_i$ is unramified.
To summarise, we have shown that if K is a number field, not totally real, in

which p splits completely, then for every prime $\mathfrak{p}_i$ of K dividing p (i.e., $\mathfrak{p}_i \in \mathcal{I}$ in the notation of Definition 3.17), there exists a $\mathbb{Z}_p$-extension $M^{(i)}/K$ such that $\mathfrak{p}_i$ is unramified in $M^{(i)}$ and therefore $M^{(i)} \in \mathcal{E}(K) \setminus \mathcal{E}^{\mathcal{I}}(K)$.
Furthermore, if $r_2(K) \geq 2$, then for every pair $(\mathfrak{p}_i, \mathfrak{p}_j)$ of primes lying above p, there exists a $\mathbb{Z}_p$-extension M of K such that $\mathfrak{p}_i$ and $\mathfrak{p}_j$ are unramified in M, i.e., $M \in \tilde{\mathcal{E}}^{\mathcal{I}\setminus\{\mathfrak{p}_i,\mathfrak{p}_j\}}(K)$. Indeed, the $\mathbb{Z}_p$-rank of the subgroup $\mathrm{T}_{i,j}$ of $\mathrm{Gal}(L/K)$ generated by T_i and T_j is less or equal to 2, and therefore

$$\mathrm{rank}_{\mathbb{Z}_p}(\mathrm{Gal}(L^{\mathrm{T}_{i,j}}/K)) \;\geq\; d-2 \;\geq\; r_2(K)+1-2 \;\geq\; 1\;.$$

More generally, this shows that there exist number fields K and $\mathbb{Z}_p$-extensions of K in which arbitrarily many primes lying above p are unramified.

Lemma 3.18 enables us to prove the following generalisation of Theorem 3.2:

Corollary 3.22. *Let L/K be a $\mathbb{Z}_p$-extension. We define, for any $n \in \mathbb{N}_0$,*

$$U(L,n) \;:=\; \mathcal{E}(L,n) \cap \tilde{\mathcal{E}}^{\mathcal{P}(L)}(K)\;,$$

where $\mathcal{E}(L,n) = \{M \in \mathcal{E}(K) \mid [(M \cap L) : K] \geq p^n\}$, as usual.
If $n \geq e(L/K)+1$, then e is locally constant on $U(L,n)$. Moreover,

(i) If $\mu(L/K) = \lambda(L/K) = 0$, then there exists an integer $n_0 \geq e(L/K)+1$ such that $\mu(M/K) = \lambda(M/K) = 0$ and $\nu(M/K) = \nu(L/K)$ for every $M \in U(L,n_0)$. In other words, the Iwasawa invariants are constant on $U(L,n_0)$.

(ii) If $\mu(L/K) = 0$, then there exists an integer $n_0 \geq e(L/K)+1$ such that $\mu(M/K) = 0$ for every $M \in U(L,n_0)$, i.e., μ is constant on $U(L,n_0)$.

Proof. The first statement is obvious, since Lemma 3.16, (i) implies that we have $\mathcal{P}(M) = \mathcal{P}(L)$ for every $M \in U(L,n)$, provided that $n \geq e(L/K)+1$. Now we can copy the proof of Theorem 3.2:

For (i), note that $\mu(L/K) = \lambda(L/K) = 0$ implies that there exists an integer $n_0 \geq e(L/K)+1$ such that $|A_m^{(L)}| = |A_{n_0}^{(L)}|$ for every $m \geq n_0$ (see Theorem 1.32). Then we can use Fukuda's Theorem to deduce $|A_m^{(M)}| = |A_{n_0}^{(L)}|$ for every $M \in U(L,n_0+1)$ and $m \geq n_0$, and therefore $\mu(M/K) = \lambda(M/K) = 0$ and $p^{\nu(M/K)} = |A_{n_0}^{(M)}| = |A_{n_0}^{(L)}| = p^{\nu(L/K)}$ for every $M \in U(L,n_0+1)$.

In order to prove (ii), we use the fact that $\mu(L/K) = 0$ if and only if the p-ranks of the $A_n^{(L)}$ remain bounded as n tends to ∞, which again is equivalent to saying that there exists an integer $n_0 \in \mathbb{N}$ such that $\mathrm{rank}_p(A_m) = \mathrm{rank}_p(A_{n_0})$ for every $m \geq n_0$, as we have shown in the proof of Theorem 3.2, (ii). Now we can use the second statement of Fukuda's Theorem 3.1 and continue as in the proof of (i). □

Remarks 3.23.

(1) Of course the statements of the corollary are non-trivial only for $\mathbb{Z}_p$-extensions L/K such that $\tilde{\mathcal{E}}^{\mathcal{P}(L)}(K)$ is infinite. Note that for any set $I \subseteq \mathcal{I}$, the condition that $\mathcal{E}^I(K)$ is finite is equivalent to saying that $|\mathcal{E}^I(K)| \leq 1$. Indeed, if there exist at least two different $\mathbb{Z}_p$-extensions L and M with

$\mathcal{P}(L) = I = \mathcal{P}(M)$, then we can consider the composite $L \cdot M$, and Lemma 3.19, (ii) yields the existence of infinitely many elements of $\mathcal{E}^I(K)$ being contained in $L \cdot M$.

(2) If $\mathcal{P}(L) = \mathcal{I}$, then $U(L,n) = \mathcal{E}(L,n)$ for every $n \geq e(L/K) + 1$. One drawback of Corollary 3.22 is the fact that for $\mathcal{P}(L) \subsetneqq \mathcal{I}$, we make a prediction on the $M \in U(L,n)$, but not on the larger and canonical set $\mathcal{E}(L,n)$.

(3) If there is only one prime of K lying above p, then $\mathcal{E}(K) = \mathcal{E}^{\mathcal{I}}(K)$, and so we obtain Theorem 3.2 as a special case of the above corollary.
If $|\mathcal{I}| = 2$, i.e., there are exactly two primes $\mathfrak{p}_1$ and $\mathfrak{p}_2$ of K which divide p, then we have a decomposition

$$\mathcal{E}(K) \;=\; \mathcal{E}^{\{\mathfrak{p}_1\}}(K) \;\dot{\bigcup}\; \mathcal{E}^{\{\mathfrak{p}_2\}}(K) \;\dot{\bigcup}\; \mathcal{E}^{\mathcal{I}}(K)$$

into disjoint sets. If the first two sets are empty (which does happen, see Lemma 3.30, (i) below), then $\mathcal{E}^{\mathcal{I}}(K) = \mathcal{E}(K)$, and $U(L,n) = \mathcal{E}(L,n)$ for each $L \in \mathcal{E}(K)$ and every $n \in \mathbb{N}_0$.
If one of the first two sets is infinite, we can apply Corollary 3.22 in order to obtain information about the corresponding $\mathbb{Z}_p$-extensions L/K with $\mathcal{P}(L) = \{\mathfrak{p}_i\}$ which is not covered by Theorem 3.2.

(4) If L/K denotes a $\mathbb{Z}_p$-extensions with $|\mathcal{P}(L)| = 1$, then there is an effective upper bound on $e(L/K)$, given by the exponent of the Galois group of the Hilbert class field of K over K.

(5) Note that for $L \notin \mathcal{E}^{\mathcal{I}}(K)$, the sets $U(L,n)$ will not be open in the sense of Greenberg's topology (compare Lemma 3.18, (iii)), and therefore Corollary 3.22 does not imply that the sets

$$\{L \in \mathcal{E}(K) \mid \mu(L/K) = \lambda(L/K) = 0\}$$

or

$$\{L \in \mathcal{E}(K) \mid \mu(L/K) = 0\}$$

are Greenberg open, as was the statement of Theorem 3.2 in the case $|\mathcal{I}| = 1$. We will now define a modified topology on $\mathcal{E}(K)$ that allows us to get a result analogous to Theorem 3.2.

Definition 3.24. For every $\mathbb{Z}_p$-extension L of K and any $n \in \mathbb{N}_0$, we let

$$\begin{aligned} U(L,n) &:= \mathcal{E}(L,n) \cap \tilde{\mathcal{E}}^{\mathcal{P}(L)}(K) \\ &= \{M \in \mathcal{E}(K) \mid [(M \cap L) : K] \geq p^n \text{ and } \mathcal{P}(M) \subseteq \mathcal{P}(L)\}\,, \end{aligned}$$

as in Corollary 3.22. Then the $U(L,n)$ generate a topology on $\mathcal{E}(K)$ (see Lemma 3.25 below), which we call the ***Greenberg-R-topology***.

Using this terminology, Corollary 3.22 can be restated as follows:

Corollary 3.22': *The sets*

$$\{L \in \mathcal{E}(K) \mid \mu(L/K) = \lambda(L/K) = 0\}$$

and

$$\{L \in \mathcal{E}(K) \mid \mu(L/K) = 0\}$$

are open with regard to the Greenberg-R-topology.

Lemma 3.25.
(i) *The sets $U(L,n)$, with $L \in \mathcal{E}(K)$ and $n \in \mathbb{N}_0$, generate a topology on $\mathcal{E}(K)$.*
(ii) *For every L and n, $U(L,n)$ is closed with respect to Greenberg's topology. It is Greenberg open if and only if $\mathcal{P}(L) = \mathcal{I}$.*
(iii) *e is constant on $U(L,n)$ if $n \geq e(L/K)+1$.*
(iv) *The set $\mathcal{E}(K)$ of all $\mathbb{Z}_p$-extensions of K is compact with respect to the Greenberg-R-topology if and only if $\mathcal{E}(K) = \mathcal{E}^{\mathcal{I}}(K)$.*

Proof. (i) First of all, $\mathcal{E}(K) = U(K_\infty, 0)$, where K_∞ denotes the cyclotomic $\mathbb{Z}_p$-extension of K. We will show now that for any $L, M \in \mathcal{E}(K)$ and arbitrary $n, m \in \mathbb{N}_0$, the set $U(L,n) \cap U(M,m)$ is a (possibly empty) finite union of sets $U(N_i, n_i)$. Then $\{U(L,n) \mid L \in \mathcal{E}(K), n \in \mathbb{N}_0\}$ generate a topology on $\mathcal{E}(K)$.
We may assume that $n \geq m$. If $M \notin \mathcal{E}(L,m)$, then $U(L,n) \cap U(M,m) = \emptyset$. Otherwise, we have

$$\begin{aligned} U(L,n) \cap U(M,m) &= \mathcal{E}(L,n) \cap \tilde{\mathcal{E}}^{\mathcal{P}(L)}(K) \cap \tilde{\mathcal{E}}^{\mathcal{P}(M)}(K) \\ &= \mathcal{E}(L,n) \cap \tilde{\mathcal{E}}^{\mathcal{P}(L)\cap\mathcal{P}(M)}(K)\ . \end{aligned}$$

If there does not exist any $\mathbb{Z}_p$-extension $N \in \mathcal{E}(L,n)$ satisfying

$$\mathcal{P}(N) \subseteq \mathcal{P}(L) \cap \mathcal{P}(M)\ ,$$

then again $U(L,n) \cap U(M,m) = \emptyset$. Otherwise, we choose sets

$$I_1, \ldots, I_r \subseteq \mathcal{P}(L) \cap \mathcal{P}(M)$$

such that

- for every $i = 1, \ldots, r$, there exists an element $N_i \in \mathcal{E}(L,n)$ with $\mathcal{P}(N_i) = I_i$, and
- for every $N \in \mathcal{E}(L,n)$ with $\mathcal{P}(N) \subseteq \mathcal{P}(L) \cap \mathcal{P}(M)$, there exists an $i \in \{1, \ldots, r\}$ such that $\mathcal{P}(N) \subseteq I_i$.

Then it is easy to see that $U(L,n) \cap U(M,m) = \bigcup_{i=1}^{r} U(N_i, n)$.

(ii) Since $U(L,n) = \mathcal{E}(L,n) \cap \tilde{\mathcal{E}}^{\mathcal{P}(L)}(K)$, the assertions follow from Lemma 3.18, (i), (iii) and (v).

(iii) Compare the proof of Corollary 3.22.

(iv) We obviously have

$$\mathcal{E}(K) \subseteq \bigcup_{\substack{L \in \mathcal{E}(K) \\ n \geq e(L/K)+1}} U(L,n)\ ,$$

and by (iii), e is constant on every $U(L,n)$ occurring on the right hand side. This means that e would be globally bounded on $\mathcal{E}(K)$ if this set was compact with respect to the Greenberg-R-topology, since in this case, it could be covered by finitely many of the $U(L,n)$. But we have seen in Lemma 3.18, (vi) that e is unbounded if $\mathcal{E}(K) \neq \mathcal{E}^{\mathcal{I}}(K)$.

If, on the other hand, $\mathcal{E}(K) = \mathcal{E}^{\mathcal{I}}(K)$, then $U(L,n) = \mathcal{E}(L,n)$ for every $\mathbb{Z}_p$-extension L of K and every $n \in \mathbb{N}_0$, respectively, i.e., the Greenberg-R-topology and the Greenberg topology coincide, and $\mathcal{E}(K)$ is compact by Lemma 2.26.

□

Remarks 3.26.

(1) The proof of the last part of Lemma 3.25 shows that whenever we have $\mathcal{E}(K) \supsetneqq \mathcal{E}^{\mathcal{I}}(K)$, i.e., the classical theorem of Fukuda does not apply in general, and whenever $\mathcal{T}$ is a topology on $\mathcal{E}(K)$ such that e is locally constant (or even only locally bounded) with respect to $\mathcal{T}$ – which implies that we can nevertheless use Fukuda-like arguments to study the local behaviour of Iwasawa's invariants –, then $\mathcal{E}(K)$ cannot be compact with regard to the topology $\mathcal{T}$, and so we cannot gather global information such as the boundedness of some invariant on the whole set $\mathcal{E}(K)$.
More briefly: there seems to be no topology on $\mathcal{E}(K)$ that allows dealing with local and global properties of Iwasawa invariants simultaneously.

(2) If $\mathbb{K}/K$ denotes a $\mathbb{Z}_p^k$-extension, $k \in \mathbb{N}$, and if $\mathcal{E}^{\subseteq \mathbb{K}}(K)$ consists of the $\mathbb{Z}_p$-extensions of K contained in $\mathbb{K}$, then $\mathcal{E}^{\subseteq \mathbb{K}}(K)$ is compact with respect to the Greenberg-R-topology if and only if every $M \in \mathcal{E}^{\subseteq \mathbb{K}}(K)$ has the same ramification set $\mathcal{P}(M) = P$, $P \subseteq \mathcal{I}$ fixed. This can be proved analogously to Lemma 3.25, (iv) by using Lemma 3.18, (vi) and noting that Greenberg's Lemma 2.26 actually remains valid in this more general situation, i.e., the set $\mathcal{E}^{\subseteq \mathbb{K}}(K)$ is compact with respect to Greenberg's topology.

(3) For every $L, M \in \mathcal{E}(K)$ and each $n \in \mathbb{N}$, we know that $L \in \mathcal{E}(M,n)$ if and only if $M \in \mathcal{E}(L,n)$. This is not longer the case if we consider the $U(L,n)$, at least if $\mathcal{E}(K) \neq \mathcal{E}^{\mathcal{I}}(K)$. This missing symmetry, resulting from the ramification condition in the definition of the $U(L,n)$, shows that there will not be a metric on $\mathcal{E}(K)$ lying behind the Greenberg-R-topology. Note that on the contrary the classical Greenberg topology is induced by

$$d(L,M) := \begin{cases} 0 & : L = M \\ p^{-n(L,M)} & : L \neq M \end{cases},$$

where $n(L,M)$ is determined by $[(L \cap M) : K] = p^{n(L,M)}$, compare Section 2.3.

We want to study which subsets of $\mathcal{I}$ typically appear as ramification sets of $\mathbb{Z}_p$-extensions of K. We will show that in general, it is likely to have $\mathcal{E}^I(K) = \emptyset$ for at least some subsets $I \subseteq \mathcal{I} = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_t\}$.

Lemma 3.27. *Let K be a number field, let $\mathbb{K}$ denote the composite of the $\mathbb{Z}_p$-extensions of K. Then $\mathbb{K}/K$ is a $\mathbb{Z}_p^d$-extension, for some $d \in \mathbb{N}$.*

(i) Let us denote by a_i the rank *of $\mathcal{E}^{\{\mathfrak{p}_i\}}(K)$, $i = 1, \ldots, t$, i.e., the maximal number of pairwise independent $\mathbb{Z}_p$-extensions $M \in \mathcal{E}^{\{\mathfrak{p}_i\}}(K)$. Then $\sum_{i=1}^{t} a_i \leq d$. In particular, at most d of the sets $\mathcal{E}^{\{\mathfrak{p}_i\}}(K)$ are non-empty.*

(ii) *More generally, if* $I_1, \ldots, I_k \subseteq \mathcal{I}$ *denote subsets such that* $I_j \cap (\bigcup_{i \neq j} I_i) = \emptyset$ *for each* $1 \leq j \leq k$, *then* $\sum_{i=1}^{k} \mathrm{rank}(\mathcal{E}^{I_i}(K)) \leq d$, *where* $\mathrm{rank}(\mathcal{E}^{I_i}(K))$ *denotes the maximal number of pairwise independent* $M \in \mathcal{E}^{I_i}(K)$, *respectively.*

(iii) *For every* $\mathfrak{p}_i \in \mathcal{I}$, *we let* $\mathfrak{P}_i$ *be any fixed prime of* $\mathbb{K}$ *lying above* $\mathfrak{p}_i$. *Let* $\mathrm{T}_i := \mathrm{T}_{\mathfrak{P}_i|\mathfrak{p}_i}(\mathbb{K}/K)$ *denote the inertia subgroup of* $\mathfrak{P}_i$ *in* $\mathbb{K}/K$, $1 \leq i \leq t$. *If* $\mathrm{T}_i = \{0\}$, *then* $\mathcal{E}^{\{\mathfrak{p}_i\}}(K) = \emptyset$.
More generally, if $\mathrm{rank}(\mathcal{E}^{\{\mathfrak{p}_i\}}(K)) = a_i \in \mathbb{N}_0$, *then* $\mathrm{rank}_{\mathbb{Z}_p}(\mathrm{T}_i) \geq a_i$.

Proof. (i) This is a special case of (ii).

(ii) Let $I_1, I_2 \subseteq \mathcal{I}$ denote subsets such that $I_1 \cap I_2 = \emptyset$. Let $L^{(i)}$ denote the composite of all $\mathbb{Z}_p$-extensions of K contained in $\mathcal{E}^{I_i}(K)$, $i = 1, 2$. Then $L^{(1)} \cap L^{(2)}$ is a finite extension of K, since every $\mathbb{Z}_p$-extension M of K contained in $L^{(i)}$ satisfies $\mathcal{P}(M) \subseteq I_i$, respectively. Therefore

$$\mathrm{Gal}((L^{(1)} \cdot L^{(2)})/K) \;\cong\; \mathbb{Z}_p^{r_1+r_2} \,,$$

where $r_i = \mathrm{rank}(\mathcal{E}^{I_i}(K))$, respectively, i.e., $\mathrm{Gal}(L^{(i)}/K) \cong \mathbb{Z}_p^{r_i}$, $i = 1, 2$. Inductively, if $k \in \mathbb{N}$, $I_1, \ldots, I_k \subseteq \mathcal{I}$ denote subsets such that

$$I_j \;\cap\; (\bigcup_{i \neq j} I_i) = \emptyset$$

for each $1 \leq j \leq k$, and if $L^{(i)}$ denotes the composite of the $\mathbb{Z}_p$-extensions of K contained in $\mathcal{E}^{I_i}(K)$, $1 \leq i \leq k$, then

$$\mathrm{Gal}((L^{(1)} \cdot \ldots \cdot L^{(k)})/K) \;\cong\; \mathbb{Z}_p^{r_1+\ldots+r_k} \,,$$

where $r_i = \mathrm{rank}(\mathcal{E}^{I_i}(K))$, $1 \leq i \leq k$.
Indeed, suppose that the statement is true for $k-1$. Then $L^{(1)} \cdot \ldots \cdot L^{(k-1)}$ is a $\mathbb{Z}_p^{r_1+\ldots+r_{k-1}}$-extension of K. Since $I_k \cap (\bigcup_{i=1}^{k-1} I_i) = \emptyset$, each prime $\mathfrak{p} \in I_k$ is unramified in $(L^{(1)} \cdot \ldots \cdot L^{(k-1)})/K$, and therefore $L^{(k)} \cap (L^{(1)} \cdot \ldots \cdot L^{(k-1)})$ is finite over K. In other words,

$$\mathrm{Gal}((L^{(1)} \cdot \ldots \cdot L^{(k)})/K) \;\cong\; \mathbb{Z}_p^{r_1+\ldots+r_k} \,,$$

proving our claim. Assertion (ii) follows because $(L^{(1)} \cdot \ldots \cdot L^{(k)}) \subseteq \mathbb{K}$.

(iii) We first note that the subfield

$$\tilde{K} \;:=\; \mathbb{K}^{\prod_{i=1}^{t} \mathrm{T}_i}$$

of $\mathbb{K}$ fixed by the smallest subgroup of $\mathrm{Gal}(\mathbb{K}/K)$ generated by all the inertia subgroups T_i (which is simply $\prod_i \mathrm{T}_i$, since $\mathrm{Gal}(\mathbb{K}/K)$ is abelian) has to be a finite extension of K, since every prime of $\mathcal{I}$ is unramified in $\tilde{K}$, and therefore

$$[\tilde{K} : K] \;\leq\; [H(K) : K] \;<\; \infty \,,$$

where $H(K)$ denotes the maximal unramified p-abelian extension of K.

Therefore $\mathrm{rank}_{\mathbb{Z}_p}(\prod_{i=1}^{t} \mathrm{T}_i) = d$. But this implies that we have, for any fixed $i \in \{1, \ldots, t\}$,

$$\begin{aligned} \mathrm{T}_i = \{0\} &\iff \mathrm{rank}_{\mathbb{Z}_p}(\mathrm{T}_i) = 0 \\ &\implies \mathrm{rank}_{\mathbb{Z}_p}(\prod_{j \neq i} \mathrm{T}_j) = d \\ &\iff L^{(i)} := \mathbb{K}^{\prod_{j \neq i} \mathrm{T}_j} \text{ is a finite extension of } K \\ &\iff \mathcal{E}^{\{\mathfrak{p}_i\}}(K) = \emptyset\,, \end{aligned}$$

noting that a $\mathbb{Z}_p$-extension M of K is contained in $L^{(i)}$ if and only if $M \in \mathcal{E}^{\{\mathfrak{p}_i\}}(K)$.
More generally, $\mathrm{rank}_{\mathbb{Z}_p}(\mathcal{E}^{\{\mathfrak{p}_i\}}(K)) = a_i$ implies that there exists a $\mathbb{Z}_p^{a_i}$-extension $M^{(i)}$ of K such that $M^{(i)} \subseteq \mathbb{K}^{\prod_{j \neq i} \mathrm{T}_j}$. This is equivalent to the fact that

$$\mathrm{rank}_{\mathbb{Z}_p}(\prod_{j \neq i} \mathrm{T}_j) \;\leq\; d - a_i\,.$$

Since $\mathrm{rank}_{\mathbb{Z}_p}(\prod_i \mathrm{T}_i) = d$, by the above, this implies that $\mathrm{rank}_{\mathbb{Z}_p}(\mathrm{T}_i) \geq a_i$. Note that the reverse conclusion of this last step in general will not be true, since the subgroups $\mathrm{T}_i \subseteq \mathrm{Gal}(\mathbb{K}/K)$ might have non-trivial intersection.
□

In particular, if K denotes a number field such that $|\mathcal{I}| > d$, then Lemma 3.27, (i) implies that $\mathcal{E}^{\{\mathfrak{p}_i\}}(K) = \emptyset$ for at least some of the $\mathfrak{p}_i \in \mathcal{I}$. Using class field theory, we will be able to get much more precise information about the sets $\mathcal{E}^I(K)$ and $\tilde{\mathcal{E}}^I(K)$. Starting point will be the following lemma, which is a direct generalisation of [La 90], Chapter 5, Theorem 5.1, and [Wa 97], Corollary 13.6 (compare Lemma 1.8):

Lemma 3.28. *Let $\mathbb{K}$ denote the composite of all $\mathbb{Z}_p$-extensions of K. Let $I \subseteq \mathcal{I}$ be a set of primes of K dividing p. Assume that L/K denotes the maximal p-abelian extension of K which is contained in $\mathbb{K}$ and unramified outside I. Then*

$$\begin{aligned} \mathrm{Gal}(L/K) &\sim \textit{ p-part of } (\prod_{\mathfrak{p} \in I} U_{\mathfrak{p}}) \,/\, \overline{\psi_I(E)} \\ &\cong (\prod_{\mathfrak{p} \in I} U_{\mathfrak{p}}^{(1)}) \,/\, (\overline{\psi_I(E)} \cap \prod_{\mathfrak{p} \in I} U_{\mathfrak{p}}^{(1)})\,, \end{aligned}$$

where the first map is a pseudo-isomorphism*, i.e., a homomorphism with finite kernel and cokernel (compare Definition 1.19). Here E denotes the set of units of K, $U_{\mathfrak{p}}$ and $U_{\mathfrak{p}}^{(1)}$ are the sets of units, respectively, 1-units, in the completion $K_{\mathfrak{p}}$ of K, and $\overline{\psi_I(E)}$ denotes the closure (with respect to the product topology on $\prod_{\mathfrak{p} \in I} U_{\mathfrak{p}}$) of E under the diagonal embedding $\psi_I : E \hookrightarrow \prod_{\mathfrak{p} \in I} U_{\mathfrak{p}}$ mapping $\varepsilon \mapsto (\varepsilon, \ldots, \varepsilon)$.*
Moreover, if $k \subseteq K$ denotes a subfield of K such that K/k is galois, and if $\sigma(I) \subseteq I$ for every $\sigma \in \mathrm{Gal}(K/k)$, then the above pseudo-isomorphism actually is a homomorphism of $\mathbb{Z}_p[\mathrm{Gal}(K/k)]$-modules.

Proof. The proof is analogous to the proofs of the above-mentioned theorems (which deal with the special case $I = \mathcal{I}$). First of all, since L/K is an abelian p-extension, class field theory implies that

$$\mathrm{Gal}(L/K) \;\cong\; C_K/H_L \;,$$

where C_K denotes the group of idèle classes of K and $H_L \subseteq C_K$ is a closed subgroup associated to L/K (compare, for example, Theorem 14 in the appendix of [Wa 97]). Moreover, a prime $\mathfrak{q}$ of K is unramified in L/K if and only if $U_\mathfrak{q} \cdot K^*/K^* \subseteq H_L$ (by the same theorem).

Since $\mathbb{K}/K$ is of finite index in the maximal p-abelian p-ramified extension of K (compare [Wa 97], p. 269), the definition of L implies that $\mathrm{Gal}(L/K)$ is pseudo-isomorphic to (the p-part of) $J_K/((\prod_{\mathfrak{p}\notin I} U_\mathfrak{p}) \cdot K^*)$, where J_K denotes the group of idèles of K (i.e., $C_K = J_K/K^*$). Here the product runs over all (finite and infinite) primes $\mathfrak{p}$ of K that are not contained in I and therefore are unramified in L/K.

Now we consider the inclusions

$$J_K \;\supseteq\; (\prod_{\mathfrak{p}\in I} U_\mathfrak{p} \cdot \prod_{\mathfrak{p}\notin I} U_\mathfrak{p}) \cdot K^* \;\supseteq\; \overline{(\prod_{\mathfrak{p}\notin I} U_\mathfrak{p}) \cdot K^*} \;,$$

where the closure is taken with respect to the canonical topology on J_K. Note that $(\prod_\mathfrak{p} U_\mathfrak{p}) \cdot K^*$ is a closed subgroup of J_K. The quotient of the first two groups $J_K/\prod_{\mathfrak{p}\in I} U_\mathfrak{p} \cdot \prod_{\mathfrak{p}\notin I} U_\mathfrak{p} \cdot K^*$ is isomorphic to the ideal class group of K and is therefore finite (see [Neu 92], Theorem VI.1.3). The quotient group of the last two groups is

$$\prod_{\mathfrak{p}\in I} U_\mathfrak{p} \cdot \prod_{\mathfrak{p}\notin I} U_\mathfrak{p} \cdot K^* \,/\, \overline{\prod_{\mathfrak{p}\notin I} U_\mathfrak{p} \cdot K^*} \;\cong\; \prod_{\mathfrak{p}\in I} U_\mathfrak{p} \,/\, (\prod_{\mathfrak{p}\in I} U_\mathfrak{p} \cap \overline{\prod_{\mathfrak{p}\notin I} U_\mathfrak{p} \cdot K^*}) \;.$$

In the next lemma, which is the analogon of Lemma 13.5 in [Wa 97], we will show that

$$\prod_{\mathfrak{p}\in I} U_\mathfrak{p} \cap \overline{\prod_{\mathfrak{p}\notin I} U_\mathfrak{p} \cdot K^*} \;=\; \overline{\psi_I(E)} \;,$$

where ψ_I is defined in the statement of Lemma 3.28. This proves the existence of the desired pseudo-isomorphism.

Moreover, if $k \subseteq K$ is a subfield such that K/k is galois, then also L/k is galois, by the maximality of L. Since L/K is abelian, $\mathrm{Gal}(K/k)$ acts on $\mathrm{Gal}(L/K)$ by conjugation, as in Section 1.3.

Now we describe the action of $\mathrm{Gal}(K/k)$ on

$$U_I \;:=\; \prod_{\mathfrak{p}\in I} U_\mathfrak{p} \;\subseteq\; \prod_{\mathfrak{p}\in I} K_\mathfrak{p} =: \mathcal{K}_I \;.$$

We define an absolute value on $\mathcal{K}_I$ by letting $d(x) := \max_\mathfrak{p}(|x_\mathfrak{p}|_\mathfrak{p})$ for every $x = (x_\mathfrak{p})_{\mathfrak{p}\in I} \in \mathcal{K}_I$.

By the Approximation Theorem (see [Neu 92], Theorem II.3.4), $K \subseteq \mathcal{K}_I$, embedded diagonally, is dense with respect to the above absolute value. Therefore, every element $x = (x_\mathfrak{p})_{\mathfrak{p}\in I} \in \mathcal{K}_I$ can be viewed as the limit $x = \lim_n x_n$ of a

sequence of elements $x_n \in K$. Let now $\sigma \in \mathrm{Gal}(K/k)$. Then $\sigma(x) := \lim_n \sigma(x_n)$. We will now show that this is well-defined.

Since every component $K_\mathfrak{p}$ of $\mathcal{K}_I$ is complete with respect to the absolute value $|\,.\,|_\mathfrak{p}$, respectively, we immediately see that $\mathcal{K}_I$ is complete with respect to the absolute value d. In particular, a sequence in $\mathcal{K}_I$ converges with respect to d if and only if it satisfies the Cauchy condition. The convergence $x_n \longrightarrow x$ in $\mathcal{K}_I$ implies that for every $N \in \mathbb{N}$, there exists an integer $M \in \mathbb{N}$ such that $d(x_n - x_m) < p^{-N}$ for every $n, m \geq M$, i.e.,

$$x_n - x_m \in \mathfrak{p}^N \quad \text{for each } \mathfrak{p} \in I \ .$$

But then

$$\sigma(x_n) - \sigma(x_m) \in \sigma(\mathfrak{p})^N \quad \text{for each } \mathfrak{p} \in I \ ,$$

and therefore $\sigma(x_n) - \sigma(x_m) \in \mathfrak{p}^N$ for every $\mathfrak{p} \in I$, since $\sigma(I) \subseteq I$ for every $\sigma \in \mathrm{Gal}(K/k)$ and therefore in fact $\sigma(I) = I$ for each σ. This shows that $(\sigma(x_n))$ forms a Cauchy sequence with respect to d and therefore converges to an element $\sigma(x) \in \mathcal{K}_I$. Moreover, the limit $\sigma(x)$ does not depend on the choice of the sequence $x_n \longrightarrow x$, and therefore $\sigma(x)$ is well-defined.

It is easy to see that this defines a $\mathrm{Gal}(K/k)$-module structure on the quotient $(\prod_{\mathfrak{p}\in I} U_\mathfrak{p})/\overline{\psi_I(E)}$; it suffices to note that $\psi_I(E) \subseteq U_I$ are $\mathrm{Gal}(K/k)$-submodules of $\mathcal{K}_I$.

If $\mathfrak{q}$ denotes a prime of K and if $\sigma \in \mathrm{Gal}(K/k)$, then the Frobenius homomorphism of $\sigma(\mathfrak{q})$ is the conjugate of the Frobenius homomorphism of $\mathfrak{q}$ by a lift of σ to $\mathrm{Gal}(L/k)$ (compare [Rib 01], 25.(B)). Therefore the above pseudo-isomorphism

$$\mathrm{Gal}(L/K) \ \sim \ p\text{-part of } (\prod_{\mathfrak{p}\in I} U_\mathfrak{p})/\overline{\psi_I(E)}$$

translates the conjugation operation of $\mathrm{Gal}(K/k)$ on $\mathrm{Gal}(L/K)$ into the action on $(\prod_{\mathfrak{p}\in I} U_\mathfrak{p})/\overline{\psi_I(E)}$, because Artin's correspondence identifies an idèle

$$x = (x_\mathfrak{p})_{\mathfrak{p}\in I} \in \prod_{\mathfrak{p}\in I} U_\mathfrak{p} \hookrightarrow J_K$$

with the ideal $\prod_{\mathfrak{p}\in I} \mathfrak{p}^{v_\mathfrak{p}(x_\mathfrak{p})}$ of K (compare [Neu 92], p. 375). Therefore the pseudo-isomorphism actually is a $\mathbb{Z}_p[\mathrm{Gal}(K/k)]$-module homomorphism.

It remains to prove the following lemma.

Lemma 3.29. *With the above notation, we have*

$$\prod_{\mathfrak{p}\in I} U_\mathfrak{p} \cap \overline{\prod_{\mathfrak{p}\notin I} U_\mathfrak{p} \cdot K^*} = \overline{\psi_I(E)} \ .$$

Proof. We modify the proof of Lemma 13.5 in [Wa 97] in order to deal with our more general situation.

'$\supseteq$' : By definition, we have $\psi_I(E) \subseteq \prod_{\mathfrak{p}\in I} U_\mathfrak{p}$. We can regard $\psi_I(E)$ as a subgroup of $U := \prod_{\text{all } \mathfrak{p}} U_\mathfrak{p}$ in the following sense:

$$E \ni \varepsilon \ \mapsto \ (\psi_I(\varepsilon)) = \begin{Bmatrix} \varepsilon \in U_\mathfrak{p} & : \mathfrak{p} \in I \\ 1 \in U_\mathfrak{p} & : \mathfrak{p} \notin I \end{Bmatrix} \in U \ .$$

Using this identification, we can write

$$\psi_I(\varepsilon) \;=\; (\varepsilon)\cdot(\frac{\psi_I(\varepsilon)}{\varepsilon}) \;\in\; K^*\cdot\prod_{\mathfrak{p}\notin I} U_{\mathfrak{p}}\;,$$

since $\frac{\psi_I(\varepsilon)}{\varepsilon}$ has component 1 at all $\mathfrak{p}\in I$. Taking the closures in $\prod_{\mathfrak{p}\in I} U_{\mathfrak{p}}$, we obtain $\overline{\psi_I(E)} \subseteq \overline{K^*\cdot\prod_{\mathfrak{p}\notin I} U_{\mathfrak{p}}}\cap\prod_{\mathfrak{p}\in I} U_{\mathfrak{p}}$.

'$\subseteq$' : The sets $U_{\mathfrak{p}}^{(n)} := \{x\in U_{\mathfrak{p}} \mid x\equiv 1 \bmod \mathfrak{p}^n\}$ of n-units, $n\in\mathbb{N}$, form a basis of neighbourhoods of the unit element in $U_{\mathfrak{p}}$, respectively. Letting $U_I^{(n)} := \prod_{\mathfrak{p}\in I} U_{\mathfrak{p}}^{(n)}$, and denoting by $U^{(n)}$ the image of $U_I^{(n)}$ in U, respectively (i.e., putting 1 in all components $U_{\mathfrak{p}}$, $p\notin I$), we conclude that

$$\overline{K^*\cdot\prod_{\mathfrak{p}\notin I} U_{\mathfrak{p}}} \;=\; \bigcap_{n\geq 1}(K^*\cdot\prod_{\mathfrak{p}\notin I} U_{\mathfrak{p}}\cdot U^{(n)})$$

and $\overline{\psi_I(E)} \;=\; \bigcap\limits_{n\geq 1}(\psi_I(E)\cdot U^{(n)})$.

It therefore suffices to show that

$$\prod_{\mathfrak{p}\in I} U_{\mathfrak{p}}\cap(K^*\cdot\prod_{\mathfrak{p}\notin I} U_{\mathfrak{p}}\cdot U^{(n)}) \;\subseteq\; \psi_I(E)\cdot U^{(n)}$$

for every $n\geq 1$. Let $x\in K^*$, $u'\in\prod_{\mathfrak{p}\notin I} U_{\mathfrak{p}}$ and $u\in U^{(n)}$ be elements such that $x\cdot u'\cdot u\in\prod_{\mathfrak{p}\in I} U_{\mathfrak{p}} =: U_I$. Then we have $x\cdot u'\in U_I$, since $u\in U^{(n)}$, and therefore $x\cdot u'$ has component 1 at all $p\notin I$. Since $u'\in\prod_{\mathfrak{p}\notin I} U_{\mathfrak{p}}$ is a unit at these places, it follows that $x\in K^*$ is a local unit at every $\mathfrak{p}\notin I$.

On the other hand, u' has component 1 at all $\mathfrak{p}\in I$, and therefore $x\cdot u'\in U_I$ implies that x is also a unit at the places in I, i.e., x is a local unit at every place of K and therefore has to be a global unit (see [Neu 92], p.72). But then $x\cdot u'\in\psi_I(E)$, since it has component 1 at all $\mathfrak{p}\notin I$, and since the component at each $\mathfrak{p}\in I$ is given by the unit x, because $u'\in\prod_{\mathfrak{p}\notin I} U_{\mathfrak{p}}$. □

Returning to the proof of Lemma 3.28, we see that it remains to deal with the second isomorphism. But this canonical isomorphism simply arises from the fact that for every prime $\mathfrak{p}\in I$, we have $U_{\mathfrak{p}} \cong U_{\mathfrak{p}}^{(1)}\times C_{\mathfrak{p}}$, where $C_{\mathfrak{p}}$ is a finite group which does not contribute to the p-part (see [Neu 92], Theorem II.5.3). □

Using the previous results, we will now determine, in some cases, the structure of the sets $\mathcal{E}^I(K)$. We will consider number fields $K/\mathbb{Q}$ in which the rational prime p is completely decomposed. In this case it will be rather easy to obtain information about the size of the sets $\mathcal{E}^I(K)$ for small I.

Lemma 3.30. *Let K be a number field such that the fixed rational prime p splits completely in K.*

(i) If $K\neq\mathbb{Q}$ is not imaginary quadratic, then $\mathcal{E}^{\{\mathfrak{p}_i\}}(K)=\emptyset$, $i=1,\ldots,t$.

(ii) If K is imaginary quadratic, then $\mathcal{E}^{\{\mathfrak{p}_i\}}(K)$ contains exactly one element, $i=1,2$.

(iii) *Let $I \subseteq \mathcal{I}$ be a set such that $|I| = 2$. Then, under the assumptions of (i), we have $|\mathcal{E}^I(K)| \leq 1$.*

Note that if K is imaginary quadratic and $\mathcal{I} = I = \{\mathfrak{p}, \overline{\mathfrak{p}}\}$, then of course $|\mathcal{E}^I(K)| = \infty$, by (ii) and Lemma 3.18, (iii), since in fact $|\mathcal{E}(K) \setminus \mathcal{E}^I(K)| = 2$.

Proof. (i) Let $i \in \{1, \ldots, t\}$ be arbitrary, but fixed. Let $L^{(i)} \subseteq \mathbb{K}$ be the maximal p-abelian extension of K that is unramified outside the prime $\mathfrak{p}_i$. By Lemma 3.28, we have

$$\mathrm{Gal}(L^{(i)}/K) \sim p\text{-part of } U_{\mathfrak{p}_i}/\overline{\psi_i(E)} \cong U_{\mathfrak{p}_i}^{(1)}/(U_{\mathfrak{p}_i}^{(1)} \cap \overline{\psi_i(E)}) ,$$

where we let $\psi_i := \psi_{\{\mathfrak{p}_i\}}$ for simplification. Since p is totally decomposed in $K/\mathbb{Q}$, we have $\mathrm{rank}_{\mathbb{Z}_p}(U_{\mathfrak{p}_i}^{(1)}) = 1$ (see Example 3.21 and [Neu 92], Theorem II.5.7). Since $K \neq \mathbb{Q}$ is not imaginary quadratic, the $\mathbb{Z}$-rank of the set E of global units of K equals $r_1(K)+r_2(K)-1 \geq 1$ by Dirichlet's Unit Theorem, i.e., E is an infinite set. Therefore also $\psi_i(E)$ and $\overline{\psi_i(E)}$ are infinite, i.e., $\mathrm{rank}_{\mathbb{Z}_p}(\overline{\psi_i(E)}) \geq 1$. Since $\overline{\psi_i(E)} \cap U_{\mathfrak{p}_i}^{(1)} \subseteq U_{\mathfrak{p}_i}^{(1)}$ is a closed subgroup, it follows that it is of finite index in $U_{\mathfrak{p}_i}^{(1)}$, and therefore $\mathrm{Gal}(L^{(i)}/K)$ is finite, which implies that $\mathcal{E}^{\{\mathfrak{p}_i\}}(K) = \emptyset$.

(ii) If K is an imaginary quadratic field, then the arguments used for the proof of (i) remain valid, except that now the group E is finite. But then also the $\psi_i(E)$ are finite sets, and since $U_{\mathfrak{p}_i}^{(1)}$ is a Hausdorff space (see [Neu 92], p. 377), it follows that $\overline{\psi_i(E)} = \psi_i(E)$ has $\mathbb{Z}_p$-rank equal to 0. Therefore $\mathrm{Gal}(L^{(i)}/K)$ is pseudo-isomorphic to $\mathbb{Z}_p$, which proves that $|\mathcal{E}^{\{\mathfrak{p}_i\}}(K)| = 1$, $i = 1, 2$.

(iii) Assume that $|\mathcal{E}^I(K)| \geq 2$ for some ramification set $I = \{\mathfrak{p}_i, \mathfrak{p}_j\}$. Let L^1 and L^2 be two different $\mathbb{Z}_p$-extensions of K such that $\mathcal{P}(L^1) = I = \mathcal{P}(L^2)$. Let $M := L^1 \cdot L^2$, and consider the inertia subgroup $T \subseteq \mathrm{Gal}(M/K)$ of any prime $\mathfrak{P}_i$ of M lying above the prime $\mathfrak{p}_i \in I$. By class field theory, this inertia subgroup $T = \mathrm{T}_{\mathfrak{P}_i|\mathfrak{p}_i}(M/K)$ is isomorphic to a quotient of $U_{\mathfrak{p}_i}$ (compare Example 3.21), which has $\mathbb{Z}_p$-rank equal to 1 since p is totally decomposed in $K/\mathbb{Q}$. Therefore $\mathrm{rank}_{\mathbb{Z}_p}(T) \leq 1$, which means that there exists a $\mathbb{Z}_p$-extension $\tilde{M} \subseteq M$ of K contained in the fixed field M^T. In particular, $\mathfrak{p}_i$ is not ramified in $\tilde{M}/K$, and since $\tilde{M}/K$ cannot be unramified, we would conclude that $\mathcal{P}(\tilde{M}) = \{\mathfrak{p}_j\}$, in contradiction to the fact that $\mathcal{E}^{\{\mathfrak{p}_j\}}(K) = \emptyset$, by (i).

□

We will from now on assume that K is a CM-field.

Lemma 3.31. *Let K be a number field, and let p be an odd rational prime that splits completely in K. Assume that K is a CM-field, and that $[K : \mathbb{Q}] \geq 4$.*

(i) *Let $I \subseteq \mathcal{I}$ be such that $|I| = 2$. Then $|\mathcal{E}^I(K)| \leq 1$. In fact, $|\mathcal{E}^I(K)| = 1$ for the sets $I = \{\mathfrak{p}_i, \overline{\mathfrak{p}_i}\}$ consisting of a pair of complex conjugate primes of K.*

(ii) *More generally, if $I \subseteq \mathcal{I}$ is any subset that contains a number of $n_I \in \mathbb{N}_0$ pairs of complex conjugate primes $\{\mathfrak{p}_i, \overline{\mathfrak{p}_i}\}$ of K, then* $\operatorname{rank}(\tilde{\mathcal{E}}^I(K)) \geq n_I$. *Here the rank is defined to be the $\mathbb{Z}_p$-rank of the Galois group* $\operatorname{Gal}(L/K)$, *where $L \subseteq \mathbb{K}$ denotes the maximal p-abelian extension of K such that $\mathcal{P}(L) \subseteq I$, as in Lemma 3.27.*

(iii) *If $|I| > 2$ and $n_I \geq 1$, then* $\mathcal{E}^I(K) \neq \emptyset \iff |\mathcal{E}^I(K)| = \infty$.

(iv) *For every I, we have $\mathcal{E}^I(K) \neq \emptyset$ if and only if there exist $r_I := \operatorname{rank}(\tilde{\mathcal{E}}^I(K))$ many pairwise independent $\mathbb{Z}_p$-extensions in $\mathcal{E}^I(K)$.*

Proof. (i) We have shown in Lemma 3.30, (iii) that $|\mathcal{E}^I(K)| \leq 1$ whenever $|I| = 2$. Let now $I = \{\mathfrak{p}_i, \overline{\mathfrak{p}_i}\}$, let K^+ denote the maximal real subfield of K, and let j be a generator of $\operatorname{Gal}(K/K^+) \cong \mathbb{Z}/2\mathbb{Z}$, i.e., j is induced by the complex conjugation on $\mathbb{C}$. The automorphism j acts on the unit group E of K. If E^+ denotes the group of units of K^+, and if furthermore $E^- := \{\varepsilon \in E \mid j(\varepsilon) = \varepsilon^{-1}\}$, then $E^+ \cdot E^- \subseteq E$ is a subgroup of finite index, because for each unit $\varepsilon \in E$, we have $\varepsilon^2 = \varepsilon^{1+j} \cdot \varepsilon^{1-j} \in E^+ \cdot E^-$. Since K is a CM-field, we actually know that $[E : (W \cdot E^+)] \leq 2$ is finite, where W denotes the group of roots of unity contained in K (see [Wa 97], Theorem 4.13). But then also E^+ is of finite index in E, since W is a finite set. Using the notation from Lemma 3.28, this means that also $\psi_I(E^+)$ is of finite index in $\psi_I(E)$.
Recall that we have an action of j on

$$U_I := \prod_{\mathfrak{p} \in I} U_{\mathfrak{p}} \subseteq \prod_{\mathfrak{p} \in I} K_{\mathfrak{p}} =: \mathcal{K}_I ,$$

where $K_{\mathfrak{p}}$ denotes, as usual, the completion of K with respect to the prime $\mathfrak{p}$. We define an absolute value on $\mathcal{K}_I$ by letting $d(x) := \max_{\mathfrak{p}}(|x_{\mathfrak{p}}|_{\mathfrak{p}})$ for every $x = (x_{\mathfrak{p}})_{\mathfrak{p} \in I} \in \mathcal{K}_I$.
Since K/K^+ is normal and $j(I) = I$, we may proceed as in the proof of Lemma 3.28: Every element $x = (x_{\mathfrak{p}})_{\mathfrak{p} \in I} \in \mathcal{K}_I$ can be viewed as the limit $x = \lim_n x_n$ of a sequence of elements $x_n \in K$. We then define $j(x) = j_I(x) := \lim_n j(x_n)$.
It is easy to see that the map $x \mapsto j(x)$ yields an involution on $\mathcal{K}_I$, i.e., $j(j(x)) = x$, $j(x+y) = j(x)+j(y)$ and $j(x \cdot y) = j(x) \cdot j(y)$ for all $x, y \in \mathcal{K}_I$, with component-wise addition and multiplication.
We recall from the proof of Lemma 3.28 that the same construction of a conjugation isomorphism works for an arbitrary set $I \subseteq \mathcal{I}$ which is closed under conjugation (this means that for every prime $\mathfrak{p} \in I$, we also have $\overline{\mathfrak{p}} \in I$). This will be used in the proof of (ii) below.
Returning to the case $I = \{\mathfrak{p}_i, \overline{\mathfrak{p}_i}\}$, we look at an element

$$x = (u, v) \in U_I = U_{\mathfrak{p}_i} \times U_{\overline{\mathfrak{p}_i}} .$$

We choose a sequence $(x_n)_n \subseteq K$ such that $x = \lim_n x_n$. Then we have

$$x_n \xrightarrow{|\,.\,|_{\mathfrak{p}_i}} u \quad \text{(convergence in } K_{\mathfrak{p}_i})$$

and

$$x_n \xrightarrow{\ |\,.\,|_{\overline{\mathfrak{p}_i}}\ } v \quad \text{(convergence in } K_{\overline{\mathfrak{p}_i}})$$

simultaneously, by definition of the absolute value d on $\mathcal{K}_I$. This implies that

$$j(x_n) \xrightarrow{\ |\,.\,|_{\overline{\mathfrak{p}_i}}\ } j_{\overline{\mathfrak{p}_i}}(u) \quad \text{(convergence in } K_{\overline{\mathfrak{p}_i}})$$

and

$$j(x_n) \xrightarrow{\ |\,.\,|_{\mathfrak{p}_i}\ } j_{\mathfrak{p}_i}(v) \quad \text{(convergence in } K_{\mathfrak{p}_i})$$

for elements $j_{\mathfrak{p}_i}(v) \in K_{\mathfrak{p}_i}$ and $j_{\overline{\mathfrak{p}_i}}(u) \in K_{\overline{\mathfrak{p}_i}}$, so $j_I((u,v)) = (j_{\mathfrak{p}_i}(v), j_{\overline{\mathfrak{p}_i}}(u))$. In particular, letting

$$U_I^+ := \{x \in U_I \mid j_I(x) = x\} \quad \text{and} \quad U_I^- := \{x \in U_I \mid j_I(x) = x^{-1}\}\,,$$

we see that

$$U_I^+ := \{x \in U_I \mid x = (u, j_{\overline{\mathfrak{p}_i}}(u))\} \quad \text{and} \quad U_I^- := \{x \in U_I \mid x = (u, \frac{1}{j_{\overline{\mathfrak{p}_i}}(u)})\}\,,$$

since $j_{\mathfrak{p}_i}(j_{\overline{\mathfrak{p}_i}}(u)) = u$ by construction.
For $\varepsilon \in E^+$, i.e., $j(\varepsilon) = \varepsilon$, we obviously have $j_I(\psi_I(\varepsilon)) = \psi_I(\varepsilon)$, since $\psi_I(\varepsilon) \in U_I \subseteq \mathcal{K}_I$ can be represented by the constant sequence (ε). Therefore $\psi_I(E^+) \subseteq U_I^+$, and analogously $\psi_I(E^-) \subseteq U_I^-$. In view of Lemma 3.28, we are interested in the $\mathbb{Z}_p$-rank of (the p-part of) $(U_{\mathfrak{p}_i} \times U_{\overline{\mathfrak{p}_i}}) \,/\, \overline{\psi_I(E)}$. Since p is totally decomposed in $K/\mathbb{Q}$, we know that the $\mathbb{Z}_p$-ranks of $U_{\mathfrak{p}_i}$ and $U_{\overline{\mathfrak{p}_i}}$ both are equal to 1, and therefore $\mathrm{rank}_{\mathbb{Z}_p}(U_{\mathfrak{p}_i} \times U_{\overline{\mathfrak{p}_i}}) = 2$.
We will explain below that

$$\begin{aligned} \mathrm{rank}_{\mathbb{Z}_p}(U_I \,/\, \overline{\psi_I(E)}) &\overset{(\star)}{\geq} \mathrm{rank}_{\mathbb{Z}_p}(U_I^- \,/\, (\overline{\psi_I(E)} \cap U_I^-)) \\ &\overset{(\star\star)}{=} \mathrm{rank}_{\mathbb{Z}_p}(U_I^- \,/\, (\overline{\psi_I(E^-)} \cap U_I^-))\,. \end{aligned}$$

Since E^- and therefore also $\overline{\psi_I(E^-)} \subseteq U_I^-$ are finite, this latter rank is equal to 1 because $(U_{\mathfrak{p}_i} \times U_{\overline{\mathfrak{p}_i}})^- \cong U_{\mathfrak{p}_i}$ via the map $(u, \frac{1}{j_{\overline{\mathfrak{p}_i}}(u)}) \mapsto u$. This proves the existence of a $\mathbb{Z}_p$-extension M of K such that $\mathcal{P}(M) = I$, using Lemma 3.28 and noting that $\tilde{\mathcal{E}}^I(K) = \mathcal{E}^I(K)$ by Lemma 3.30, (i).
The inequality $(\star)$ is obvious in view of the surjective homomorphism

$$\varphi : U_I \,/\, \overline{\psi_I(E)} \longrightarrow U_I^- \,/\, (\overline{\psi_I(E)} \cap U_I^-)$$

induced by the inclusion $U_I^- \subseteq U_I$. Finally, the equality of ranks $(\star\star)$ results from the fact that $\overline{\psi_I(E^+)} \cap U_I^- \subseteq U_I^+ \cap U_I^-$ is finite.

(ii) This is proved analogously. We consider (the p-part of) $U_I/\overline{\psi_I(E)}$, with

$$I = \{\underbrace{\mathfrak{p}_1, \overline{\mathfrak{p}_1}, \ldots, \mathfrak{p}_{n_I}, \overline{\mathfrak{p}_{n_I}}}_{=:\,\tilde{I}}, \mathfrak{p}_{n_I+1}, \ldots, \mathfrak{p}_s\}$$

and

$$U_I \;=\; \underbrace{\prod_{i=1}^{n_I} U_{\mathfrak{p}_i} \times U_{\overline{\mathfrak{p}_i}}}_{=:\,U_{\tilde{I}}} \;\cdot\; \prod_{i=n_I+1}^{s} U_{\mathfrak{p}_i} \;\subseteq\; K_I \;=\; \prod_{\mathfrak{p}\in I} K_{\mathfrak{p}}\;.$$

The absolute value $d(x) := \max_{\mathfrak{p}\in I} |x_{\mathfrak{p}}|_{\mathfrak{p}}$, $x = (x_{\mathfrak{p}})_{\mathfrak{p}\in I} \in K_I$, induces an absolute value on $\mathcal{K}_{\tilde{I}}$. Then we consider the conjugation map $j_{\tilde{I}}$ on the subgroup $U_{\tilde{I}} \subseteq U_I$, which may be defined as in (i), since $\tilde{I}$ is closed under complex conjugation.
We define

$$U_{\tilde{I}}^{+} := \{x \in U_{\tilde{I}} \mid j_I(x) = x\}$$

and

$$U_{\tilde{I}}^{-} := \{x \in U_{\tilde{I}} \mid j_I(x) = x^{-1}\}\;.$$

Since multiplication is defined component-wise, the equation $j_I(x) = x^{\pm 1}$ is equivalent to the system of corresponding equations in the components $U_{\mathfrak{p}_i}\times U_{\overline{\mathfrak{p}_i}}$, $i = 1,\ldots,n_I$. These conditions in turn are equivalent to $(x_{\mathfrak{p}_i}, x_{\overline{\mathfrak{p}_i}})$ being of the form $(x_{\mathfrak{p}_i}, j_{\overline{\mathfrak{p}_i}}(x_{\mathfrak{p}_i}))$, respectively,$(x_{\mathfrak{p}_i}, \frac{1}{j_{\overline{\mathfrak{p}_i}}(x_{\mathfrak{p}_i})})$, as shown in the proof of (i).
In particular, $U_{\tilde{I}}^{-} \;\cong\; \prod\limits_{i=1}^{n_I} U_{\mathfrak{p}_i}$ via the isomorphism $\varphi_{\tilde{I}}$ mapping

$$(x_{\mathfrak{p}_1}, \frac{1}{j_{\overline{\mathfrak{p}_1}}(x_{\mathfrak{p}_1})}, x_{\mathfrak{p}_2}, \frac{1}{j_{\overline{\mathfrak{p}_2}}(x_{\mathfrak{p}_2})}, \ldots, x_{\mathfrak{p}_{n_I}}, \frac{1}{j_{\overline{\mathfrak{p}_{n_I}}}(x_{\mathfrak{p}_{n_I}})}) \;\in\; U_{\tilde{I}}^{-}$$

to the element $(x_{\mathfrak{p}_1},\ldots,x_{\mathfrak{p}_{n_I}})$.
Using similar arguments as in the proof of (i), we obtain

$$\begin{aligned}
\mathrm{rank}_{\mathbb{Z}_p}(U_I \,/\, \overline{\psi_I(E)}) &\overset{(1)}{\geq} \mathrm{rank}_{\mathbb{Z}_p}(U_{\tilde{I}} \,/\, \overline{\psi_{\tilde{I}}(E)}) \\
&\overset{(2)}{\geq} \mathrm{rank}_{\mathbb{Z}_p}(U_{\tilde{I}}^{-} \,/\, (\overline{\psi_{\tilde{I}}(E)} \cap U_{\tilde{I}}^{-})) \\
&\overset{(3)}{=} \mathrm{rank}_{\mathbb{Z}_p}(U_{\tilde{I}}^{-} \,/\, (\overline{\psi_{\tilde{I}}(E^{-})} \cap U_{\tilde{I}}^{-})) \\
&\overset{(4)}{=} \mathrm{rank}_{\mathbb{Z}_p}(U_{\tilde{I}}^{-}) \;\overset{(5)}{=}\; n_I\;,
\end{aligned}$$

where the inequalities (1) and (2) are based on the surjections

$$U_I \,/\, \overline{\psi_I(E)} \;\longrightarrow\; U_{\tilde{I}} \,/\, \overline{\psi_{\tilde{I}}(E)} \;\longrightarrow\; U_{\tilde{I}}^{-} \,/\, (\overline{\psi_{\tilde{I}}(E^{-})} \cap U_{\tilde{I}}^{-})\;,$$

and the rank identities hold since
(3) $\psi_{\tilde{I}}(E^{+}) \subseteq U_{\tilde{I}}^{+}$, $U_{\tilde{I}}^{+} \subseteq U_{\tilde{I}}$ is closed, and $U_{\tilde{I}}^{+} \cap U_{\tilde{I}}^{-}$ is finite,
(4) $\overline{\psi_{\tilde{I}}(E^{-})}$ is finite because E^{-} is finite, and
(5) we have the isomorphism $\varphi_{\tilde{I}} : U_{\tilde{I}}^{-} \;\longrightarrow\; \prod\limits_{i=1}^{n_I} U_{\mathfrak{p}_i}$, and each of the groups $U_{\mathfrak{p}_i}$ has $\mathbb{Z}_p$-rank equal to 1, since p is totally decomposed in $K/\mathbb{Q}$.

(iii) Let $I \subseteq \mathcal{I}$ be such that $|I| > 2$, $n_I \geq 1$ and $\mathcal{E}^I(K) \neq \emptyset$. Let $\{\mathfrak{p}_i, \overline{\mathfrak{p}_i}\}$ denote a pair of complex conjugate primes contained in I, and consider $\mathbb{Z}_p$-extensions $L^1 \in \mathcal{E}^I(K)$ and $L^2 \in \mathcal{E}^{\{\mathfrak{p}_i, \overline{\mathfrak{p}_i}\}}$, the latter being non-empty by (i). Using Lemma 3.19, (ii), we find infinitely many $\mathbb{Z}_p$-extensions $\tilde{M}$ of K contained in $L^1 \cdot L^2$ such that $\mathcal{P}(\tilde{M}) = I \cup \{\mathfrak{p}_i, \overline{\mathfrak{p}_i}\} = I$.

(iv) Let $M \in \mathcal{E}^I(K)$. Let $L^2, \ldots, L^{r_I} \in \tilde{\mathcal{E}}^I(K)$ be such that $M, L^2, \ldots, L^{r_I}$ are pairwise independent $\mathbb{Z}_p$-extensions of K. Then $L^i \not\subseteq \prod_{j \neq i} L^j$ for every $1 \leq i \leq r_I$, where we let $L^1 := M$.
Using Lemma 3.19, (ii), we see that $\mathcal{P}(N) = I$ for almost every $\mathbb{Z}_p$-extension N contained in $M \cdot L^2$. Therefore, L^2 may be replaced by an extension $\tilde{L}^2$ satisfying $\mathcal{P}(\tilde{L}^2) = I$ such that $\tilde{L}^2 \cdot M \subseteq L^2 \cdot M$ is of finite index. Inductively, we may replace $L^3, \ldots, L^{r_I}$ by independent elements of $\mathcal{E}^I(K)$.

□

We will conclude the present section by putting some emphasis on the special role of the cyclotomic $\mathbb{Z}_p$-extension. Assume that K denotes a CM-field for which Leopoldt's Conjecture is true (e.g., assume that $K/\mathbb{Q}$ is abelian). In this case, there exist exactly $d = r_2(K) + 1$ pairwise linearly independent $\mathbb{Z}_p$-extensions of K (compare Theorem 1.7). Let us assume that $[K : \mathbb{Q}] \geq 4$. As before, p is assumed to be totally split in $K/\mathbb{Q}$; for the sake of simplicity, we will assume that $p \neq 2$.

We write $\mathcal{I} = \{\mathfrak{p}_1, \overline{\mathfrak{p}_1}, \ldots, \mathfrak{p}_t, \overline{\mathfrak{p}_t}\}$, $t = \frac{[K:\mathbb{Q}]}{2} = r_2(K)$. Lemma 3.31, (i) shows that for every $i \in \{1, \ldots, t\}$, there exists exactly one $\mathbb{Z}_p$-extension $M^i \in \mathcal{E}(K)$ with $\mathcal{P}(M^i) = \{\mathfrak{p}_i, \overline{\mathfrak{p}_i}\}$. Let $\Omega^-(K) := M^1 \cdot \ldots \cdot M^t$ denote the composite of these $\mathbb{Z}_p$-extensions of K. Then $\mathrm{Gal}(\Omega^-(K)/K) \cong \mathbb{Z}_p^{r_2(K)}$, since the M^i are pairwise linearly independent because of their disjoint ramification sets. We will now show that in $\Omega^-(K)$, complex conjugate primes always ramify simultaneously:

Lemma 3.32. *Assume that $L \subseteq \Omega^-(K)$ is a $\mathbb{Z}_p$-extension of K. If some prime ideal $\mathfrak{p}_i \in \mathcal{I}$ ramifies in L/K, then also $\overline{\mathfrak{p}_i}$ ramifies in L/K.*

Proof. Assume that $\mathfrak{p}_i \in \mathcal{P}(L)$, but $\overline{\mathfrak{p}_i} \notin \mathcal{P}(L)$. The composite $M := L \cdot \prod_{k \neq i} M^k$ satisfies $\mathrm{Gal}(M/K) \cong \mathbb{Z}_p^{r_2(K)}$, since L cannot be contained in $\prod_{k \neq i} M^k$ because $\mathfrak{p}_i \in \mathcal{P}(L)$. Moreover, as $\overline{\mathfrak{p}_i}$ ramifies in M^i/K and at the same time is unramified in $M = L \cdot \prod_{k \neq i} M^k$, it follows that $M^i \not\subseteq M$. Since $M^i \cdot M \subseteq \Omega^-(K)$, we obtain the contradiction $\mathrm{Gal}(\Omega^-(K)/K) \cong \mathbb{Z}_p^{r_2(K)+1}$. □

Lemma 3.33. *The cyclotomic $\mathbb{Z}_p$-extension K_∞ of K satisfies*

$$K_\infty \cap \Omega^-(K) \;=\; K\,.$$

Proof. As usual, we denote by $\mathbb{K}$ the composite of all $\mathbb{Z}_p$-extensions of K. Then $\mathbb{K}/K$ is abelian with Galois group $G = \mathrm{Gal}(\mathbb{K}/K) \cong \mathbb{Z}_p^d$. By infinite Galois theory, $K_\infty \subseteq \mathbb{K}$ and $\Omega^-(K) \subseteq \mathbb{K}$ uniquely determine two closed subgroups $H_1, H_2 \subseteq G$ fixing them, respectively.

Embedding the algebraic extension $\mathbb{K}/K$ into the algebraic closure $\mathbb{C}$ of K, we may consider the restriction to $\mathbb{K}$ of the complex conjugation map j. If $L \subseteq \mathbb{K}$ denotes a $\mathbb{Z}_p$-extension of K, then $j(L)$ is a $\mathbb{Z}_p$-extension of $j(K) = K$, and thus $j(L) \subseteq \mathbb{K}$. This shows that $j(\mathbb{K}) \subseteq \mathbb{K}$.

j acts on G by conjugation, since K is a CM-field and therefore $j(K) = K$. Let $G^+ := \{g \in G \mid j(g) = g\}$ and $G^- := \{g \in G \mid j(g) = g^{-1}\}$. Then $G = G^+ \oplus G^-$, since $p \neq 2$.

We will show that G^- is contained in the subgroup H_1 of G fixing K_∞. If this was not true, then there would exist an element $\varphi \in \mathrm{Gal}(K_\infty/K) = G/H_1$ such that $\varphi \neq \mathrm{id}$ and $j \circ \varphi \circ j^{-1} = \varphi^{-1}$, where j here means the restriction to K_∞. Let $l \in \mathbb{N}_0$ be the largest integer such that K contains a primitive p^l-th root of unity ζ_{p^l}.

If $l \geq 1$, then $K_\infty = \bigcup_{n\geq 0} K_n$ with $K_n = K(\zeta_{p^{l+n}})$, and $\varphi \in \mathrm{Gal}(K_\infty/K)$ is uniquely determined through its values $\varphi(\zeta_{p^{l+n}}) = \zeta_{p^{l+n}}^{u_n}$ with $u_n \in (\mathbb{Z}/p^{l+n}\mathbb{Z})^*$ satisfying $u_n \equiv 1 \bmod p^l$, respectively. But $(j \circ \varphi \circ j^{-1})(\zeta_{p^{l+n}}) = \varphi(\zeta_{p^{l+n}})$ for every n, and therefore $j \circ \varphi \circ j^{-1} = \varphi$. Therefore $\varphi^{-1} = \varphi$, i.e., $\varphi^2 = \mathrm{id}$, and thus $\varphi = \mathrm{id}$, because $-1 \not\equiv 1 \bmod p^l$, recalling that $p \neq 2$.

If $l = 0$, then $[K(\zeta_{p^{n+1}}) : K_n] = [K(\zeta_p) : K]$ for every $n \in \mathbb{N}$, and $\mathrm{Gal}(K_n/K)$ is a quotient of the cyclic group $\mathrm{Gal}(K(\zeta_{p^{n+1}})/K)$, respectively. Every $\tau_n \in \mathrm{Gal}(K(\zeta_{p^{n+1}})/K)$ satisfies $j \circ \tau_n \circ j^{-1} = \tau_n$ by the above, so that $j \circ \varphi_n \circ j^{-1} = \varphi_n$ for every $\varphi_n \in \mathrm{Gal}(K_n/K)$. Since $K_\infty = \bigcup_{n\geq 0} K_n$, it follows that $j \circ \varphi \circ j^{-1} = \varphi$ for every $\varphi \in \mathrm{Gal}(K_\infty/K)$, and we may continue as before.

We have therefore shown that H_1 contains G^-. On the other hand,

$$\mathrm{Gal}(\Omega^-(K)/K) \sim (p\text{-part of}) \, U_{\mathcal{I}}^- / \overline{\Psi_{\mathcal{I}}(E^-)} \, ,$$

by construction of the fields M^i in Lemma 3.31, (i). Therefore $j \circ \varphi \circ j^{-1} = \varphi^{-1}$ for every $\varphi \in \mathrm{Gal}(\Omega^-(K)/K)$, since the pseudo-homomorphism is compatible with $j \in \mathrm{Gal}(K/K^+)$, by Lemma 3.28. This proves that G^+ is contained in the subgroup H_2 of G fixing $\Omega^-(K)$.

In particular, since $G^+ \oplus G^- = G$, it follows that $H_1 + H_2 = G$, and therefore $K_\infty \cap \Omega^-(K) = K$. □

Corollary 3.34. *Using the notation from the above proof, we have*

$$\mathbb{K} \;=\; K_\infty \cdot \Omega^-(K) \;=\; K_\infty \cdot M^1 \cdot \ldots \cdot M^t \, .$$

In particular, $K_\infty = \mathbb{K}^{H_1} = \mathbb{K}^{G^-}$ *and* $\Omega^-(K) = \mathbb{K}^{H_2} = \mathbb{K}^{G^+}$.

Proof. By definition, $\mathbb{K}$ is the composite of all $\mathbb{Z}_p$-extensions of K. Since we assume that Leopoldt's Conjecture holds for K, we know that $\mathrm{Gal}(\mathbb{K}/K) \cong \mathbb{Z}_p^d$ with $d = r_2(K) + 1$ (compare Theorem 1.7). Therefore the corollary follows from Lemma 3.33 and the fact that $\mathrm{Gal}(\Omega^-(K)/K) \cong \mathbb{Z}_p^{r_2(K)}$.

Indeed, if $K_\infty \cdot \Omega^-(K) \subsetneqq K$, then the closed subgroup $H_1 \cap H_2 \subseteq \mathrm{Gal}(\mathbb{K}/K)$ was non-trivial, and therefore $\mathrm{rank}_{\mathbb{Z}_p}(H_1 \cap H_2) \geq 1$. But then

$$\mathrm{rank}_{\mathbb{Z}_p}(\mathrm{Gal}((K_\infty \cdot \Omega^-(K))/K)) \;=\; \mathrm{rank}_{\mathbb{Z}_p}(G/(H_1 \cap H_2)) \;\leq\; r_2(K) \, .$$

On the other hand, $K_\infty \cap \Omega^-(K) = K$ by Lemma 3.33, and therefore

$$\mathrm{Gal}((K_\infty \cdot \Omega^-(K))/K) \;\cong\; \mathbb{Z}_p^{r_2(K)+1}\,,$$

yielding a contradiction. □

Theorem 3.35. *Suppose that K denotes a CM-field, $[K:\mathbb{Q}] \geq 4$, and that p splits completely in $K/\mathbb{Q}$. We assume that Leopoldt's Conjecture is valid for K. For each $I \subseteq \mathcal{I}$, we let $r(I)$ denote the number of primes $\mathfrak{p} \in I$ such that $\overline{\mathfrak{p}} \notin I$, and we let $n(I)$ be the number of pairs $\{\mathfrak{p}, \overline{\mathfrak{p}}\}$ contained in I.*

(i) Suppose that $M \in \mathcal{E}(K)$ satisfies $M \not\subseteq \Omega^-(K)$ and $r(\mathcal{P}(M)) = 0$. Then $\mathcal{P}(M) = \mathcal{I}$. In other words, if $r(\mathcal{P}(M)) = 0$ and $\mathcal{P}(M) \neq \mathcal{I}$, then $M \subseteq \Omega^-(K)$.

(ii) $\mathcal{E}^I(K) \neq \emptyset$ for every $I \subseteq \mathcal{I}$ with $|I| = |\mathcal{I}| - 1$. In particular, we have $\mathrm{rank}(\tilde{\mathcal{E}}^I(K)) = r_2(K)$ for such I.

(iii) $\mathrm{rank}(\tilde{\mathcal{E}}^I(K)) = n_I$ for every $\emptyset \neq I \subsetneq \mathcal{I}$ with $r(I) = 0$.

(iv) Let $\emptyset \neq I \subseteq \mathcal{I}$ satisfy $r(I) > 0$. Then $\mathcal{E}^I(K) \neq \emptyset$ if and only if $|I| = |\mathcal{I}| - r(I)$.

Proof. (i) Let $I := \mathcal{P}(M)$, let M^I denote the composite of all $\mathbb{Z}_p$-extensions of K contained in $\tilde{\mathcal{E}}^I(K)$. We assume that $I \neq \mathcal{I}$. Let $H \subseteq G = \mathrm{Gal}(\mathbb{K}/K)$ denote the subgroup fixing M^I. Since $M \not\subseteq \Omega^-(K)$, the intersection $G^+ \cap H$ is finite (note that $\mathrm{rank}_{\mathbb{Z}_p}(G^+) = 1$, because $\delta(K) = 0$). Since $G \cong \mathbb{Z}_p^{r_2(K)+1}$ does not contain any element of finite order, we may in fact assume that $G^+ \cap H = \{1\}$.
On the other hand, the assumption that $I \neq \mathcal{I}$ implies that $K_\infty \not\subseteq M^I$, so that H is not contained in G^-. This means that there exists an element

$$g \;=\; x \cdot y \in H \subseteq G = G^+ \oplus G^-$$

such that $x \in G^+$, $x \notin H$, and $y \in G^-$, $y \notin H$.
Now we consider the cosets $[x], [y]$ of x and y in $\mathrm{Gal}(M^I/K) \cong G/H$. Since $[x \cdot y] = [1]$, it follows that $[x^{-1}] = [y]$ in $\mathrm{Gal}(M^I/K)$. If $L \in \tilde{\mathcal{E}}^I(K)$, then $j(L)$ is a $\mathbb{Z}_p$-extension of $j(K) = K$ with $\mathcal{P}(j(L)) \subseteq I$, using the fact that $r(I) = 0$. Therefore M^I is invariant under complex conjugation, so that j acts on $\mathrm{Gal}(M^I/K)$. Moreover,

$$[y]^{-1} \;=\; j([y]) \;=\; j([x^{-1}]) \;=\; [x^{-1}] \;=\; [y]\,,$$

and therefore $[y]^2 = [1]$. But then $[y] = [1]$, since $\mathrm{Gal}(M^I/K)$ is a free $\mathbb{Z}_p$-module of rank equal to $\mathrm{rank}(\tilde{\mathcal{E}}^I(K))$, and therefore $y \in H$, contradiction. This shows that either $H \subseteq G^-$ (so that $K_\infty \subseteq M^I$ and $I = \mathcal{I}$), or $M \subseteq \Omega^-(K)$.

(ii) Assume that $|I| = |\mathcal{I}| - 1$, and let $\mathfrak{p} \in \mathcal{I}$, $\mathfrak{p} \notin I$. By Lemma 3.31, (i), there exists a $\mathbb{Z}_p$-extension M of K such that $\mathcal{P}(M) = \{\mathfrak{p}, \overline{\mathfrak{p}}\}$. Now we consider the composite $K_\infty \cdot M$ with the cyclotomic $\mathbb{Z}_p$-extension K_∞ of K. Since p is totally decomposed in $K/\mathbb{Q}$, there exists $N \subseteq K_\infty \cdot M$ such that $\mathfrak{p} \notin \mathcal{P}(N)$ (compare Lemma 3.19, (ii)). Moreover, $\mathfrak{q} \in \mathcal{P}(N)$ for every $\mathfrak{q} \notin \{\mathfrak{p}, \overline{\mathfrak{p}}\}$ by the same lemma, since $\mathcal{P}(K_\infty) = \mathcal{I}$.

If $\overline{\mathfrak{p}}$ was not contained in $\mathcal{P}(N)$, then $r(\mathcal{P}(N)) = 0$. However, $N \not\subseteq \Omega^-(K)$, since $M \subseteq \Omega^-(K)$ and $K_\infty \cap \Omega^-(K) = K$, and therefore (i) would imply that $\mathcal{P}(N) = \mathcal{I}$, contradiction. Therefore $\overline{\mathfrak{p}} \in \mathcal{P}(N)$, i.e., $\mathcal{P}(N) = I$.
We will now prove that $\mathrm{rank}(\tilde{\mathcal{E}}^I(K)) = r_2(K)$. We first note that

$$\mathrm{rank}(\tilde{\mathcal{E}}^I(K)) \;\geq\; r_2(K) - 1 \;,$$

by Lemma 3.31, (ii). Since we have shown that $\mathcal{E}^I(K) \neq \emptyset$, we actually know that $\mathrm{rank}(\tilde{\mathcal{E}}^I(K)) \geq r_2(K)$. But

$$r_2(K) + 1 \;=\; \mathrm{rank}(\tilde{\mathcal{E}}^{\mathcal{I}}(K)) \;\geq\; \mathrm{rank}(\tilde{\mathcal{E}}^I(K)) + 1 \;,$$

because the cyclotomic $\mathbb{Z}_p$-extension of K is ramified at $\mathfrak{p}$ and therefore is not contained in $\tilde{\mathcal{E}}^I(K)$.

(iii) Suppose first that $r(I) = 0$ and $n_I = r_2(K) - 1$. Then $|I| = |\mathcal{I}| - 2$, and $\mathcal{I} = I \cup \{\mathfrak{p}, \overline{\mathfrak{p}}\}$ for a suitable prime $\mathfrak{p}$. By (ii), we have

$$\mathrm{rank}(\tilde{\mathcal{E}}^{I\cup\{\mathfrak{p}\}}(K)) = r_2(K)$$

and

$$\mathrm{rank}(\tilde{\mathcal{E}}^I(K)) \;<\; \mathrm{rank}(\tilde{\mathcal{E}}^{I\cup\{\mathfrak{p}\}}(K)) \;,$$

since $\mathcal{E}^{I\cup\{\mathfrak{p}\}}(K) \neq \emptyset$. Therefore $\mathrm{rank}(\tilde{\mathcal{E}}^I(K)) \leq r_2(K) - 1$. On the other hand, $\mathrm{rank}(\tilde{\mathcal{E}}^I(K)) \geq r_2(K) - 1 = n_I$, by Lemma 3.31, (ii).
Let now $I \subseteq \mathcal{I}$ denote an arbitrary subset satisfying $r(I) = 0$. We may assume that $n_I < r_2(K) - 1$. Let $I' \supseteq I$ denote any subset of $\mathcal{I}$ satisfying $r(I') = 0$ and $|I'| = |\mathcal{I}| - 2$. On the one hand, $\mathrm{rank}(\tilde{\mathcal{E}}^I(K)) \geq n_I$ by Lemma 3.31, (ii). On the other hand,

$$\mathrm{rank}(\tilde{\mathcal{E}}^I(K)) \;\leq\; \mathrm{rank}(\tilde{\mathcal{E}}^{I'}(K)) - (r_2(K) - 1 - n_I) \;,$$

since every 'new' pair $\{\mathfrak{p}, \overline{\mathfrak{p}}\}$ raises the rank by one, using Lemma 3.31, (i). The statement now follows from the fact that $\mathrm{rank}(\tilde{\mathcal{E}}^{I'}(K)) = r_2(K) - 1$.

(iv) Let us first assume that $\mathcal{E}^I(K) \neq \emptyset$, but $|I| < |\mathcal{I}| - r(I)$. Then there exists at least one pair $\{\mathfrak{p}, \overline{\mathfrak{p}}\} \subseteq \mathcal{I}$ such that both $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ are not contained in I. We may assume that there exists in fact exactly one such pair:
If $\{\mathfrak{p}_1, \overline{\mathfrak{p}_1}\}, \ldots, \{\mathfrak{p}_s, \overline{\mathfrak{p}_s}\}$ denote all the pairs in $\mathcal{I} \setminus I$, then we consider $I' := I \cup \{\mathfrak{p}_2, \overline{\mathfrak{p}_2}, \ldots, \mathfrak{p}_s, \overline{\mathfrak{p}_s}\}$. Then $\mathcal{E}^{I'}(K) \neq \emptyset$, which can be proved inductively using Lemma 3.31, (i). Moreover, $|I'| < |\mathcal{I}| - r(I')$, because of $\{\mathfrak{p}_1, \overline{\mathfrak{p}_1}\}$. It would therefore be sufficient to derive a contradiction for I' instead of I.
Since $\mathcal{E}^I(K) \neq \emptyset$, by assumption, we know that $\mathrm{rank}(\tilde{\mathcal{E}}^I(K)) \geq n_I + 1$, because $r(I) > 0$. If $\mathfrak{p}_{n_I+1}, \mathfrak{p}_{n_I+2}, \ldots, \mathfrak{p}_{n_I+r} \in I$, $r = r(I)$, denote the primes whose complex conjugates $\overline{\mathfrak{p}_{n_I+j}}$, $1 \leq j \leq r$, are not contained in I, respectively, then we may inductively conclude that

$$\mathrm{rank}(\tilde{\mathcal{E}}^{I\cup\{\overline{\mathfrak{p}_{n_I+1}},\ldots,\overline{\mathfrak{p}_{n_I+j}}\}}(K)) \;\geq\; n_I + 1 + j$$

for every j, by using the existence of suitable $M^{n_I+j} \in \mathcal{E}^{\{\mathfrak{p}_{n_I+j},\overline{\mathfrak{p}_{n_I+j}}\}}(K)$, guaranteed by Lemma 3.31, (i), respectively. In particular, if we define $I' := I \cup \{\overline{\mathfrak{p}_{n_I+1}}, \ldots, \overline{\mathfrak{p}_{n_I+r}}\}$, then

$$\mathrm{rank}(\tilde{\mathcal{E}}^{I'}(K)) \;\geq\; n_I + 1 + r \;=\; n_{I'} + 1 \;,$$

in contradition to (iii) (note that $I' \neq \mathcal{I}$, since $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ are missing).
Let us now assume that $|I| = |\mathcal{I}| - r$, $r = r(I)$. We will prove the statement via induction on r. If $r = 1$, then $\mathcal{E}^I(K) \neq \emptyset$ by (ii). Let us assume that the statement is true for some $r' \geq 1$. If $r(I) = r' + 1$ and $|I| = |\mathcal{I}| - (r' + 1)$, then we choose any prime $\mathfrak{p} \in I$ such that $\overline{\mathfrak{p}} \notin I$, and we define $I' := I \cup \{\overline{\mathfrak{p}}\}$. Since $r(I') = (r' + 1) - 1 > 0$ and $|I'| = |\mathcal{I}| - r'$, the induction hypothesis implies that $\mathcal{E}^{I'}(K) \neq \emptyset$.
We now consider the composite of some $M \in \mathcal{E}^{I'}(K)$ with an extension $M' \in \mathcal{E}^{\{\mathfrak{p},\overline{\mathfrak{p}}\}}(K)$, which exists by Lemma 3.31, (i). Then there exists a $\mathbb{Z}_p$-extension $N \subseteq M \cdot M'$ of K such that $\mathcal{P}(N) \subseteq I = I' \setminus \{\overline{\mathfrak{p}}\}$. Moreover, $I' \setminus \{\mathfrak{p}, \overline{\mathfrak{p}}\} \subseteq \mathcal{P}(N)$, since M' is unramified outside $\{\mathfrak{p}, \overline{\mathfrak{p}}\}$.
If $\mathcal{P}(N) = I' \setminus \{\mathfrak{p}, \overline{\mathfrak{p}}\}$, then $r(\mathcal{P}(N)) = r' \geq 1$, but

$$|\mathcal{P}(N)| = |I'| - 2 = |\mathcal{I}| - r' - 2 ,$$

so that we obtain a contradiction to the first part of (iv). Therefore

$$\mathcal{P}(N) = I' \setminus \{\overline{\mathfrak{p}}\} = I ,$$

i.e., $\mathcal{E}^I(K) \neq \emptyset$.

□

Remarks 3.36.

(1) The last part of Theorem 3.35 shows that in a given $\mathbb{Z}_p$-extension of K, for every pair $\{\mathfrak{p}, \overline{\mathfrak{p}}\}$, at least one of the two primes ramifies.

(2) A special case of Theorem 3.35, (iv) is the following: If $\mathfrak{p}_i \neq \mathfrak{p}_j \in \mathcal{I}$ are not complex conjugates, then $\mathcal{E}^{\{\mathfrak{p}_i,\mathfrak{p}_j\}}(K) = \emptyset$ as soon as $[K : \mathbb{Q}] > 4$. Moreover, Theorem 3.35, (iv) also generalises the first two statements of Lemma 3.30.

(3) If Leopoldt's Conjecture is not true for K, then $\mathbb{K}/K$ is a $\mathbb{Z}_p^{r_2(K)+1+\delta(K)}$-extension, with $\delta(K) > 0$. We let $\tilde{\mathbb{K}} := K_\infty \cdot \Omega^-(K)$, where, as usual, K_∞ denotes the cyclotomic $\mathbb{Z}_p$-extension of K.
$\Omega^-(K)$ is the composite of $\mathbb{Z}_p$-extensions $M^1, \ldots, M^{r_2(K)}$ of K such that $\mathcal{P}(M^i) = \{\mathfrak{p}_i, \overline{\mathfrak{p}_i}\}$, respectively, as defined in Lemma 3.31. In particular, $j(M^i) = M^i$ for every i, because $\operatorname{rank}(\tilde{\mathcal{E}}^{\{\mathfrak{p}_i,\overline{\mathfrak{p}_i}\}}(K)) \leq 1$ by Lemma 3.31, (i). Therefore $j(\Omega^-(K)) = \Omega^-(K)$ and $j(K_\infty) = K_\infty$, i.e., $j(\tilde{\mathbb{K}}) = \tilde{\mathbb{K}}$.
$G^+ \subseteq G = \operatorname{Gal}(\mathbb{K}/K)$ still equals the subgroup fixing $\Omega^-(K) \subseteq \tilde{\mathbb{K}}$, but we now have $\operatorname{rank}(G^+) = \delta(K) + 1$. Moreover, G^- now is properly contained in the subgroup of G fixing K_∞.
If we define $\tilde{G} := \operatorname{Gal}(\mathbb{K}/\tilde{\mathbb{K}}) \subseteq G$, then j acts on $\operatorname{Gal}(\tilde{\mathbb{K}}/K) \cong G/\tilde{G}$, since $j(\tilde{G}) = \tilde{G}$, and

$$G/\tilde{G} \cong (G/\tilde{G})^+ \oplus (G/\tilde{G})^- .$$

Note that $\tilde{\mathbb{K}}$ is a $\mathbb{Z}_p^{r_2(K)+1}$-extension of K which is an analogue of $\mathbb{K}/K$ for the case of $\delta(K) > 0$. If we replace $\operatorname{rank}(\tilde{\mathcal{E}}^I(K))$ by $\operatorname{rank}(\tilde{\mathcal{E}}^{I,\subseteq\tilde{\mathbb{K}}}(K))$ in Theorem 3.35 (i.e., we only consider $\mathbb{Z}_p$-extensions of K that are contained in $\tilde{\mathbb{K}}$), then the statements of the theorem carry over to this more general situation.

(4) In the setting of (3), we define $\mathbb{K}^+ := \mathbb{K}^{G^-}$, so that

$$\mathrm{Gal}(\mathbb{K}^+/K) \sim (p\text{-part of}) (U_{\mathcal{I}}/\overline{\psi_{\mathcal{I}}(E)})^+ ,$$

using the notation introduced in the proofs of Lemma 3.28 and Lemma 3.31. If $\delta(K) > 0$, and if $I \subseteq \mathcal{I}$ satisfies $r(I) = 0$ and $n_I > r_2(K) - 1 - \delta(K)$, then

$$\mathrm{rank}_{\mathbb{Z}_p}(U_I^+/(\overline{\psi_I(E)} \cap U_I^+)) \geq 1$$

and in fact

$$\mathrm{rank}(\tilde{\mathcal{E}}^{I,\subseteq \mathbb{K}^+}(K)) \geq n_I - (r_2(K) - 1 - \delta(K))$$

(compare the proof of Lemma 3.31, (ii)).

(5) Suppose that $I \subseteq \mathcal{I}$ satisfies $r(I) = |I| = r_2(K) - 1$. Then we have $\mathrm{rank}(\tilde{\mathcal{E}}^I(K)) = \delta(K)$.

Proof. Since $|I| + r(I) < |\mathcal{I}| = 2 \cdot r_2(K)$, Theorem 3.35, (iv) implies that $\mathcal{E}^{I,\subseteq \tilde{\mathbb{K}}}(K) = \emptyset$ ($\tilde{\mathbb{K}}$ has been defined in (3)). Moreover, this is also true for every subset $\emptyset \neq I' \subseteq I$, since $|I'| = r(I') > 0$ and

$$|I'| + r(I') \leq |I| + r(I) < |\mathcal{I}|$$

for every such I'. This means that $\mathrm{rank}(\tilde{\mathcal{E}}^{I,\subseteq \tilde{\mathbb{K}}}(K)) = 0$, and therefore $\mathrm{rank}(\tilde{\mathcal{E}}^I(K)) \leq \delta(K)$.
On the other hand, $\mathrm{rank}(\tilde{\mathcal{E}}^I(K)) = \mathrm{rank}_{\mathbb{Z}_p}(U_I^{(1)}/(\overline{\psi_I(E)} \cap U_I^{(1)}))$, by Lemma 3.28. Here $U_I^{(1)} := \prod_{\mathfrak{p} \in I} U_{\mathfrak{p}}^{(1)}$. But

$$\mathrm{rank}_{\mathbb{Z}_p}(\overline{\psi_I(E)} \cap U_I^{(1)}) \leq \mathrm{rank}_{\mathbb{Z}_p}(\overline{\psi_{\mathcal{I}}(E)}) \leq r_2(K) - 1 - \delta(K)$$

and $\mathrm{rank}_{\mathbb{Z}_p}(U_I^{(1)}) = |I|$, so that

$$\mathrm{rank}(\tilde{\mathcal{E}}^I(K)) \geq |I| - r_2(K) + \delta(K) + 1 = \delta(K) .$$

□

(6) If $[K : \mathbb{Q}] \geq 4$, then the Leopoldt defect $\delta(K)$ is strictly smaller than $r_2(K) - 1$: Otherwise, $\mathrm{rank}_{\mathbb{Z}_p}(\overline{\psi_{\mathcal{I}}(E)}) = 0$, in contradiction to the fact that $E \hookrightarrow \psi_{\mathcal{I}}(E)$ is infinite.

(7) If $\delta(K) = r_2(K) - 2$, then $\mathrm{rank}(\tilde{\mathcal{E}}^I(K)) = |I| - 1$ for every subset $I \subseteq \mathcal{I}$.

Proof. As we have seen in the proof of (5), we have $\mathrm{rank}(\tilde{\mathcal{E}}^I(K)) \geq |I| - 1$ for each I. In view of Lemma 3.30, (i), this means that in particular, $\mathcal{E}^I(K) \neq \emptyset$ for every I with $|I| = 2$. But this implies that

$$\begin{aligned} 2 \cdot r_2(K) - 1 &= r_2(K) + 1 + \delta(K) \\ &= \mathrm{rank}(\tilde{\mathcal{E}}^{\mathcal{I}}(K)) \\ &\geq \mathrm{rank}(\tilde{\mathcal{E}}^I(K)) + (|\mathcal{I}| - |I|) \end{aligned}$$

for every I with $|I| \geq 2$: Let $\tilde{\mathfrak{p}} \in I$, let $\mathfrak{p} \in \mathcal{I}$ denote any prime ideal that is not contained in I. The fact that $\mathcal{E}^{\{\mathfrak{p},\tilde{\mathfrak{p}}\}}(K) \neq \emptyset$ then implies that

$\operatorname{rank}(\tilde{\mathcal{E}}^{I\cup\{\mathfrak{p}\}}(K)) \geq \operatorname{rank}(\tilde{\mathcal{E}}^{I}(K)) + 1$. Inductively, we obtain the stated inequality. This implies that

$$\begin{aligned} \operatorname{rank}(\tilde{\mathcal{E}}^{I}(K)) &\leq 2\cdot r_2(K) - 1 - |\mathcal{I}| + |I| \\ &= 2\cdot r_2(K) - 1 - 2\cdot r_2(K) + |I| \;=\; |I| - 1\,. \end{aligned}$$

□

3.3 Local boundedness results

We have started the investigations of the local behaviour of Iwasawa invariants, at the beginning of the current chapter, with a discussion of the following result (see Theorem 3.2). If K contains only one prime dividing p, and if L/K is a $\mathbb{Z}_p$-extension, then the following holds:

- If $\mu(L/K) = 0$, then the μ-invariant vanishes on a whole neighbourhood of L.
- If $\mu(L/K) = \lambda(L/K) = 0$, then all the three Iwasawa invariants are constant in any sufficiently small neighbourhood of L.

These statements are formulated with respect to Greenberg's topology, which has been introduced in Section 2.3.

In the current section, we will prove our main results concerning local properties of Iwasawa's invariants, with respect to the Greenberg-R-topology introduced in the preceding section. We will use our generalisation 3.6 of Fukuda's Theorem.

We will first consider two problems:

Let L/K be any $\mathbb{Z}_p$-extension.

Question 1. *Is μ* **locally bounded***, i.e., is there a neighbourhood $U \subseteq \mathcal{E}(K)$ of L such that $\mu(M/K) \leq C < \infty$ for some fixed constant C and every $M \in U$?*

Question 2. *Suppose that $\mu(L/K) = 0$. Is λ* **locally bounded***, i.e., is there a neighbourhood $U \subseteq \mathcal{E}(K)$ of L such that $\lambda(M/K) \leq C < \infty$ for some fixed constant C and every $M \in U$?*

These questions have been answered partially by R. Greenberg for a special subset of $\mathbb{Z}_p$-extensions, with respect to the Greenberg topology (compare Theorems 2.27-2.30).

Our method of proof, using Theorem 3.6, will be completely different from Greenberg's approach.

At the end of his article [Gr 73], Greenberg supposed that maybe, under appropriate assumptions, μ, respectively, λ, are not only locally bounded, but in fact locally maximal. We will be able to prove these statements (compare Theorem 3.57 below). We will also prove a result bounding the p-adic valuation of the constant coefficients of characteristic polynomials.

3.3.1 $\mu = 0 \implies \lambda$ is locally bounded

We will start with Question 2, because it is more easy to answer. We first recall some notation. For every $n \geq 0$, we let $A_n = A_n^{(L)}$ be the p-Sylow subgroup

of the ideal class group of the unique subfield $L_n \subseteq L$ of degree p^n over K, respectively. Let $A = \varprojlim A_n$. We have shown in Section 1.3 that A is a finitely generated torsion Λ-module.

Therefore we have a pseudo-isomorphism

$$\varphi : A \xrightarrow{\sim} E_A := \left(\bigoplus_{i=1}^{s} \Lambda/(p^{n_i}) \right) \oplus \left(\bigoplus_{j=1}^{t} \Lambda/(f_j(T)^{l_j}) \right)$$

with distinguished irreducible polynomials $f_j(T) \in \mathbb{Z}_p[T]$, $j = 1, \ldots, t$, by Theorem 1.24, and there is also a pseudo-isomorphism $\psi : E_A \xrightarrow{\sim} A$, since both modules are finitely generated and Λ-torsion (compare Remarks 1.20, (2)). Furthermore, we have $\mu(L/K) = \sum_{i=1}^{s} n_i$ and $\lambda(L/K) = \sum_{j=1}^{t} l_j \cdot \deg(f_j(T))$; see Proposition 1.28.

Now assume that $\mu(L/K) = 0$.

Lemma 3.37. *Let K be a number field, let L/K be a $\mathbb{Z}_p$-extension such that $\mu(L/K) = 0$. Then there exists an integer $n \in \mathbb{N}$ such that λ is bounded on $U(L,n)$, i.e., $\lambda(M/K) \leq C$ for some fixed constant $C < \infty$ and every element $M \in U(L,n)$.*
Here $U(L,n) = \{M \in \mathcal{E}(L,n) \mid \mathcal{P}(M) \subseteq \mathcal{P}(L)\}$, as in Section 3.2.

Proof. Since $\mu(L/K) = 0$, there are pseudo-isomorphisms

$$\varphi : A \xrightarrow{\sim} E_A := \bigoplus_{j=1}^{t} \Lambda/(f_j(T)^{l_j})$$

and $\psi : E_A \xrightarrow{\sim} A$. Since E_A does not contain any non-trivial finite submodules (compare Remarks 2.25, (2)), the map ψ actually is an injection having finite cokernel, so that $A \cong M_1 \oplus \mathbb{Z}_p^r$ as $\mathbb{Z}_p$-module, with M_1 finite and $r = \mathrm{rank}_{\mathbb{Z}_p}(E_A)$ (compare Proposition 1.45, (ii)). In particular,

$$\begin{aligned} \mathrm{rank}_p(E_A) &= \dim_{\mathbb{F}_p}(E_A/(p \cdot E_A)) = \dim_{\mathbb{F}_p}(\bigoplus_{j=1}^{t} \Lambda/(p, f_j(T)^{l_j})) \\ &= \dim_{\mathbb{F}_p}(\bigoplus_{j=1}^{t} \Lambda/(p, T^{\deg(f_j(T)) \cdot l_j})) \,, \end{aligned}$$

since we have an equality

$$|\Lambda/(p, f_j(T)^{l_j})| = |\Lambda/(p, T^{\deg(f_j(T)) \cdot l_j})| \,,$$

which results from the fact that the $f_j(T)^{l_j}$ are distinguished polynomials, see Definition 1.11. Therefore

$$\mathrm{rank}_p(E_A) = \sum_{j=1}^{t} \deg(f_j(T)) \cdot l_j = \lambda(L/K)$$

is bounded by $\mathrm{rank}_p(A)$. This rank is finite, since we assumed that $\mu(L/K) = 0$.

Now we choose an integer $n \geq e(L/K)$ such that $\mathrm{rank}_p(A_n^{(L)}) = \mathrm{rank}_p(A_{n+1}^{(L)})$. Then $\mu(M/K) = 0$ and

$$\mathrm{rank}_p(A^{(M)}) \;=\; \mathrm{rank}_p(A^{(L)}) \;<\; \infty$$

for every $M \in U(L, n+1)$, by Theorem 3.6, (ii), since $e(M/K) = e(L/K)$ for these M by Corollary 3.22. In particular,

$$\lambda(M/K) \;\leq\; \mathrm{rank}_p(A^{(M)}) \;=\; \mathrm{rank}_p(A^{(L)}) \;<\; \infty$$

for every $M \in U(L, n)$. □

Corollary 3.38. *Let L/K be a $\mathbb{Z}_p$-extension such that $\mu(L/K) = 0$. Assume that the Λ-module $A^{(L)} = \varprojlim A_n^{(L)}$ does not contain any nontrivial finite Λ-submodule. Then there exists an integer $n \in \mathbb{N}$ such that $\lambda(M/K) \leq \lambda(L/K)$ for every $M \in U(L, n)$ (i.e., λ is* **locally maximal***).*

Proof. By assumption on $A^{(L)}$, the Λ-module homomorphism $\varphi : A^{(L)} \longrightarrow E_{A^{(L)}}$ has to be an injection. In particular, $\mathrm{rank}_p(A^{(L)}) = \mathrm{rank}_p(E_{A^{(L)}})$, since we already know that $\mathrm{rank}_p(E_{A^{(L)}}) \leq \mathrm{rank}_p(A^{(L)})$ (compare the proof of Lemma 3.37). Choose n as in the previous lemma. Then

$$\lambda(M/K) \;\leq\; \mathrm{rank}_p(A^{(M)}) \;=\; \mathrm{rank}_p(A^{(L)}) \;=\; \mathrm{rank}_p(E_{A^{(L)}}) \;=\; \lambda(L/K)$$

for every $M \in U(L, n)$. □

Remark 3.39. The assumption that $A^{(L)}$ does not contain any nontrivial finite Λ-submodule is equivalent to the condition that $\mathrm{rank}_p(A^{(L)}) = \mathrm{rank}_p(E_{A^{(L)}})$. In Section 3.3.3, we will prove the result of the corollary for arbitrary $\mathbb{Z}_p$-extensions L/K with $\mu(L/K) = 0$. In Section 3.5, we will give another proof of this result.

3.3.2 μ is locally bounded

We will now consider the μ-invariant and study the first of the two questions raised at the beginning of this section.

Let L/K be a $\mathbb{Z}_p$-extension. We will first consider the case $\lambda(L/K) = 0$. Then

$$E_A \;=\; \bigoplus_{i=1}^{s} \Lambda/(p^{n_i}) \;\cong\; \bigoplus_{i=1}^{s} (\mathbb{Z}_p/p^{n_i}\mathbb{Z}_p)[[T]] \;\cong\; \bigoplus_{i=1}^{s} (\mathbb{Z}/p^{n_i}\mathbb{Z})[[T]] \;.$$

The idea is to look at the module $A/(T \cdot A)$, since

$$E_A/(T \cdot E_A) \;=\; \bigoplus_{i=1}^{s} \Lambda/(T, p^{n_i}) \;\cong\; \bigoplus_{i=1}^{s} \mathbb{Z}_p/p^{n_i}\mathbb{Z}_p \;\cong\; \bigoplus_{i=1}^{s} \mathbb{Z}/p^{n_i}\mathbb{Z}$$

is a finite abelian group of order $p^{\mu(L/K)}$. If N denotes any Λ-module, then we define

$$\mathrm{rank}_T(N) \;:=\; v_p(|N/(T \cdot N)|) \;,$$

provided that the right hand side is finite. Here v_p denotes the usual p-adic valuation (i.e., $v_p(p) = 1$). Then

$$\mathrm{rank}_T(E_A) \;=\; \mu(L/K)\;.$$

Let M_1 denote the kernel of the pseudo-isomorphism $\varphi : A \longrightarrow E_A$, which is a finite abelian p-group. Then $\varphi(A/M_1) =: \tilde{E}_A \subseteq E_A$ is a submodule of finite index.

We will show below (compare Proposition 3.41) that

$$\mathrm{rank}_T(\tilde{E}_A) \;=\; \mathrm{rank}_T(E_A)$$

and that

$$\mathrm{rank}_T(\tilde{E_A}) \;=\; \mathrm{rank}_T(A/M_1) \;\leq\; \mathrm{rank}_T(A)\;.$$

This means that $\mu(L/K) = \mathrm{rank}_T(E_A)$ is bounded by $\mathrm{rank}_T(A)$. We will use our generalisation of Fukuda's Theorem (Theorem 3.6) and the Quotient Lemma 3.10 in order to find a neighbourhood $U(L,n)$ such that $\mathrm{rank}_T(A^{(M)})$ is bounded in $U(L,n)$. This will then also bound the μ-invariants $\mu(M/K)$, $M \in U(L,n)$.

In the case of non-vanishing $\lambda(L/K)$, we have

$$E_A \;=\; \left(\bigoplus_{i=1}^{s} \Lambda/(p^{n_i})\right) \;\oplus\; \left(\bigoplus_{j=1}^{t} \Lambda/(f_j(T)^{l_j})\right)\;.$$

Again, A/M_1 is isomorphic to some submodule $\tilde{E}_A \subseteq E_A$ of finite index. However, $E_A/(T \cdot E_A)$ will only be finite if T does not divide the characteristic polynomial $\prod_{j=1}^{t} f_j(T)^{l_j}$ of A. In order to nevertheless bound $\mu(L/K)$ in terms of an invariant attached to the Λ-module A, we have to more generally consider suitably chosen distinguished polynomials $f(T)$, coprime to the characteristic polynomial of A, instead of T. This motivates the following

Definition 3.40. Let $f(T) \in \Lambda$ denote a distinguished polynomial; define the ***f*-rank** of a Λ-module A to be

$$\mathrm{rank}_f(A) \;:=\; v_p(|A/(f(T) \cdot A)|)\;,$$

whenever this is finite. Otherwise, we let $\mathrm{rank}_f(A) := \infty$.

Proposition 3.41. *Let $f(T) \in \Lambda$ denote a distinguished polynomial. Then the following statements hold:*

(i) Suppose that $\mathfrak{p} \in \Lambda$ denotes an irreducible element that is coprime to $f(T)$. If $\hat{C} \subseteq \Lambda/(\mathfrak{p}^n)$, $n \in \mathbb{N}$, denotes a Λ-submodule of finite index, then

$$\mathrm{rank}_f(\hat{C}) \;=\; \mathrm{rank}_f(\Lambda/(\mathfrak{p}^n)) \;<\; \infty\;.$$

(ii) More generally, let $E := \bigoplus_{i=1}^{s} \Lambda/(\mathfrak{p}_i^{n_i})$ be an elementary torsion Λ-module such that $\mathfrak{p}_1^{n_1} \cdot \ldots \cdot \mathfrak{p}_s^{n_s}$ is coprime to $f(T)$, and let $\tilde{E} \subseteq E$ be a Λ-submodule of finite index. Then

$$\mathrm{rank}_f(\tilde{E}) \;=\; \mathrm{rank}_f(E) \;<\; \infty\;.$$

(iii) *Let A, B denote Λ-modules such that at least one of the ranks $\mathrm{rank}_f(A)$, $\mathrm{rank}_f(B)$ is finite. Assume that there exists a Λ-module isomorphism*

$$\varphi : A \xrightarrow{\sim} B \ .$$

Then both $\mathrm{rank}_f(A)$ and $\mathrm{rank}_f(B)$ are finite, and

$$\mathrm{rank}_f(A) \ = \ \mathrm{rank}_f(B) \ .$$

(iv) *Let A denote a Λ-module such that $\mathrm{rank}_f(A)$ is finite. Then*

$$\mathrm{rank}_f(A/M) \ \leq \ \mathrm{rank}_f(A)$$

for every Λ-submodule M of A.

(v) *If a Λ-module $A \ \cong \ B_1 \oplus B_2$ is isomorphic to the direct sum of two Λ-modules B_1 and B_2, and if $\mathrm{rank}_f(B_1)$ and $\mathrm{rank}_f(B_2)$ are finite, then $\mathrm{rank}_f(A)$ is also finite, and*

$$\mathrm{rank}_f(A) \ = \ \mathrm{rank}_f(B_1) + \mathrm{rank}_f(B_2) \ .$$

Proof. We will give an abstract proof using the following notation (which generalises Exercise 13.12 in [Wa 97]):

Definition 3.42. Let $\lambda \in \Lambda$. For any Λ-module N, we let

$$N[\lambda] \ := \ \{x \in N \mid \lambda \cdot x = 0\} \ ,$$

and we define $Q_\lambda(N) := \frac{|N[\lambda]|}{|N/(\lambda \cdot N)|}$, whenever both orders are finite.

Proposition 3.43.

(i) *If N is finite, then $Q_\lambda(N) = 1$.*

(ii) *If*

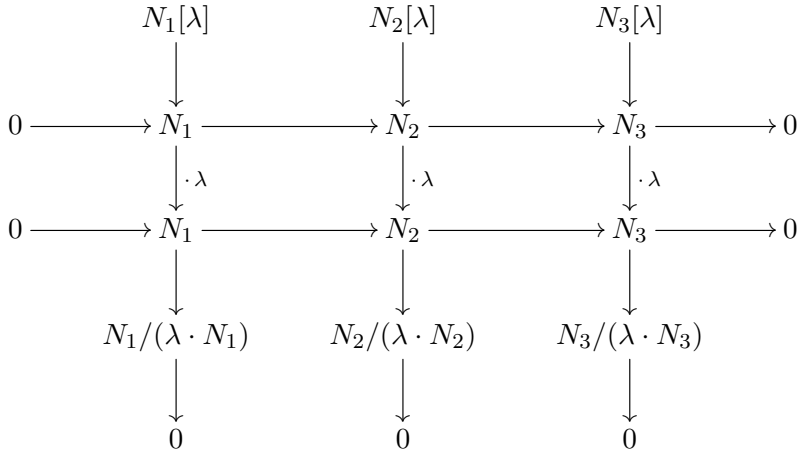
$$0 \longrightarrow N_1 \longrightarrow N_2 \longrightarrow N_3 \longrightarrow 0$$

is an exact sequence of Λ-modules, then $Q_\lambda(N_2) = Q_\lambda(N_1) \cdot Q_\lambda(N_3)$, i.e., whenever two of the $Q_f(N_i)$ are finite, then so is the third, and then equality holds.

Proof. (i) It is easy to see that the action of $\lambda \in \Lambda$ on N induces a Λ-module isomorphism $N/N[\lambda] \cong \lambda \cdot N$. Therefore, since N is finite,

$$|N/(\lambda \cdot N)| \ = \ |N[\lambda]| \ .$$

(ii) We apply the Snake Lemma to the commutative diagram



and obtain a long exact sequence

$$0 \longrightarrow N_1[\lambda] \longrightarrow N_2[\lambda] \longrightarrow N_3[\lambda] \longrightarrow N_1/(\lambda \cdot N_1) \longrightarrow N_2/(\lambda \cdot N_2) \longrightarrow N_3/(\lambda \cdot N_3) \longrightarrow 0 \, .$$

If at least two of the factors $Q_\lambda(N_i)$ are defined, then the corresponding four modules in the long exact sequence are finite. In each of the three possible cases, this implies that in fact all six abelian groups occurring in the exact sequence are finite. Moreover, we may conclude that

$$1 \;=\; \frac{|N_1[\lambda]|}{|N_2[\lambda]|} \cdot \frac{|N_3[\lambda]|}{|N_1/\lambda N_1|} \cdot \frac{|N_2/\lambda N_2|}{|N_3/\lambda N_3|} \;=\; \frac{Q_\lambda(N_1) \cdot Q_\lambda(N_3)}{Q_\lambda(N_2)} \, .$$

□

We will now start with the proof of Proposition 3.41.

(i) It is easy to see that $\mathrm{rank}_f(\hat{C})$ and $\mathrm{rank}_f(\Lambda/(\mathfrak{p}^n))$ are finite (this will be justified more generally in (ii)). Since $\hat{C} \subseteq \Lambda/(\mathfrak{p}^n)$ is of finite index, we have an exact sequence

$$0 \longrightarrow \hat{C} \longrightarrow \Lambda/(\mathfrak{p}^n) \longrightarrow (\Lambda/(\mathfrak{p}^n))/\hat{C} \longrightarrow 0 \, ,$$

and $N := (\Lambda/(\mathfrak{p}^n))/\hat{C}$ is finite. Then $Q_f(\hat{C}) = Q_f(\Lambda/(\mathfrak{p}^n))$, using Proposition 3.43, (i) and (ii).
But $(\Lambda/(\mathfrak{p}^n))[f] = \{0\}$, because $\mathfrak{p}$ and $f(T)$ are coprime elements in the unique factorisation domain Λ. Moreover, $\hat{C} \subseteq \Lambda/(\mathfrak{p}^n)$, and therefore also $\hat{C}[f] = \{0\}$. But this means that

$$Q_f(\hat{C}) \;=\; p^{-\mathrm{rank}_f(\hat{C})} \quad \text{and} \quad Q_f(\Lambda/(\mathfrak{p}^n)) \;=\; p^{-\mathrm{rank}_f(\Lambda/(\mathfrak{p}^n))} \, .$$

(ii) We first note that $\mathrm{rank}_f(E)$ and $\mathrm{rank}_f(\tilde{E})$ are finite, since $f(T)$ is coprime to each $\mathfrak{p}_i$. Indeed, $\mathrm{rank}_f(\Lambda/(\mathfrak{p}_i^{n_i}))$ is finite for every $i \in \{1, \ldots, s\}$, by Lemma 1.17, (i). Therefore

$$\mathrm{rank}_f(E) \;=\; \sum_{i=1}^{s} \mathrm{rank}_f(\Lambda/(\mathfrak{p}_i^{n_i}))$$

is also finite, making use of (v) below. Moreover, $\Lambda/(f, \mathfrak{p}_1^{n_1} \cdot \ldots \cdot \mathfrak{p}_s^{n_s})$ is finite, again by Lemma 1.17, (i). Since f and $\mathfrak{p}_1^{n_1} \cdot \ldots \cdot \mathfrak{p}_s^{n_s}$ both annihilate the quotient $\tilde{E}/(f \cdot \tilde{E})$, and since $\tilde{E}$ is finitely generated as a Λ-module, it follows that $\mathrm{rank}_f(\tilde{E}) < \infty$.
Now we apply Proposition 3.43 to the exact sequence

$$0 \longrightarrow \tilde{E} \longrightarrow E \longrightarrow E/\tilde{E} \longrightarrow 0\,.$$

This implies that $Q_f(\tilde{E}) = Q_f(E)$. But $E[f] = \{0\}$ and therefore also $\tilde{E}[f] = \{0\}$, as in the proof of (i).

(iii) φ induces a Λ-module homomorphism $\overline{\varphi} : A/(f(T) \cdot A) \longrightarrow B/(f(T) \cdot B)$, sending the class $[a]$ of an element $a \in A$ to the class $[\varphi(a)]$; this is well-defined since $\varphi(f(T) \cdot A) = f(T) \cdot \varphi(A) = f(T) \cdot B$. One easily checks that $\overline{\varphi}$ is an isomorphism, using the fact that φ is bijective.

(iv) For any Λ-submodule M of A, the order of

$$(A/M)/(f(T) \cdot A/M) \;=\; A/(M + f(T) \cdot A)$$

is less than or equal to the order of $A/(f(T) \cdot A)$, proving (iv).

(v) Using (iii), we may assume that in fact $A = B_1 \oplus B_2$. But then

$$A/(f(T) \cdot A) \;=\; B_1/(f(T) \cdot B_1) \oplus B_2/(f(T) \cdot B_2)\,.$$

This concludes the proof of the proposition.

□

We choose a distinguished polynomial $f(T)$ which is coprime to the characteristic polynomial of $A = A^{(L)}$. We would like to bound μ-invariants by $\mathrm{rank}_f(A) < \infty$ in a certain neighbourhood U of L. The following lemma shows that we may indeed find a neighbourhood U of L such that for every $M \in U$, $f(T)$ is coprime to the characteristic polynomial of $A^{(M)}$, respectively, and therefore $\mathrm{rank}_f(A^{(M)}) < \infty$.

Lemma 3.44. *Let L/K be a $\mathbb{Z}_p$-extension, and let $\gamma^{(L)}$ denote a fixed topological generator of the Galois group $\mathrm{Gal}(L/K) \cong \mathbb{Z}_p$. Let*

$$F_{A^{(L)}} \;:=\; F_{A^{(L)},\gamma^{(L)}} \;=\; \prod_{j=1}^{t} f_j(T)^{l_j} \in \mathbb{Z}_p[T]$$

denote the characteristic polynomial of $A^{(L)} = \varprojlim A_n^{(L)}$ with respect to the given generator $\gamma^{(L)}$ (compare Remark 1.30).

Let $f(T) \in \mathbb{Z}_p[T]$ denote a distinguished polynomial that is coprime to $F_{A^{(L)}}$. Then there exists an integer $n \in \mathbb{N}$ such that f is coprime to $F_{A^{(M)},\gamma^{(M)}}$ for every $M \in U(L,n)$, where $\gamma^{(M)}$ denotes a generator of $\mathrm{Gal}(M/K)$ that coincides with $\gamma^{(L)}$ on $M_n = L_n$. More precisely, with these choices of generators, we have $\mathrm{rank}_f(A^{(M)}) = \mathrm{rank}_f(A^{(L)}) < \infty$ for $M \in U(L,n)$.

Proof. For every choice of a topological generator $\gamma^{(L)}$ of $\mathrm{Gal}(L/K) \cong \mathbb{Z}_p$, we obtain an isomorphism $\mathbb{Z}_p[[\mathrm{Gal}(L/K)]] \cong \mathbb{Z}_p[[T^{(L)}]]$, induced by

$$\gamma^{(L)} \mapsto 1 + T^{(L)} ;$$

we identify $\mathbb{Z}_p[[\mathrm{Gal}(L/K)]]$ with the ring of formal power series $\Lambda^{(L)} = \mathbb{Z}_p[[T^{(L)}]]$ for some fixed indeterminate $T := T^{(L)}$. Choosing another topological generator of $\mathrm{Gal}(L/K)$ therefore corresponds to a change of variables: If $\tilde{\gamma} = \gamma^a$ with $a \in \mathbb{Z}_p^*$ is the new topological generator, then the new indeterminate $\tilde{T} = \tilde{T}^{(L)}$ is given by $\tilde{T} = (1+T)^a - 1$. In particular, the characteristic polynomial of $A^{(L)}$ depends on the choice of $\gamma^{(L)}$ (compare Remark 1.30). This becomes crucial when we try to compare the characteristic polynomials of different $\mathbb{Z}_p$-extensions. Fix some $\gamma^{(L)}$.

Choose a pseudo-isomorphism $\varphi : A^{(L)} \longrightarrow E_{A^{(L)}}$. Let $M_1^{(L)}$ denote the finite kernel of φ. Since f is coprime to $F_{A^{(L)}}$ by assumption, we know that $\mathrm{rank}_f(E_{A^{(L)}})$ is finite. Indeed,

$$E_{A^{(L)}} \;=\; \bigoplus_{i=1}^{s} \Lambda/(p^{n_i}) \,\oplus\, \bigoplus_{j=1}^{t} \Lambda/(f_j(T)^{l_j})$$

and therefore $\mathrm{rank}_f(E_{A^{(L)}}) = \sum \mathrm{rank}_f(\Lambda/(p^{n_i})) + \sum \mathrm{rank}_f(\Lambda/(f_j(T)^{l_j}))$ is finite, because $f(T)$ and p, respectively, $f(T)$ and the $f_j(T)$, are pairwise coprime in Λ (compare Lemma 1.17, (i)).

Then also

$$\begin{aligned} \mathrm{rank}_f(A^{(L)}) &\leq \mathrm{rank}_f(A^{(L)}/M_1^{(L)}) + v_p(|M_1^{(L)}|) \\ &= \mathrm{rank}_f(E_{A^{(L)}}) + v_p(|M_1^{(L)}|) \end{aligned}$$

is finite, using Proposition 3.41, (ii) and (iii).

For every $m \geq n \geq e = e(L/K)$, the norm maps $A_m^{(L)} \longrightarrow A_n^{(L)}$ induce surjective maps

$$A^{(L)}/(f(T)\cdot A^{(L)}) \twoheadrightarrow A_m^{(L)}/(f(T)\cdot A_m^{(L)}) \twoheadrightarrow A_n^{(L)}/(f(T)\cdot A_n^{(L)}) .$$

These are well-defined since the norm maps are Λ-module homomorphisms.

In particular, $\mathrm{rank}_f(A^{(L)}) \geq \mathrm{rank}_f(A_m^{(L)}) \geq \mathrm{rank}_f(A_n^{(L)})$ for all integers $m \geq n \geq e(L/K)$. This proves that there exists an integer $n_0 \geq e(L/K)+1$ such that

$$\mathrm{rank}_f(A_{n_0}^{(L)}) = \mathrm{rank}_f(A_{n_0+1}^{(L)}) \;=\; \mathrm{rank}_f(A^{(L)}) .$$

We have $e(M/K) = e(L/K)$ for every $M \in U(L, n_0+1)$, by Corollary 3.22. We want to compare the orders of the quotients $A_n^{(L)}/(f(T^{(L)})\cdot A_n^{(L)})$

and $A_n^{(M)}/(f(T^{(M)}) \cdot A_n^{(M)})$. It is important to note that, as mentioned above, in fact two different rings $\Lambda^{(L)} = \mathbb{Z}_p[[T^{(L)}]]$ and $\Lambda^{(M)} = \mathbb{Z}_p[[T^{(M)}]]$ act on $A^{(L)}$, respectively, $A^{(M)}$, arising from the different Galois groups $\mathrm{Gal}(L/K)$ and $\mathrm{Gal}(M/K)$. This means that for $M \in U(L,n)$, we will have $L_n = M_n$ and $A_n^{(L)} = A_n^{(M)}$, but this will not immediately imply that

$$|A_n^{(L)}/(f(T^{(L)}) \cdot A_n^{(L)})| \;=\; |A_n^{(M)}/(f(T^{(M)}) \cdot A_n^{(M)})| \,.$$

However, if we choose a topological generator $\gamma^{(M)}$ of $\mathrm{Gal}(M/K)$ such that $\gamma^{(M)}$ coincides with the fixed generator $\gamma^{(L)}$ of $\mathrm{Gal}(L/K)$ on $M_{n_0+1} = L_{n_0+1}$, then

$$T^{(L)} \cdot A_{n_0}^{(L)} \;=\; (\gamma^{(L)}|_{L_{n_0}} - 1) \cdot A_{n_0}^{(L)} \;=\; (\gamma^{(M)}|_{M_{n_0}} - 1) \cdot A_{n_0}^{(M)} \;=\; T^{(M)} \cdot A_{n_0}^{(M)}$$

and $T^{(L)} \cdot A_{n_0+1}^{(L)} = T^{(M)} \cdot A_{n_0+1}^{(M)}$. Then we have a chain of equalities

$$\mathrm{rank}_f(A_{n_0+1}^{(M)}) \;=\; \mathrm{rank}_f(A_{n_0+1}^{(L)}) \;=\; \mathrm{rank}_f(A_{n_0}^{(L)}) \;=\; \mathrm{rank}_f(A_{n_0}^{(M)}) \,,$$

which implies that $\mathrm{rank}_f(A^{(M)}) = \mathrm{rank}_f(A^{(L)}) < \infty$ for every such M. Indeed, $A^{(M)} = \varprojlim A_n^{(M)}$ is a Fukuda module with index barrier $e(M/K)$, by Corollary 3.9. Therefore also $A^{(M)}/(f(T^{(M)}) \cdot A^{(M)})$ is a Fukuda module, by the Quotient Lemma 3.10. This means that we can apply Theorem 3.6, (i).

In particular, f is coprime to $F_{A^{(M)},\gamma^{(M)}}$: Otherwise $E_{A^{(M)}}/(f(T) \cdot E_{A^{(M)}})$ would contain a factor $\Lambda/(f)$, which is infinite by Lemma 1.17, (ii). But since $\mathrm{rank}_f(A^{(M)}) < \infty$, we have

$$\begin{aligned} \mathrm{rank}_f(E_{A^{(M)}}) \;&\leq\; \mathrm{rank}_f(\tilde{E}_{A^{(M)}}) + v_p(|E_{A^{(M)}}/\tilde{E}_{A^{(M)}}|) \\ &=\; \mathrm{rank}_f(A^{(M)}/M_1^{(M)}) + v_p(|E_{A^{(M)}}/\tilde{E}_{A^{(M)}}|) \\ &\leq\; \mathrm{rank}_f(A^{(M)}) + v_p(|E_{A^{(M)}}/\tilde{E}_{A^{(M)}}|) \;<\; \infty \,, \end{aligned}$$

using Proposition 3.41, (iii) and (iv). □

Remarks 3.45.

(1) In the following, we will usually study sets of $\mathbb{Z}_p$-extensions contained in a small neighbourhood $U(L,n)$ of a fixed $\mathbb{Z}_p$-extension L/K. We will from now on suppress the dependence of the indeterminate $T \in \Lambda$ on the corresponding $\mathbb{Z}_p$-extension from our notation. This means that we will simply write $T \cdot A^{(M)}$ for each $M \in U(L,n)$, instead of using the notation $T^{(M)} \cdot A^{(M)}$. We keep in mind that this may be justified by choosing the corresponding topological generators of the galois groups $\mathrm{Gal}(M/K)$ properly.

(2) Let $f(T) \in \Lambda$ denote a distinguished polynomial. Let L/K denote a $\mathbb{Z}_p$-extension, $A = \varprojlim A_n^{(L)}$, and let E_A denote the elementary Λ-module attached to A. Then we have shown in the proof of Lemma 3.44, using Proposition 3.41, that

$$\boxed{\mathrm{rank}_f(A) < \infty \quad\Longleftrightarrow\quad \mathrm{rank}_f(E_A) < \infty} \,.$$

Note that the same proof works for any finitely generated torsion Λ-module X with corresponding elementary Λ-module E_X.

Using arguments similar to those applied in the proof of Lemma 3.44, we may actually also prove the following boundedness result:

Corollary 3.46. *Assume that L/K is a $\mathbb{Z}_p$-extension such that T does not divide the characteristic polynomial $F_{A^{(L)}}$. Then there exists an integer $n \in \mathbb{N}$ such that for every $M \in U(L,n)$, T does not divide the characteristic polynomial $F_{A^{(M)}}$. Moreover, the p-adic valuation of the constant coefficients of the polynomials $F_{A^{(M)}}$ is bounded on $U(L,n)$.*
In particular, this bounds the number of distinguished factors of $F_{A^{(M)}}(T)$, since each of them raises the valuation of the constant coefficient.

Proof. Lemma 3.44 yields a neighbourhood $U(L,n)$ of L such that $T \nmid F_{A^{(M)}}$ for every $M \in U(L,n)$. Moreover, we know that

$$\operatorname{rank}_T(E_{A^{(M)}}) \;\leq\; \operatorname{rank}_T(A^{(M)}) \;=\; \operatorname{rank}_T(A^{(L)}) \;<\; \infty$$

for $M \in U(L,n)$, using Proposition 3.41, (ii), (iii) and (iv). Now

$$\begin{aligned} E_{A^{(M)}}/(T \cdot E_{A^{(M)}}) \;&=\; \bigoplus_{i=1}^{s} \Lambda/(T, p^{n_i}) \;\oplus\; \bigoplus_{j=1}^{t} \Lambda/(T, f_j(T)^{l_j}) \\ &\cong\; \bigoplus_{i=1}^{s} \mathbb{Z}/p^{n_i}\mathbb{Z} \;\oplus\; \bigoplus_{j=1}^{t} \mathbb{Z}/p^{m_j}\mathbb{Z}\,, \end{aligned}$$

where m_j denotes the p-adic valuation of the (non-zero!) constant coefficient of the distinguished polynomial $f_j(T)^{l_j}$, respectively. Therefore

$$\sum_{i=1}^{s} n_i \;+\; \sum_{j=1}^{t} m_j \;\leq\; \operatorname{rank}_T(A^{(L)}) \;<\; \infty$$

is bounded on $U(L,n)$, and this is exactly the sum of $\mu(M/K)$ and the p-adic valuation of the constant coefficient of $F_{A^{(M)}}(T) = \prod_{j=1}^{t} f_j(T)^{l_j}$. □

Remarks 3.47.

(1) Note that the proof of Corollary 3.46 shows that the μ-invariant is locally bounded in a neighbourhood of L/K, provided that T does not divide the characteristic polynomial $F_{A^{(L)}}(T)$.

(2) Let M/K denote a $\mathbb{Z}_p$-extension. We will now prove that $T \nmid F_{A^{(M)}}(T)$ if and only if the order $|(A_n^{(M)})^{\mathrm{Gal}(M_n/K)}|$ of elements in $A_n^{(M)}$ that are fixed by $\mathrm{Gal}(M_n/K) \cong \mathbb{Z}/p^n\mathbb{Z}$ is bounded for all n.
Indeed, we already know that $T \nmid F_{A^{(M)}}(T)$ if and only if $\operatorname{rank}_T(A^{(M)}) < \infty$ (compare Remarks 3.45, (2)). Since

$$\operatorname{rank}_T(A_m^{(M)}) \;\geq\; \operatorname{rank}_T(A_n^{(M)})$$

for every $m \geq n \geq e(M/K)$, this is equivalent to the fact that $\operatorname{rank}_T(A_n^{(M)})$ remains bounded as $n \to \infty$.

For each $n \in \mathbb{N}$, we let $A_n^{(M)}[T]$ denote the submodule of elements of $A_n^{(M)}$ that are annihilated by T. Then the exact sequences

$$0 \longrightarrow A_n^{(M)}[T] \longrightarrow A_n^{(M)} \xrightarrow{\cdot T} T \cdot A_n^{(M)} \longrightarrow 0$$

imply that $|A_n^{(M)}/(T \cdot A_n^{(M)})| = |A_n^{(M)}[T]|$ for every n (compare Proposition 3.43, (i)).
But $|A_n^{(M)}[T]| = |(A_n^{(M)})^{\mathrm{Gal}(M_n/K)}|$, because T acts on $A_n^{(M)}$ as $\gamma^{(M)} - 1$, where $\gamma^{(M)}$ denotes a topological generator of $\mathrm{Gal}(M/K)$ and therefore $\gamma^{(M)}|_{M_n}$ generates $\mathrm{Gal}(M_n/K)$. This shows that $\mathrm{rank}_T(A^{(M)})$ is finite if and only if $|(A_n^{(M)})^{\mathrm{Gal}(M_n/K)}|$ is bounded as $n \to \infty$.

(3) J. Carroll and H. Kisilevsky proved that $|(A_n^{(M)})^{\mathrm{Gal}(M_n/K)}|$ is bounded as $n \to \infty$ if exactly one prime $\mathfrak{p}$ of K ramifies in M/K (see Lemma 4 in [CK 81]). The proof is based on *Chevalley's Theorem* (compare [La 90], Lemma 13.4.1):

$$\begin{aligned} |(A_n^{(M)})^{\mathrm{Gal}(M_n/K)}| &= \frac{h(K) \cdot e(M_n/K)}{[M_n : K] \cdot (E_K : N_{M_n/K}(M_n^\star) \cap E_K)} \\ &\leq \frac{h(K) \cdot p^n}{p^n \cdot (E_K : N_{M_n/K}(M_n^\star) \cap E_K)} \\ &\leq h(K) < \infty \end{aligned}$$

for every n, where $h(K)$ denotes the class number of K, $e(M_n/K)$ is defined to be the product of the ramification indices $e_{\mathfrak{P}|\mathfrak{p}}(M_n/K)$ of all the (finite or infinite) primes $\mathfrak{p}$ of K, and E_K denotes the group of units of K; in particular, $e(M_n/K)$ divides $[M_n : K] = p^n$ here, by assumption on M/K. This shows that Corollary 3.46 can be applied to every $\mathbb{Z}_p$-extension M/K satisfying $|\mathcal{P}(M)| = 1$ (of course, the statement of the corollary is non-trivial only if the set $\mathcal{E}^{\mathcal{P}(M)}(K)$ is infinite).

Lemma 3.48. *Let L/K be a $\mathbb{Z}_p$-extension, and let $F_{A^{(L)}}(T)$ denote the characteristic polynomial of $A^{(L)}$. Suppose that $f(T) \in \mathbb{Z}_p[T]$ denotes a distinguished polynomial that is coprime to $F_{A^{(L)}}$.*
Let $U = U(L,n)$ be a neighbourhood of L as constructed in Lemma 3.44, i.e., $\mathrm{rank}_f(A_n^{(L)}) = \mathrm{rank}_f(A_{n-1}^{(L)})$ and thus $\mathrm{rank}_f(A^{(M)}) = \mathrm{rank}_f(A^{(L)})$ for every $M \in U(L,n)$.
Then there exists an integer $k \in \mathbb{N}$ such that

$$\mathrm{rank}_g(A^{(M)}) = \mathrm{rank}_f(A^{(M)})$$

for every $M \in U(L,n)$ and every $g \in \Lambda$ satisfying

$$g \equiv f \mod (p,T)^k .$$

Proof. By construction of U in the proof of Lemma 3.44, we have

$$\mathrm{rank}_f(A_n^{(L)}) = \mathrm{rank}_f(A_{n-1}^{(L)}) ,$$

and $n = n_0(f) + 1$ is the smallest integer with this property, i.e.,

$$\mathrm{rank}_f(A_m^{(L)}) \;>\; \mathrm{rank}_f(A_{m-1}^{(L)})$$

for every $m < n$.

$A_n^{(M)} \cong A_n^{(L)}$ is a finite compact Λ-module for every $M \in U$. Now we apply the following observation.

Remark 3.49. Let A denote a finite Λ-module which is a p-group. Then there exists an integer $k \in \mathbb{N}$ such that

$$T^k \cdot A \;=\; p^k \cdot A \;=\; \{0\}\,.$$

Moreover, we may in fact achieve that $g^k \cdot A = \{0\}$ for every non-unit $g \in \Lambda \setminus \Lambda^*$. For example, it is sufficient to take k large enough to ensure that $p^k > |A|$.

Proof. We may assume that $A \neq \{0\}$. Then multiplication by T on A cannot be injective, since otherwise it would also be surjective, and thus $A = T \cdot A$. Using Nakayama's Lemma 1.43, it would then follow that $A = \{0\}$, in contradiction to our assumption.
In particular, $|T \cdot A| \leq \frac{1}{p}|A|$. Now $T \cdot A$ is again a finite Λ-module of p-power order, and we analogously see that $|T^2 \cdot A| \leq \frac{1}{p}|T \cdot A|$. An induction proves that $T^k \cdot A = \{0\}$ if k is sufficiently large.
The same argument in fact works for every element $g \in \Lambda \setminus \Lambda^* = (p, T)$. □

Choosing $k \in \mathbb{N}$ such that $h^k \cdot A_n^{(L)} = \{0\}$ for every $h \in (p, T)$, we may conclude that

$$g \cdot A_n^{(L)} \;=\; f \cdot A_n^{(L)}$$

for every $g \in \Lambda$ that is congruent to f modulo $(p, T)^k$. Therefore

$$\mathrm{rank}_g(A_n^{(L)}) \;=\; \mathrm{rank}_f(A_n^{(L)})$$

and analogously $\mathrm{rank}_g(A_{n-1}^{(L)}) = \mathrm{rank}_f(A_{n-1}^{(L)})$ for each such g. Moreover, the same argument works for every $M \in U(L, n)$, since $h^k \cdot A_n^{(M)} = \{0\}$ for every $h \in (p, T)$ and every $M \in U$. Now the statement follows from the Quotient Lemma 3.10 and Theorem 3.6, (i). □

Iterating the argument of Lemma 3.48, we obtain neighbourhoods U of L such that the characteristic polynomials $F_{A^{(M)}}$ for $M \in U$ are coprime to the polynomials contained in a finite union of residue classes modulo $(p, T)^l$, where l denotes the maximum of the corresponding k's. This leads to the following question:

Is it possible to bound the integers $k = k(f)$ attached to polynomials $f \in \mathbb{Z}_p[T]$ coprime to $F_{A^{(L)}}(T)$? If this is not the case, then an iteration of the above process is not very reasonable.

Note that the proofs of Lemma 3.44 and Lemma 3.48 imply that the $k(f)$ are bounded if and only if the stabilisation indices $n_0 = n_0(f)$ are bounded.

Lemma 3.50. *Let L/K be a fixed $\mathbb{Z}_p$-extension. For simplicity, we assume that $e(L/K) = 0$. Let $\mathfrak{M}_L \subseteq \mathbb{Z}_p[T]$ denote an arbitrary subset of distinguished polynomials coprime to $F_{A^{(L)}}(T)$. Then the set of stabilisation indices*

$$S_1 \;:=\; \{n_0(f) \mid f \in \mathfrak{M}_L, n_0 \text{ minimal such that } \operatorname{rank}_f(A^{(L)}_{n_0+1}) = \operatorname{rank}_f(A^{(L)}_{n_0})\}$$

is bounded if and only if the set

$$S_2 \;:=\; \{\operatorname{rank}_f(A^{(L)}) \mid f \in \mathfrak{M}_L\}$$

is bounded.

Proof. Suppose first that S_2 is bounded. It is a general fact that

$$\operatorname{rank}_f(A^{(L)}) \;\geq\; n_0(f)\,,$$

since $\operatorname{rank}_f(A^{(L)}_{n+1}) > \operatorname{rank}_f(A^{(L)}_n)$ for each $n < n_0 = n_0(f)$, using Theorem 3.6 and the minimality of n_0. Therefore also the set S_1 is bounded.

Suppose now that the stabilisation indices are bounded by some integer $N \in \mathbb{N}$. Then $\operatorname{rank}_f(A^{(L)}) \leq v_p(|A^{(L)}_{N+1}|)$ for every $f \in \mathfrak{M}_L$, by Theorem 3.6. □

Corollary 3.51. *Using the above notation, we let $\mathfrak{M}_L$ denote the set of* all *distinguished polynomials coprime to $F_{A^{(L)}}(T)$. Then the following statements are equivalent:*

(i) $S_1 := \{n_0(f) \mid f \in \mathfrak{M}_L, n_0$ *minimal with* $\operatorname{rank}_f(A^{(L)}_{n_0+1}) = \operatorname{rank}_f(A^{(L)}_{n_0})\}$ *is bounded.*

(ii) $S_2 := \{\operatorname{rank}_f(A^{(L)}) \mid f \in \mathfrak{M}_L\}$ *is bounded.*

(iii) $A^{(L)}$ *is finite.*

Proof. We have seen in the previous lemma that statements (i) and (ii) are equivalent.

'(i) $\Longrightarrow$ (iii)': Let $N \in \mathbb{N}$ denote a bound for S_1. Then

$$\operatorname{rank}_f(A^{(L)}_{N+1}) \;=\; \operatorname{rank}_f(A^{(L)}_N)$$

for every $f \in \mathfrak{M}_L$. This means that the kernel Y_N of the projection map $\mathrm{pr}_N : A^{(L)} \longrightarrow A^{(L)}_N$ is contained in $f \cdot A^{(L)}$ for every $f \in \mathfrak{M}_L$ (compare the proof of Theorem 3.6, (ii)).

Note that for each $n \in \mathbb{N}$, there exists a distinguished polynomial

$$f \;\in\; \mathfrak{m}^n \;=\; (p, T)^n$$

such that f is coprime to $F_{A^{(L)}}$.

Therefore

$$Y_N \;\subseteq\; \bigcap_{f \in \mathfrak{M}_L} (f \cdot A^{(L)}) \;\subseteq\; \bigcap_{n \geq 0} (\mathfrak{m}^n \cdot A^{(L)}) \;=\; \{0\}\,.$$

But this means that $|A^{(L)}| = |A^{(L)}_N|$ is finite.

'(iii) $\Longrightarrow$ (ii)': If, on the other hand, $A^{(L)}$ is finite, then of course

$$\operatorname{rank}_f(A^{(L)}) \;\leq\; v_p(|A^{(L)}|)$$

for every $f \in \mathfrak{M}_L$, and thus S_2 is bounded.

□

We will now prove our first result bounding μ-invariants:

Lemma 3.52. *Let K be a number field, let L/K be a $\mathbb{Z}_p$-extension. Then there exists an integer $n \in \mathbb{N}$ such that μ is bounded on $U(L,n)$, i.e., $\mu(M/K) \leq C$ for some fixed constant $C < \infty$ and every $M \in U(L,n)$.*

Proof. Let L/K be any given $\mathbb{Z}_p$-extension. In view of Corollary 3.46 (compare Remarks 3.47, (1)), it remains to consider the case where T divides the characteristic polynomial of $A^{(L)}$. We let

$$f(T) \;:=\; T^k + p\;,$$

where we choose $k \in \mathbb{N}$ minimal such that $f(T)$ is different from the irreducible distinguished factors $f_1(T), \ldots, f_t(T)$ dividing the characteristic polynomial of $A^{(L)}$. $f(T)$ is irreducible in $\mathbb{Z}_p[T]$ and therefore in Λ (compare Proposition 1.27, (iv)) by Eisenstein's Irreducibility Criterion. This means that $f(T)$ and $f_j(T)$ are coprime for $j = 1, \ldots, t$, and therefore $\Lambda/(f_j(T)^{l_j}, f(T))$ is finite for every j (compare Lemma 1.17, (i)). In particular,

$$\begin{aligned} E_{A^{(L)}}/(f(T) \cdot E_{A^{(L)}}) \;&\cong\; \bigoplus_{i=1}^{s} \Lambda/(p^{n_i}, f(T)) \;\oplus\; \underbrace{\bigoplus_{j=1}^{t} \Lambda/(f_j(T)^{l_j}, f(T))}_{=:\,C} \\ &=\; \bigoplus_{i=1}^{s} \Lambda/(p^{n_i}, T^k + p) \;\oplus\; C\;, \end{aligned}$$

where C is a finite abelian p-group. The order of each quotient $\Lambda/(p^{n_i}, T^k + p)$ is equal to $p^{n_i \cdot k}$, respectively, by the Division Lemma 1.10.

We have thus shown that

$$\operatorname{rank}_f(E_{A^{(L)}}) \;=\; k \cdot \mu(L/K) + v_p(|C|) \;<\; \infty\;.$$

In particular, $\operatorname{rank}_f(A^{(L)}) < \infty$ (compare Remarks 3.45, (2)), and therefore $\operatorname{rank}_f(A^{(M)}) < \infty$ for every $M \in U(L,n)$, if n is large enough. This means that f is coprime to the characteristic polynomial of $A^{(M)}$ for each $M \in U(L,n)$. Analogously to the above, this implies that

$$\operatorname{rank}_f(E_{A^{(M)}}) \;=\; k \cdot \mu(M/K) + v_p(|C^{(M)}|)\;,$$

respectively.

Using Proposition 3.41, we obtain inequalities

$$k \cdot \mu(M/K) \;\leq\; \operatorname{rank}_f(E_{A^{(M)}}) \;\leq\; \operatorname{rank}_f(A^{(M)}) \;=\; \operatorname{rank}_f(A^{(L)})\;,$$

which are valid for every $M \in U(L,n)$. □

Remarks 3.53.

(1) In his article [Gr 73], GREENBERG proved that μ is bounded on $\mathcal{E}(L,n)$ for $n \in \mathbb{N}$ being large enough, provided that only finitely many primes of L lie above p (compare Theorem 2.27). This is the case, for example, if $\mathcal{P}(L) = \mathcal{I}$, and this case is covered by Lemma 3.52. In particular, if only one prime of K divides p, i.e., $|\mathcal{I}| = 1$, then μ is globally bounded on the compact set $\mathcal{E}^{\mathcal{I}}(K) = \mathcal{E}(K)$ (compare Greenberg's Theorem 2.29).
Furthermore, Greenberg proved that the subset $\mathcal{E}'(K)$ consisting of every $\mathbb{Z}_p$-extension of K in which no prime dividing p splits completely is open and dense in $\mathcal{E}(K)$; see Proposition 4 in [Gr 73]. Therefore Lemma 3.52 has already been proved by Greenberg for 'almost every' $L \in \mathcal{E}(K)$, using completely different arguments (compare Section 4.1). In addition, Greenberg's formulation is stronger in general because it shows boundedness on the set $\mathcal{E}(L,n)$, which is stricly larger than $U(L,n)$ if $\mathcal{P}(L) \subsetneqq \mathcal{I}$.

(2) At the end of his article, Greenberg supposed that probably μ is not only locally bounded but actually locally maximal. We are able to prove this, first under quite restrictive assumptions:

Corollary 3.54. *Suppose that L/K is a $\mathbb{Z}_p$-extension with $\lambda(L/K) = 0$, such that the Λ-module $A^{(L)} = \varprojlim A_n^{(L)}$ does not contain any nontrivial finite Λ-submodule. Then there exists an integer $n \in \mathbb{N}$ such that $\mu(M/K) \leq \mu(L/K)$ for every $M \in U(L,n)$ (i.e., μ is* **locally maximal**).

Proof. By assumption on $A^{(L)}$, the pseudo-isomorphism $\varphi : A^{(L)} \longrightarrow E_{A^{(L)}}$ has to be an injection. φ induces an isomorphism $A^{(L)} \xrightarrow{\sim} \tilde{E}_{A^{(L)}}$, where $\tilde{E}_{A^{(L)}} \subseteq E_{A^{(L)}}$ is of finite index. In particular, using Proposition 3.41, (ii) and (iii), we have

$$\operatorname{rank}_T(A^{(L)}) \;=\; \operatorname{rank}_T(\tilde{E}_{A^{(L)}}) \;=\; \operatorname{rank}_T(E_{A^{(L)}})\,,$$

noting that $\operatorname{rank}_T(E_A^{(L)}) < \infty$, since $\lambda(L/K) = 0$ by assumption. Furthermore, we may choose an integer $n \in \mathbb{N}$ such that $\operatorname{rank}_T(A^{(M)}) = \operatorname{rank}_T(A^{(L)})$ for every $M \in U(L,n)$, as in Corollary 3.46. But then

$$\begin{aligned} \mu(M/K) &\leq \operatorname{rank}_T(E_{A^{(M)}}) \\ &\leq \operatorname{rank}_T(A^{(M)}) \;=\; \operatorname{rank}_T(A^{(L)}) \\ &= \operatorname{rank}_T(E_{A^{(L)}}) \;=\; \mu(L/K) \end{aligned}$$

for every $M \in U(L,n)$, where the last equality arises from the fact that $\lambda(L/K) = 0$. □

Remark 3.55. The assumption that $A^{(L)}$ does not contain any nontrivial finite Λ-submodule is equivalent to the condition $\operatorname{rank}_T(A^{(L)}) = \operatorname{rank}_T(E_{A^{(L)}})$, provided that these ranks are finite. Indeed, we will show in Proposition 3.58 that

$$\begin{aligned} \operatorname{rank}_T(A^{(L)}) &= \operatorname{rank}_T(A^{(L)}/M_1^{(L)}) + \operatorname{rank}_T(M_1^{(L)}) \\ &= \operatorname{rank}_T(E_{A^{(L)}}) + \operatorname{rank}_T(M_1^{(L)})\,, \end{aligned}$$

where $M_1^{(L)}$ denotes the kernel of the pseudo-isomorphism $\varphi : A \longrightarrow E_A$, i.e., the maximal finite Λ-submodule of A (see Remarks 2.25, (3)). Furthermore, $\mathrm{rank}_T(M_1^{(L)}) = 0$ if and only if $M_1^{(L)} = \{0\}$, by Nakayama's Lemma 1.43.
Actually, we may completely remove the assumptions made in Corollary 3.54, by choosing a 'good' polynomial $f(T)$ instead of using T, as we will show now.

Lemma 3.56. *Let L/K denote any $\mathbb{Z}_p$-extension. Then $\mu(L/K)$ is locally maximal.*

Proof. Fix a pseudo-isomorphism $A^{(L)} \xrightarrow{\sim} E_{A^{(L)}}$, and let $M_1^{(L)}$ denote the finite kernel of this map, i.e., $A^{(L)}/M_1^{(L)} \cong \tilde{E}_{A^{(L)}} \subseteq E_{A^{(L)}}$ is of finite index. Write $|M_1^{(L)}| = p^m$, $m \in \mathbb{N}_0$. We define

$$f(T) := T^{m+1} \cdot F_{A^{(L)}}(T) + p \, .$$

Then $f(T)$ is a distinguished polynomial, and irreducible by Eisenstein's Criterion. Moreover, $f(T)$ is coprime to $F_{A^{(L)}}(T)$, so that $\mathrm{rank}_f(E_{A^{(L)}})$ and therefore $\mathrm{rank}_f(A^{(L)})$ are finite. If $d \in \mathbb{N}$ denotes the degree of $F_{A^{(L)}}(T)$, then the degree of $f(T)$ is equal to $m + d + 1$.

Now we choose a neighbourhood $U(L, n)$ of $L \in \mathcal{E}(K)$ such that we have $\mathrm{rank}_f(A^{(M)}) = \mathrm{rank}_f(A^{(L)}) < \infty$ for every $M \in U(L, n)$. Then

$$\begin{aligned}
(m + d + 1) \cdot \mu(M/K) &\leq \mathrm{rank}_f(A^{(M)}) = \mathrm{rank}_f(A^{(L)}) \\
&\leq v_p(|M_1^{(L)}|) + \mathrm{rank}_f(\tilde{E}_{A^{(L)}}) \\
&\overset{3.41}{=} m + \mathrm{rank}_f(E_{A^{(L)}}) \\
&\leq m + d + (m + d + 1) \cdot \mu(L/K)
\end{aligned}$$

for each $M \in U(L, n)$, where the first inequality has been shown in the proof of Lemma 3.52. The last inequality furthermore makes use of the fact that for every divisor $f_j(T)^{l_j}$ of $F_{A^{(L)}}(T)$, we have

$$|\Lambda/(f(T), f_j(T)^{l_j})| \leq p^{l_j \cdot \deg(f_j(T))} \, ,$$

since $p \in (f(T), f_j(T)^{l_j})$, by definition of $f(T)$.

Since $\mu(L/K)$ and $\mu(M/K)$ are integers, it follows that $\mu(M/K) \leq \mu(L/K)$. □

3.3.3 Local maximality

We will now prove our main theorem. This result will not only contain a new proof of Lemma 3.56, but also improves our results concerning the λ-invariant (i.e., Lemma 3.37 and Corollary 3.38). Furthermore, our method will even be fine enough to obtain information about ν-invariants. The key idea is to use, as in the study of the μ-invariant, modules of the form

$$A/(f(T) \cdot A) \, ,$$

for some suitable distinguished polynomial $f(T)$. We will in fact choose a sequence of polynomials and consider the corresponding ranks.

The following theorem is the most important result of Chapter 3.

Theorem 3.57. *Let L/K be a $\mathbb{Z}_p$-extension. Let $\mu := \mu(L/K)$, $\lambda := \lambda(L/K)$. Then the following holds.*

(i) $\mu(L/K)$ *is* **locally maximal**, *i.e., there exists an integer $n \in \mathbb{N}$ such that for every $M \in U(L,n)$, we have*

$$\mu(M/K) \leq \mu(L/K) .$$

(ii) If $\mu = 0$, then $\lambda(L/K)$ is **locally maximal**, *i.e., there exists some $n \in \mathbb{N}$ such that for each $M \in U(L,n)$, we have $\mu(M/K) = 0$ and $\lambda(M/K) \leq \lambda(L/K)$.*

(iii) More generally, if $\mu := \mu(L/K) \in \mathbb{N}_0$ is arbitrary, then $\lambda(L/K)$ is locally maximal on the set $\mathcal{E}^{\mu}(K)$ of $\mathbb{Z}_p$-extensions M/K satisfying $\mu(M/K) = \mu$, i.e., there exists an integer $n \in \mathbb{N}$ such that

$$\lambda(M/K) \leq \lambda(L/K)$$

for every $M \in U(L,n) \cap \mathcal{E}^{\mu}(K)$.

(iv) If $\mathcal{E}^{\mu,\lambda}(K)$ denotes the set of $\mathbb{Z}_p$-extensions M/K satisfying $\mu(M/K) = \mu$ and $\lambda(M/K) = \lambda$, then there exists an integer $n \in \mathbb{N}$ such that

$$|M_1^{(M)}| = |M_1^{(L)}| \quad \text{and} \quad \nu(M/K) = \nu(L/K)$$

for every $M \in U(L,n) \cap \mathcal{E}^{\mu,\lambda}(K)$, i.e., the ν-invariant is **locally constant** *in this set. Here $M_1^{(M)}$ denotes the maximal finite Λ-submodule of the projective limit $A^{(M)} = \varprojlim A_n^{(M)}$, respectively.*

Proof. (i) Let $n > m \geq e(L/K)$. We make use of the distinguished polynomials $\nu_{(n,m)}(T)$ introduced in Section 1.2. Since $\nu_{(n,m)} = \frac{(T+1)^{p^n}-1}{(T+1)^{p^m}-1}$, the roots of $\nu_{(n,m)}$ in an algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ are of the form $\zeta - 1$, where $\zeta^{p^n} = 1$, $\zeta^{p^m} \neq 1$, i.e., $\zeta = \zeta_{p^l}$ is a primitive p^l-th root of unity, $m < l \leq n$. We note that

$$v_p(\zeta_{p^l} - 1) = \frac{1}{p^{l-1}(p-1)} < \frac{1}{p^{m-1}(p-1)}$$

for every $l > m$, where v_p denotes the extension of the usual p-adic valuation to $\mathbb{Q}_p(\zeta_{p^l})$ (i.e., $v_p(p) = 1$). The degree of $F_{A^{(L)}}(T)$ is equal to $\lambda = \lambda(L/K)$. We choose m large enough to ensure that $\frac{\lambda}{p^{m-1}(p-1)} < 1$. Then, since $F_{A^{(L)}}(T)$ is a distinguished polynomial, we have

$$v_p(F_{A^{(L)}}(\zeta_{p^l} - 1)) = \frac{\lambda}{p^{l-1}(p-1)} < 1 \tag{3.1}$$

for every $l > m$. For every l, there exist exactly $p^{l-1}(p-1)$ primitive p^l-th roots of unity. We may conclude that

$$\begin{aligned} |\Lambda/(F_{A^{(L)}}, \nu_{(n,m)})| &= \prod_{\substack{m<l\leq n\,, \\ \zeta^{p^l}=1}} p^{v_p(F_{A^{(L)}}(\zeta-1))} \\ &= \prod_{m<l\leq n} (p^{\frac{\lambda}{p^{l-1}(p-1)}})^{p^{l-1}(p-1)} = (p^{\lambda})^{n-m} , \end{aligned}$$

where the first product runs over the primitive p^l-th roots of unity, respectively. Indeed, $Z := \Lambda/(\nu_{(n,m)})$ is isomorphic to a free $\mathbb{Z}_p$-module of rank $\deg(\nu_{(n,m)}) = p^n - p^m$, by the Division Lemma 1.10. Multiplication by T is a $\mathbb{Z}_p$-linear map $T : Z \longrightarrow Z$ with eigenvalues $\zeta_{p^l} - 1$, $m < l \leq n$. $\Lambda/(F_{A^{(L)}}, \nu_{(n,m)})$ is the cokernel of the linear map on Z given by multiplication by $F_{A^{(L)}}(T)$. This map has eigenvalues $F_{A^{(L)}}(\zeta_{p^l} - 1)$, $m < l \leq n$, and the order of the cokernel equals the p-valuation of the determinant, which is the product of the eigenvalues. Note that $\nu_{(n,m)}$ is coprime to $F_{A^{(L)}}(T)$ for every $n \geq m \geq e(L/K)$, by Proposition 1.44, and therefore $F_{A^{(L)}}(\zeta_{p^l} - 1) \neq 0$ for each $m < l \leq n$, i.e., $|\Lambda/(F_{A^{(L)}}, \nu_{(n,m)})| < \infty$ and $\mathrm{rank}_{\nu_{(n,m)}}(A^{(L)}) < \infty$.
More generally, for every divisor $f_j(T)^{l_j}$ of $F_{A^{(L)}}(T)$ arising in the decomposition of $E_{A^{(L)}}$, we have $|\Lambda/(\nu_{(n,m)}, f_j(T)^{l_j})| = p^{(n-m)\cdot l_j \cdot \deg(f_j(T))}$.
In particular,

$$\begin{aligned} \mathrm{rank}_{\nu_{(n,m)}}(A^{(L)}) &\leq \mathrm{rank}_{\nu_{(n,m)}}(\tilde{E}_{A^{(L)}}) + \underbrace{v_p(|M_1^{(L)}|)}_{=:C} \\ &= \mathrm{rank}_{\nu_{(n,m)}}(E_{A^{(L)}}) + C \\ &= (p^n - p^m)\cdot\mu + (n-m)\cdot\lambda + C\,. \end{aligned} \tag{3.2}$$

Now we choose a neighbourhood $U(L, w_0)$ of L such that

$$\mathrm{rank}_{\nu_{(n,m)}}(A^{(M)}) = \mathrm{rank}_{\nu_{(n,m)}}(A^{(L)}) < \infty$$

for every $M \in U(L, w_0)$, using Lemma 3.44. Then

$$\begin{aligned} \mathrm{rank}_{\nu_{(n,m)}}(E_{A^{(M)}}) &= \mathrm{rank}_{\nu_{(n,m)}}(\tilde{E}_{A^{(M)}}) = \mathrm{rank}_{\nu_{(n,m)}}(A^{(M)}/M_1^{(M)}) \\ &\leq \mathrm{rank}_{\nu_{(n,m)}}(A^{(M)}) = \mathrm{rank}_{\nu_{(n,m)}}(A^{(L)}) \end{aligned} \tag{3.3}$$

for these M.
Let $M \in U(L, w_0)$ be arbitrary, but fixed. We will develop a formula that will be useful to bound μ- and λ-invariants. The latter means bounding the degree $\lambda^{(M)} := \lambda(M/K)$ of the characteristic polynomial $F_{A^{(M)}}(T)$. For arbitrary $l \in \{m+1, \ldots, n\}$, it is not clear whether $\frac{\lambda^{(M)}}{p^{l-1}(p-1)} < 1$, i.e., whether (3.1) holds for $F_{A^{(M)}}(T)$.
We therefore let $l_1, \ldots, l_r \in \{m+1, \ldots, n\}$ denote the values of l for which (3.1) fails. Then $l_i = m + i$, $1 \leq i \leq r$. Thus, $v_p(F_{A^{(M)}}(\zeta_{p^l} - 1)) \geq 1$ for $l \leq m + r$, and $v_p(F_{A^{(M)}}(\zeta_{p^l} - 1)) = \frac{\lambda^{(M)}}{p^{l-1}(p-1)} < 1$ for $l > m + r$. Note that at the moment, we have not said anything about r (so $r = n - m$ is possible) and therefore have not bounded $\lambda^{(M)}$ yet.
However, we know that

$$\begin{aligned} \mathrm{rank}_{\nu_{(n,m)}}(E_{A^{(M)}}) &= (p^n - p^m)\cdot\mu(M/K) + |\Lambda/(F_{A^{(M)}}(T), \nu_{(n,m)})| \\ &\overset{(3.3)}{\leq} \mathrm{rank}_{\nu_{(n,m)}}(A^{(L)}) \\ &\overset{(3.2)}{\leq} (p^n - p^m)\cdot\mu + (n-m)\cdot\lambda + C\,, \end{aligned}$$

where $C = v_p(|M_1^{(L)}|)$ has been defined above, and therefore

$$\begin{aligned} & (p^n - p^m)\mu(M/K) + p^m(p-1) + p^{m+1}(p-1) + \ldots + p^{m+r-1}(p-1) \\ & \qquad + (n-m-r)\cdot\lambda^{(M)} \\ = \;& p^m(p^{n-m}-1)\mu(M/K) + p^m(p^r-1) + (n-m-r)\cdot\lambda^{(M)} \qquad (3.4) \\ \leq \;& p^m(p^{n-m}-1)\mu + (n-m)\cdot\lambda + C\ . \end{aligned}$$

For every pair of integers $n > m \geq e(L/K)$, we have found a neighbourhood $U(L, w_0)$, $w_0 = w_0(n,m)$, such that for every $M \in U(L,w_0)$, (3.4) holds with a suitable integer

$$r = r(n,m,M) \in \{0, \ldots, n-m\}\ .$$

We will now choose special values for n and m, namely sequences $(n_i)_{i\geq 0}$, $(m_i)_{i\geq 0}$ defined by $n_i := 2i$ and $m_i := i$ for every $i \geq 0$. If $i_1 \geq e(L/K)$ is large enough to ensure that $\frac{\lambda}{p^{i_1-1}(p-1)} < 1$ and

$$p^{m_{i_1}}(p^{i_1}-1) \;=\; p^{i_1}(p^{i_1}-1) \;>\; i_1\cdot\lambda + C \;=\; (n_{i_1}-m_{i_1})\cdot\lambda + C\ ,$$

then (3.4) implies that $\mu(M/K) \leq \mu = \mu(L/K)$.

(ii) If $\mu(L/K) = 0$, then Corollary 3.22, (ii) implies that there exists some $\tilde{w_0} \geq w_0$ such that $\mu(M/K) = 0$ for each $M \in U(L,\tilde{w_0})$. In particular, for these M, (3.4) reduces to

$$p^m(p^r-1) + (n-m-r)\cdot\lambda^{(M)} \;\leq\; (n-m)\cdot\lambda + C\ .$$

If $i_2 \geq i_1$ is large enough to ensure that

$$p^{m_{i_2}} \;=\; p^{i_2} \;>\; i_2\cdot\lambda + C \;=\; (n_{i_2}-m_{i_2})\cdot\lambda + C\ ,$$

then (3.4) implies that $r(n_i, m_i, M) = 0$ for every $i \geq i_2$ and every M contained in the neighbourhood $U(L,w_i) \subseteq U(L,\tilde{w_0})$ corresponding to the pair (n_i, m_i).
Therefore, (3.4) yields

$$i\cdot\lambda^{(M)} \;=\; (n_i - m_i)\cdot\lambda^{(M)} \;\leq\; i\cdot\lambda + C \qquad (3.5)$$

for every $i \geq i_2$. Let now $i \geq \max(i_2, C+1)$. If $\lambda^{(M)} > \lambda$, then

$$(C+1)\cdot(\lambda^{(M)} - \lambda) \;\leq\; i\cdot(\lambda^{(M)} - \lambda) \;\leq\; C\ ,$$

contradiction. Therefore $\lambda^{(M)} \leq \lambda$ for every $M \in U(L,w_i)$.

(iii) If M satisfies $\mu(M/K) = \mu$, then we may subtract $\mu\cdot(p^n - p^m)$ on both sides of the inequality (3.4) and obtain the same inequality as in the proof of (ii); we then may proceed as above.
Note that (3.4) in general does not yield bounds for the λ-invariants of $\mathbb{Z}_p$-extensions M/K with $\mu(M/K) \leq \mu - 1$, since $r \leq n-m$ and therefore in this case, the inequality

$$p^m\cdot(p^r-1) \;\leq\; \underbrace{(\mu - \mu(M/K))}_{\geq 1}\cdot p^m\cdot(p^{n-m}-1)$$

is always true, for every choice of n and m. We will have to put further technical restrictions on the characteristic polynomials $F_{A^{(M)}}(T)$ in order to obtain results concerning such $\mathbb{Z}_p$-extensions (compare Lemma 3.62 below).

(iv) In the proof of the preceding statements, we have used the inequality $\mathrm{rank}_{\nu_{(n,m)}}(A^{(M)}/M_1^{(M)}) \leq \mathrm{rank}_{\nu_{(n,m)}}(A^{(M)})$ (compare (3.3)). We can make this more precise, using the following

Proposition 3.58. *Let $\lambda \in \Lambda$ denote either a distinguished polynomial, or $\lambda = p$. Let M/K denote a $\mathbb{Z}_p$-extension, and assume that λ is coprime to the characteristic polynomial $F_{A^{(M)}}(T)$ of $A^{(M)}$ (this means that we want $\lambda \neq p$ if $\mu(M/K) \neq 0$). Then*

$$\begin{aligned} \mathrm{rank}_\lambda(A^{(M)}) &= \mathrm{rank}_\lambda(A^{(M)}/M_1^{(M)}) + \mathrm{rank}_\lambda(M_1^{(M)}) \\ &= \mathrm{rank}_\lambda(A^{(M)}/M_1^{(M)}) + v_p(|M_1^{(M)}/(\lambda \cdot M_1^{(M)})|) \, . \end{aligned}$$

Proof. We will make use of Proposition 3.43. Recall that for every element $\lambda \in \Lambda$ and every Λ-module N, we defined $N[\lambda] := \{x \in N \mid \lambda \cdot x = 0\}$ and $Q_\lambda(N) := \frac{|N[\lambda]|}{|N/(\lambda \cdot N)|}$, whenever both orders are finite (compare Definition 3.42).
In our situation, Proposition 3.43, (ii), applied to the exact sequence

$$0 \longrightarrow M_1^{(M)} \longrightarrow A^{(M)} \longrightarrow A^{(M)}/M_1^{(M)} \longrightarrow 0 \, ,$$

implies that $Q_\lambda(A^{(M)}) = Q_\lambda(A^{(M)}/M_1^{(M)}) \cdot Q_\lambda(M_1^{(M)})$. Since $M_1^{(M)}$ is finite, we have $Q_\lambda(M_1^{(M)}) = 1$, by Proposition 3.43, (i).
Furthermore, λ acts injectively on $A^{(M)}/M_1^{(M)} \cong E_{A^{(M)}}$, using our assumption that λ is coprime to the characteristic polynomial of $A^{(M)}$. Therefore $A^{(M)}[\lambda] \subseteq M_1^{(M)}[\lambda]$, and $Q_\lambda(A^{(M)}/M_1^{(M)}) = p^{-\mathrm{rank}_\lambda(A^{(M)}/M_1^{(M)})}$. It follows that

$$\begin{aligned} p^{-\mathrm{rank}_\lambda(A^{(M)}/M_1^{(M)})} &= Q_\lambda(A^{(M)}) = \frac{|A^{(M)}[\lambda]|}{|A^{(M)}/(\lambda \cdot A^{(M)})|} \\ &= \frac{|M_1^{(M)}[\lambda]|}{p^{\mathrm{rank}_\lambda(A^{(M)})}} = p^{\mathrm{rank}_\lambda(M_1^{(M)}) - \mathrm{rank}_\lambda(A^{(M)})} \, , \end{aligned}$$

proving Proposition 3.58. □

We therefore may replace inequality (3.3) by the equality

$$\mathrm{rank}_{\nu_{(n,m)}}(A^{(M)}/M_1^{(M)}) + \mathrm{rank}_{\nu_{(n,m)}}(M_1^{(M)}) = \mathrm{rank}_{\nu_{(n,m)}}(A^{(M)}) \, .$$

Now

$$|M_1^{(M)}/(\nu_{(n,m)} \cdot M_1^{(M)})| = \prod_{i=m}^{n-1} |(\nu_{(i,m)} \cdot M_1^{(M)})/(\nu_{(i+1,m)} \cdot M_1^{(M)})| \, .$$

Applying Nakayama's Lemma 1.43 to the compact Λ-module $M_1^{(M)}$, we see that

$$\text{either} \quad M_1^{(M)} = \{0\} \quad \text{or} \quad \nu_{(m+1,m)} \cdot M_1^{(M)} \neq M_1^{(M)} \ ,$$

i.e., $|M_1^{(M)}/(\nu_{(m+1,m)} \cdot M_1^{(M)})| \geq p$. Analogously,

$$\text{either} \quad \nu_{(m+1,m)} \cdot M_1^{(M)} = \{0\} \quad \text{or} \quad \nu_{(m+2,m)} \cdot M_1^{(M)} \neq \nu_{(m+1,m)} \cdot M_1^{(M)} \ ,$$

i.e., $|(\nu_{(m+1,m)} \cdot M_1^{(M)})/(\nu_{(m+2,m)} \cdot M_1^{(M)})| \geq p$ and therefore

$$\mathrm{rank}_{\nu_{(n,m)}}(M_1^{(M)}) \ \geq \ 2 \ .$$

Inductively, we obtain that $\mathrm{rank}_{\nu_{(n,m)}}(M_1^{(M)}) \geq n-m$ as long as we don't have $\nu_{(n,m)} \cdot M_1^{(M)} = \{0\}$. But in the latter case, $M_1^{(M)}[\nu_{(n,m)}] = M_1^{(M)}$, and therefore $\mathrm{rank}_{\nu_{(n,m)}}(M_1^{(M)}) = v_p(|M_1^{(M)}|)$. We have thus shown that

$$\mathrm{rank}_{\nu_{(n,m)}}(M_1^{(M)}) \ \geq \ n-m \qquad \text{whenever} \qquad |M_1^{(M)}| \ \geq \ p^{n-m} \ .$$

More generally, this argument shows that for every $j \leq n-m$, we have

$$\mathrm{rank}_{\nu_{(n,m)}}(M_1^{(M)}) \ \geq \ j \qquad \text{whenever} \qquad |M_1^{(M)}| \ \geq \ p^j \ .$$

Choosing $n_i = 2i$ and $m_i = i$ with $i \geq \max(i_2, C+1)$, as in the proof of (ii), the inequality (3.5) from that proof yields that for every $j \leq i = n_i - m_i$ and every $M \in U(L, w_i)$ satisfying $\mu(M/K) = \mu(L/K)$,

$$\text{either} \quad |M_1^{(M)}| < p^j \quad \text{or} \quad i \cdot \lambda^{(M)} + j \leq i \cdot \lambda + C \ .$$

In particular, if $M \in U(L, w_i)$ also satisfies $\lambda^{(M)} = \lambda$, then

$$\text{either} \quad |M_1^{(M)}| < p^j \quad \text{or} \quad j \leq C$$

for every $j \leq i$. Letting $j = C+1$, we may conclude that

$$|M_1^{(M)}| \ < \ p^{C+1} \ = \ p \cdot |M_1^{(L)}| \ ,$$

using the definition of C, and therefore

$$|M_1^{(M)}| \ \leq \ |M_1^{(L)}| \ .$$

Remark 3.59. Note that actually we have proved a bit more: If we apply Proposition 3.58 to both $A^{(M)}$ and $A^{(L)}$, then we can turn the inequality (3.2) into an equality and replace the right-hand side $i \cdot \lambda + C$ of (3.5) by the better upper bound $i \cdot \lambda + |M_1^{(L)}[\nu_{(n_i,m_i)}]|$. This means that

$$|M_1^{(M)}[\nu_{(n_i,m_i)}]| \ = \ |M_1^{(L)}[\nu_{(n_i,m_i)}]|$$

for every $M \in U(L, w_i)$ satisfying $\lambda^{(M)} = \lambda$, provided that $i \geq i_2$. In particular, if $i \geq v_p(|M_1^{(L)}|) \geq v_p(|M_1^{(M)}|)$, then

$$M_1^{(L)}[\nu_{(n_i,m_i)}] \;=\; M_1^{(L)} \quad \text{and} \quad M_1^{(M)}[\nu_{(n_i,m_i)}] \;=\; M_1^{(M)}$$

for every $M \in U(L, w_i)$ satisfying $\mu(M/K) = \mu$ and $\lambda(M/K) = \lambda$, and thus

$$|M_1^{(M)}| \;=\; |M_1^{(L)}|$$

for these M. We will give another proof of this fact in Corollary 3.75, under the assumption that $\mu(L/K) = 0$.

Now fix i as in Remark 3.59. For $M \in U(L, w_i)$, we let $Y_i^{(M)}$ denote the kernel of the i-th projection map $A^{(M)} \longrightarrow A_i^{(M)}$, respectively. Then $A_n^{(M)} \cong A^{(M)}/(\nu_{(n,i)} \cdot Y_i^{(M)})$ for every $n \geq i$. Moreover,

$$\begin{aligned} |A_n^{(M)}| &= |A^{(M)}/(\nu_{(n,i)} \cdot A^{(M)})| \cdot |(\nu_{(n,i)} \cdot A^{(M)})/(\nu_{(n,i)} \cdot Y_i^{(M)})| \\ &= p^{\mathrm{rank}_{\nu_{(n,i)}}(A^{(M)})} \cdot |A_i^{(M)}| \cdot \frac{|Y_i^{(M)} \cap M_1^{(M)}|}{|M_1^{(M)}|} \end{aligned}$$

for every $n \geq 2i$, because the map

$$\phi_{(n,i)} \,:\, A^{(M)}/Y_i^{(M)} \;\longrightarrow\; (\nu_{(n,i)} \cdot A^{(M)})/(\nu_{(n,i)} \cdot Y_i^{(M)})$$

given by multiplication by $\nu_{(n,i)}$ is a surjective homomorphism having kernel $(Y_i^{(M)} + M_1^{(M)})/Y_i^{(M)}$ (apply Proposition 1.44 and use the fact that $\nu_{(n,i)}$ annihilates $M_1^{(M)}$ if $n - i \geq i$).
In particular, if $U \subseteq U(L, w_i)$ is a sufficiently small neighbourhood, then

$$|Y_i^{(M)} \cap M_1^{(M)}| \;=\; |Y_i^{(L)} \cap M_1^{(L)}|$$

for every $M \in U$. Since $Y_i^{(M)} \cap M_1^{(M)}$ is the maximal finite Λ-submodule of $Y_i^{(M)} \subseteq A^{(M)}$, respectively, Proposition 3.58 implies that

$$\mathrm{rank}_{\nu_{(n,m)}}(Y_i^{(M)}) \;=\; \mathrm{rank}_{\nu_{(n,m)}}(Y_i^{(L)})$$

for every $M \in U$ and for all pairs $n > m \geq i$ satisfying $n - m = m$.
But then

$$|A_n^{(M)}| \;=\; |A_i^{(M)}| \cdot |Y_i^{(M)}/(\nu_{(n,i)} \cdot Y_i^{(M)})| \;=\; |A_n^{(L)}|$$

for arbitrarily large n, proving that $\nu(M/K) \;=\; \nu(L/K)$ for every $M \in U$. □

Corollary 3.60. *Suppose that $\mathbb{K}/K$ is a $\mathbb{Z}_p^k$-extension, $k \in \mathbb{N}$. Let $\mathcal{E}^{\subseteq \mathbb{K}}(K)$ denote the set of $\mathbb{Z}_p$-extensions of K contained in $\mathbb{K}$. If there exist an integer $0 \leq \mu \in \mathbb{Z}$ and a set $P \subseteq \mathcal{I}$ of prime ideals of K dividing p such that $\mu(M/K) = \mu$ and $\mathcal{P}(M) = P$ for every $M \in \mathcal{E}^{\subseteq \mathbb{K}}(K)$, then $\lambda(M/K)$ is* **globally bounded** *on the set $\mathcal{E}^{\subseteq \mathbb{K}}(K)$.*

Proof. Since $\mu(M/K) = \mu$ for every $M \in \mathcal{E}^{\subseteq \mathbb{K}}(K)$, λ is locally maximal, and in particular locally bounded, in appropriate neighbourhoods of every $M \in \mathcal{E}^{\subseteq \mathbb{K}}(K)$. Moreover, since $\mathcal{P}(M) = P$ for every M, the set $\mathcal{E}^{\subseteq \mathbb{K}}(K)$ is compact with respect to the Greenberg-R-topology (compare Remarks 3.26, (2)). This proves the corollary. □

Remark 3.61. Note that this corollary generalises Greenberg's Theorem 2.30, which is the case $\mu = 0$ and $P = \mathcal{I} = \{\mathfrak{p}\}$.

We cannot say much in the case of a 'jump' of the μ-invariant, i.e., if $\mu(M/K) < \mu(L/K)$ for some $M \in U(L, n)$. In order to obtain boundedness results in this situation, we have to put technical assumptions on the involved characteristic polynomials, as in the following lemma. In fact, it seems likely that the λ-invariant can be unbounded in the neighbourhood of a $\mathbb{Z}_p$-extension L whose μ-invariant is 'isolated', i.e., if $\mu(L/K) > \mu(M/K)$ for infinitely many M contained in some small neighbourhood of L (compare Theorem 4.43).

Lemma 3.62. *Let L/K be a $\mathbb{Z}_p$-extension. Write $\mu := \mu(L/K)$. Let further $y \in \mathbb{N}_0$. As in Theorem 3.57, we define the set $\mathcal{E}^y(K)$ to consist of those $\mathbb{Z}_p$-extensions M/K satisfying $\mu(M/K) = y$. For every $x \in \mathbb{N}$, we let $\mathcal{E}_x(K)$ denote the set of $\mathbb{Z}_p$-extensions $M \in \mathcal{E}(K)$ such that every coefficient of the characteristic polynomial $F_{A^{(M)}}(T)$, besides the leading coefficient, is divisible by p^x, respectively. Then there exists an integer $w \in \mathbb{N}$ such that the following holds:*
For $0 \leq x \leq \mu$, λ is bounded in each of the sets $\mathcal{E}^{\mu-x}(K) \cap \mathcal{E}_{x+1}(K) \cap U(L, w)$, respectively.

Proof. We will use the notation introduced in the proof of Theorem 3.57. If $F_{A^{(M)}}(T)$ is a distinguished polynomial such that every coefficient, besides the leading one, is divisible by p^{x+1}, then either

$$v_p(F_{A^{(M)}}(\zeta_{p^l} - 1)) \;=\; \frac{\lambda^{(M)}}{p^{l-1}(p-1)} \;<\; x + 1 \;,$$

or $v_p(F_{A^{(M)}}(\zeta_{p^l} - 1)) \geq x + 1$. This means that the inequality (3.4) from the proof of Theorem 3.57 may be strengthened to

$$\begin{aligned} & (p^n - p^m) \cdot \mu(M/K) \,+\, (x+1) \cdot p^m(p^r - 1) \,+\, (n - m - r) \cdot \lambda^{(M)} \\ \leq\; & (p^n - p^m) \cdot \mu \,+\, (n-m) \cdot \lambda \,+\, C \;. \end{aligned}$$

Choosing the sequences $m_i := i \to \infty$, $n_i := m_i + i$, $i \geq 0$, this implies that for i large enough to ensure that $\frac{\lambda}{p^{i-1}(p-1)} < 1$, we have

$$\begin{aligned} & p^{m_i}(p^i - 1) \cdot \mu(M/K) \,+\, (x+1) \cdot p^{m_i}(p^{r_i} - 1) \,+\, (i - r_i) \cdot \lambda^{(M)} \\ \leq\; & p^{m_i}(p^i - 1) \cdot \mu \,+\, \lambda \,+\, C \;. \end{aligned}$$

Choosing $i_1 \in \mathbb{N}$ such that $p^{m_{i_1}}(p^{i_1} - 1) > \lambda + C$, we may conclude that $r_i < i$ for every pair (n_i, m_i) with $i \geq i_1$ and every M contained in the neighbourhood $U(L, w_i) \cap \mathcal{E}_{x+1}(K) \cap \mathcal{E}^{\mu-x}(K)$ of L. In particular, by definition of r_i,

$\frac{\lambda^{(M)}}{p^{l-1}(p-1)} < x+1$ for $l = m_{i_1} + i_1 = n_{i_1}$, and therefore

$$\lambda^{(M)} \ < \ (x+1) \cdot p^{2i_1-1}(p-1)$$

is bounded in this (restricted) neighbourhood of L. □

3.3.4 Further generalisations

Let L/K denote a $\mathbb{Z}_p$-extension. So far, we have only worked with the Fukuda module $A^{(L)} = \varprojlim A_n^{(L)}$. However, the general results concerning Fukuda modules developed in Section 3.1, in particular the Quotient Lemma 3.10 and the study of Λ-complementable submodules in Lemma 3.12, yield several more general classes of Fukuda modules that may be studied analogously. In the following theorem, we summarise the corresponding results for two main classes of Fukuda modules related to $A^{(L)}$ that have been introduced in Examples 3.11 and 3.14, respectively.

Theorem 3.63. *Let L/K and $A^{(L)} = \varprojlim A_n^{(L)}$ be as above.*

(1) Let $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ denote a finite set of primes of K. Let $S' := S \cup \mathcal{I}$ denote the union of S with the set of primes dividing p. Assume that every prime $\mathfrak{p} \in S'$ is finitely decomposed in L/K. We define the module $(A^{(L)})^S := \varprojlim_n A_n^{(L)}/(D_n^{(L)})^S$, as in Example 3.11, (2). Let $\mu^S(L/K)$, $\lambda^S(L/K)$ and $\nu^S(L/K)$ denote the corresponding Iwasawa invariants. Then

- *(i) $\mu^S(L/K)$ is locally maximal, i.e., there exists an integer $n \in \mathbb{N}$ such that $\mu^S(M/K) \leq \mu^S(L/K)$ for every $M \in U(L,n)$.*
- *(ii) Assume that $\mu^S(L/K) = 0$. Then λ^S is locally maximal. If, more generally, $\mu^S(L/K) > 0$, then $\lambda^S(L/K)$ is locally maximal if we restrict to the subset of $\mathbb{Z}_p$-extensions M/K with $\mu^S(M/K) = \mu^S(L/K)$.*
- *(iii) If $\mu^S(L/K) = \lambda^S(L/K) = 0$, then there exists some $n \in \mathbb{N}$ such that $\mu^S(M/K) = \lambda^S(M/K) = 0$ and $\nu^S(M/K) = \nu^S(L/K)$ for every $M \in U(L,n)$. More generally, $\nu^S(L/K)$ is locally constant if we restrict to the subset of $\mathbb{Z}_p$-extensions M of K that satisfy $\mu^S(M/K) = \mu^S(L/K)$ and $\lambda^S(M/K) = \lambda^S(L/K)$.*

(2) In the situation of (1), we may even more generally consider R-generalised S-class groups, as defined in Example 3.11, (3).

(3) Assume that $k \subseteq K$ is a subfield such that K/k is abelian of degree prime to p. Let $\Delta := \mathrm{Gal}(K/k)$, and denote by $\mathcal{E}(K|k) \subseteq \mathcal{E}(K)$ the subset of $\mathbb{Z}_p$-extensions L of K that are galois over k with Galois group

$$\mathrm{Gal}(L/k) \ \cong \ \mathrm{Gal}(L/K) \times \Delta \ .$$

Assume that $L \in \mathcal{E}(K|k)$. Then we have a decomposition of $\mathbb{Z}_p[\Delta]$-modules

$$A^{(L)} \ = \ \bigoplus_{i=1}^{s} \varepsilon_i \cdot A^{(L)} \ ,$$

where $\varepsilon_1, \ldots, \varepsilon_s$ denote the idempotents introduced in Example 3.14, (1). Each module $\varepsilon_i \cdot A^{(L)}$ is a finitely generated torsion Λ-module. Let $\mu_i(L/K)$, $\lambda_i(L/K)$ and $\nu_i(L/K)$ denote the corresponding Iwasawa invariants, respectively.
Then for every $i \in \{1, \ldots, s\}$, statements analogous to (1), (i), (ii) and (iii) hold when restricted to $\mathcal{E}(K|k)$. For example, for each $i \in \{1, \ldots, s\}$,
(i) $\mu_i(L/K)$ is locally maximal in $U(L, n) \cap \mathcal{E}(K|k)$ for suitable $n \in \mathbb{N}$.

Proof. (1) Since every prime $\mathfrak{p} \in S'$ is finitely decomposed in L/K, we know that $(A^{(L)})^S = \varprojlim (A_n^{(L)})^S$ is a Fukuda module, where we let

$$(A_n^{(L)})^S := A_n^{(L)}/(D_n^{(L)})^S\,, \quad n \in \mathbb{N}_0$$

(compare Example 3.11, (2)). Moreover, there exists an integer $n_0 \in \mathbb{N}$ such that the number of primes of L_n dividing some prime $\mathfrak{p} \in S'$ stabilises for $n \geq n_0$. We may assume that $n_0 \geq e(L/K)$. Then we consider an arbitrary $\mathbb{Z}_p$-extension $M \in \mathcal{E}(L, n_0 + 1)$. Since for every prime $\mathfrak{p} \in S'$, the corresponding primes in $L_{n_0} = M_{n_0}$ are either ramified or inert in $L_{n_0+1} = M_{n_0+1}$, it follows that each $\mathfrak{p} \in S'$ is ramified or inert in M (using the uniqueness of the intermediate fields in the abelian extension M/K; compare the proof of Theorem 3.2, (i)). In particular, each $\mathfrak{p} \in S'$ is finitely decomposed in M/K, so that $(A^{(M)})^S = \varprojlim (A_n^{(M)})^S$ is defined. If $M \in U(L, n)$ with $n > n_0 \geq e(L/K)$, then $e(M/K) = e(L/K)$ and furthermore $(A_i^{(M)})^S = (A_i^{(L)})^S$ for every $i \leq n$. Therefore, the statements (i), (ii) and (iii) can be proved by using the same arguments as in Lemma 3.56, respectively, Theorem 3.57, respectively, Corollary 3.22, replacing the Fukuda module A by the Fukuda module A^S.
(2) This can be proved analogously to (1).
(3) Lemma 3.12 implies that each factor $\varepsilon_k \cdot A^{(L)}$ in the decomposition of $A^{(L)}$ is a Fukuda module (compare Example 3.14, (1)).
Now we may copy the proof of (1), applying our results to every component $\varepsilon_i \cdot A^{(L)}$, respectively.

□

Note for (1): The case of the cyclotomic $\mathbb{Z}_p$-extension of K and $S = \mathcal{I}$ has been studied before by Y. Mizusawa in [Miz 10], obtaining part of (ii) and (iii).

Remark 3.64. Note that the condition in (3) to be a $\mathbb{Z}_p$-extension contained in $\mathcal{E}(K|k) \subseteq \mathcal{E}(K)$ is restrictive: in general, an arbitrarily chosen $\mathbb{Z}_p$-extension L of K will not satisfy this condition. However, at least $r_2(k)$ independent $\mathbb{Z}_p$-extensions of K with these properties do exist: For every $\mathbb{Z}_p$-extension l of k, we may take $L := l \cdot K$, since $p \nmid [K : k]$ and therefore $K \cap l = k$, i.e., $\mathrm{Gal}(L/k) \cong \mathrm{Gal}(l/k) \times \mathrm{Gal}(K/k)$, as desired.

3.4 Stabilisation of Capitulation kernels and the λ-invariant

In the current section, we will introduce the concept of *capitulation* and describe the relations to Iwasawa invariants. More precisely, we will study the growth of the *capitulation kernels* in a $\mathbb{Z}_p$-extension L/K. These are defined as follows. If we denote by

$$i_n := i_{n,n+1} : A_n \longrightarrow A_{n+1}$$

the ideal lift map between the p-Sylow subgroups of the ideal class groups of the intermediate fields L_n and L_{n+1}, $n \geq 0$, then the kernel of i_n is called the n-th ***capitulation kernel***. It consists of all ideal classes $C \in A_n$ that ***capitulate*** in A_{n+1}. If $C \in A_n$, and if an ideal I of $\mathcal{O}_{L_n}$ denotes any representative of C, then C capitulates in A_{n+1} if and only if the lift $I \cdot \mathcal{O}_{L_{n+1}}$ becomes a principal ideal.

We will establish a connection between the p-ranks of these capitulation kernels for large n on the one side and Iwasawa's λ-invariant on the other side. Moreover, we will show that the capitulation kernels in a natural way correspond to the finite torsion submodule of $A = \varprojlim A_n$.

We start with an algebraic analysis of the structure of the groups A_n for large n.

Lemma 3.65 (Mihăilescu)**.** *Let G and H be two finite abelian p-groups (written additively), and let $N : H \longrightarrow G$ and $i : G \longrightarrow H$ be two group homomorphisms such that:*
(i) *N is surjective.*
(ii) $\mathrm{rank}_p(G) = \mathrm{rank}_p(H)$.
(iii) *$N(i(x)) = p \cdot x$ for every $x \in G$.*
(iv) $\mathrm{subexp}(G) := \min\{\mathrm{ord}(x) \mid x \in G \setminus p \cdot G\} > p$.
Then $i(G) = p \cdot H$.

Proof. See [Be 12], Theorem 4.2.1. □

We will show now how to apply this result to the ideal class groups of the intermediate fields in a $\mathbb{Z}_p$-extension.

Lemma 3.66. *Let L/K be a $\mathbb{Z}_p$-extension satisfying $\mu(L/K) = 0$. We denote by $i_n : A_n \longrightarrow A_{n+1}$ the ideal lift map, $n \geq 0$. Then there exists an integer $N_1 \in \mathbb{N}_0$ such that*

$$i_n(A_n) \;=\; p \cdot A_{n+1}$$

for every $n \geq N_1$.

Proof. We will check the conditions from Lemma 3.65. Let $n \in \mathbb{N}_0$ be arbitrary; step by step, we will choose it large enough in order to make things work. Define $G := A_n$, $H := A_{n+1}$, $i := i_n$, and let

$$N := N_{n+1,n} : A_{n+1} \longrightarrow A_n$$

be the norm map. Then it follows from class field theory that N is surjective if $n \geq e(L/K) =: e$ (see [Wa 97], Theorem 10.1).

Furthermore, it is a well-known fact that $N_{n+1,n}(i_n(x)) = p \cdot x$ for every $n \geq 0$ and any $x \in A_n$. Since the Norm maps $N_{n+1,n} : A_{n+1} \longrightarrow A_n$ are surjective for $n \geq e$, it follows that $\mathrm{rank}_p(A_{n+1}) \geq \mathrm{rank}_p(A_n)$ for such n. But $\mu(L/K) = 0$, and therefore $\mathrm{rank}_p(A_n)$ is bounded for $n \to \infty$. Therefore there exists an integer $n_0 \in \mathbb{N}$, $n_0 > e$, such that $\mathrm{rank}_p(A_m) = \mathrm{rank}_p(A_{n_0})$ for every $m \geq n_0$.

It remains to show that the subexp-assumption of Lemma 3.65 is satisfied for large n. In order to deal with this problem, we will study the algebraic structure of the A_n for $n > n_0$. Since A_n is a finite abelian p-group, we may write

$$A_n \cong \mathbb{Z}/p^{e_{n,1}}\mathbb{Z} \oplus \mathbb{Z}/p^{e_{n,2}}\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/p^{e_{n,k_n}}\mathbb{Z} \oplus \underbrace{\mathbb{Z}/p\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/p\mathbb{Z}}_{\alpha_n \text{ factors}}$$

with integers $\alpha_n, k_n \in \mathbb{N}_0$, $e_{n,i} \in \mathbb{N}$, $i \in \{1, \ldots, k_n\}$, such that

$$e_{n,1} \geq e_{n,2} \geq \ldots \geq e_{n,k_n} > 1 \, .$$

We write $A_n = B_n \oplus A'_n$, where A'_n corresponds to the p-elementary subgroup in the above decomposition, and where B_n corresponds to the 'well-behaved' part satisfying the subexp $> p$-condition.

Note that $\alpha_n := \mathrm{rank}_p(A'_n)$ is independent from the choice of the specific maximal p-elementary subgroup A'_n of A_n.

Proposition 3.67. *With the above notation, $\alpha_m \leq \alpha_n$ whenever $m \geq n \geq n_0$.*

Proof. It suffices to prove this for $m = n + 1$. Consider the decompositions

$$A_{n+1} \cong \mathbb{Z}/p^{e_{n+1,1}}\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/p^{e_{n+1,k_{n+1}}}\mathbb{Z} \oplus \underbrace{\mathbb{Z}/p\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/p\mathbb{Z}}_{\alpha_{n+1} \text{ factors}}$$

$$A_n \cong \mathbb{Z}/p^{e_{n,1}}\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/p^{e_{n,k_n}}\mathbb{Z} \oplus \underbrace{\mathbb{Z}/p\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/p\mathbb{Z}}_{\alpha_n \text{ factors}}$$

and the norm map $N := N_{n+1,n} : A_{n+1} \longrightarrow A_n$. For $i = 1, \ldots, k_{n+1} + \alpha_{n+1}$, choose generators $x_i^{(n+1)} \in A_{n+1}$ of the cyclic factors contained in A_{n+1} which under a fixed isomorphism correspond to the $\mathbb{Z}/p^{e_{n+1,i}}\mathbb{Z}$-factor, respectively. In particular, $x_{k_{n+1}+1}^{(n+1)}, \ldots, x_{k_{n+1}+\alpha_{n+1}}^{(n+1)}$ generate a p-elementary subgroup A'_{n+1} of A_{n+1}.

Since $n \geq n_0$, we have

$$k_{n+1} + \alpha_{n+1} = \mathrm{rank}_p(A_{n+1}) = \mathrm{rank}_p(A_n) = k_n + \alpha_n \, .$$

Since the Norm map is surjective, there is a decomposition of A_n into cyclic groups such that every generator $x_i^{(n+1)} \in A_{n+1}$ yields a generator

$$x_i^{(n)} := N(x_i^{(n+1)}) \in A_n \, .$$

If $0 \neq x_i^{(n+1)} \in A'_{n+1}$, then $p \cdot x_i^{(n+1)} = 0$ and therefore

$$p \cdot x_i^{(n)} = p \cdot N(x_i^{(n+1)}) = N(p \cdot x_i^{(n+1)}) = 0 \, .$$

By the above, $N(x_i^{(n+1)}) \neq 0$ because otherwise the p-rank of $A_n = N(A_{n+1})$ would be smaller than the p-rank of A_{n+1}. In fact, this rank equality implies that the kernel of N has to be contained in $p \cdot A_{n+1}$ (compare the proof of Proposition 3.68, (iv) below).

Therefore $x_i^{(n)}$ generates a cyclic subgroup of order p. Since $x_i^{(n)} = N(x_i^{(n+1)})$ cannot be contained in $p \cdot A_n$, by the surjectivity of N, we conclude that $x_i^{(n)}$ generates a cyclic factor of A_n'. This shows that

$$\alpha_n \;=\; \mathrm{rank}_p(A_n') \;\geq\; \mathrm{rank}_p(A_{n+1}') \;=\; \alpha_{n+1}\;,$$

since the images $x_i^{(n)} = N(x_i^{(n+1)})$, $i \in \{k_{n+1}+1, \ldots, k_{n+1}+\alpha_{n+1}\}$, generate a p-elementary subgroup of A_n of rank α_{n+1}.

Note that α_n can be strictly larger than α_{n+1} since the norm map in general is not injective. □

Now we look at the sequence $(\alpha_i)_{i \geq n_0}$. Since $\alpha_j \leq \alpha_i$ for $j \geq i$ and as

$$\alpha_i \;\leq\; \mathrm{rank}_p(A_i) \;\leq\; \mathrm{rank}_p(A) \;<\; \infty$$

for every i, there exists an integer $N_1 \geq n_0$ such that $\alpha_n = \alpha_{N_1} =: \alpha$ for all $n \geq N_1$, i.e. the p-rank of A_n' stabilises. Then also

$$\mathrm{rank}_p(B_n) \;=\; \mathrm{rank}_p(B_{N_1})$$

for every $n \geq N_1$. Now let $n \geq N_1$ be arbitrary. Look at the decomposition $A_{n+1} = B_{n+1} \oplus A_{n+1}'$ induced by

$$A_{n+1} \;\cong\; \mathbb{Z}/p^{e_{n+1,1}}\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/p^{e_{n+1,k_{n+1}}}\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/p\mathbb{Z}\;.$$

Proposition 3.68. *With the above notation, we have:*
(i) $N|_{A_{n+1}'} : A_{n+1}' \longrightarrow A_n$ *is injective.*
(ii) $N(A_{n+1}') = A_n'$ *is a p-elementary subgroup of A_n of p-rank equal to α_n.*
(iii) Letting $B_n := N(B_{n+1})$, we have $B_n \cap A_n' = \{0\}$ and $A_n = B_n \oplus A_n'$.
(iv) We have $i(B_n) \subseteq B_{n+1}$ and $i(A_n') \subseteq p \cdot B_{n+1}$.

Proof. (i) If $0 \neq y \in A_{n+1}'$ was such that $N(y) = 0$, then we would have

$$\begin{aligned} \mathrm{rank}_p(A_n) \;&=\; \mathrm{rank}_p(N(A_{n+1})) \;=\; \mathrm{rank}_p(N(A_{n+1}/{<}y{>})) \\ &\leq\; \mathrm{rank}_p(A_{n+1}/{<}y{>}) \;\leq\; \mathrm{rank}_p(A_{n+1}) - 1\;, \end{aligned}$$

since every proper quotient of a p-elementary group has strictly smaller rank. But for $n \geq N_1$, we have $\mathrm{rank}_p(A_n) = \mathrm{rank}_p(A_{n+1})$.

(ii) We have already seen above that the group $N(A_{n+1}')$ has to be p-elementary. Since $\alpha_n = \alpha_{n+1}$ for $n \geq N_1$, the order of A_n' is equal to

$$|N(A_{n+1}')| \;\overset{(i)}{=}\; |A_{n+1}'| \;=\; p^{\alpha_{n+1}} \;=\; p^{\alpha_n}\;.$$

(iii) Since $N : A_{n+1} \longrightarrow A_n$ is surjective, we have

$$A_n = N(A_{n+1}) = N(B_{n+1} \oplus A'_{n+1}) \subseteq N(B_{n+1}) + N(A'_{n+1})$$

and therefore $A_n = B_n + A'_n$. If $B_n \cap A'_n \neq \{0\}$, then we would have

$$\begin{aligned} \operatorname{rank}_p(A_n) \;=\; \operatorname{rank}_p(B_n + A'_n) \;&<\; \operatorname{rank}_p(B_n) + \operatorname{rank}_p(A'_n) \\ &\leq\; \operatorname{rank}_p(A_{n+1})\ , \end{aligned}$$

since $A'_n \cap B_n \subseteq A'_n$ is p-elementary. This again gives a contradiction.

(iv) Let $x \in B_n$. Assume that $i(x) = y + z$ with $y \in B_{n+1}$ and $z \in A'_{n+1}$. Then

$$B_n \ni p \cdot x \;=\; N(i(x)) \;=\; N(y+z) \;=\; \underbrace{N(y)}_{\in B_n} + \underbrace{N(z)}_{\in A'_n}\ .$$

Therefore $N(z) = p \cdot x - N(y) \in B_n \cap A'_n = \{0\}$. Using (i), we see that $z = 0$, i.e., $i(x) = y \in B_{n+1}$.
Now let $x \in A'_n$. Write $i(x) = y + z$ with $y \in B_{n+1}$ and $z \in A'_{n+1}$. Then we have

$$0 \;=\; p \cdot x \;=\; N(i(x)) \;=\; N(y) + N(z)$$

and therefore $N(y) = -N(z) \in B_n \cap A'_n = \{0\}$. In particular, $N(z) = 0$ and therefore $z = 0$ by (i). This means that $i(x) = y \in B_{n+1} \cap \operatorname{Ker}(N)$. Now consider the map

$$\overline{N} : A_{n+1}/p \cdot A_{n+1} \longrightarrow A_n/p \cdot A_n$$

induced by N. $\overline{N}$ is well-defined because $N(p \cdot A_{n+1}) = p \cdot A_n$, and surjective because N is surjective. Since $\operatorname{rank}_p(A_n) = \operatorname{rank}_p(A_{n+1})$ for $n \geq n_0$, $\overline{N}$ is also injective as being a map between finite sets of the same cardinality. But this shows that the kernel of N is contained in $p \cdot A_{n+1}$. In particular, $y \in p \cdot A_{n+1}$, and so $i(x) \in B_{n+1} \cap p \cdot A_{n+1} = p \cdot B_{n+1}$.

□

Now we return to the proof of Lemma 3.66. Consider an arbitrary $n \geq N_1$ and look at the decomposition $A_{n+1} = B_{n+1} \oplus A'_{n+1}$ which, as decribed above, induces a decomposition $A_n = B_n \oplus A'_n$. Then we can apply Lemma 3.65 to the groups $G := B_n$ and $H := B_{n+1}$, which satisfy all the conditions in 3.65, by Proposition 3.68. Therefore $i(B_n) = p \cdot B_{n+1}$.

But this means that

$$i(A_n) \;=\; i(B_n \oplus A'_n) \;=\; p \cdot B_{n+1} \;=\; p \cdot A_{n+1}\ ,$$

using Proposition 3.68, (iii) and (iv), Lemma 3.65 and the fact $p \cdot A'_{n+1} = \{0\}$, respectively. □

Remarks 3.69.

(1) Using the notation from the preceding proof, let $n \geq n_0$, i.e., assume that $\operatorname{rank}_p(A_n) = \operatorname{rank}_p(A_{n+1})$. Then $i_n(B_n) = p \cdot B_{n+1}$ if and only if $\alpha_n = \alpha_{n+1}$.

Proof. '$\Longleftarrow$' : See the proof of Lemma 3.66.
'$\Longrightarrow$' : We have $\alpha_{n+1} \leq \alpha_n$, by Proposition 3.67. Suppose that $\alpha_{n+1} < \alpha_n$. Then

$$\begin{aligned} \mathrm{rank}_p(i_n(B_n)) \;=\; \mathrm{rank}_p(p \cdot B_{n+1}) \;&=\; \mathrm{rank}_p(B_{n+1}) \\ &>\; \mathrm{rank}_p(B_n) \;\geq\; \mathrm{rank}_p(i_n(B_n))\;, \end{aligned}$$

which gives a contradiction. □

Note that each of the two statements implies that $i_n(A_n) = p \cdot A_{n+1}$ (compare the end of the proof of Lemma 3.66).

(2) The statement of Lemma 3.66 has been proved by M. Grandet and J.-F. Jaulent in [GJ 85], using the Λ-module structure of the A_n (compare Theorem 3.73 below).

The following theorem establishes the connection between the preceding algebraic structure theory and the study of Iwasawa's λ-invariant.

Theorem 3.70. *Let L/K be a $\mathbb{Z}_p$-extension satisfying $\mu(L/K) = 0$. As usual, we let $A = \varprojlim A_n$.*
Then there exists an integer $N \in \mathbb{N}_0$ such that $\lambda(L/K) = r - r'_n$ for every $n \geq N$, where $r = \mathrm{rank}_p(A) < \infty$ and where r'_n denotes the p-rank of the capitulation kernel $\mathrm{Ker}(i_n : A_n \longrightarrow A_{n+1})$, respectively.

Proof. By Iwasawa's Theorem 1.32, there exists an integer $N_2 \in \mathbb{N}_0$ such that for every $n \geq N_2$, $|A_n| = p^{\mu p^n + \lambda n + \nu}$ where μ, λ and ν denote the Iwasawa invariants of L/K. Let N_1 be the integer defined in Lemma 3.66, and let $N := \max\{N_2, N_1\}$. Let $n \geq N$ be arbitrary, but fixed.

Since $n \geq N_2$, we have $\frac{|A_{n+1}|}{|A_n|} = p^\lambda$, using our assumption that $\mu(L/K) = 0$. The map $i_n : A_n \longrightarrow A_{n+1}$ is a homomorphism between the finite groups A_n and A_{n+1}, and

$$|A_n| \;=\; |\mathrm{Im}(i_n)| \cdot |\mathrm{Ker}(i_n)|\;.$$

If $x \in \mathrm{Ker}(i_n)$, then $p \cdot x = N(i(x)) = N(0) = 0$. This shows that $\mathrm{Ker}(i_n)$ is a p-elementary group. Therefore $|\mathrm{Ker}(i_n)| = p^{r'_n}$ with $r'_n := \mathrm{rank}_p(\mathrm{Ker}(i_n))$. If $n \geq N_1$, then $r_n := \mathrm{rank}_p(A_n) = \mathrm{rank}_p(A)$ by definition of N_1 (compare the proof of Lemma 3.66), and $i_n(A_n) = p \cdot A_{n+1}$. We conclude that

$$p^\lambda \;=\; \frac{|A_{n+1}|}{|A_n|} \;=\; \frac{|A_{n+1}|}{|\mathrm{Im}(i_n)| \cdot p^{r'_n}} \;=\; \frac{|A_{n+1}|}{|pA_{n+1}|} \cdot p^{-r'_n} \;=\; p^{r_n - r'_n} \;=\; p^{r - r'_n}$$

for $n \geq N$. □

Corollary 3.71. *With the above notation, the p-ranks of the capitulation kernels $\mathrm{Ker}(i_n : A_n \longrightarrow A_{n+1})$ stabilise, i.e., there exists an integer $N \in \mathbb{N}$ such that $\mathrm{rank}_p(\mathrm{Ker}(i_n)) = \mathrm{rank}_p(\mathrm{Ker}(i_N))$ for every $n \geq N$.*
Conversely, if the p-ranks of the capitulation kernels and the p-ranks of the A_n have stabilised at $N \in \mathbb{N}$, and if N is larger than the integer N_1 from Lemma 3.66, then also the quotients $\frac{|A_{n+1}|}{|A_n|}$ have stabilised and therefore $|A_n| = p^{\lambda n + \nu}$ for $n \geq N$.

An important improvement of Lemma 3.66 is given by the following result, which yields an effective upper bound on the integer N_1 that will be very useful later:

Lemma 3.72. *Suppose that p is an odd rational prime. Let L/K denote a $\mathbb{Z}_p$-extension satisfying $\mu(L/K) = 0$. Choose an integer $N_0 \geq e(L/K)$ such that*

$$\mathrm{rank}_p(A_{N_0}) \,=\, \mathrm{rank}_p(A_{N_0+1}) \,=\, \mathrm{rank}_p(A) \,=:\, r\ .$$

Let $N_1 \geq N_0$ be such that

$$p^{N_1} > r\ .$$

Then $i_n(A_n) = p \cdot A_{n+1}$ for every $n \geq N_1$.

Proof. This proof is essentially due to P. MIHĂILESCU. We have already seen in the proof of Proposition 3.68, (iv) that $i_n(A_n) \subseteq p \cdot A_{n+1}$ for every $n \geq N_0$. Indeed, $N_{n+1,n}(i_n(x)) = p \cdot x$ for every $x \in A_n$, and therefore the induced map

$$\overline{N_{n+1,n} \circ i_n} : A_n/pA_n \longrightarrow A_n/pA_n$$

is the zero map. But $\overline{N_{n+1,n}} : A_{n+1}/pA_{n+1} \longrightarrow A_n/pA_n$ is an isomorphism, because $n \geq N_0$, proving that $\overline{i_n} : A_n/pA_n \longrightarrow A_{n+1}/pA_{n+1}$ is the zero map.

We will prove that also $p \cdot A_{n+1} \subseteq i_n(A_n)$ if n is taken large enough.

Suppose that $n \geq N_1$, and let $b := b_{n+1} \in A_{n+1}$. If γ denotes a topological generator of $\mathrm{Gal}(L/K) \cong \mathbb{Z}_p$, then $\mathrm{Gal}(L_{n+1}/L_n) \,\cong\, <\sigma> / <\sigma^p>$, where we let $\sigma := \gamma^{p^n}$.

We consider the submodule $M := \Lambda \cdot b$ of the Λ-module A_{n+1}, and we let $\overline{M} := M/pM$, which in a natural way bears a $\mathbb{F}_p$-vector space structure. Since $M \subseteq A_{n+1}$ is a subgroup, we can conclude that

$$\dim_{\mathbb{F}_p}(\overline{M}) \,=\, \mathrm{rank}_p(M) \,\leq\, \mathrm{rank}_p(A_{n+1}) \,=\, r\ .$$

If $\overline{b}$ denotes the coset of $b \in M$ in $\overline{M}$, then this means that the elements

$$\overline{b},\, T \cdot \overline{b},\, \ldots,\, T^{p^n-1} \cdot \overline{b}$$

have to be linearly dependent. Therefore we can write some $T^i \cdot \overline{b}$, $i \leq p^n - 1$, as a linear combination of the other powers $T^j \cdot \overline{b}$. Lifting the relation to M, we obtain a polynomial

$$f(T) \,=\, c_0 \cdot T^{p^n-1} + c_1 T^{p^n-2} + \ldots + c_{p^n-1} \,\in\, \mathbb{Z}_p[T]$$

such that $f(T) \cdot b \,=\, p \cdot x \cdot b$ for some element $x \in \Lambda$ and such that at least one of the coefficients may be assumed to equal 1. In fact, we may assume that $f(T)$ is a distinguished polynomial in $\mathbb{Z}_p[T]$ (see Definition 1.11). Indeed, using the Weierstraß Preparation Theorem 1.14, we can write

$$f(T) \,=\, \tilde{f}(T) \cdot U(T)$$

for some distinguished polynomial $\tilde{f}(T)$ of degree at most $p^n - 1$ and a unit $U(T) \in \Lambda^*$. Then

$$\tilde{f}(T) \cdot b \,=\, p \cdot x \cdot U(T)^{-1} \cdot b \,=\, p \cdot x' \cdot b$$

with $x' := x \cdot U(T)^{-1} \in \Lambda$.

Actually, we may also assume that $x \in \mathbb{Z}_p[T]$ is a polynomial. Indeed, Remark 3.49 implies that there exists an integer $k \in \mathbb{N}$ such that $T^k \cdot A_{n+1} = \{0\}$. In particular, T^k annihilates b, so that we may think of x as being a polynomial of degree less then k.

Now we use Theorem 1.9 and identify $s := \sigma - 1 = \gamma^{p^n} - 1$ with the distinguished polynomial

$$(T+1)^{p^n} - 1 =: T^{p^n} + p \cdot h(T) \,,$$

$h(T) \in \mathbb{Z}_p[T]$ appropriate. Since $f(T)$ is monic, division with remainder in $\mathbb{Z}_p[T]$ yields the existence of two polynomials $q(T), r(T) \in \mathbb{Z}_p[T]$ such that

$$s \;=\; f(T)q(T) + r(T)$$

and such that the degree of $r(T)$ is smaller than $p^n - 1$, which is a bound for the degree of $f(T)$ (this includes the case $r(T) = 0$). Moreover, every coefficient of $r(T)$ is divisible by p because the monic leading terms of s and $f(T)$ cancel (note that $q(T) \neq 0$, since $\deg(f(T)) \leq p^n - 1 < \deg(s)$). Using the equality $f(T) \cdot b = p \cdot x \cdot b$ obtained above, we have therefore shown that

$$s \cdot b \;=\; (p \cdot g(T)) \cdot b$$

for some polynomial $g(T) \in \mathbb{Z}_p[T]$.

Then

$$s^2 \cdot b \;=\; s \cdot s \cdot b \;=\; s \cdot (p \cdot g(T)) \cdot b \;=\; (p \cdot g(T)) \cdot s \cdot b \;=\; (p \cdot g(T))^2 \cdot b \,,$$

and inductively, we obtain

$$s^k \cdot b \;=\; (p \cdot g(T))^k \cdot b \qquad (\star)$$

for every $k \in \mathbb{N}$.

Now we use the fact that the norm

$$N = N_{n+1,n} \;=\; 1 + \sigma + \ldots + \sigma^{p-1} \;=\; \frac{\sigma^p - 1}{\sigma - 1} \;=\; \frac{(s+1)^p - 1}{s}$$

may be written as

$$N \;=\; s^{p-1} + p \cdot u(T) \,,$$

where

$$u(T) \;=\; 1 + \frac{p-1}{2} \cdot s + \ldots \;\in \Lambda^*$$

is a unit, since $s = s(T)$ is distinguished. Letting $b_n := N(b) \in A_n$, we may conclude that

$$\begin{aligned} i_n(b_n) \;&=\; i_n(N(b)) \;=\; (s^{p-1} + p \cdot u(T)) \cdot b \\ &\overset{(\star)}{=}\; p \cdot u(T) \cdot (1 + u(T)^{-1} \cdot p^{p-2} \cdot g(T)^{p-1}) \cdot b \,. \end{aligned}$$

Since $v(T) := 1 + u(T)^{-1} \cdot p^{p-2} \cdot g(T)^{p-1} \in \Lambda^*$ (recall that $p \neq 2$), it follows that

$$p \cdot b \;=\; (u(T)^{-1} \cdot v(T)^{-1}) \cdot i_n(b_n) \;\in\; i_n(A_n) \,,$$

using the fact that $i_n(A_n)$ is a Λ-module since $i_n : A_n \longrightarrow A_{n+1}$ is a Λ-module homomorphism. $\square$

Consider a $\mathbb{Z}_p$-extension L/K satisfying $\mu(L/K) = 0$, and let $A = \varprojlim A_n$, $i_n : A_n \longrightarrow A_{n+1}$, etc. be defined as above. Let

$$T := A[p] := \{a \in A \mid p \cdot a = 0\} .$$

Then $T \subseteq A$ is a Λ-submodule of A, and we can write $T = \varprojlim T_n$, where we let $T_n := \mathrm{pr}_n(T)$ denote the images of T under the n-th projection map $\mathrm{pr}_n : A \longrightarrow A_n$, respectively.

We will desribe now an important connection between $T = \varprojlim T_n$ and the capitulation kernels $\mathrm{Ker}(i_n)$, proved by M. Grandet and J.-F. Jaulent. The following theorem is part of the main result of their article [GJ 85].

Theorem 3.73 (Grandet, Jaulent)**.** *Under the above assumptions, let $\mathfrak{T}$ denote the $\mathbb{Z}_p$-torsion submodule of A, i.e., $A \cong \mathbb{Z}_p^{\lambda} \oplus \mathfrak{T}$, with $\lambda = \lambda(L/K)$ (compare Proposition 1.45, (ii)).*
Then there exist integers $N \in \mathbb{N}$, $a_1, \ldots, a_\lambda \in \mathbb{Z}$ and $a_{\lambda+1}, \ldots, a_r \in \mathbb{N}$, where $r = \mathrm{rank}_p(A)$, such that for any $n \geq N$, the following statements hold.

(i) *$\mathfrak{T}_n \subseteq A_n$ is isomorphic to the kernel of the ideal lift map $i_{n,\infty} : A_n \longrightarrow A$, which contains all classes of A_n that capitulate in some L_m, $m \geq n$.*

(ii) *More precisely, there is a bijection between the elements in $\mathfrak{T}_n$ of order p^k and the kernel of the map $i_{n,n+k} : A_n \longrightarrow A_{n+k}$.*
In particular, we have $|T_n| = |\mathrm{Ker}(i_n = i_{n,n+1} : A_n \longrightarrow A_{n+1})|$.

(iii)

$$A_n \cong \left(\bigoplus_{i=1}^{\lambda} \mathbb{Z}/p^{n+a_i}\mathbb{Z} \right) \oplus \left(\bigoplus_{i=\lambda+1}^{r} \mathbb{Z}/p^{a_i}\mathbb{Z} \right) .$$

Here the right sum corresponds to the torsion, i.e., by the above, measures the capitulation. In particular, the subexp *of the left group tends to infinity.*

Proof. See [GJ 85]. □

Remarks 3.74.

(1) If $M_1 \subseteq A$ denotes the maximal finite Λ-submodule (compare Remarks 2.25, (3)), then $\mathfrak{T} = M_1$. Indeed, $\mathfrak{T}$ is obviously a finite Λ-submodule of A, since A is finitely generated as a $\mathbb{Z}_p$-module by Proposition 1.31, (iii). If, on the other hand, $x \in A$ generates a finite Λ-submodule, then in particular $p^k \cdot x = 0$ for some $k \in \mathbb{N}$.

(2) The decomposition of the A_n in Theorem 3.73, (iii) in general differs from our decomposition $A_n = B_n \oplus A'_n$: We have seen above that the A'_n stabilise for $n \geq N_1$; for such n, the norm maps $N : A'_{n+1} \longrightarrow A'_n$ are bijections by Proposition 3.68. This shows that the projective limit of the A'_n yields a p-elementary $\mathbb{Z}_p$-torsion submodule of A. Therefore the A'_n for large n correspond to the factors of exponent p occurring in the right sum of the theorem. Note that in general there exist also torsion elements of higher order, i.e., $\mathfrak{T} \neq T$.

We will conclude the present section by giving another proof of Remark 3.59 ('$|M_1|$ is locally constant'). We will see that, in the case of vanishing

μ-invariants, a local boundedness result concerning the orders of the torsion subgroups is enough to prove that in fact λ and ν are locally constant.

Corollary 3.75. *Let L/K denote a $\mathbb{Z}_p$-extension satisfying $\mu(L/K) = 0$.*

(i) Let $\mathcal{U}$ denote a neighbourhood of L (with respect to the Greenberg-R-topology) such that $\mu(M/K) = 0$ and $\lambda(M/K) \leq \lambda(L/K)$ for every $M \in \mathcal{U}$. Then there exists a neighbourhood $U(L,n) \subseteq \mathcal{U}$ such that $\nu(M/K) = \nu(L/K)$ for every $M \in U(L,n)$ satisfying $\lambda(M/K) = \lambda(L/K)$.

(ii) Let $t \in \mathbb{N}$. Then there exists a neighbourhood $U(L,n)$ of L such that $\mu(M/K) = 0$, $\lambda(M/K) = \lambda(L/K)$ and $\nu(M/K) = \nu(L/K)$ for every $M \in U(L,n)$ satisfying $v_p(|M_1^{(M)}|) \leq t$.

Proof. (i) First we note that a neighbourhood $\mathcal{U}$ as in the statement of the corollary exists by Theorem 3.57, (ii). Using Theorem 3.57, (iv), we may choose a neighbourhood $U(L,n) \subseteq \mathcal{U}$ such that $v_p(|M_1^{(M)}|) \leq v_p(|M_1^{(L)}|)$ for every $M \in U(L,n)$ satisfying $\lambda(M/K) = \lambda(L/K)$.
We may assume that $\mathrm{rank}_p(A^{(M)}) = \mathrm{rank}_p(A^{(L)})$ for every $M \in U(L,n)$. Then

$$\mathrm{rank}_p(\mathfrak{T}^{(M)}) = \mathrm{rank}_p(\mathfrak{T}^{(L)})$$

for every $M \in U(L,n)$ satisfying $\lambda(M/K) = \lambda(L/K)$, where $\mathfrak{T}^{(M)} = M_1^{(M)}$ denotes the $\mathbb{Z}_p$-torsion submodule of $A^{(M)}$.
Now we assume that $n \geq e(L/K) + v_p(|M_1^{(L)}|)$. Since $M_1^{(L)} = \mathfrak{T}^{(L)}$ is a Fukuda module by Example 3.15, it follows that

$$|\mathfrak{T}_n^{(L)}| = |\mathfrak{T}^{(L)}| \,.$$

Analogously, since $e(M/K) = e(L/K)$ and $v_p(|M_1^{(M)}|) \leq v_p(|M_1^{(L)}|)$ for the $M \in U(L,n)$ under consideration, we have

$$|\mathfrak{T}_m^{(M)}| = |\mathfrak{T}^{(M)}|$$

for every $m \geq n$.
Now we assume that n, moreover, is larger than $N + v_p(|M_1^{(L)}|) + 1$, where N denotes the integer attached to L/K by Theorem 3.73. Then Theorem 3.73, (iii) implies that the exponent of each cyclic subgroup of the 'left term' in the decomposition of $A_n^{(L)}$, corresponding to the 'λ-part', is at least $v_p(|M_1^{(L)}|)+1$. Therefore none of the corresponding cyclic subgroups in $A_n^{(M)} \cong A_n^{(L)}$ can contribute to the torsion subgroup $\mathfrak{T}_n^{(M)}$ of M/K, because $v_p(|M_1^{(M)}|) \leq v_p(|M_1^{(L)}|)$.
In view of the equality

$$\mathrm{rank}_p(\mathfrak{T}_n^{(L)}) = \mathrm{rank}_p(\mathfrak{T}^{(L)}) = \mathrm{rank}_p(\mathfrak{T}^{(M)}) = \mathrm{rank}_p(\mathfrak{T}_n^{(M)}) \,,$$

we therefore have in fact

$$|\mathfrak{T}^{(M)}| = |\mathfrak{T}_n^{(M)}| = |\mathfrak{T}_n^{(L)}| = |\mathfrak{T}^{(L)}| \,.$$

As we have seen in the proof of Theorem 3.57, (iv), this implies that $\nu(M/K) = \nu(L/K)$ for every $M \in U(L,n)$, provided that n is sufficiently large.

(ii) Conversely, let $t \in \mathbb{N}$, and denote by $\mathfrak{M}$ the subset of $M \in \mathcal{E}(K)$ satisfying $v_p(|M_1^{(M)}|) \leq t$. Since $\mu(L/K) = 0$, we know that $E_{A^{(L)}}/(p^{t+1} \cdot E_{A^{(L)}})$ is finite, and therefore

$$\mathrm{rank}_{p^{t+1}}(A^{(L)}) := v_p(|A^{(L)}/(p^{t+1} \cdot A^{(L)})|) < \infty .$$

Moreover, $A^{(L)}/(p^{t+1} \cdot A^{(L)})$ is a Fukuda module by the Quotient Lemma 3.10. This means that we may choose a neighbourhood $U(L,n)$ of L such that

$$\mathrm{rank}_{p^{t+1}}(A_n^{(M)}) = \mathrm{rank}_{p^{t+1}}(A^{(M)}) = \mathrm{rank}_{p^{t+1}}(A^{(L)}) = \mathrm{rank}_{p^{t+1}}(A_n^{(L)})$$

for each $M \in U(L,n)$. In particular, we then have

$$\mathrm{rank}_p(A^{(M)}) = \mathrm{rank}_p(A^{(L)}) < \infty ,$$

i.e., $\mu(M/K) = 0$ for $M \in U(L,n)$.
We assume that n is large enough to ensure that in the decomposition of $A_n^{(L)}$ according to Theorem 3.73, (iii), each cyclic subgroup corresponding to the 'λ-part' has exponent larger than t. If $M \in \mathfrak{M} \cap U(L, n+1)$, then none of these cyclic subgroups in $A_n^{(L)} \cong A_n^{(M)}$ contributes to $M_1^{(M)}$, and therefore $\lambda(M/K) \geq \lambda(L/K)$ and $\mathrm{rank}_p(M_1^{(M)}) \leq \mathrm{rank}_p(M_1^{(L)})$.
On the other hand, we have $\mathrm{rank}_{p^{t+1}}(A^{(M)}) = \mathrm{rank}_{p^{t+1}}(A^{(L)})$ for each $M \in U(L,n)$. In particular, if $N(M)$ denotes the integer of Theorem 3.73 for M (note that a priori, $N(M)$ could be much larger than $N(L)$), and if $m \geq \max(n, N(M))$, then

$$\mathrm{rank}_{p^{t+1}}(A_{m+1}^{(M)}) = \mathrm{rank}_{p^{t+1}}(A_m^{(M)}) = \mathrm{rank}_{p^{t+1}}(A_n^{(M)}) .$$

This means that none of the cyclic subgroups of $A_n^{(M)} \cong A_n^{(L)}$ of exponent smaller than $t+1$ can contribute to the λ-part of M, and therefore $\lambda(M/K) = \lambda(L/K)$, $\mathrm{rank}_p(M_1^{(M)}) = \mathrm{rank}_p(M_1^{(L)})$ and $|M_1^{(M)}| = |M_1^{(L)}|$. □

3.5 Capitulation kernels and units

In the preceding section, we have shown that the Iwasawa λ-invariant is closely related to the asymptotic growth of capitulation kernels. This motivates the study of this arithmetic phenomenon in the present section. We will establish a link between the orders of capitulation kernels on the one side and the orders of suitable cohomology groups of units on the other side. This will then be used in order to obtain a new proof of the fact that λ is locally maximal if μ vanishes (compare Theorem 3.57, (ii)).

Starting point of the well-known theory linking capitulation kernels and units was the following observation of K. Iwasawa: In [Iw 73], Iwasawa constructed isomorphisms between capitulation kernels of quotients of the ideal class groups and the cohomology groups of p-units. If $A = \varprojlim A_n$ denotes

the projective limit of the ideal class groups attached to a $\mathbb{Z}_p$-extension L/K, respectively, then we let $A'_n := A_n/B_n$, $n \geq 0$, where $B_n \subseteq A_n$ is the subgroup generated by ideal classes which contain an ideal all of whose prime factors are ramified in L_{n+1}/L_n, respectively (compare Example 3.11). For every $m \geq n \geq 0$, we denote by $i'_{n,m} : A'_n \longrightarrow A'_m$ the ideal lift map. Furthermore, we define $E' := \bigcup_{n\geq 0} E'_n$, where E'_n denotes the group of p-units in L_n, i.e., the units of the ring $\mathcal{O}_{L_n}[\frac{1}{p}]$ of p-integers in L_n, respectively.

We briefly recall some basic definitions concerning cohomology theory of finite groups: Let G denote a finite cyclic group generated by an element σ. Let A be a G-module, i.e., an abelian group on which G operates. Let n denote the order of G, and consider the elements $s := 1-\sigma$ and $N := 1+\sigma+\ldots+\sigma^{n-1}$ in the group ring $\mathbb{Z}[G]$ acting on A. Then $\mathrm{im}(N) \subseteq \ker(s)$ and $\mathrm{im}(s) \subseteq \ker(N)$ because of the formal identities $N \cdot s = s \cdot N = 0$ in $\mathbb{Z}[G]$. One defines

$$\mathrm{H}^0(G,A) := \frac{\ker(s : A \longrightarrow A)}{N(A)} \quad \text{and} \quad \mathrm{H}^{-1}(G,A) := \frac{\ker(N : A \longrightarrow A)}{s(A)} \ .$$

Note that $s(A) = \{\tau a - a \mid \tau \in G,\, a \in A\}$. Indeed, if $\tau = \sigma^k \in G$, then $\tau a - a = -s \cdot (\sigma^{k-1} + \sigma^{k-2} + \ldots + 1) \cdot a \in s(A)$ for each $a \in A$.

Remark 3.76. There exists a much more general theory, defining cohomology groups $\mathrm{H}^n(G,A)$ for arbitrary $n \in \mathbb{Z}$. For finite cyclic groups G, we have $\mathrm{H}^n(G,A) \cong \mathrm{H}^{-1}(G,A)$ for every odd integer n and $\mathrm{H}^n(G,A) \cong \mathrm{H}^0(G,A)$ for every even n (the isomorphisms being induced by the cup product, compare [NSW 08], Prop. 1.7.1). In the literature, the cohomology group $\mathrm{H}^{-1}(G,A)$ sometimes is denoted by $\mathrm{H}^1(G,A)$.

Theorem 3.77 (Iwasawa)**.** *There are isomorphisms*

$$\varphi'_{n,m} : \ \ker(i'_{n,m} : A'_n \longrightarrow A'_m) \ \xrightarrow{\sim}\ \mathrm{H}^{-1}(\mathrm{Gal}(L_m/L_n), E'_m)$$

for every $m \geq n \geq 0$, and also

$$\varphi_n : \ \ker(i'_{n,\infty} : A'_n \longrightarrow \varinjlim_m A'_m) \ \xrightarrow{\sim}\ \mathrm{H}^{-1}(\mathrm{Gal}(L/L_n), E') \ ,$$

where the direct limit $\varinjlim A'_m$ is taken with respect to the ideal lift maps.

Proof. This is Theorem 12 in [Iw 73]. Iwasawa explicitly defines $\varphi'_{n,m}$, as follows.

Fix a generator σ of $\mathrm{Gal}(L_m/L_n)$. For $c \in \ker(i'_{n,m})$ and a representative $\mathfrak{A} \in c$, we know that $\mathfrak{A} \cdot \mathcal{O}_{L_m}[\frac{1}{p}] = (\alpha)$ becomes principal, and we may assume that $\alpha \neq 0$. Then

$$\varepsilon := \alpha^{\sigma-1}$$

is a p-unit in E'_m, since $\mathfrak{A}^\sigma = \mathfrak{A}$ because $\mathfrak{A} \subseteq \mathcal{O}_{L_n}[\frac{1}{p}] \subseteq L_n$. Furthermore, $N_{L_m/L_n}(\varepsilon) = 1$, since $N_{L_m/L_n} \cdot (\sigma - 1) = 0$ in $\mathbb{Z}[\mathrm{Gal}(L_m/L_n)]$. Therefore, ε is the representative of a class $\overline{\varepsilon} \in \mathrm{H}^{-1}(\mathrm{Gal}(L_m/L_n), E'_m)$. Iwasawa shows that the map

$$\varphi'_{n,m} : \ker(i'_{n,m}) \longrightarrow \mathrm{H}^{-1}(\mathrm{Gal}(L_m/L_n), E'_m), \quad c \mapsto \overline{\varepsilon},$$

is a well-defined homomorphism, and in fact a bijection. □

Remark 3.78. There exist similar canonical homomorphisms

$$\varphi_{n,m} : \ker(i_{n,m} : A_n \longrightarrow A_m) \longrightarrow \mathrm{H}^{-1}(\mathrm{Gal}(L_m/L_n), E_m), \quad m \geq n,$$

and

$$\varphi_n : \ker(i_{n,\infty} : A_n \longrightarrow \varinjlim A_m) \longrightarrow \mathrm{H}^{-1}(\mathrm{Gal}(L/L_n), E),$$

with $E_n = \mathcal{O}_{L_n}^*$ and $E = \bigcup_{n\geq 0} E_n$. Iwasawa remarks in [Iw 73] that these maps are injective, but usually not surjective.

Proof. Let $c \in A_n$ be such that $i_{n,m}(c) = 0$. If $\mathfrak{A} \in c$, then $\mathfrak{A} \cdot \mathcal{O}_{L_m} = (\alpha)$ is a principal ideal, and $\varphi_{n,m}(c) = \alpha^{\sigma-1}$, where σ generates $\mathrm{Gal}(L_m/L_n)$.

Now suppose that

$$\varepsilon := \alpha^{\sigma-1}$$

is contained in the trivial class of $\mathrm{H}^{-1}(\mathrm{Gal}(L_m/L_n), E_m)$. Then $\varepsilon = \delta^{\sigma-1}$ for some $\delta \in E_m$. Therefore $\alpha^{\sigma-1} = \delta^{\sigma-1}$, i.e., $(\alpha/\delta)^{\sigma-1} = 1$ and therefore $\alpha/\delta =: x \in L_n$. But then $(\alpha) = (\delta \cdot x) = (x)$, and therefore $\mathfrak{A} = (x)$ is principal already in L_n. This proves that $\varphi_{n,m}$ is injective.

If $c \in A_n$ satisfies $i_{n,\infty}(c) = 0$, then there exists some $m \geq n$ such that $i_{n,m}(c) = 0$. Therefore also φ_n is injective, $n \in \mathbb{N}_0$.

Now let $(\alpha) \in \mathcal{O}_{L_m}$ denote a ramified principal prime ideal (for example, if L/K is the cyclotomic $\mathbb{Z}_p$-extension, then we can take $\alpha = \zeta_{p^k} - 1$ for a suitable $k \in \mathbb{N}$). Then $(\alpha)^\sigma = (\alpha)$ and therefore $\varepsilon := \alpha^{\sigma-1} \in E_m$.

We claim that the class of ε in $\mathrm{H}^{-1}(\mathrm{Gal}(L_m/L_n), E_m)$ cannot lie in the image of $\varphi_{m-1,m}$. Indeed, otherwise there exists an ideal $\mathfrak{A}$ of L_{m-1} such that $\mathfrak{A} \cdot \mathcal{O}_{L_m} = (\alpha)$. But (α) is ramified in L_m/L_{m-1} and therefore does not lie in the image of the ideal lift map $i_{m-1,m}$. □

Note that the absence of an isomorphism φ analogous to Theorem 3.77 is not very obstructive to our purposes, since we are mainly interested in the *order* of the capitulation kernels $\ker(i_{n,m})$, rather than in their specific group structure. In fact, the following theorem will yield enough information for us.

Theorem 3.79. *Let L/K be a cyclic extension with Galois group $G = <\sigma>$. Then there exists an isomorphism*

$$\varphi = \varphi_{L/K} : P_L^G / i_{K,L}(P_K) \xrightarrow{\sim} \mathrm{H}^{-1}(G, E_L),$$

where P_K and P_L denote the groups of principal fractional ideals of K and L, respectively, and where

$$P_L^G = \{(\gamma) \in P_L : (\gamma)^\tau = (\gamma)\ \forall\, \tau \in G\} = \{(\gamma) \in P_L : (\gamma)^\sigma = (\gamma)\}.$$

φ is the analogon of the maps from Theorem 3.77: For $\gamma \in L^*$, the coset $(\gamma) \cdot i_{K,L}(P_K)$ is mapped to the class $\overline{\varepsilon} \in \mathrm{H}^{-1}(G, E_L)$ of $\varepsilon := \gamma^{\sigma-1}$.

Proof. See Satz 2 and p. 47 in [Sc 85]. □

Remarks 3.80.

(1) In the article [Sc 85], Theorem 3.79 is actually proved for arbitrary Galois extensions L/K.

(2) If L/K is unramified, then every ideal $\mathfrak{A}$ in P_L^G is the image $i_{K,L}(\mathfrak{A}')$ of some ideal $\mathfrak{A}'$ of K (see Theorem 93 in [Hi 97]). Therefore

$$P_L^G/i_{K,L}(P_K) \cong \ker(i_{K,L}) ,$$

i.e., the analogon of Theorem 3.77 is valid in this case. Since a $\mathbb{Z}_p$-extension cannot be unramified, this situation is only possible for intermediate extensions L_m/L_n with small values of n and m.

(3) We have already seen in Remark 3.78 that the existence of ramified primes in L/K implies that the map from Theorem 3.79 will not be an isomorphism. In fact, in general we cannot hope for having an isomorphism, as we will see now by relating the orders of $\mathrm{H}^{-1}(G, E_L)$ and $\ker(i_{K,L})$; compare Corollary 3.81 below.

If $\mathrm{Gal}(L/K) = <\sigma>$ is cyclic, then $(\alpha) \in P_L^G$ if and only if $(\alpha)^\sigma = (\alpha)$. Moreover, Hilbert's Theorem 93 implies that each such (α) may be written as $(\alpha) = \mathfrak{B} \cdot \mathfrak{C}$ for two ideals $\mathfrak{B}$ and $\mathfrak{C}$ of L (possibly trivial) such that every prime factor of $\mathfrak{B}$ ramifies in L/K and such that $\mathfrak{C} = i_{K,L}(\mathfrak{C}')$ for some ideal $\mathfrak{C}'$ of K.

In particular, if $[L : K] = p$, then

$$|P_L^G \,/\, i_{K,L}(P_K)| \;=\; p^{s_L} \cdot |\ker(i_{K,L})| ,$$

where p^{s_L} denotes the number of ideals $\mathfrak{B}$ of L such that every prime factor of $\mathfrak{B}$ ramifies in L/K and occurs in $\mathfrak{B}$ with exponent in $\{1, \ldots, p-1\}$, and such that there exists an ideal $\mathfrak{C}'$ of K such that $\mathfrak{B} \cdot i_{K,L}(\mathfrak{C}') = (\alpha)$ is a principal ideal in L. For the moment, we will call these ramified ideals of L 'pseudo-principal'.

Indeed, we have

$$\begin{aligned} |P_L^G \,/\, i_{K,L}(P_K)| &= |P_L^G \,/\, (i_{K,L}(I_K) \cap P_L^G)| \cdot |(i_{K,L}(I_K) \cap P_L^G) \,/\, i_{K,L}(P_K)| \\ &= |P_L^G \,/\, (i_{K,L}(I_K) \cap P_L^G)| \cdot |\ker(i_{K,L})| , \end{aligned}$$

where I_K denotes the group of fractional ideals of K.

Moreover,

$$P_L^G \,/\, (i_{K,L}(I_K) \cap P_L^G) \;\cong\; (P_L^G \cdot i_{K,L}(I_K)) \,/\, i_{K,L}(I_K) .$$

The class of $(\alpha) = \mathfrak{B} \cdot i_{K,L}(\mathfrak{C}')$ in this quotient equals the class of $\mathfrak{B}$. We are therefore counting classes of ramified pseudo-principal ideals $\mathfrak{B}$ of L, modulo $i_{K,L}(K)$. Note that the number of these classes is a power of p, because each class $\overline{\mathfrak{B}} \neq \overline{1}$ has order p in $(P_L^G \cdot i_{K,L}(I_K)) \,/\, i_{K,L}(I_K)$, since $\mathfrak{B}^p \in i_{K,L}(I_K)$.

We have thus proved the following result.

Corollary 3.81.
(i) Let L/K be a cyclic extension of degree p. Then

$$|\mathrm{H}^{-1}(\mathrm{Gal}(L/K), E_L)| \;=\; p^{s_L} \cdot |\ker(i_{K,L})|\,,$$

where p^{s_L} denotes the number of pseudo-principal ramified ideals of L, as defined above.
(ii) In particular, if L/K is unramified, then

$$|\ker(i_{K,L})| \;=\; |\mathrm{H}^{-1}(\mathrm{Gal}(L/K), E_L)|\,,$$

and in fact the map φ from Theorem 3.79 yields an isomorphism between the two groups.

Now we are reduced to studying orders of cohomology groups. The following lemma will be a crucial ingredient in our proof that λ is locally maximal.

Lemma 3.82. *Let p denote an odd prime, let L/K denote a $\mathbb{Z}_p$-extension such that $\mu(L/K) = 0$. If $N_1(L/K)$ denotes the integer defined in Lemma 3.72, then $\mu(M/K) = 0$ and*

$$|\mathrm{H}^0(\mathrm{Gal}(M_{n+1}/M_n), E_{n+1}^{(M)})| \;\leq\; |\mathrm{H}^0(\mathrm{Gal}(M_{n+2}/M_{n+1}), E_{n+2}^{(M)})|$$

for every $n \geq N_1$ and every $M \in U(L,n)$. Here M_n and $E_n^{(M)}$ denote the unique subfield of M of degree p^n over K and its group of units, respectively.

Proof. Since $\mu(L/K) = 0$, $\mathrm{rank}_p(A_n)$ is bounded as $n \to \infty$ (see Proposition 1.45, (i)), and there exists an integer $N_0 \geq e(L/K)$ such that

$$\mathrm{rank}_p(A_n) \;=\; \mathrm{rank}_p(A_{N_0}) \;=\; \mathrm{rank}_p(A)$$

for every $n \geq N_0$. In particular, $\mu(M/K) = 0$ and $\mathrm{rank}_p(A^{(M)}) = \mathrm{rank}_p(A^{(L)})$ for each $M \in U(L, N_0+1)$.

Let $n \geq N_0 + 1$ be arbitrary, but fixed.

Assume that $|\mathrm{H}^0(\mathrm{Gal}(M_{n+1}/M_n), E_{n+1}^{(M)})| > |\mathrm{H}^0(\mathrm{Gal}(M_{n+2}/M_{n+1}), E_{n+2}^{(M)})|$ for some $M \in U(L,n)$.
Then there exists a unit $\varepsilon \in E_n^{(M)} \subseteq E_{n+1}^{(M)}$ such that $\varepsilon \notin N_{n+1,n}(E_{n+1}^{(M)})$, i.e., $\overline{\varepsilon} \neq \overline{1}$ in $\mathrm{H}^0(\mathrm{Gal}(M_{n+1}/M_n), E_{n+1}^{(M)})$, but such that $\varepsilon = N_{n+2,n+1}(e)$ for some $e \in E_{n+2}^{(M)}$. We want to show that this cannot be the case if n is chosen large enough.

If γ denotes a topological generator of $\mathrm{Gal}(M/K) \cong \mathbb{Z}_p$, then we know that $\mathrm{Gal}(M/M_i) = <\gamma^{p^i}>$ for every $i \in \mathbb{N}$. Therefore, letting $\sigma := \gamma^{p^n}$, we conclude that $\mathrm{Gal}(M_{n+1}/M_n) = <\sigma> \,/\, <\sigma^p>$ and $\mathrm{Gal}(M_{n+2}/M_{n+1}) = <\sigma^p> / <\sigma^{p^2}>$. In order to simplify the notation, we will for the moment write the action of these Galois groups multiplicatively.

Since $\varepsilon \in M_n$, it follows that $\sigma(\varepsilon) = \varepsilon$, and therefore

$$1 \;=\; \varepsilon^{\sigma-1} \;=\; (N_{n+2,n+1}(e))^{\sigma-1} \;=\; N_{n+2,n+1}(e^{\sigma-1})\,,$$

using the fact that $\mathrm{Gal}(M_{n+2}/M_n) = <\sigma> / <\sigma^{p^2}>$ is abelian. Hilbert's Theorem 90, applied to the cyclic extension M_{n+2}/M_{n+1}, implies that there exists an element $\delta \in M_{n+2}$ such that

$$e^{\sigma-1} \;=\; \delta^{\sigma^p-1} \;=\; (\delta^{N_{n+1,n}})^{\sigma-1} \;.$$

Here we use the formal identity $(\sigma-1)\cdot N_{n+1,n} = \sigma^p - 1$ in the group ring $\mathbb{Z}[\mathrm{Gal}(M_{n+2}/M_n)]$. Therefore $(e/\delta^{N_{n+1,n}})^{\sigma-1} = 1$, i.e.,

$$e \;=\; \delta^{N_{n+1,n}} \cdot d \qquad (\star)$$

for some element $d \in M_n$. But then

$$\begin{aligned} \varepsilon \;=\; N_{n+2,n+1}(e) \;&\overset{(\star)}{=}\; N_{n+2,n+1}(\delta^{N_{n+1,n}} \cdot d) \\ &=\; \delta^{N_{n+2,n+1}\cdot N_{n+1,n}} \cdot d^p \;=\; \delta^{N_{n+1,n}\cdot N_{n+2,n+1}} \cdot d^p \qquad (\star\star) \\ &=\; N_{n+1,n}(\delta^{N_{n+2,n+1}} \cdot d) \;, \end{aligned}$$

since $d \in M_n$ and because $\mathbb{Z}[\mathrm{Gal}(M_{n+2}/M_n)]$ is abelian.

Now we consider the ideal (δ) of M_{n+2}. Since

$$(\delta^{\sigma^p-1}) \;=\; (e^{\sigma-1}) \;=\; (1)\,,$$

it follows that $(\delta)^{\sigma^p} = (\delta)$, and therefore Hilbert's Theorem 93 (compare [Hi 97] and [Neu 92], Corollary III.2.12) implies that

$$(\delta) \;=\; i_{n+1,n+2}(\mathfrak{D}) \cdot \mathfrak{A}$$

with ideals $\mathfrak{D}$ of M_{n+1} and $\mathfrak{A}$ of M_{n+2} such that every prime ideal dividing $\mathfrak{A}$ is ramified in M_{n+2}/M_{n+1} .

We first show that we may actually choose $\mathfrak{A} = (1)$, i.e., $(\delta) = i_{n+1,n+2}(\mathfrak{D})$, if n is large enough. In order to prove this, let us assume that $\mathfrak{A}$ has been chosen minimal, i.e., $\mathfrak{A} = \prod_{j=1}^{k} \mathfrak{P}_{2,j}^{e_j}$ with $0 \le e_j < p$ for every $j = 1, \ldots, k$; note that for each j, $\mathfrak{P}_{2,j}^p$ equals $i_{n+1,n+2}(\mathfrak{P}_{1,j})$ for some prime $\mathfrak{P}_{1,j}$ of M_{n+1} and therefore may be absorbed into $i_{n+1,n+2}(\mathfrak{D})$.

Since $n > e(L/K) = e(M/K)$, every prime $\mathfrak{P}_{2,j}$ is totally ramified in M_{n+2}/M_n. For each $j = 1, \ldots, k$, let $\mathfrak{P}_{1,j}$, respectively, $\mathfrak{P}_{0,j}$, denote the unique primes of M_{n+1}, respectively, M_n that are divisible by $\mathfrak{P}_{2,j}$.

For any fixed $j \in \{1, \ldots, k\}$, we consider the normalised valuation $v := v_{\mathfrak{P}_{2,j}}$ induced by the prime $\mathfrak{P}_{2,j}$, i.e.,

$$v(\mathfrak{P}_{1,j} \cdot \mathcal{O}_{M_{n+2}}) = p \quad \text{ and } \quad v(\mathfrak{P}_{0,j} \cdot \mathcal{O}_{M_{n+2}}) = p^2 \;.$$

Then

$$\begin{aligned} 0 \;&=\; v((e)) \;\overset{(\star)}{=}\; v((\delta^{N_{n+1,n}})) + v((d)) \\ &=\; v((\delta^{N_{n+1,n}})) + p^2 \cdot c \;, \end{aligned}$$

where $c \in \mathbb{Z}$ is the exponent of $\mathfrak{P}_{0,j}$ in $(d) \subseteq M_n$, i.e., $c = v_{\mathfrak{P}_{0,j}}((d))$. Moreover,

$$v((\delta^{N_{n+1,n}})) \;=\; p \cdot v((\delta))\,,$$

because the extension M_{n+2}/M_n is galois and therefore

$$v((\sigma(\delta))) \;=\; v((\delta))\,.$$

But if $0 \;=\; p\cdot v((\delta))+p^2\cdot c$, then we must have $v((\delta)) \equiv 0 \bmod p$, i.e., $e_j = 0$ in the above decomposition of $\mathfrak{A}$ into prime factors. Since this holds for every $j = 1,\ldots,k$, we may conclude that we can choose $\mathfrak{D}$ with $(\delta) = i_{n+1,n+2}(\mathfrak{D})$, i.e., $\mathfrak{A} = (1)$.

Now we will deal with the ideal $\mathfrak{D}$ of M_{n+1}. We claim that

$$N_{n+1,n}(\mathfrak{D}) \;=\; (d^{-1})\,.$$

Indeed, since $i_{n+1,n+2}(\mathfrak{D}) = (\delta)$, the class of $\mathfrak{D}$ in the group $A_{n+1}^{(M)}$ has order at most p, because $\ker(i_{n+1,n+2})$ is p-elementary. This means that $\mathfrak{D}^p = (\beta)$ for some $\beta \in M_{n+1}$. Therefore $i_{n+1,n+2}((\beta)) = (\delta)^p$, i.e., $\beta = \delta^p \cdot e_2$ for some unit $e_2 \in E_{n+2}^{(M)}$. But then

$$\begin{aligned}
N_{n+1,n}(\mathfrak{D})^p &= (\beta^{N_{n+1,n}}) \;=\; \beta^{N_{n+1,n}}\cdot\mathcal{O}_{M_n}\\
&= (\beta^{N_{n+1,n}}\cdot\mathcal{O}_{M_{n+2}})\cap M_n\\
&= ((\delta^p\cdot e_2)^{N_{n+1,n}}\cdot\mathcal{O}_{M_{n+2}})\cap M_n\\
&= ((\delta^p)^{N_{n+1,n}}\cdot\mathcal{O}_{M_{n+2}})\cap M_n\\
&= ((d^{-1})^p\cdot\mathcal{O}_{M_{n+2}})\cap M_n\\
&= (d^{-1})^p\cdot\mathcal{O}_{M_n}\,,
\end{aligned}$$

because $\delta^{N_{n+1,n}}\cdot d \;=\; e \in E_{n+2}^{(M)}$ by $(\star)$. This implies that $N_{n+1,n}(\mathfrak{D}) \;=\; (d^{-1})$, as claimed, since the group of fractional ideals of M_n is $\mathbb{Z}$-free.

Furthermore, the ideal $\mathfrak{D}$ of M_{n+1} cannot be a principal ideal. Indeed, if $\mathfrak{D} = (\alpha)$ for some element $\alpha \in M_{n+1}$, then

$$i_{n+1,n+2}(\mathfrak{D}) \;=\; (\alpha) \;=\; (\delta)\,,$$

and therefore $\delta = \alpha\cdot e_2$ with some unit $e_2 \in E_{n+2}^{(M)}$. But then

$$e^{\sigma-1} \;=\; \delta^{\sigma^p-1} \;=\; (\alpha\cdot e_2)^{\sigma^p-1} \;=\; e_2^{\sigma^p-1}\,,$$

since $\alpha \in M_{n+1}$. Using e_2 instead of δ, $(\star)$ and $(\star\star)$ then would imply that $\varepsilon \in N_{n+1,n}(E_{n+1}^{(M)})$, in contradiction to our assumptions on ε.

Therefore, $1 \neq \overline{\mathfrak{D}} \in A_{n+1}^{(M)}$ and $N_{n+1,n}(\overline{\mathfrak{D}}) = \overline{1}$, since $N_{n+1,n}(\mathfrak{D}) = (d^{-1})$ is a principal ideal. Recall that $n \geq N_0$ and thus $\mathrm{rank}_p(A_{n+1}^{(M)}) = \mathrm{rank}_p(A_n^{(M)})$, implying that $\ker(N_{n+1,n}) \subseteq p\cdot A_{n+1}^{(M)}$, because the induced map

$$\overline{N_{n+1,n}} : A_{n+1}^{(M)}/pA_{n+1}^{(M)} \longrightarrow A_n^{(M)}/pA_n^{(M)}$$

is an isomorphism (compare the proof of Proposition 3.68, (iv)).

Now let $N_1 \geq N_0$ denote the integer attached to L/K in Lemma 3.72. This means that N_1 is large enough to ensure that $p^{N_1} > \mathrm{rank}_p(A^{(L)})$. Note that the

same integer N_1 works for every $M \in U(L,n)$, since $\mathrm{rank}_p(A^{(M)}) = \mathrm{rank}_p(A^{(L)})$ for these M.

We now assume that $n \geq N_1$. Returning to our fixed $M \in U(L,n)$, Lemma 3.72 implies that $p \cdot A_{n+1}^{(M)} \subseteq i_{n,n+1}(A_n^{(M)})$. Therefore $\mathfrak{D} \cdot (\alpha_1) = i_{n,n+1}(\mathfrak{A})$ for some element $\alpha_1 \in M_{n+1}$ and an ideal $\mathfrak{A}$ of M_n. But

$$(\delta \cdot \alpha_1)^{\sigma^p - 1} \;=\; \delta^{\sigma^p - 1} \;\overset{(\star)}{=}\; e^{\sigma - 1}\,,$$

so that we may replace δ by $\delta \cdot \alpha_1$ and also $\mathfrak{D}$ by $\mathfrak{D} \cdot (\alpha_1)$. This means that we may without loss of generality assume that $\mathfrak{D} = i_{n,n+1}(\mathfrak{A})$ and $(\delta) = i_{n,n+2}(\mathfrak{A})$. Therefore, in the ring of integers of M_{n+1},

$$\begin{aligned}(\delta^{N_{n+2,n+1}} \cdot d) &= (\delta^{N_{n+2,n+1}}) \cdot i_{n,n+1}((d)) \\ &= N_{n+2,n+1}(i_{n,n+2}(\mathfrak{A})) \cdot i_{n,n+1}(N_{n+1,n}(i_{n,n+1}(\mathfrak{A})))^{-1} \\ &= i_{n,n+1}(\mathfrak{A})^p \cdot i_{n,n+1}(\mathfrak{A})^{-p} \;=\; (1)\,,\end{aligned}$$

so that $(\star\star)$ implies that $\varepsilon \in N_{n+1,n}(E_{n+1}^{(M)})$, contrary to our assumptions.

This shows that the inclusion $E_n^{(M)} \subseteq E_{n+1}^{(M)}$ induces an injective map

$$\mathrm{H}^0(\mathrm{Gal}(M_{n+1}/M_n), E_{n+1}^{(M)}) \hookrightarrow \mathrm{H}^0(\mathrm{Gal}(M_{n+2}/M_{n+1}), E_{n+2}^{(M)})\;.$$

Since $M \in U(L,n)$ was chosen arbitrary, this proves the lemma. □

Corollary 3.83. *Let p be an odd prime number, and let L/K denote a $\mathbb{Z}_p$-extension such that $\mu(L/K) = 0$. Then there exists an integer $N_1 \in \mathbb{N}$ such that $\mu(M/K) = 0$, $\mathrm{rank}_p(A^{(M)}) = \mathrm{rank}_p(A^{(L)})$ and*

$$|\ker(i_{n,n+1}^{(M)} : A_n^{(M)} \longrightarrow A_{n+1}^{(M)})| \;\leq\; |\ker(i_{n+1,n+2}^{(M)} : A_{n+1}^{(M)} \longrightarrow A_{n+2}^{(M)})|$$

for every $n \geq N_1$ and every $M \in U(L,n)$.

Proof. Using Corollary 3.81 and Lemma 3.82, we already know that for suitable $N_1 \in \mathbb{N}$,

$$\begin{aligned}p^{s_{M_{n+1}}} \cdot |\ker(i_{n,n+1}^{(M)})| &= |\mathrm{H}^{-1}(\mathrm{Gal}(M_{n+1}/M_n), E_{n+1}^{(M)})| \\ &= p \cdot |\mathrm{H}^0(\mathrm{Gal}(M_{n+1}/M_n), E_{n+1}^{(M)})| \\ &\leq p \cdot |\mathrm{H}^0(\mathrm{Gal}(M_{n+2}/M_{n+1}), E_{n+2}^{(M)})| \\ &= |\mathrm{H}^{-1}(\mathrm{Gal}(M_{n+2}/M_{n+1}), E_{n+2}^{(M)})| \\ &= p^{s_{M_{n+2}}} \cdot |\ker(i_{n+1,n+2}^{(M)})|\end{aligned}$$

for every $M \in U(L,N_1)$. Here we have also used the fact that

$$|\mathrm{H}^{-1}(\mathrm{Gal}(F/G), E_F)| \;=\; p \cdot |\mathrm{H}^0(\mathrm{Gal}(F/G), E_F)|$$

for every cyclic extension F/G of degree p that is unramified at infinity (see [Ja 73], Theorem V.2.4).

In particular, $|\ker(i_{n,n+1}^{(M)})| \leq p^{s_{M_{n+2}}-s_{M_{n+1}}} \cdot |\ker(i_{n+1,n+2}^{(M)})|$. We will show now that $s_{M_{n+2}} \leq s_{M_{n+1}}$ if $n \geq N_1$. Recall that $p^{s_{M_{n+2}}}$ (respectively, $p^{s_{M_{n+1}}}$) denotes the number of 'pseudo-principal' ramified ideals of M_{n+2} (respectively, M_{n+1}).

Let $\mathfrak{B}_{n+2}$ be such an ideal of M_{n+2}, i.e., assume that every prime divisor of $\mathfrak{B}_{n+2}$ is ramified in M_{n+2}/M_{n+1} and occurs with exponent in $\{1,\ldots,p-1\}$, and that there exists an ideal $\mathfrak{C}_{n+1}$ of M_{n+1} such that

$$\mathfrak{B}_{n+2} \cdot i_{n+1,n+2}(\mathfrak{C}_{n+1}) \;=\; (\alpha)$$

is a principal ideal in $\mathcal{O}_{M_{n+2}}$.

We apply the norm map $N := N_{n+2,n+1}$. Then each prime factor of

$$\mathfrak{B}_{n+1} \;:=\; N(\mathfrak{B}_{n+2}) \subseteq M_{n+1}$$

is ramified in M_{n+1}/M_n, since $n \geq e(M/K)$, and divides $\mathfrak{B}_{n+1}$ with exponent in $\{1,\ldots,p-1\}$. Moreover,

$$\mathfrak{B}_{n+1} \cdot \mathfrak{C}_{n+1}^{p} \;=\; (N(\alpha))\;,$$

since $N(i_{n+1,n+2}(\mathfrak{C}_{n+1})) = \mathfrak{C}_{n+1}^{p}$. But $p \cdot A_{n+1}^{(M)} \subseteq i_{n,n+1}(A_n^{(M)})$ for $n \geq N_1$, and therefore $\mathfrak{C}_{n+1}^{p} = i_{n,n+1}(\mathfrak{C}_n) \cdot (\beta)$ for some ideal $\mathfrak{C}_n$ of M_n and a suitable element $\beta \in M_{n+1}$. This means that

$$\mathfrak{B}_{n+1} \cdot i_{n,n+1}(\mathfrak{C}_n) \;=\; (N(\alpha) \cdot \beta^{-1})$$

is principal, and therefore $s_{M_{n+2}} \leq s_{M_{n+1}}$. □

Now we are ready to prove the main result of this section, which corresponds to Theorem 3.57, (ii).

Theorem 3.84. *Let p be an odd prime number, and let L/K be a $\mathbb{Z}_p$-extension such that $\mu(L/K) = 0$. Then the Iwasawa λ-invariant is* **locally maximal** *with respect to the Greenberg-R-topology, i.e., there exists an integer $N \in \mathbb{N}$ such that $\lambda(M/K) \leq \lambda(L/K)$ for every $M \in U(L,n)$.*

Proof. We choose $N_1 \in \mathbb{N}$ as in Corollary 3.83, and we let $N_2 = N_2(L/K)$ be the integer N defined in Theorem 3.70. This means that

$$\lambda(L/K) \;=\; r - r_n$$

for every $n \geq N_2$, where $r := \mathrm{rank}_p(A^{(L)})$ and

$$r_n \;:=\; \mathrm{rank}_p(\ker(i_n := i_{n,n+1} : A_n^{(L)} \longrightarrow A_{n+1}^{(L)}))\;.$$

Now we define $N := \max(N_1, N_2)+1$ and consider a $\mathbb{Z}_p$-extension $M \in U(L,N)$.

Since $N \geq N_1$, we know that the statement of Corollary 3.83 is valid for M. In particular, $\mu(M/K) = 0$ and

$$r^{(M)} \;:=\; \mathrm{rank}_p(A^{(M)}) \;=\; \mathrm{rank}_p(A^{(L)}) \;=\; r\;.$$

If $N_2(M/K) \leq N-1$, then

$$\mathrm{rank}_p(\ker(i^{(M)}_{N_2(M/K),N_2(M/K)+1})) \;=\; \mathrm{rank}_p(\ker(i^{(L)}_{N_2(M/K),N_2(M/K)+1}))\;,$$

and therefore $\lambda(M/K) = \lambda(L/K)$, using Theorem 3.70.

Now $N_2(M/K)$ might be strictly larger than $N-1$. But then Corollary 3.83 implies that

$$\begin{aligned} r^{(M)}_{N_2(M/K)} &:= \mathrm{rank}_p(\ker(i^{(M)}_{N_2(M/K),N_2(M/K)+1})) \\ &\geq \mathrm{rank}_p(\ker(i^{(M)}_{N-1,N})) \\ &= \mathrm{rank}_p(\ker(i^{(L)}_{N-1,N}))\;, \end{aligned}$$

since the capitulation kernels $\ker(i^{(M)}_{k,k+1})$ are p-elementary and therefore

$$|\ker(i^{(M)}_{k,k+1})| \;=\; p^{\mathrm{rank}_p(\ker(i^{(M)}_{k,k+1}))}$$

for every $k \in \mathbb{N}_0$.

This means that in any case, we may conclude that

$$\lambda(M/K) \;=\; r^{(M)} - r^{(M)}_{N_2(M/K)} \;=\; r - r^{(M)}_{N_2(M/K)} \;\leq\; r - r_{N-1} \;=\; \lambda(L/K)\;,$$

proving that $\lambda(L/K)$ is locally maximal. □

Chapter 4

The global approach

In this chapter, we want to briefly describe a different approach to the study of Iwasawa's invariants which originates in GREENBERG's article [Gr 73] and which is more capable if one wants to deduce global results. In the first two sections, we will describe work of R. GREENBERG and V. BABAĬCEV, who proved that the set $\{\mu(L/K) \mid L \in \mathcal{E}(K)\}$ is bounded for every number field K. In Section 4.3, we will turn to λ-invariants. The analogous question, i.e., whether the set $\{\lambda(L/K) \mid L \in \mathcal{E}(K)\}$ is bounded for an arbitrary number field K, is still open. In fact, no example of unbounded λ-invariants is known. We will derive a sufficient criterion for the existence of such an example, using the theory developed in the first two sections.

4.1 Greenberg's boundedness results

Let p denote a fixed rational prime, let K denote a number field such that there exist infinitely many $\mathbb{Z}_p$-extensions of K. Let $\mathbb{K}$ be the composite of all $\mathbb{Z}_p$-extensions of K, i.e., $\mathrm{Gal}(\mathbb{K}/K) \cong \mathbb{Z}_p^d$ with $d \geq 2$. In the article [Gr 73], R. GREENBERG introduced the Greenberg topology on the set $\mathcal{E}(K)$ of $\mathbb{Z}_p$-extensions of K, and he proved the following results (compare Theorems 2.27-2.30):

Theorem 4.1 (Greenberg)**.**

(i) *Let L be a $\mathbb{Z}_p$-extension of K such that only finitely many prime ideals of L lie over p. Then there exist integers n_0 and $c \in \mathbb{N}$ such that $\mu(M/K) < c$ for any $M \in \mathcal{E}(L, n_0)$.*

(ii) *Let L be a $\mathbb{Z}_p$-extension of K such that only finitely many primes of L lie over p. Assume further that $\mu(L/K) = 0$. Then there exist integers n_0 and $c \in \mathbb{N}$ such that $\mu(M/K) = 0$ and $\lambda(M/K) < c$ for any $M \in \mathcal{E}(L, n_0)$.*

(iii) *Let K be a number field which contains only one prime dividing p. Then there exists a constant c such that $\mu(L/K) < c$ for every $\mathbb{Z}_p$-extension of K.*

(iv) *Let K be a number field which contains only one prime dividing p. Assume that $\mu(L/K) = 0$ for* every *$L \in \mathcal{E}(K)$. Then there exists a constant c such that $\lambda(L/K) < c$ for every $\mathbb{Z}_p$-extension of K.*

Note that the assumptions made in Theorem 4.1 imply that no prime of K dividing p splits completely in L/K.

We will now briefly describe Greenberg's method of proof, which is quite different from our approach used in Chapter 3. In particular, we will see the motivation for assuming that no prime of K lying above p splits completely in L/K; using our local method, we are free to allow infinitely split primes. On the other hand, we have to put assumptions on the ramification, being coded into the Greenberg-R-topology (see Definition 3.24).

In [Gr 73], Greenberg started with a fixed $\mathbb{Z}_p$-extension L/K, and he considered the canonical restriction map which is a surjective homomorphism

$$\mathrm{Gal}(\mathbb{K}/K) \twoheadrightarrow \mathrm{Gal}(L/K) \ .$$

This map induces a surjective ring homomorphism

$$\pi_L : \Lambda_{\mathbb{K}} := \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{K}/K)]] \twoheadrightarrow \Lambda_L := \mathbb{Z}_p[[\mathrm{Gal}(L/K)]]$$

of the corresponding completed group rings (see Definition 2.9). Note that

$$\Lambda_L \cong \mathbb{Z}_p[[T]] = \Lambda \quad \text{and} \quad \Lambda_{\mathbb{K}} \cong \mathbb{Z}_p[[T_1, \ldots, T_d]] = \Lambda_d \ ,$$

using Theorems 1.9 and 2.18, respectively.

Now let $\mathfrak{A}_L$ denote the kernel of π_L; then $\mathfrak{A}_L \subseteq \Lambda_{\mathbb{K}}$ is an ideal. If Y denotes a noetherian torsion $\Lambda_{\mathbb{K}}$-module, then

$$Y_L := Y/(\mathfrak{A}_L \cdot Y)$$

can be regarded as a module over $\Lambda_{\mathbb{K}}/\mathfrak{A}_L \cong \Lambda_L$. Indeed, if $\overline{\lambda} \in \Lambda_L$, then we choose a pre-image λ under the surjective homomorphism π_L, and we define $\overline{\lambda} \cdot y := \lambda \cdot y$, $y \in Y/(\mathfrak{A}_L \cdot Y)$. This is well-defined since any other lift $\lambda + a$, $a \in \mathfrak{A}_L$, yields the same element $\lambda \cdot y \in Y_L = Y/(\mathfrak{A}_L \cdot Y)$.

Y_L becomes a noetherian Λ_L-module, but it is not necessarily a torsion module. Greenberg defined, for fixed K and Y, $\mathcal{E}(Y) = \mathcal{E}(Y, K) \subseteq \mathcal{E}(K)$ to be the set of all $\mathbb{Z}_p$-extensions L of K such that Y_L is a torsion Λ_L-module. $\mathcal{E}(Y)$ bears the subspace topology induced by the Greenberg topology on $\mathcal{E}(K)$. For each $L \in \mathcal{E}(Y)$, the Iwasawa invariants of the module Y_L are defined via Proposition 1.28, using the isomorphism $\Lambda_L \cong \Lambda$.

Lemma 4.2 (Greenberg)**.** *Let Y denote a fixed noetherian torsion $\Lambda_{\mathbb{K}}$-module, and let $\mathcal{E}(Y)$ be defined as above.*

(i) *$L \in \mathcal{E}(Y)$ if and only if the annihilator ideal of Y in $\Lambda_{\mathbb{K}}$ is not contained in the kernel $\mathfrak{A}_L$ of π_L. If $L \in \mathcal{E}(Y)$, then we may choose an annihilator f of Y such that $f \equiv \pm h^t \pmod{\mathfrak{A}_L}$, where $h \in \Lambda_{\mathbb{K}}$ denotes the lift of an annihilator of Y_L, and t is the minimal number of generators of Y, as $\Lambda_{\mathbb{K}}$-module.*

(ii) *The invariant $\mu(Y_L)$ is locally bounded on $\mathcal{E}(Y)$.*

(iii) *If $\mu(Y_L) = 0$ for some $L \in \mathcal{E}(Y)$, then then there exist an open neighbourhood $U \subseteq \mathcal{E}(Y)$ of L and a constant $c \in \mathbb{N}$ such that $\mu(Y_M) = 0$ and $\lambda(Y_M) \leq c$ for every $M \in U$.*

Proof. For the proof of (i), see p. 208 in [Gr 73]: If $g \in \Lambda_{\mathbb{K}}$, $g \notin \mathfrak{A}_L$, annihilates Y, then $0 \neq \pi_L(g) \in \Lambda_L$ satisfies $\pi_L(g) \cdot Y_L = \{0\}$. If, on the other hand, Y_L is Λ_L-torsion, then we may choose an element $h \in \Lambda_{\mathbb{K}}$ such that $h \cdot Y \subseteq \mathfrak{A}_L \cdot Y$ and $h \notin \mathfrak{A}_L$. If $y_1, \ldots, y_t$ denote generators of the $\Lambda_{\mathbb{K}}$-module Y, then

$$h \cdot y_i \;=\; \sum_{j=1}^{t} c_{ij} \cdot y_j \;, \quad 1 \leq i \leq t \;,$$

with $c_{ij} \in \mathfrak{A}_L$ for every i and j, so

$$\sum_{j=1}^{t} (c_{ij} - \delta_{ij} h) \cdot y_j \;=\; 0$$

for every $1 \leq i \leq t$, where

$$\delta_{ij} = \begin{cases} 1 & : i = j \\ 0 & : i \neq j \;. \end{cases}$$

Let $f := \det((c_{ij} - \delta_{ij} h)_{i,j}) \in \Lambda_{\mathbb{K}}$. Then $f \cdot Y = 0$ and $f \equiv \pm h^t \,(\mathrm{mod}\ \mathfrak{A}_L)$, and in particular $f \notin \mathfrak{A}_L$, since $\pi_L(f) \;=\; \pi_L(\pm h^t) \;=\; \pm\, \pi_L(h)^t \;\neq\; 0$.

For (ii) and (iii), compare Theorems 2 and 3 in [Gr 73]. We will sketch the proof in the case of an elementary $\Lambda_{\mathbb{K}}$-module $Y = \Lambda_{\mathbb{K}}/(f)$, $f \in \Lambda_{\mathbb{K}}$.

The connection to Greenberg's topology is given by the observation that

$$\mathfrak{A}_M \;\subseteq\; \mathfrak{A}_L + \mathfrak{m}^{n+1} \qquad \text{for every } M \in \mathcal{E}(L,n), \tag{$\star$}$$

where $\mathfrak{m}$ denotes the maximal ideal of the local ring $\Lambda_{\mathbb{K}}$ (i.e., $\mathfrak{m}$ corresponds to $(p, T_1, \ldots, T_d) \subseteq \mathbb{Z}_p[[T_1, \ldots, T_d]] \cong \Lambda_{\mathbb{K}}$, compare Proposition 2.17, (i)).

For $Y = \Lambda_{\mathbb{K}}/(f)$, $\mu(Y_L)$ is given by the exponent of the largest power of p dividing

$$\overline{f} \;:=\; \pi_L(f) \;=\; f + \mathfrak{A}_L \;\in\; \Lambda_{\mathbb{K}}/\mathfrak{A}_L \;\cong\; \Lambda_L \;.$$

If $\mathfrak{m}_L$ denotes the maximal ideal of $\Lambda_L \cong \Lambda$, then

$$\bigcap_{n=0}^{\infty} \mathfrak{m}_L^n \;=\; \{0\} \;.$$

Moreover, $\pi_L(\mathfrak{m}) = \mathfrak{m}_L$, because π_L is a surjective ring homomorphism. We may conclude that for sufficiently large $s \in \mathbb{N}$, we have

$$f \;\notin\; (p^{\mu(Y_L)+1}) + \mathfrak{A}_L + \mathfrak{m}^s \;.$$

It follows that for every $M \in \mathcal{E}(L,s)$, we have $f \notin (p^{\mu(Y_L)+1}) + \mathfrak{A}_M$, using $(\star)$ above.

Analogously, if $\mu(Y_L) = 0$ for some $L \in \mathcal{E}(Y)$, then $\lambda(Y_L)$ is equal to the smallest index j such that the coefficient a_j in the expansion

$$\pi_L(f) \;=\; \overline{f} \;=\; a_0 + a_1 \cdot T + a_2 \cdot T^2 + \ldots \;\in\; \Lambda \cong \Lambda_L$$

is a p-adic unit (compare the Weierstraß Preparation Theorem 1.14). Now (iii) may be proved similarly to part (ii). $\square$

Greenberg applied this theory to $X := \mathrm{Gal}(H(\mathbb{K})/\mathbb{K})$, the Galois group of the maximal unramified p-abelian extension of $\mathbb{K}$. X is a finitely generated torsion $\Lambda_{\mathbb{K}}$-module (see Theorem 1 in [Gr 73]) and therefore may be used in position of Y. If L/K is a $\mathbb{Z}_p$-extension such that only finitely many primes of L divide p, then $L \in \mathcal{E}(X)$:

In order to prove that $X/(\mathfrak{A}_L \cdot X)$ is a torsion Λ_L-module, Greenberg considered the Galois group $G := \mathrm{Gal}(H(\mathbb{K})/L)$, together with its topological commutator subgroup G'. He showed that G' contains $\mathfrak{A}_L \cdot X$, and that $D := G'/(\mathfrak{A}_L \cdot X)$ is a finitely generated $\mathbb{Z}_p$-module of rank at most $\frac{(d-1)(d-2)}{2}$ and a Λ_L-torsion module (this generalises Lemma 1.36, (i)).

In order to prove that also G/G' is Λ_L-torsion, Greenberg considered the finitely many primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ of L dividing p, and he defined $T := T_1 \cdot \ldots \cdot T_s$, where T_j denotes the inertia subgroup of $\mathfrak{p}_j$ in the maximal abelian extension of L contained in $H(\mathbb{K})$, respectively. Then $T \subseteq G/G'$, and each T_j is isomorphic to a subgroup of $\mathrm{Gal}(\mathbb{K}/L) \cong \mathbb{Z}_p^{d-1}$, since $T_j \cap X/G' = \{1\}$, $j = 1, \ldots, s$. Therefore T is finitely generated over $\mathbb{Z}_p$ and thus Λ_L-torsion. Finally, $(G/G')/T \cong \mathrm{Gal}(H(L)/L)$, where $H(L)$ denotes the maximal unramified p-abelian extension of L, and this is a torsion Λ_L-module by Lemma 1.39. This shows that G/G' and therefore also X/G' are Λ_L-torsion, proving the claim that $L \in \mathcal{E}(K)$.

In the following lemma, we will slightly generalise Greenberg's approach.

Lemma 4.3.

(i) *Assume that only finitely many primes of L divide p. Then $L \in \mathcal{E}(X)$ and $\mu(L/K) = \mu(X_L)$. In particular, if $\mu(L/K) = 0$ in this case, then X_L is a finitely generated $\mathbb{Z}_p$-module.*

(ii) *More generally, let $\mathbb{K}/K$ denote a $\mathbb{Z}_p^i$-extension, $i \in \mathbb{N}$, and let $\mathcal{E}^{\subseteq \mathbb{K}}(K)$ denote the set of $\mathbb{Z}_p$-extensions L/K such that $L \subseteq \mathbb{K}$ (compare Remarks 3.26, (2)). Fix some $L \in \mathcal{E}^{\subseteq \mathbb{K}}(K)$. Let $H(\mathbb{K})$ denote the maximal p-abelian unramified extension of $\mathbb{K}$, and let $X := \mathrm{Gal}(H(\mathbb{K})/\mathbb{K})$ denote the Greenberg module of $\mathbb{K}/K$. If*

$$\pi_L : \Lambda_{\mathbb{K}} := \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{K}/K)]] \longrightarrow\!\!\!\!\!\rightarrow \Lambda_L := \mathbb{Z}_p[[\mathrm{Gal}(L/K)]]$$

denotes the ring homomorphism induced by the restriction map, then the quotient $X_L := X/(\ker(\pi_L) \cdot X)$ becomes a Λ_L-module.
If no prime of L ramifying in $\mathbb{K}$ is completely decomposed in L/K, then X_L is a finitely generated torsion Λ_L-module, and $\mu(X_L) = \mu(L/K)$.
Moreover,

$$\lambda(X_L) \;\leq\; \lambda(L/K) + \frac{(i-1)(i-2)}{2} + j(\mathbb{K}/L)$$

and

$$\lambda(L/K) \;\leq\; \lambda(X_L) + i - 1\,,$$

where $j(\mathbb{K}/L)$ denotes the sum of the $\mathbb{Z}_p$-ranks of the finitely many inertia subgroups of $\mathrm{Gal}(H(\mathbb{K})^{\mathrm{ab}}/L)$. Here $H(\mathbb{K})^{\mathrm{ab}}$ denotes the maximal abelian extension of L contained in $H(\mathbb{K})$.

Proof. (i) We will make use of the notation introduced above. We already mentioned that $L \in \mathcal{E}(X)$ if only finitely many primes of L divide p. If $\mu(L/K) = 0$, then the torsion Λ_L-module $\mathrm{Gal}(H(L)/L) \cong (G/G')/T$ is finitely generated over $\mathbb{Z}_p$ (compare Proposition 1.45, (ii)). Since also $D = G'/(\mathfrak{A}_L \cdot X)$ and T are finitely generated $\mathbb{Z}_p$-modules, it follows that $X_L = X/(\mathfrak{A}_L \cdot X)$, too, is finitely generated. More generally, for arbitrary $\mu(L/K)$, it follows that

$$\mu(L/K) \;=\; \mu(\mathrm{Gal}(H(L)/L)) \;=\; \mu(X_L)\;,$$

see p. 213 in [Gr 73].

(ii) In the proof of (i), we have not used the fact that $\mathbb{K}$ is the composite of all $\mathbb{Z}_p$-extensions of K. Therefore the above arguments remain valid for an arbitrary $\mathbb{Z}_p^i$-extension $\mathbb{K}/K$, $i \leq d$. It is sufficient to note that only finitely many primes of L ramify in $H(\mathbb{K})/L$, since the primes that split in L/K by assumption will be unramified in $\mathbb{K}/L$ and in $H(\mathbb{K})/\mathbb{K}$. Therefore the product T of all the inertia subgroups of $\mathrm{Gal}(H(\mathbb{K})^{\mathrm{ab}}/L)$ will be a finitely generated $\mathbb{Z}_p$-module whose $\mathbb{Z}_p$-rank is bounded by $j(\mathbb{K}/L)$, and therefore it will not have impact on μ-invariants, as in the proof of (i). Moreover,

$$\mathrm{rank}_{\mathbb{Z}_p}(D) \;\leq\; \frac{(i-1)(i-2)}{2}\;,$$

proving that

$$\lambda(X_L) \;\leq\; \lambda(L/K) + \frac{(i-1)(i-2)}{2} + j(\mathbb{K}/L)$$

(compare the proof of Proposition 2 in [Gr 73] and p. 232 in [Mo 81]). We will now prove the last inequality; this inequality actually holds for every $L \in \mathcal{E}^{\subseteq \mathbb{K}}(K) \cap \mathcal{E}(X)$. Indeed, let π_L, Λ_L be defined as above, and let $\mathfrak{A}_L := \ker(\pi_L)$. By definition,

$$\mu(L/K) \;=\; \mu(\mathrm{Gal}(H(L)/L)) \quad \text{and} \quad \lambda(L/K) \;=\; \lambda(\mathrm{Gal}(H(L)/L))\;.$$

The inclusion $H(L) \cdot \mathbb{K} \subseteq H(\mathbb{K})$ induces a surjective homomorphism

$$X \;=\; \mathrm{Gal}(H(\mathbb{K})/\mathbb{K}) \;\longrightarrow\!\!\!\!\!\rightarrow\; \mathrm{Gal}(H(L)\cdot\mathbb{K}/\mathbb{K})\;.$$

Since $\mathfrak{A}_L = \{\sigma - 1 \mid \sigma \in \mathrm{Gal}(\mathbb{K}/L)\}$ by definition, we have

$$\mathfrak{A}_L \cdot \mathrm{Gal}((H(L)\cdot\mathbb{K})/\mathbb{K}) \;=\; \{1\}\;,$$

because

$$\tau^{\sigma-1} \;=\; \sigma\tau\sigma^{-1}\tau^{-1} \;=\; \tau\tau^{-1} \;=\; 1$$

for every $\tau \in \mathrm{Gal}((H(L)\cdot\mathbb{K})/\mathbb{K})$ and every $\sigma \in \mathrm{Gal}(\mathbb{K}/L)$. Therefore the above map induces a surjective Λ_L-module homomorphism

$$X_L = X/(\mathfrak{A}_L \cdot X) \;\longrightarrow\!\!\!\!\!\rightarrow\; \mathrm{Gal}((H(L)\cdot\mathbb{K})/\mathbb{K}) \;\cong\; \mathrm{Gal}(H(L)/(\mathbb{K}\cap H(L)))\;.$$

In particular,

$$\lambda(\mathrm{Gal}(H(L)/(\mathbb{K}\cap H(L)))) \;\leq\; \lambda(X_L)\;.$$

Now

$$\begin{aligned}\lambda(L/K) &= \lambda(\mathrm{Gal}(H(L)/L))\\ &\leq \lambda(\mathrm{Gal}(H(L)/(\mathbb{K}\cap H(L)))) + \lambda(\mathrm{Gal}((\mathbb{K}\cap H(L))/L))\\ &\leq \lambda(X_L) + \lambda(\mathrm{Gal}(\mathbb{K}/L)) \;\leq\; \lambda(X_L) + i - 1\;,\end{aligned}$$

since $\mathrm{Gal}(\mathbb{K}/L) \cong \mathbb{Z}_p^{i-1}$.

□

Remark 4.4. Let $\mathcal{E}'(K)$ denote the set of $\mathbb{Z}_p$-extensions L/K such that only finitely many primes of L divide p. Then $\mathcal{E}'(K) \subseteq \mathcal{E}(K)$ is open and dense with respect to Greenberg's topology.

Proof. See Proposition 3 in [Gr 73]. Note that the fact that $\mathcal{E}'(K) \subseteq \mathcal{E}(K)$ is dense also follows from Lemma 3.18, (iii). □

We conclude the section by restricting to the special case of the composite $\mathbb{K}$ of all $\mathbb{Z}_p$-extensions of K, returning to Greenberg's proof of Theorem 4.1.

Corollary 4.5 (Greenberg)**.** *Let $\mathbb{K}$ denote the composite of all $\mathbb{Z}_p$-extensions of K, let $X = \mathrm{Gal}(H(\mathbb{K})/\mathbb{K})$, $L \in \mathcal{E}(X)$ and let $X_L = X/(\mathfrak{A}_L \cdot X)$ be defined as above. Then*

(i) $\lambda(L/K) \leq \lambda(X_L) + d - 1$, *and*

(ii) $\mu(L/K) \leq \mu(X_L)$. *If no prime dividing p splits completely in L/K, then $\mu(L/K) = \mu(X_L)$ (compare Lemma 4.3).*

Proof. (i) is a special case of the last inequality obtained in Lemma 4.3, (ii). In course of the proof of this lemma, we have shown that there exists a surjective Λ_L-module homomorphism

$$X_L \;=\; X/(\mathfrak{A}_L \cdot X) \;\longrightarrow\!\!\!\!\!\rightarrow\; \mathrm{Gal}((H(L)\cdot\mathbb{K})/\mathbb{K}) \;\cong\; \mathrm{Gal}(H(L)/(\mathbb{K}\cap H(L)))\;.$$

Therefore

$$\begin{aligned}\mu(L/K) &\leq \mu(\mathrm{Gal}(H(L)/(\mathbb{K}\cap H(L)))) \,+\, \mu(\mathrm{Gal}((\mathbb{K}\cap H(L))/L)\\ &\leq \mu(X_L) \,+\, \mu(\mathrm{Gal}(\mathbb{K}/L)) \;=\; \mu(X_L)\;,\end{aligned}$$

since $\mathrm{Gal}(\mathbb{K}/L)$ is a finitely generated $\mathbb{Z}_p$-module and thus $\mu(\mathrm{Gal}(\mathbb{K}/L)) = 0$ (compare Proposition 1.31, (iii)). □

Theorem 4.1 now immediately follows from Lemma 4.2.

4.2 Projective varieties and the μ-invariant

In a series of articles (see [Ba 76], [Ba 81] and [Ba 82]), V. A. BABAĬCEV has proved several global boundedness results concerning the Iwaswa invariant μ, regarded as a function on the set $\mathcal{E}(K)$ of $\mathbb{Z}_p$-extensions of a fixed number field K. These results build on Greenberg's work in [Gr 73] (and in particular generalise Theorem 4.1, (iii)). In order to obtain these results, Babaĭcev considered the sets $\mathcal{E}^{\mu>c}(K)$ consisting of all $\mathbb{Z}_p$-extensions L of K satisfying $\mu(L/K) > c$, $c \in \mathbb{N}_0$, and he showed how to equip them with the structure of a projective variety, respectively. The most important special case will be $c = 0$, the study of which will show that $\mathbb{Z}_p$-extensions L/K with $\mu(L/K) > 0$ usually are supposed to be somewhat 'rare' (see, for example, Theorem 4.15 below).

In this section, we will describe in detail Babaĭcev's approach to study global properties of Iwasawa invariants, which is a refinement of Greenberg's method that has been introduced in the last section. We will take the opportunity to state several auxiliary results that will become important in later parts of our work. Although some of these results have been proved by Babaĭcev, we will usually include full proofs whenever these make use of methods or notions that will be useful later.

4.2.1 Introduction

Let $\mathbb{K}$ denote the composite of all $\mathbb{Z}_p$-extensions of K, i.e., $\mathrm{Gal}(\mathbb{K}/K) \cong \mathbb{Z}_p^d$ for some $d \in \mathbb{N}$, and suppose that $d \geq 2$. In the preceding section, we considered homomorphisms

$$\pi_L : \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{K}/K)]] \longrightarrow\!\!\!\!\!\rightarrow \mathbb{Z}_p[[\mathrm{Gal}(L/K)]]$$

for any fixed $\mathbb{Z}_p$-extension L of K. Babaĭcev more generally studied the set of all surjective homomorphisms

$$\pi : \Lambda_d \longrightarrow\!\!\!\!\!\rightarrow \Lambda \ ,$$

where $\Lambda = \Lambda_1 = \mathbb{Z}_p[[T]]$ and $\Lambda_d = \mathbb{Z}_p[[T_1, \ldots, T_d]]$ (see Definition 2.16).

Let Γ^d, respectively, Γ, denote free abelian pro-p-groups of rank d, respectively, of rank 1. Then we have topological isomorphisms $\Gamma^d \cong \mathbb{Z}_p^d$ and $\Gamma \cong \mathbb{Z}_p$.

We will use some notation introduced in Section 2.1. Let

$$\varepsilon(\Gamma^d) := \{\pi : \Gamma^d \longrightarrow\!\!\!\!\!\rightarrow \Gamma\}$$

denote the set of all surjective $\mathbb{Z}_p$-module homomorphisms (i.e., continuous group homomorphisms) from Γ^d into Γ. In what follows, we will usually write the groups Γ^d and Γ multiplicatively, since in our applications, these groups will come up as Galois groups. Using the isomorphisms $\Gamma^d \cong \mathbb{Z}_p^d$ and $\Gamma \cong \mathbb{Z}_p$, we will identify $\varepsilon(\Gamma^d)$ with the set

$$\varepsilon(\mathbb{Z}_p^d) := \{\pi : \mathbb{Z}_p^d \longrightarrow\!\!\!\!\!\rightarrow \mathbb{Z}_p\}$$

that has been studied in Section 2.1.

We will identify two homomorphisms $\pi_1, \pi_2 : \mathbb{Z}_p^d \longrightarrow \mathbb{Z}_p$ if $\pi_1 = \pi_2^u$ for some $u \in \mathbb{Z}_p^*$. This will be important for the application to $\mathbb{Z}_p$-extensions (compare Remarks 2.6, (1) and Lemma 2.7), and makes it possible to obtain an isomorphism between $\varepsilon(\mathbb{Z}_p^d)$ and the $(d-1)$-dimensional projective space $\mathbb{P}^{d-1}(\mathbb{Z}_p)$ over $\mathbb{Z}_p$ introduced in Definition 2.1 (compare Proposition 2.5). Therefore $\varepsilon(\Gamma^d)$ may be seen as a projective variety.

Using the isomorphism $\mathrm{Gal}(\mathbb{K}/K) \cong \mathbb{Z}_p^d$, we may furthermore identify $\varepsilon(\mathbb{Z}_p^d)$ and

$$\varepsilon(\mathrm{Gal}(\mathbb{K}/K)) \;:=\; \{\pi : \mathrm{Gal}(\mathbb{K}/K) \;\twoheadrightarrow\; \mathbb{Z}_p\} \;\; .$$

This has been used in Lemma 2.7 in order to obtain a bijection

$$\mathcal{E}(K) \;\xrightarrow{\sim}\; \varepsilon(\mathrm{Gal}(\mathbb{K}/K)) \; ;$$

roughly speaking, each $L \in \mathcal{E}(K)$ corresponds to the restriction map

$$\pi_L : \mathrm{Gal}(\mathbb{K}/K) \twoheadrightarrow \mathrm{Gal}(L/K) \; ,$$

respectively.

Now let Γ and Γ^d be as above. Note that each homomorphism $\pi \in \varepsilon(\Gamma^d)$ defines a homomorphism

$$\pi : \; \mathbb{Z}_p[[\Gamma^d]] \;\twoheadrightarrow\; \mathbb{Z}_p[[\Gamma]]$$

of the corresponding completed group rings. Let $\gamma_1, \ldots, \gamma_d$ denote topological generators of Γ^d. Then Theorem 2.18 implies that there exists an isomorphism

$$\varphi : \; \mathbb{Z}_p[[\Gamma^d]] \;\xrightarrow{\sim}\; \Lambda_d \;=\; \mathbb{Z}_p[[T_1, \ldots, T_d]]$$

induced by the map $\gamma_i \mapsto 1 + T_i$, $1 \leq i \leq d$.

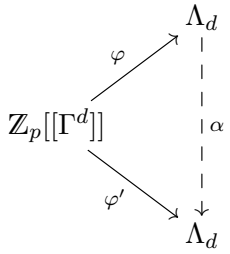
If $\gamma_1', \ldots, \gamma_d'$ is another system of topological generators of Γ^d, then

$$\gamma_j' \;=\; \prod_{i=1}^{d} \gamma_i^{a_{i,j}} \; , \qquad 1 \leq j \leq d \; ,$$

and $A := (a_{i,j})_{i,j} \in \mathrm{GL}_d(\mathbb{Z}_p)$ is an invertible matrix over $\mathbb{Z}_p$. The map induced by $\gamma_j' \mapsto 1 + T_j$, $1 \leq j \leq d$, yields another isomorphism

$$\varphi' : \; \mathbb{Z}_p[[\Gamma^d]] \;\xrightarrow{\sim}\; \Lambda_d \;\; ,$$

again using Theorem 2.18. The commutative diagram



defines an automorphism $\alpha : \Lambda_d \xrightarrow{\sim} \Lambda_d$, given by the substitution

$$T_j \;\mapsto\; T_j' \;:=\; \prod_{i=1}^{d} (1+T_i)^{a_{i,j}} - 1\;, \quad 1 \leq j \leq d\;.$$

Definition 4.6. A change of variables in Λ_d of the above shape is called ***admissible***.

Lemma 4.7 (Babaĭcev)**.** *Let $f(T_1, \ldots, T_d)$ be a formal power series different from zero having coefficients in a commutative ring E of characteristic $p \neq 0$. Then there exists an admissible change of variables of the form*

$$\begin{aligned} X_1 &= (1+T_1)(1+T_d)^{a_1} - 1\,, \\ &\vdots \\ X_{d-1} &= (1+T_{d-1})(1+T_d)^{a_{d-1}} - 1\,, \\ X_d &= T_d\;, \end{aligned}$$

with $a_1, \ldots, a_{d-1} \in \mathbb{N}$, under which f is carried to a series $g(X_1, \ldots, X_d)$ such that $g(0, \ldots, 0, X_d) \neq 0$. Actually, $a_1, \ldots, a_{d-1}$ may be chosen as

$$a_1 \;=\; \ldots \;=\; a_{d-1} \;=\; p^l\;,$$

with $l \in \mathbb{N}$ sufficiently large.

Proof. See [Ba 76], Lemma 1. The proof given there in fact is an adaption of Lemmas 2 and 3 in [Bou 89], Chapter 7, §3, with the additional property that we want the changes of variables to be admissible. □

Let $\pi \in \varepsilon(\Gamma^d)$. If the topological generators of Γ^d are chosen such that the kernel of $\pi : \Gamma^d \longrightarrow \Gamma$ is generated by $\gamma_1, \ldots, \gamma_{d-1}$, and if $\delta := \pi(\gamma_d)$, then δ is a topological generator of Γ. The induced homomorphism $\pi : \Lambda_d \longrightarrow \Lambda$ is then given by

$$\pi(T_i) \;=\; \pi(\gamma_i - 1) \;=\; \pi(\gamma_i) - \pi(1) \;=\; 1 - 1 \;=\; 0$$

for every $1 \leq i \leq d-1$, and

$$\pi(T_d) \;=\; \pi(\gamma_d) - 1 \;=\; \delta - 1 \;=\; T\;.$$

If $f \in \mathbb{Z}_p[[\Gamma^d]] \cong \mathbb{Z}_p[[T_1, \ldots, T_d]]$, then we simply have $\pi(f) = f(0, \ldots, 0, T)$.

We will now see that for a given π, we may always choose topological generators of Γ^d such that π obtains this canonical form.

Remark 4.8. For every $\pi \in \varepsilon(\Gamma^d)$, we may choose topological generators $\gamma_1, \ldots, \gamma_d$ of Γ^d such that the kernel of $\pi : \Gamma^d \longrightarrow \Gamma$ is generated by $\gamma_1, \ldots, \gamma_{d-1}$.

Proof. The kernel of $\pi : \Gamma^d \longrightarrow \Gamma$ is a $\mathbb{Z}_p$-submodule of Γ^d and therefore is $\mathbb{Z}_p$-free. Its rank has to be strictly smaller than d, since π is surjective, and in fact, $\ker(\pi)$ has $\mathbb{Z}_p$-rank equal to $d-1$, since π induces an exact sequence

$$0 \longrightarrow \mathbb{Z}_p^{\mathrm{rank}(\ker(\pi))} \longrightarrow \mathbb{Z}_p^d \longrightarrow \mathbb{Z}_p \longrightarrow 0\;.$$

By the Principal Divisor Theorem (see [JS 06], Thm. VII.8.2), there exists a basis $\gamma_1, \ldots, \gamma_d$ of Γ^d (i.e., a set of topological generators of this multiplicatively written group) such that $\ker(\pi)$ is generated topologically by $\gamma_1^{a_1}, \ldots, \gamma_{d-1}^{a_{d-1}}$, with $a_1, \ldots, a_{d-1} \in \mathbb{Z}_p$ and $a_1 \mid a_2 \mid \ldots \mid a_{d-1}$. Let $z := \gamma_{d-1}^{a_{d-1}} \in \ker(\pi)$. Now assume that $p \mid a_{d-1}$ in $\mathbb{Z}_p$. Then we can write $z = y^p$ for some element $y \in \Gamma^d$ that does not lie in the kernel of π (since the $\gamma_i^{a_i}$ form a basis of $\ker(\pi)$, they are linearly independent). But then $x := \pi(y) \in \mathbb{Z}_p$ is different from 1, and $x^p = (\pi(y))^p = \pi(y^p) = \pi(z) = 1$, which contradicts the fact that Γ is torsion-free (as being a free $\mathbb{Z}_p$-module). Therefore p does not divide a_{d-1}, i.e., $a_1, \ldots, a_{d-1} \in \mathbb{Z}_p^*$, and $\ker(\pi)$ is generated by $\gamma_1, \ldots, \gamma_{d-1}$. □

Definition 4.9. An element $f \in \Lambda_d = \mathbb{Z}_p[[T_1, \ldots, T_d]]$ is in ***Weierstraß normal form with respect to*** T_d if

$$f \;=\; U \cdot p^m \cdot (T_d^k + a_{k-1} T_d^{k-1} + \ldots + a_0)\,,$$

where $m \in \mathbb{N}_0$, $k \in \mathbb{N}$, $U \in \Lambda_d^*$ is a unit and $a_0, \ldots, a_{k-1} \in (p, T_1, \ldots, T_{d-1})$ are contained in the maximal ideal of the local ring $\mathbb{Z}_p[[T_1, \ldots, T_{d-1}]]$. f is called ***regular in*** T_d if f is in Weierstraß normal form with respect to T_d and $m = 0$ in the corresponding representation.

Remarks 4.10.

(1) If f is in Weierstraß normal form with respect to T_d, then $f = U \cdot p^m \cdot \tilde{f}(T_d)$ with a distinguished polynomial

$$\tilde{f}(T_d) \;\in\; (\mathbb{Z}_p[[T_1, \ldots, T_{d-1}]])[T_d]$$

in the sense of Definition 1.11.

(2) If $\pi \in \varepsilon(\Gamma^d)$ is a homomorphism such that $\ker(\pi)$ is generated topologically by $\gamma_1, \ldots, \gamma_{d-1}$, then $\delta := \pi(\gamma_d)$ generates Γ. If $f \in \Lambda_d$ is in Weierstraß normal form with respect to T_d in the variables $T_1, \ldots, T_d$ induced by $\gamma_1, \ldots, \gamma_d$, then we can simply write

$$\pi(f) \;=\; \pi(U) \cdot p^m \cdot (T^k + \overline{a_{k-1}} \cdot T^{k-1} + \ldots + \overline{a_0})\,,$$

with $\overline{a_i} = \pi(a_i) = a_i(0, \ldots, 0) \in p \cdot \mathbb{Z}_p$, $0 \le i \le d-1$. In particular, $\pi(f) \neq 0$, and $p \mid \pi(f)$ if and only if $m > 0$, i.e., if and only if $p \mid f$.

(3) We may apply the Weierstraß Preparation Theorem 1.14 in the ring of power series

$$\mathbb{Z}_p[[T_1, \ldots, T_d]] \;\cong\; (\mathbb{Z}_p[[T_1, \ldots, T_{d-1}]])[[T_d]]\,,$$

since $\mathbb{Z}_p[[T_1, \ldots, T_{d-1}]]$ is a local ring with maximal ideal

$$\mathfrak{M}_{d-1} \;=\; (p, T_1, \ldots, T_{d-1})$$

which is complete with respect to the $\mathfrak{M}_{d-1}$-adic topology; compare Proposition 2.17, (i). This implies that an element $f \in \Lambda_d$ is regular with respect to T_d if and only if $f \notin (p, T_1, \ldots, T_{d-1}) \subseteq \Lambda_d$.

Lemma 4.11 (Babaĭcev)**.** *Let $f \in \mathbb{Z}_p[[\Gamma^d]]$ be non-zero. Let $U \subseteq \varepsilon(\Gamma^d)$ denote the set of homomorphisms $\pi : \Gamma^d \longrightarrow \Gamma$ such that*
(1) we can choose topological generators $\gamma_1, \ldots, \gamma_d$ of Γ^d such that $\ker(\pi)$ is generated by $\gamma_1, \ldots, \gamma_{d-1}$, and
(2) f is in Weierstraß normal form with respect to T_d in the variables induced by $\gamma_1, \ldots, \gamma_d$ via the map $\gamma_i \mapsto 1 + T_i$, $1 \leq i \leq d$.
Then $U \subseteq \varepsilon(\Gamma^d)$ is open and dense in the topology defined on $\varepsilon(\Gamma^d)$ via the bijection $\varepsilon(\Gamma^d) \xrightarrow{\sim} \varepsilon(\mathbb{Z}_p^d) \xrightarrow{\sim} \mathbb{P}^{d-1}(\mathbb{Z}_p)$ (compare Remarks 2.6, (2)).

Proof. This is basically an application of Lemma 4.7 and Remark 4.8, see Proposition 1 in [Ba 76] for details.

□

Definition 4.12. Let M denote a finitely generated Λ_d-module. For every surjective homomorphism $\pi : \Lambda_d \twoheadrightarrow \Lambda$, we define $M_\pi := M/(\ker(\pi) \cdot M)$; this is a Λ-module, where we identify $\Lambda = \Lambda_d/\ker(\pi)$.

Note that this corresponds to the notion X_L used by Greenberg (compare the preceding section).

Theorem 4.13 (Babaĭcev)**.**
(i) Let M denote a finitely generated Λ_d-module, and let $m := \operatorname{rank}_{\Lambda_d}(M)$. Then the subset

$$U \;:=\; \{\pi \in \varepsilon(\Gamma^d) \mid \operatorname{rank}_\Lambda(M_\pi) = m\} \;\subseteq\; \varepsilon(\Gamma^d)$$

is open and dense in $\varepsilon(\Gamma^d)$.
(ii) Let M denote a finitely generated Λ_d-module, and assume that there exists a homomorphism $\pi_0 \in \varepsilon(\Gamma^d)$ such that M_{π_0} is a finitely generated $\mathbb{Z}_p$-module. Then the set $U \subseteq \varepsilon(\Gamma^d)$ containing all π such that M_π is finitely generated over $\mathbb{Z}_p$ is open and dense in $\varepsilon(\Gamma^d)$.

We recall that the Λ_d-rank of a finitely generated Λ_d-module N may be defined via

$$\operatorname{rank}_{\Lambda_d}(N) := \dim_Q(N \otimes_{\Lambda_d} Q)\,,$$

where Q denotes the quotient field of Λ_d, and $\dim_Q$ means the dimension as Q-vector space.

Proof. (i) This is Theorem 1 in [Ba 76]. Since Babaĭcev only gives a very brief proof, we will include here a proof giving full details.
Since M is a finitely generated Λ_d-module, there exists a surjection

$$F \longrightarrow M \longrightarrow 0$$

for some free Λ_d-module F with basis $f_1, \ldots, f_l$. Let $R \subseteq F$ denote the kernel of this map. Then R is finitely generated over Λ_d, since F is Noetherian as being finitely generated over the Noetherian ring Λ_d, and $\operatorname{rank}_{\Lambda_d}(M) = m$ if and only if $\operatorname{rank}_{\Lambda_d}(R) = l - m$. Indeed, the sequence

$$0 \longrightarrow R \longrightarrow F \longrightarrow M \longrightarrow 0$$

of Λ_d-modules is exact by construction, and therefore the following sequence of Q-vector spaces also is exact:

$$0 \longrightarrow (R \otimes Q) \longrightarrow (F \otimes Q) \longrightarrow (M \otimes Q) \longrightarrow 0 \ . \qquad (\star)$$

Note that in general, tensoring a sequence of Λ_d-modules with a Λ_d-module N will be only right-exact (see [JS 06], p. 184 for an example over the ring $\mathbb{Z}$). A Λ_d-module N is called *flat* if tensoring with N is exact on both sides. In our situation, $N = Q = \mathrm{Quot}(\Lambda_d)$ is equal to the quotient field of Λ_d, and therefore flat by Corollary 3.6 in [AM 69], proving the exactness of the sequence $(\star)$. But the dimension of vector spaces is additive on exact sequences, and therefore

$$\begin{aligned} \mathrm{rank}_{\Lambda_d}(R) + \mathrm{rank}_{\Lambda_d}(M) &= \dim_Q(R \otimes Q) + \dim_Q(M \otimes Q) \\ &= \dim_Q(F \otimes Q) \\ &= \mathrm{rank}_{\Lambda_d}(F) = l \ , \end{aligned}$$

proving that $\mathrm{rank}_{\Lambda_d}(M) = m$ if and only if $\mathrm{rank}_{\Lambda_d}(R) = l - m$.
Let $r_1, \ldots, r_q$ denote generators of $R \subseteq F$. There exist elements $a_{i,j} \in \Lambda_d$ such that

$$r_i = \sum_{j=1}^{l} a_{ij} f_j \ , \quad 1 \leq i \leq q \ .$$

Now the condition $\mathrm{rank}_{\Lambda_d}(R) = l - m$ is equivalent to the fact that there exists a non-vanishing minor of the matrix $(a_{ij})_{i,j}$ of order $l-m$, whereas every minor of order greater than $l-m$ is zero. Let $f \in \Lambda_d$ denote the non-trivial minor of $(a_{ij})_{i,j}$. By Lemma 4.11, there exists an open and dense subset $U \subseteq \varepsilon(\Gamma^d)$ such that for every $\pi \in U$, $\pi(f)$ is in Weierstraß normal form, and in particular non-zero. We will show that $\mathrm{rank}_{\Lambda_d}(M_\pi) = m$ for $\pi \in U$, proving (i).
We have a surjection

$$F_\pi = F/(\ker(\pi) \cdot F) \xrightarrow{\overline{\psi}} M_\pi = M/(\ker(\pi) \cdot M) \longrightarrow 0$$

induced by the surjective Λ_d-module homomorphism $F \xrightarrow{\psi} M \longrightarrow 0$, which maps $\ker(\pi) \cdot F$ into $\ker(\pi) \cdot M$. The map $R_\pi \xrightarrow{\overline{\varphi}} F_\pi$ induced by $0 \longrightarrow R \xrightarrow{\varphi} F$ perhaps is not injective, so we divide out the kernel X_π and define a Λ-module $\tilde{R}_\pi := R_\pi / X_\pi$. Then the sequence

$$0 \longrightarrow \tilde{R}_\pi \xrightarrow{\tilde{\varphi}} F_\pi \xrightarrow{\overline{\psi}} M_\pi \longrightarrow 0 \qquad (\star\star)$$

is exact, where the induced injective map $\tilde{\varphi} : \tilde{R}_\pi \longrightarrow F_\pi$ is defined via $\overline{r} + \ker(\overline{\varphi}) \mapsto \overline{\varphi}(\overline{r})$.
Indeed, it remains to show that $\ker(\overline{\psi}) \subseteq \mathrm{im}(\tilde{\varphi})$. Let $f \in F$ be such that $\overline{\psi}(f + \ker(\pi) \cdot F) \in \ker(\pi) \cdot M$. Write

$$\psi(f) = \sum_i \alpha_i \cdot m_i$$

with elements $\alpha_i \in \ker(\pi)$, $m_i \in M$. For every i, we choose a pre-image $f_i \in F$ such that $\psi(f_i) = m_i$. Then $\psi(f - \sum_i \alpha_i \cdot f_i) = 0$, so that

$$f - \sum_i \alpha_i \cdot f_i \;=\; \varphi(r)$$

for some $r \in R$. But then $\tilde{\varphi}(\overline{r}) = \overline{f - \sum_i \alpha_i \cdot f_i} = \overline{f}$, i.e., $\overline{f} \in \mathrm{im}(\tilde{\varphi})$. The exact sequence $(\star\star)$ implies that

$$\mathrm{rank}_\Lambda(\tilde{R}_\pi) + \mathrm{rank}_\Lambda(M_\pi) \;=\; \mathrm{rank}_\Lambda(F_\pi) \;=\; \mathrm{rank}_{\Lambda_d}(F) \;=\; l\ .$$

Here we use the fact that $F \cong \Lambda_d^l$, and therefore $F_\pi \cong \Lambda^l$ as Λ-modules. It therefore suffices to prove that $\mathrm{rank}_\Lambda(\tilde{R}_\pi) = \mathrm{rank}_{\Lambda_d}(R) =: r$ for $\pi \in U$. We know from the first part of the proof that there exists a non-vanishing minor $f \in \Lambda_d$ of the matrix $(a_{ij})_{i,j}$ of order r. The set $U \subseteq \varepsilon(\Gamma^d)$ has been chosen such that $\pi(f) \neq 0$ in $\Lambda = \Lambda_d/(\ker(\pi))$ for every $\pi \in U$. Fixing an arbitrary $\pi \in U$, we know that R_π is generated by the cosets

$$\overline{r}_1, \ldots, \overline{r}_q \in R_\pi = R/(\ker(\pi) \cdot R)$$

of the generators $r_1, \ldots, r_q$ of R. Furthermore, since $r_i = \sum_j a_{ij} \cdot f_j$, $1 \leq i \leq q$, we obtain relations

$$\overline{\varphi}(\overline{r}_i) \;=\; \sum_{j=1}^{l} \overline{a}_{ij} \cdot \overline{f}_j\ , \quad 1 \leq i \leq q\ ,$$

with $\overline{f}_j$ being the coset of f_j in $F_\pi = F/(\ker(\pi) \cdot F)$, respectively. Consider the matrix $(\overline{a}_{ij})_{i,j}$, with $\overline{a}_{ij} = \pi(a_{ij}) \in \Lambda$ for every i and j. Since $\pi(f) \neq 0$, this matrix has a non-vanishing minor of order r, proving that $\mathrm{rank}_\Lambda(R_\pi) \geq \mathrm{rank}_\Lambda(\overline{\varphi}(R_\pi)) \geq r$. Let $J \subseteq \{1, \ldots, q\}$ denote the set of indices corresponding to the submatrix of (a_{ij}) whose determinant is the minor f.
Now assume that $\mathrm{rank}_\Lambda(\tilde{R}_\pi) < r \leq \mathrm{rank}_\Lambda(R_\pi)$, Then, by definition of $\tilde{R}_\pi$,

$$\sum_{i \in I} \overline{\lambda}_i \cdot \overline{r}_i \;\in\; \ker(\overline{\varphi})$$

and therefore

$$\sum_{i \in I} \sum_{j=1}^{l} \overline{\lambda}_i \cdot \overline{a}_{ij} \cdot \overline{f}_j \;=\; \overline{0} \;\in\; F_\pi$$

for each subset $I \subseteq \{1, \ldots, q\}$ of order r and coefficients $\overline{\lambda}_i \in \Lambda$ such that $\overline{\lambda_i} \neq 0$ for some $i \in I$, respectively. We will show that this cannot hold for the special set $I \neq J$ of order r.
Choose lifts $\lambda_i \in \Lambda_d$ of $\overline{\lambda_i}$, respectively. Since $\{f_j : 1 \leq j \leq l\}$ is a basis of F, we may conclude that

$$\sum_{i \in I} \sum_{j=1}^{l} \lambda_i \cdot a_{ij} \cdot f_j \;=\; \sum_{j=1}^{l} \beta_j \cdot f_j$$

with $\beta_j \in \ker(\pi) \subseteq \Lambda_d$, $j = 1, \ldots, l$. But then

$$0 \;=\; \sum_{j=1}^{l} (\sum_{i \in I} \lambda_i a_{ij} - \beta_j) \cdot f_j$$

and therefore $\sum_{i \in I} \lambda_i a_{ij} = \beta_j \in \ker(\pi)$ for all $1 \leq j \leq l$, recalling that the f_j are Λ_d-linear independent.
If I was equal to J, then we would obtain a non-trivial vanishing linear combination of the rows of $(\overline{a_{ij}})_{i,j \in J}$ in $\Lambda = \Lambda_d / \ker(\pi)$. But this would contradict the fact that

$$\pi(f) \;=\; \det((\overline{a_{ij}})_{i,j \in J}) \;\neq\; 0 \,.$$

Therefore, $\mathrm{rank}_\Lambda(\tilde{R}_\pi) \geq |J| = r$.
On the other hand, if $\mathrm{rank}_\Lambda(\tilde{R}_\pi)$ was strictly larger than r, then there would exist a non-vanishing minor $\overline{g}$ of the matrix $(\overline{a}_{ij})$ of order greater than r, since $\tilde{R}_\pi$ is generated by the cosets of $r_1, \ldots, r_q$. Since $\pi : \Lambda_d \longrightarrow \Lambda$ is surjective, we could lift $\overline{g}$ to a non-vanishing minor of (a_{ij}) of order greater than r, in contradiction to the fact that $\mathrm{rank}_{\Lambda_d}(R) = r$.

(ii) Now suppose that M_{π_0} is a finitely generated $\mathbb{Z}_p$-module. Then M_{π_0} is a torsion Λ-module. Greenberg has shown that this happens only if there exists an annihilator $f \in \Lambda_d$ of M such that $f \notin \ker(\pi_0)$ (see Lemma 4.2, (i)). Furthermore, we may assume that f is not divisible by p. Indeed, $\mu(M_{\pi_0}) = 0$ by Proposition 1.31, (iii). Therefore the characteristic polynomial $\overline{g}(T) \in \mathbb{Z}_p[T] \subseteq \Lambda$ of M_{π_0} is not divisible by p. $\overline{g}(T)$ annihilates the elementary Λ-module $E_{M_{\pi_0}}$. Since the finite kernel of the pseudo-isomorphism $M_{\pi_0} \xrightarrow{\sim} E_{M_{\pi_0}}$ may be annihilated by an appropriate power of T, by Nakayama's Lemma (compare Remark 3.49), we may augment $\overline{g}$ in order to obtain an annihilator g of M_{π_0} that is still not divisible by p. Using the arguments from the proof of Lemma 4.2, (i), it follows that M is a torsion Λ_d-module, and that there exists an annihilator $f \in \Lambda_d$ of M such that

$$f \;\equiv\; g^l \mod (\ker(\pi_0)) \,,$$

where l denotes the number of generators of the finitely generated Λ_d-module M. In particular, $p \nmid f$.
Since there exists a surjective homomorphism $(\Lambda_d/(f))^l \longrightarrow M$, it will suffice to prove assertion (ii) for the module $N := \Lambda_d/(f)$. By Lemma 4.11 and Remarks 4.10, (2), there exists an open and dense subset $U \subseteq \varepsilon(\Gamma^d)$ such that for every $\pi \in U$, the image $\pi(f) = u \cdot \tilde{f}$ is the product of a unit $u \in \mathbb{Z}_p[[T]]^* = \Lambda^*$ and a distinguished polynomial $\tilde{f} \in \mathbb{Z}_p[T]$. Therefore

$$N_\pi \;=\; \Lambda/(\pi(f)) \;=\; \Lambda/(\tilde{f}) \;\cong\; \mathbb{Z}_p^{\deg(\tilde{f})}$$

is finitely generated over $\mathbb{Z}_p$ for every $\pi \in U$.

□

Using this theorem, Babaĭcev proved his first result concerning the Iwasawa μ-invariant in $\mathbb{Z}_p$-extensions of K. In order to apply the theory developed so

far, we let $\Gamma = \Gamma^1 := \mathbb{Z}_p$ and $\Gamma^d := \mathrm{Gal}(\mathbb{K}/K) \cong \mathbb{Z}_p^d$, where $\mathbb{K}$ denotes the composite of all $\mathbb{Z}_p$-extensions of K, as usual. Then the study of surjective $\mathbb{Z}_p$-module homomorphisms $\pi \in \varepsilon(\Gamma^d)$ corresponds to the study of $\mathbb{Z}_p$-extensions of K (compare Lemma 2.7).

Definition 4.14. Let $c \in \mathbb{N}_0$. Define $\mathcal{E}^{\mu>c}(K)$ to be the set of $\mathbb{Z}_p$-extensions L/K satisfying $\mu(L/K) > c$. Furthermore, let $\mathcal{E}^0(K)$ denote the set of $\mathbb{Z}_p$-extensions L/K such that $\mu(L/K) = 0$.

Theorem 4.15 (Babaĭcev)**.** *If there exists a $\mathbb{Z}_p$-extension $L \in \mathcal{E}^0(K)$ such that only finitely many primes of L lie over p, then the subset $\mathcal{E}^0(K)$ of $\mathcal{E}(K)$ is open and dense.*

Proof. This is Theorem 4 in [Ba 76]. Whereas the proof given there uses cohomology theory, we will use more elementary arguments. Let $Y := \mathrm{Gal}(H(\mathbb{K})/\mathbb{K})$ denote the Galois group of the maximal p-abelian unramified extension of $\mathbb{K}$. Then Y is a finitely generated torsion Λ_d-module (compare Theorem 1 in [Gr 73]). Furthermore, if π denotes the surjective homomorphism corresponding to L/K via Lemma 2.7, then our assumptions on L imply that $Y_\pi := Y/(\ker(\pi) \cdot Y)$ is a finitely generated $\mathbb{Z}_p$-module (compare Lemma 4.3, (i)).

Theorem 4.13, (ii) implies that there exists an open and dense subset U of $\varepsilon(\mathrm{Gal}(\mathbb{K}/K))$ such that Y_π is a finitely generated $\mathbb{Z}_p$-module for every $\pi \in U$.

We will now make use of the following fact.

Lemma 4.16. *For every $\mathbb{Z}_p$-extension L/K, and corresponding homomorphism $\pi \in \varepsilon(\mathrm{Gal}(\mathbb{K}/K))$, we have an exact sequence*

$$Y_\pi \longrightarrow X_\pi \longrightarrow \mathrm{Gal}((H(L) \cap \mathbb{K})/L)$$

of Λ-modules, where $X_\pi := \mathrm{Gal}(H(L)/L)$ denotes the Galois group of the maximal p-abelian unramified extension $H(L)$ of L, and Y_π is defined as above.

Proof. Let F denote the subfield of $H(\mathbb{K})$ fixed by $\ker(\pi) \cdot Y \subseteq Y$. Thus, $\mathrm{Gal}(H(\mathbb{K})/F) = \ker(\pi) \cdot Y$ and $\mathrm{Gal}(F/\mathbb{K}) \cong Y_\pi = Y/(\ker(\pi) \cdot Y)$. Assume that we have chosen a set of topological generators $\gamma_1, \ldots, \gamma_d$ of $\mathrm{Gal}(\mathbb{K}/K)$ such that the kernel of $\pi \in \varepsilon(\mathrm{Gal}(\mathbb{K}/K))$ is generated by $\gamma_1, \ldots, \gamma_{d-1}$.

Claim 4.17. *The maximal p-abelian unramified extension $H(L)$ of L is contained in F.*

Proof. Since $\ker(\pi) \subseteq \Lambda_d$ is generated by $T_1, \ldots, T_{d-1}$, the subfield F of $H(\mathbb{K})$ is fixed by $<T_1, \ldots, T_{d-1}> \cdot Y$.

Note that $H(\mathbb{K})$ actually is Galois over L. Since

$$<T_1, \ldots, T_{d-1}> \cdot Y \subseteq \mathrm{Gal}(H(\mathbb{K})/L)$$

is a closed subgroup, it follows that $F \subseteq H(\mathbb{K})$ is also Galois over L. We claim that F is the maximal subextension that is abelian over L; this relies on the fact that $<T_1, \ldots, T_{d-1}> \cdot Y$ corresponds to the topological commutator subgroup of $\mathrm{Gal}(H(\mathbb{K})/L)$, as we will see in Chapter 5 (compare Lemma 5.19).

Indeed, $\mathrm{Gal}(\mathbb{K}/L)$ acts on $\mathrm{Gal}(H(\mathbb{K})/\mathbb{K}) = Y$ via conjugation. Since

$$\gamma_i \cdot \sigma \cdot \gamma_i^{-1} \cdot \sigma^{-1}(x) \;=\; ((\gamma_i - 1) \cdot \sigma)(x) \;=\; (T_i \cdot \sigma)(x) \;=\; x$$

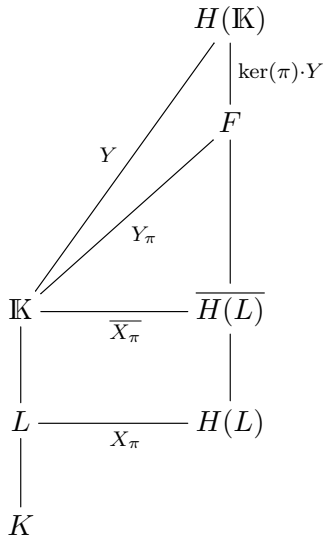
for every $\sigma \in Y$, $x \in F$, $i = 1, \ldots, d-1$, it follows that $\gamma_i \cdot \sigma \cdot \gamma_i^{-1}(x) = \sigma(x)$ for each $\sigma \in Y$, $x \in F$, i.e., $\gamma_i \cdot \sigma \cdot \gamma_i^{-1} = \sigma$ for every $\sigma \in \mathrm{Gal}(F/\mathbb{K})$, proving that F/L is abelian.

Conversely, if $M \subseteq H(\mathbb{K})$ is abelian over L, then $\gamma_i \cdot \sigma \cdot \gamma_i^{-1} = \sigma$ for every $\sigma \in \mathrm{Gal}(M/\mathbb{K})$ and every $i \in \{1, \ldots, d-1\}$, since $\mathrm{Gal}(\mathbb{K}/L)$ is generated by $\gamma_1, \ldots, \gamma_{d-1}$. But then $M \subseteq H(\mathbb{K})^{<T_1,\ldots,T_{d-1}>\cdot Y} = F$.

Since $H(L)$ is abelian over L, and $H(L) \subseteq H(\mathbb{K})$ (compare Proposition 1.34), it is now immediate that $H(L) \subseteq F$.

□

Now let $X_\pi := \mathrm{Gal}(H(L)/L)$. Then $\overline{H(L)} := H(L) \cdot \mathbb{K} \subseteq F$. We let $\overline{X_\pi} := \mathrm{Gal}(\overline{H(L)}/\mathbb{K})$ and summarise our situation in the following diagram:



Since it is possible that $\mathbb{K} \cap H(L) \supsetneqq L$, we may not conclude that $\overline{X_\pi} \cong X_\pi$. However, since $\overline{H(L)} \subseteq F$, we have a surjective map

$$Y_\pi \;\longrightarrow\!\!\!\!\!\rightarrow\; \overline{X_\pi}\,, \quad \sigma \;\longmapsto\; \sigma + \mathrm{Gal}(F/\overline{H(L)}) =: \overline{\sigma}\ .$$

Furthermore, since $\overline{X_\pi} = \mathrm{Gal}(\overline{H(L)}/\mathbb{K}) \cong \mathrm{Gal}(H(L)/(\mathbb{K} \cap H(L)))$, we obtain a map $\overline{X_\pi} \longrightarrow X_\pi$, induced by restriction to $H(L)$. Note that this latter map will not be surjective whenever $H(L) \cap \mathbb{K} \neq L$. However, the cokernel will yield us the desired exact sequence:

First note that the composite

$$i : Y_\pi \;\longrightarrow\; \overline{X_\pi} \;\longrightarrow\; X_\pi\,, \quad \sigma \;\longmapsto\; \overline{\sigma} \;\longmapsto\; \overline{\sigma}|_{H(L)}\ ,$$

is well-defined since every element in $\mathrm{Gal}(F/\overline{H(L)})$ fixes $H(L) \subseteq \overline{H(L)}$. Let

$$j : X_\pi = \mathrm{Gal}(H(L)/L) \;\longrightarrow\; \mathrm{Gal}((H(L) \cap \mathbb{K})/L)\,, \quad \tau \;\longmapsto\; \tau|_{(H(L)\cap\mathbb{K})}\ ,$$

denote the canonical restriction map. Then the sequence

$$Y_\pi \xrightarrow{\ i\ } X_\pi \xrightarrow{\ j\ } \mathrm{Gal}((H(L)\cap\mathbb{K})/L)$$

is exact. First of all, it is clear that the image of i is contained in $\ker(j)$, since $\overline{\sigma}|_{(H(L)\cap\mathbb{K})} = \mathrm{id} \in \mathrm{Gal}((H(L)\cap\mathbb{K})/L)$ for every $\overline{\sigma} \in \mathrm{Gal}(\overline{H(L)}/\mathbb{K})$. On the other hand, if $\tau|_{(H(L)\cap\mathbb{K})} = \mathrm{id}$ for some $\tau \in X_\pi = \mathrm{Gal}(H(L)/L)$, then $\tau \in \mathrm{Gal}(H(L)/(H(L)\cap\mathbb{K}))$, and therefore τ is the restriction to $H(L)$ of some element in $\mathrm{Gal}(\overline{H(L)}/\mathbb{K}) = \overline{X_\pi}$. Since $Y_\pi \twoheadrightarrow \overline{X_\pi}$ is surjective, we obtain that $\tau = i(\sigma)$ for a suitable σ. □

This shows that X_π is a finitely generated $\mathbb{Z}_p$-module if Y_π is finitely generated over $\mathbb{Z}_p$, since $\mathrm{rank}_{\mathbb{Z}_p}(\mathrm{Gal}((\mathbb{K}\cap H(L))/L)) \leq d-1$. In particular, X_π is finitely generated over $\mathbb{Z}_p$ and therefore Λ-torsion for every $\pi \in U$, i.e., $U \subseteq \mathcal{E}(X)$ in the notation of Section 4.1. The assertion of Theorem 4.15 now follows from Corollary 4.5, (ii) and Proposition 1.31, (iii). □

4.2.2 μ is globally bounded

In [Ba 81] and [Ba 82], Babaĭcev showed that Theorem 4.1, (iii), proved by Greenberg only in the case of ground fields K containing one single prime above p, actually holds in general: For any number field K, there exists a constant $C = C(K)$ such that $\mu(L/K) \leq C$ for every $L \in \mathcal{E}(K)$. The main step in Babaĭcev's proof is built up of giving the sets $\mathcal{E}^{\mu>c}(K)$ the structure of a projective variety. For this purpose, Babaĭcev considered, for every $n \in \mathbb{N}$ and $0 \leq m \leq n-1$, the Grassmannian varieties ε_n^m which we introduced in Section 2.1.

We recall some notation. For every integer $k > 0$, let $\Gamma^k \cong \mathbb{Z}_p^k$ denote a fixed free abelian pro-p-group with k generators. We let ε_n^m be the set of all surjective continuous group homomorphisms $\pi : \Gamma^{n+1} \twoheadrightarrow \Gamma^{m+1}$. In particular, $\varepsilon_{d-1}^0 = \varepsilon(\Gamma^d)$ is the set we have studied in the preceding subsection. We have shown in Section 2.1 that each set ε_n^m in a natural way bears the structure of a compact projective variety.

Let us fix n and m. We choose topological generators $\gamma_0, \ldots, \gamma_n$ of Γ^{n+1} and $\delta_0, \ldots, \delta_m$ of Γ^{m+1}, respectively. Each $\pi \in \varepsilon_n^m$ extends to a surjective homomorphism of the corresponding group rings, which may be regarded as a map

$$\pi : \mathbb{Z}_p[[X_0, \ldots, X_n]] \longrightarrow \mathbb{Z}_p[[T_0, \ldots, T_m]] ,$$

using the isomorphisms

$$\mathbb{Z}_p[[\Gamma^{n+1}]] \xrightarrow{\ \sim\ } \Lambda_{n+1} := \mathbb{Z}_p[[X_0, \ldots, X_n]]$$

and

$$\mathbb{Z}_p[[\Gamma^{m+1}]] \xrightarrow{\ \sim\ } \Lambda_{m+1} := \mathbb{Z}_p[[T_0, \ldots, T_m]]$$

(compare Theorem 2.18).

For every $f \in \Lambda_{n+1}$, let $v_p(\pi(f))$ denote the largest power of p dividing $\pi(f)$ in the unique factorisation domain Λ_{m+1}. For every $c \geq 0$, we define

$$V^m(f;c) \ := \ \{\pi \in \varepsilon_n^m \mid v_p(\pi(f)) \geq c\} \ .$$

We will now prove several auxiliary results, some of which are used in [Ba 81], that will be used several times in the next section and also in the next chapter.

For any $k, N \in \mathbb{N}$ such that $k \leq p^{2N}$, the p-adic valuation of the binomial coefficient $\binom{p^{2N}}{k}$ is given by $2N - v_p(k)$ (see, for example, Lemma 1.1 in [Ba 81]). In particular, for $k < p^N$, we have $v_p(\binom{p^{2N}}{k}) \geq N$. Therefore the following congruence holds in the ring $\mathbb{Z}_p[[T]]$ of formal power series in one variable:

$$(1+T)^{p^{2N}} - 1 \ \equiv \ 0 \mod (p^N, T^{p^N}) \ . \tag{4.1}$$

Now we consider a fixed element $\pi_0 \in \varepsilon_n^m$. We write a standard neighbourhood of π_0 as $U = U((N_{i,j})_{0 \leq i \leq n, 0 \leq j \leq m})(\pi_0)$, consisting of every surjective homomorphism $\tilde{\pi} : \Gamma^{n+1} \longrightarrow \Gamma^{m+1}$ such that

$$\tilde{\pi}(\gamma_i) \ = \ \pi_0(\gamma_i) \cdot \prod_{j=0}^{m} \delta_j^{a_{i,j}} \ , \quad v_p(a_{i,j}) \geq N_{i,j} \ , \ 0 \leq i \leq n \, , \ 0 \leq j \leq m \ .$$

Proposition 4.18. *Let $U = U((2N_{i,j})_{i,j})(\pi_0)$ be a neighbourhood of $\pi_0 \in \varepsilon_n^m$ (note the doubled precision $2N_{i,j}$), let $f \in \Lambda_{n+1}$ be arbitrary. Then*

$$\pi(f) \ \equiv \ \pi_0(f) \mod (p^N, T_0^{p^{N_0}}, \ldots, T_m^{p^{N_m}})$$

for every $\pi \in U$, where $N_j := \min_i N_{i,j}$, $0 \leq j \leq m$, and $N := \min_j N_j$.

Proof. Using (4.1), we obtain

$$\begin{aligned}
\pi(X_i) \quad &= \quad \pi(\gamma_i) - 1 \ = \ \pi_0(X_i + 1) \cdot \prod_{j=0}^{m} \delta_j^{p^{2N_{i,j}} \cdot u_{i,j}} - 1 \quad , \ u_{i,j} \in \mathbb{Z}_p \ , \\
&= \quad (\pi_0(X_i) + 1) \cdot \prod_{j=0}^{m} (T_j + 1)^{p^{2N_{i,j}} \cdot u_{i,j}} - 1 \\
&\overset{(4.1)}{\equiv} \quad (\pi_0(X_i) + 1) \cdot 1 - 1 \ = \ \pi_0(X_i) \mod (p^N, T_0^{p^{N_{i,0}}}, \ldots, T_m^{p^{N_{i,m}}})
\end{aligned}$$

for every $0 \leq i \leq n$ and every $\pi \in U$. Expanding $f \in \Lambda_{n+1} = \mathbb{Z}_p[[X_0, \ldots, X_n]]$, and using the fact that every $\pi \in \varepsilon_n^m$ is a ring homomorphism, the assertion follows (note that we have to consider at most $p^{N_0} \cdot \ldots \cdot p^{N_m}$ terms of the power series f). □

Proposition 4.18 will be used in the proofs of the following two results.

Lemma 4.19 (Babaĭcev)**.** *Let $f \in \Lambda_{n+1}$. For every integer $c \geq 0$, the set $V^m(f;c) \ = \ \{\pi \in \varepsilon_n^m \mid v_p(\pi(f)) \geq c\}$ is closed.*

Proof. This is Proposition 1.1 in [Ba 82]. We will show that $\varepsilon_n^m \setminus V^m(f;c)$ is open. Let $\pi_0 \in \varepsilon_n^m$ be such that $v_p(\pi_0(f)) < c$. Then there exists a term $a_{k_0,\ldots,k_m} \cdot T_0^{k_0} \cdot \ldots \cdot T_m^{k_m}$ of $\pi_0(f) \in \mathbb{Z}_p[[T_0,\ldots,T_m]]$ such that

$$v_p(a_{k_0,\ldots,k_m} \cdot T_0^{k_0} \cdot \ldots \cdot T_m^{k_m}) \;<\; c\;.$$

We will use the notation introduced in Proposition 4.18. Choosing a neighbourhood $U = U((2N_{i,j})_{i,j})(\pi_0)$ such that $p^{N_j} > k_j$, $0 \le j \le m$, and such that $N \ge c$, Proposition 4.18 shows that $\pi(f) \;\equiv\; \pi_0(f) \mod (p^c, T_0^{k_0+1}, \ldots, T_m^{k_m+1})$, and therefore $v_p(\pi(f)) < c$, for every $\pi \in U$. □

We will now consider the special case $m = n-1$.

Lemma 4.20 (Babaĭcev)**.** *If $f \in \Lambda_{n+1}$ satisfies $p \nmid f$, then there exist only finitely many elements $\pi \in \varepsilon_n^{n-1}$ such that $p \mid \pi(f)$, i.e., the set $V^{n-1}(f;1)$ is finite.*

Proof. This is Proposition 1.2 in [Ba 82]. Since ε_n^{n-1} is compact (see Section 2.1), and since the set $V^{n-1}(f;1)$ is closed by Lemma 4.19, it suffices to prove that this set is discrete in ε_n^{n-1}.

Let $\pi_0 \in V^{n-1}(f;1)$ be an arbitrary element. We may choose topological generators of Γ^{n+1} such that $\pi_0(X_n) = 0$ (using the same arguments as in the proof of Remark 4.8). Furthermore, we may choose generators $\delta_0,\ldots,\delta_m$ of $\Gamma^{m+1} = \Gamma^n$ such that

$$\pi_0(X_i) \;=\; T_i\;, \quad 0 \le i \le n-1\;.$$

Note that this choice of variables does not affect the property $v_p(\pi_0(f)) > 0$.

Writing $f \in \Lambda_{n+1}$ as $f = a_0(X_0,\ldots,X_{n-1}) + \sum_{i=k}^{\infty} a_i(X_0,\ldots,X_{n-1}) \cdot X_n^i$ for some $k > 0$, we obtain $\pi_0(f) = a_0(T_0,\ldots,T_{n-1})$. Since $p \mid \pi_0(f)$, we have $p \mid a_0(X_0,\ldots,X_{n-1})$. Now $p \nmid f$, by assumption, and therefore we can write

$$f \;=\; g \;+\; \sum_{i=k'}^{\infty} a_i(X_0,\ldots,X_{n-1}) \cdot X_n^i\;,$$

with $k' > 0$, $p \mid g \in \Lambda_{n+1}$ and $p \nmid a_{k'}(X_0,\ldots,X_{n-1})$. The last property implies that there exists a tuple $(b_0,\ldots,b_{n-1})$ of non-negative integers such that p does not divide the coefficient c of $X_0^{b_0} \cdot \ldots \cdot X_{n-1}^{b_{n-1}}$ in $a_{k'}(X_0,\ldots,X_{n-1})$.

Let $M \in \mathbb{N}$ be a power of p that is larger than the maximum of the b_i. Using Proposition 4.18, we may choose a neighbourhood $U = U((2N_{i,j})_{i,j})(\pi_0)$ such that

$$\begin{aligned} \pi(a_{k'}(X_0,\ldots,X_{n-1})) \;&\equiv\; \pi_0(a_{k'}(X_0,\ldots,X_{n-1})) \\ &=\; a_{k'}(T_0,\ldots,T_{n-1}) \qquad \mod (p, T_0^M,\ldots,T_{n-1}^M) \end{aligned}$$

for every $\pi \in U$. In particular, $p \nmid \pi(a_{k'}(X_0,\ldots,X_{n-1}))$ for these π, since by definition of M, the coefficient of $T_0^{b_0} \cdot \ldots \cdot T_{n-1}^{b_{n-1}}$ in $\pi(a_{k'}(X_0,\ldots,X_{n-1}))$ will be congruent to c modulo p.

Let $\pi \in U$ be fixed. Then there exists a power series $h \in \mathbb{Z}_p[[T_0, \ldots, T_{n-1}]]$ such that

$$\pi(a_{k'}(X_0, \ldots, X_{n-1})) \equiv a_{k'}(T_0, \ldots, T_{n-1}) + T_0^M \cdot h \mod (p, T_1^M, \ldots, T_{n-1}^M) .$$

Now we note that $p \nmid \pi(X_n)$, since $\pi_0(X_n) = 0$ by our choice of topological generators. Indeed,

$$\begin{aligned} \pi(X_n) &= \underbrace{(\pi_0(X_n) + 1)}_{=1} \cdot \prod_{j=0}^{n-1} (T_j + 1)^{p^{2N_{n,j}} \cdot u_{n,j}} - 1 \\ &\equiv \sum_{\emptyset \neq S \subseteq \{0,\ldots,n-1\}} \prod_{j \in S} T_j^{p^{2N_{n,j}} \cdot u_{n,j}} \mod p , \end{aligned}$$

for suitable elements $u_{n,j} \in \mathbb{Z}_p$, $0 \leq j \leq n-1$. Therefore $\pi(X_n) \not\equiv 0 \mod p$, because $p \nmid \prod_{j=0}^{n-1} T_j^{p^{2N_{n,j}} \cdot u_{n,j}}$ in Λ_n.

Since $p \mid g$, and as π is a ring homomorphism, we may conclude that

$$\begin{aligned} \pi(f) &\equiv \underbrace{\pi(X_n)^{k'} \cdot a_{k'}(T_0, \ldots, T_{n-1})}_{\not\equiv 0 \mod p} + \pi(X_n)^{k'} \cdot T_0^M \cdot h \\ &\quad + \sum_{i=k'+1}^{\infty} \pi(a_i(X_0, \ldots, X_{n-1})) \cdot \pi(X_n)^i \mod (p, T_1^M, \ldots, T_{n-1}^M) \\ &\equiv T_0^{k' \cdot p^{2N_{n,0}} \cdot u_{n,0}} \cdot a_{k'}(T_0, \ldots, T_{n-1}) + T_0^{k' \cdot p^{2N_{n,0}} \cdot u_{n,0}} \cdot T_0^M \cdot h \\ &\quad + \sum_{i=k'+1}^{\infty} \pi(a_i(X_0, \ldots, X_{n-1})) \cdot T_0^{i \cdot p^{2N_{n,0}} \cdot u_{n,0}} \mod (p, T_1^M, \ldots, T_{n-1}^M) \\ &= T_0^{k' \cdot p^{2N_{n,0}} \cdot u_{n,0}} \cdot F \mod (p, T_1^M, \ldots, T_{n-1}^M) , \end{aligned}$$

where

$$F := a_{k'}(T_0, \ldots, T_{n-1}) + T_0^M h + \sum_{i=k'+1}^{\infty} \pi(a_i(X_0, \ldots, X_{n-1})) T_0^{(i-k') \cdot p^{2N_{n,0}} \cdot u_{n,0}} .$$

Now $a_{k'}(T_0, \ldots, T_{n-1})$ contains the term $c \cdot T_0^{b_0} \cdot \ldots \cdot T_{n-1}^{b_{n-1}} \not\equiv 0 \mod p$. Since $p^{N_{n,0}} \geq M > b_0$, the coefficient of $T_0^{b_0} \cdot \ldots \cdot T_{n-1}^{b_{n-1}}$ in F in fact equals c, proving that $p \nmid F$ and thus $p \nmid \pi(f)$. Since $\pi \in U$ was arbitrary, this shows that $V^{n-1}(f; 1)$ is discrete in ε_n^{n-1}.

□

Corollary 4.21 (Babaĭcev)**.** *Let $f \in \Lambda_{n+1}$. For every $c \geq 0$, the set $V^{n-1}(f; c)$ is either finite or equal to ε_n^{n-1}.*

Proof. If $p^c \mid f$, then $p^c \mid \pi(f)$ for every $\pi \in \varepsilon_n^{n-1}$, i.e., $V^{n-1}(f; c) = \varepsilon_n^{n-1}$. If $p^c \nmid f$, then we denote by p^i the maximal power of p dividing f, and we define $g := \frac{f}{p^i}$. Then $V^{n-1}(f; c) = V^{n-1}(g; c - i) \subseteq V^{n-1}(g; 1)$ is finite by Lemma 4.20. □

We will now interrupt the study of μ-invariants for a short remark that will be used in the next section for the investigation of λ-invariants.

Definition 4.22. Let $f \in \Lambda = \mathbb{Z}_p[[T]]$ denote an element such that $p \nmid f$. Then the ***reduced degree*** $\deg_p(f)$ of f is the smallest value $k \in \mathbb{N}_0$ such that p does not divide the coefficient of T^k in f (compare Lemma 1.10).

Lemma 4.23. *Let $n \in \mathbb{N}$, let $f \in \Lambda_{n+1}$ be such that $p \nmid f$. If $\pi_0 \in \varepsilon_n^0$ satisfies $p \mid \pi_0(f)$, and if $C \in \mathbb{N}$ is arbitrary, there exists a neighbourhood $U = U_C$ of π_0 such that $\deg_p(\pi(f)) > C$ for every $\pi_0 \neq \pi \in U$. This means that the reduced degree $\deg_p(\pi(f))$ is* **unbounded** *around π_0.*

Proof. Suppose first that $n = 1$, i.e., $f \in \Lambda_2$ and $\pi_0 \in \varepsilon_1^0$. Analogously to the proof of Lemma 4.20, we may choose a basis $\{\gamma_0, \gamma_1\}$ of Γ^2 such that $\pi_0(\gamma_0) = 1$, whereas $\pi_0(\gamma_1) = \delta$ generates Γ, i.e., $\pi_0(X_0) = 0$ and $\pi_0(X_1) = T$. Then the assumption that

$$f(0,T) \;=\; \pi_0(f) \;\equiv\; 0 \mod p$$

is equivalent to the fact that f is contained in the ideal $(p, X_0) \subseteq \Lambda_2$.

We will consider the neighbourhood $U = U((2N_{i,0})_{0 \leq i \leq 1})$ of π_0 with $N_{1,0} = 0$ and $N_{0,0} = M$, where M denotes an integer that has been chosen large enough to ensure that $p^M > C$ and such that $p \nmid \pi(f)$ for every $\pi_0 \neq \pi \in U$ (compare Lemma 4.20). Then $\deg_p(\pi(f))$ is defined for every $\pi_0 \neq \pi \in U$.

Moreover, $\pi(f) \equiv 0 \mod (p, T^{p^M})$ for every $\pi \in U$, since $f \in (p, X_0)$. In particular, $\deg_p(\pi(f)) \geq p^M > C$ for every $\pi_0 \neq \pi \in U$.

Let now $n \in \mathbb{N}$ be arbitrary, let $f \in \Lambda_{n+1}$ and $\pi_0 \in \varepsilon_n^0$ be as in the assertion. By choosing appropriate topological generators of Γ^{n+1}, respectively, Γ, we may assume that $\pi_0 : \Lambda_{n+1} = \mathbb{Z}_p[[X_0, \ldots, X_n]] \longrightarrow \mathbb{Z}_p[[T]]$ satisfies $\pi_0(X_0) = \ldots = \pi_0(X_{n-1}) = 0$ and $\pi_0(X_n) = T$.

The fact that

$$f(0, \ldots, 0, T) \;=\; \pi_0(f) \;\equiv\; 0 \mod p$$

implies that f is contained in the ideal $(p, X_0, \ldots, X_{n-1}) \subseteq \Lambda_{n+1}$. If

$$\overline{f} \;:=\; f \mod p$$

denotes the reduction of f modulo p, i.e., $\overline{f} \in \overline{\Lambda}_{n+1} := \Lambda_{n+1}/p\Lambda_{n+1}$, then $\overline{f} \neq \overline{0}$, because $p \nmid f$ by assumption. Lemma 4.7 implies that we can alter the basis $\gamma_0, \ldots, \gamma_n$ of Γ^{n+1} in order to obtain a set of generators $\tilde{\gamma}_0, \ldots, \tilde{\gamma}_n$ such that with respect to the corresponding variables

$$\tilde{X}_0, \ldots, \tilde{X}_{n-2}, \tilde{X}_{n-1} \;=\; X_{n-1}, \tilde{X}_n$$

(compare Lemma 4.7), we have

$$\overline{f}(0, \ldots, 0, \tilde{X}_{n-1}, 0) \;\neq\; 0\,,$$

i.e., $f \not\equiv 0 \mod (p, \tilde{X}_0, \ldots, \tilde{X}_{n-2}, \tilde{X}_n)$ and in particular

$$f \;\not\equiv\; 0 \mod (p, \tilde{X}_0, \ldots, \tilde{X}_{n-2})\,.$$

Note that this admissible change of variables does not affect the property that $\pi_0(\tilde{X}_0) = \ldots = \pi_0(\tilde{X}_{n-1}) = 0$ and $\pi_0(\tilde{X}_n) = T$, since $\gamma_{n-1} \in \ker(\pi_0)$. We will therefore call these new variables $X_0, \ldots, X_n$ again.

Consider now the epimorphism $\tilde{\pi} \in \varepsilon_n^1$ defined by $\tilde{\pi} : \Gamma^{n+1} \longrightarrow \Gamma^2$,

$$\tilde{\pi}(\gamma_0) \;=\; \ldots \;=\; \tilde{\pi}(\gamma_{n-2}) \;=\; 1\,,\;\; \tilde{\pi}(\gamma_{n-1}) \;=\; \delta_0 \;\text{ and }\; \tilde{\pi}(\gamma_n) \;=\; \delta_1\,,$$

where $\{\delta_0, \delta_1\}$ forms a basis of Γ^2. Writing $T_0 = \delta_0 - 1$ and $T_1 = \delta_1 - 1$, this means that

$$\tilde{\pi}(X_0) \;=\; \ldots \;=\; \tilde{\pi}(X_{n-2}) \;=\; 0\,,\;\; \tilde{\pi}(X_{n-1}) \;=\; T_0 \;\text{ and }\; \tilde{\pi}(X_n) \;=\; T_1\,.$$

If $\pi_1 \in \varepsilon_1^0$ is defined by $\pi_1(\delta_0) = 1$ and $\pi_1(\delta_1) = \delta$, i.e., $\pi_1(T_0) = 0$ and $\pi_1(T_1) = T$, then

$$\pi_0 \;=\; \pi_1 \circ \tilde{\pi}\,.$$

Now the fact that $f \not\equiv 0 \mod (p, X_0, \ldots, X_{n-2})$ implies that

$$\Lambda_2 \ni g := \tilde{\pi}(f) \;=\; f(0, \ldots, 0, T_1, T_2) \not\equiv 0 \mod p\,,$$

whereas $\pi_1(g) = \pi_0(f) \equiv 0 \bmod p$, by assumption. Let $C \in \mathbb{N}$ be given. Then the proof of the above special case yields a neighbourhood $U_1 \subseteq \varepsilon_1^0$ of π_1 such that for every $\pi_1 \neq \tilde{\pi}_1 \in U_1$, the reduced degree of $\tilde{\pi}_1(g)$ is defined and $\deg_p(\tilde{\pi}_1(g)) > C$. We consider the neighbourhood $U = U((2N_{i,0})_{0 \leq i \leq n})$ of π_0 with $N_{i,0} = p^M$ if $i = n-1$, and $N_{i,0} = 0$ otherwise, where M is large enough to ensure that U consists of homomorphisms $\pi = \tilde{\pi}_1 \circ \tilde{\pi}$ with $\tilde{\pi}_1 \in U_1$. Then

$$\deg_p(\pi(f)) \;=\; \deg_p(\tilde{\pi}_1(g)) \;>\; C$$

for every $\pi_0 \neq \pi \in U$. □

Now we return to the study of μ-invariants. In [Ba 81], Babaĭcev used the above Lemmas 4.19 and 4.20, together with a geometric study of the projective varieties ε_n^m, $m \leq n-1$, for the proof of the following result.

Theorem 4.24 (Babaĭcev)**.** *Let $0 \neq f \in \Lambda_{n+1}$. Then*

$$\sup\{v_p(\pi(f)) \mid \pi \in \varepsilon_n^m,\, \pi(f) \neq 0\} \;<\; \infty\,.$$

Proof. This is Theorem 2.1 in [Ba 81]. □

We will now prove a module-theoretic version of Theorem 4.24 which then may be applied to Iwasawa theory.

Let M denote a finitely generated torsion Λ_{n+1}-module. For every homomorphism $\pi \in \varepsilon_n^0$,

$$\pi : \Lambda_{n+1} \longrightarrow \Lambda_1 \;=\; \Lambda\,,$$

the quotient $M_\pi := M/(\ker(\pi) \cdot M)$ is a finitely generated Λ-module, as in the preceding sections.

Define $V(M) := \{\pi \in \varepsilon_n^0 \mid \operatorname{rank}_\Lambda(M_\pi) > 0\}$. For every $\pi \in \varepsilon_n^0 \setminus V(M)$, M_π is a torsion Λ-module, and therefore its Iwasawa invariant $\mu(M_\pi)$ is defined.

Theorem 4.25 (Babaĭcev)**.** *For every finitely generated torsion Λ_{n+1}-module M, we have*

$$\sup\{\mu(M_\pi) \mid \pi \in \varepsilon_n^0 \setminus V(M)\} \ < \ \infty \, .$$

Proof. Consider a presentation of the finitely generated Λ_{n+1}-module M by generators and relations:

$$M = \left\langle \, b_1, \ldots, b_l \ \mid \ \sum_{j=1}^{l} a_{ij} b_j = 0 \, , \quad 1 \le i \le q \, \right\rangle ,$$

with suitable elements $a_{ij} \in \Lambda_{n+1}$. Since M is Λ_{n+1}-torsion, we have $q \ge l$. Let $A = (a_{ij})$, $1 \le i \le q$, $1 \le j \le l$.

Lemma 4.26. *For every $\pi \in \varepsilon_n^0 \setminus V(M)$, $\mu(M_\pi)$ is equal to the exponent of the largest power of p dividing every minor of order l of the matrix $\pi(A)$.*

Proof. This is Lemma 1.2 in [Ba 82]. We first note that

$$M_\pi \ = \ M/(\ker(\pi) \cdot M) \ = \ \left\langle \, \overline{b}_1, \ldots, \overline{b}_l \ \mid \ \sum_{j=1}^{l} \pi(a_{ij}) \overline{b}_j = \overline{0} \, , \quad 1 \le i \le q \, \right\rangle \, .$$

Indeed, it is obvious that M_π is generated by the cosets of $b_1, \ldots, b_l$. Moreover, suppose that we have a relation

$$\overline{0} \ = \ \sum_{j=1}^{l} d_j \cdot \overline{b}_j$$

with given elements $d_j \in \Lambda$, $1 \le j \le l$. Since π is surjective, we may choose pre-images $c_j \in \Lambda_d$ of d_j, respectively. Then

$$\sum_{j=1}^{l} c_j b_j \in \ker(\pi) \cdot M \, .$$

Thus $\sum c_j b_j = \sum \lambda_j b_j$ for suitable $\lambda_j \in \ker(\pi) \subseteq \Lambda_d$. But then

$$\sum_{j=1}^{l} (c_j - \lambda_j) \cdot b_j \ = \ 0 \, ,$$

i.e., this relation is an appropriate linear combination of the equations

$$\sum_{j} a_{ij} \cdot b_j \ = \ 0 \, , \quad 1 \le i \le q \, ,$$

and therefore the relation $\sum\limits_{j=1}^{l} d_j \cdot \overline{b}_j = \overline{0}$ in M_π is a linear combination of relations

$$\sum_{j=1}^{l} \pi(a_{ij}) \cdot \overline{b}_j \ = \ \overline{0} \, ,$$

because $\pi(c_j - \lambda_j) = \pi(c_j) = d_j$, respectively.

Now we consider the localisation $\Lambda_{(p)}$ of Λ at p, which is a discrete valuation ring with maximal ideal (p). Since M_π is a finitely generated torsion Λ-module, there exists an exact sequence

$$0 \longrightarrow M_1 \longrightarrow M_\pi \longrightarrow E := \bigoplus_{i=1}^{s} \Lambda/(p^{n_i}) \oplus \bigoplus_{j=1}^{t} \Lambda/(f_j(T)^{l_j}) \longrightarrow M_2 \longrightarrow 0$$

of Λ-modules, with M_1 and M_2 finite, which we now localise. The localised sequence remains exact, since $N_{(p)} \cong N \otimes_\Lambda \Lambda_{(p)}$ for every Λ-module N, and because $\Lambda_{(p)}$ is a flat Λ-module (see [Ei 95], Lemma 2.4 and Proposition 2.5; the notion of flatness has been introduced in the proof of Theorem 4.13). There exists a power of T that annihilates the finite Λ-modules M_1 and M_2 (compare Remark 3.49). But $T \in \Lambda_{(p)}$ is a unit, so that we may conclude that

$$(M_1)_{(p)} \;\cong\; \Lambda_{(p)} \otimes_\Lambda M_1 \;=\; \{0\} \quad \text{and} \quad (M_2)_{(p)} \;\cong\; \Lambda_{(p)} \otimes M_2 \;=\; \{0\}\,.$$

This shows that we have an isomorphism

$$(M_\pi)_{(p)} \;\cong\; \bigoplus_{i=1}^{l} \Lambda_{(p)}/(g_i)\,,$$

with $g_i = p^{n_i}$, respectively, $g_i = f_i(T)^{l_i}$. Therefore $\mu(M_\pi) = \sum_i v_p(g_i)$ is equal to the sum of the exponents of p dividing the elementary divisors g_i of the module $(M_\pi)_{(p)}$.

Now we use the following general fact (see, for example, Theorem 2.9.6 in [Bo 03]).

Lemma 4.27. *Let N denote a finitely generated torsion module over a principal ideal domain R, with matrix of relations B. Then for every $m \leq \operatorname{rank}(B)$, the product of the first m elementary divisors of N is equal to the greatest common divisor of the minors of order m of B.*

Using this with $R = \Lambda_{(p)}$, $N = (M_\pi)_{(p)}$, $m = l$, and with B corresponding to the matrix over $\Lambda_{(p)}$ defined by the entries of $\pi(A)$ proves Lemma 4.26.

□

Lemma 4.26 implies that $\mu(M_\pi) \geq c$ if and only if every minor of order l of the matrix $\pi(A)$ is divisible by p^c. Let $f_1, \ldots, f_N$ denote the minors of order l of the matrix A. Thus, $\mu(M_\pi) \geq c$ if and only if $v_p(\pi(f_j)) \geq c$ for every $j = 1, \ldots, N$. Moreover, if $\pi \notin V(M)$, then M_π is a torsion Λ-module, and therefore at least one of the f_j is non-zero, by Lemma 4.2, (i). Theorem 4.24 implies that

$$\min_{1 \leq j \leq N} v_p(\pi(f_j))$$

is bounded on $\varepsilon_n^0 \setminus V(M)$, yielding an upper bound for $\mu(M_\pi)$. □

Now we will apply the above results to the set $\mathcal{E}(K)$ of $\mathbb{Z}_p$-extensions of a fixed number field K, proving Babaĭcevs main theorem. As we have seen in Lemma 2.7, we have an isomorphism $\mathcal{E}(K) \cong \varepsilon_{d-1}^0$. Using this isomorphism, we identify $\mathcal{E}(K)$ and ε_{d-1}^0, making $\mathcal{E}(K)$ into a projective variety.

Theorem 4.28 (Babaĭcev)**.** *Let K be a number field. Then the invariant μ is bounded on $\mathcal{E}(K)$.*

Proof. This is Theorem 3.1 in [Ba 81]. If M denotes a $\mathbb{Z}_p^i$-extension of K, $i \leq d$, then we denote by $\mathcal{E}^{\subseteq M}(K)$ the set of $\mathbb{Z}_p$-extensions of K contained in M. We will prove that μ is bounded on every set $\mathcal{E}^{\subseteq M}(K)$, using induction on i. The statement is true in the case of a single $\mathbb{Z}_p$-extension of K ($i = 1$), and we assume that there exists an integer $n \in \mathbb{N}$, $n \geq 2$, such that μ is bounded on $\mathcal{E}^{\subseteq M}(K)$ for every $\mathbb{Z}_p^i$-extension M of K with $i < n$.

Let $\mathbb{K}/K$ denote an arbitrary $\mathbb{Z}_p^n$-extension, and let $X := \mathrm{Gal}(H(\mathbb{K})/\mathbb{K})$ be the Galois group of the maximal unramified p-abelian extension of $\mathbb{K}$. Then X is a finitely generated torsion Λ_n-module (see Theorem 1 in [Gr 73] or Proposition 3.1 in [Ba 81]). Let $L \in \mathcal{E}^{\subseteq \mathbb{K}}(K)$.

We first assume that only finitely many primes of L ramify in $\mathbb{K}/L$. Let $\pi \in \varepsilon_{n-1}^0$ correspond to L via Lemma 2.7. Then Lemma 4.3, (ii) shows that $\pi \notin V(X)$ and $\mu(L/K) = \mu(X_\pi)$. Theorem 4.25 implies that $\mu(X_\pi) \leq c_0$ for every $\pi \in \varepsilon_{n-1}^0 \setminus V(X)$ and some $c_0 \in \mathbb{N}$. It therefore remains to look at those $\mathbb{Z}_p$-extensions $L \in \mathcal{E}^{\subseteq \mathbb{K}}(K)$ such that at least one prime $\tilde{\mathfrak{p}}$ of L ramifying in $\mathbb{K}$ splits completely in L/K.

Let $\tilde{\mathcal{P}} := \{\tilde{\mathfrak{p}}_1, \ldots, \tilde{\mathfrak{p}}_s\}$ denote the set of primes of L that ramify in $\mathbb{K}$. For each $\tilde{\mathfrak{p}}_j \in \tilde{\mathcal{P}}$, we let $\mathfrak{p}_j$ denote the unique prime of K divisible by $\tilde{\mathfrak{p}}_j$, respectively. If $\mathrm{Z}_{\mathfrak{p}_j} \subseteq \mathrm{Gal}(\mathbb{K}/K) \cong \mathbb{Z}_p^n$ denotes the decomposition group of $\mathfrak{p}_j$ in $\mathbb{K}/K$, respectively, then $\mathfrak{p}_j$ is split in L if and only if $L \subseteq \mathbb{K}^{\mathrm{Z}_{\mathfrak{p}_j}}$. Moreover, $\mathrm{Gal}(\mathbb{K}^{\mathrm{Z}_{\mathfrak{p}_j}}/K) \cong \mathbb{Z}_p^{n_j}$ for some $n_j < n$, since $\tilde{\mathfrak{p}}_j$ ramifies in $\mathbb{K}/L$ and therefore $\mathfrak{p}_j$ cannot be totally split in $\mathbb{K}/K$. Therefore the induction hypothesis implies that $\mu(L/K) \leq c_j$ for every $\mathbb{Z}_p$-extension $L \subseteq \mathbb{K}^{\mathrm{Z}_{\mathfrak{p}_j}}$ and some constant $c_j \in \mathbb{N}$, respectively. Letting $M := \max(\{c_0, c_1, \ldots, c_s\})$, we may conclude that $\mu(L/K) \leq M$ for every $\mathbb{Z}_p$-extension $L \in \mathcal{E}^{\subseteq \mathbb{K}}(K)$. □

4.3 Boundedness of λ-invariants

In the last section, we studied μ-invariants of $\mathbb{Z}_p$-extensions L/K of a fixed number field K, and we discussed in detail Babaĭcev's proof that μ is globally bounded on $\mathcal{E}(K)$. It is unknown whether the λ-invariants of the $\mathbb{Z}_p$-extensions $L \in \mathcal{E}(K)$ are bounded in general. In the current section, we will develop a sufficient criterion for the existence of a sequence $(M^{(n)})_n \subseteq \mathcal{E}(K)$ having unbounded λ-invariants. This will make use of the results obtained in the last sections.

In [Mo 81], P. Monsky proved some results in the case $d = 2$ (i.e., he considered $\mathbb{Z}_p$-extensions L of K contained in some fixed $\mathbb{Z}_p^2$-extension $\mathbb{K}/K$). Monsky obtained a criterion that is related to ours (compare Proposition 4.40 below). In order to briefly describe Monsky's result, we have to introduce some notation.

Let $\mathbb{K}/K$ be a fixed $\mathbb{Z}_p^d$-extension, $d \in \mathbb{N}$, let $X := \mathrm{Gal}(H(\mathbb{K})/\mathbb{K})$, where $H(\mathbb{K})$ denotes the maximal p-abelian unramified extension of $\mathbb{K}$. Then X is a

finitely generated torsion Λ_d-module, where

$$\Lambda_d \;=\; \mathbb{Z}_p[[X_1,\ldots,X_d]] \;\cong\; \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{K}/K)]]$$

(compare Proposition 3.1 in [Ba 81]). By the Structure Theorem 2.23, X is pseudo-isomorphic to an elementary torsion module $\bigoplus_{i=1}^{s} \Lambda_d/\mathfrak{p}_i^{n_i}$, where $s \in \mathbb{N}_0$, $n_i \in \mathbb{N}$ for $i = 1,\ldots,s$, and with suitable principal prime ideals $\mathfrak{p}_i = (g_i) \subseteq \Lambda_d$ (compare Remarks 2.25, (1)). Then $f := \prod_{i=1}^{s} g_i^{n_i} \in \Lambda_d$ is called the ***characteristic power series*** of X.

There are different possible descriptions of f. For example, the Λ_d-module X can be described via generators and relations, as in the proof of Theorem 4.25:

$$X \;=\; \Big\langle\, b_1,\ldots,b_l \;\mid\; \sum_{j=1}^{l} a_{ij}b_j = 0\,,\quad 1 \le i \le q\,,\; a_{ij} \in \Lambda_d \,\Big\rangle\;.$$

Since X is Λ_d-torsion, $q \ge l$. Let $A = (a_{ij})$, $1 \le i \le q$, $1 \le j \le l$. If $f_1,\ldots,f_r$ denote the minors of the matrix A of order l, then one can show that the characteristic power series f of X is (up to multiplication by a unit) equal to the greatest common divisor of the f_i (compare the proof of Lemma 4.26).

Definition 4.29.
(1) We will also call $f \in \Lambda_d$ the ***characteristic power series*** of the $\mathbb{Z}_p^d$-extension $\mathbb{K}/K$. It is unique up to multiplication by a unit.
(2) The ideal $\mathfrak{F}(X)$ generated by the minors $f_1,\ldots,f_r$ is called the (zeroth) ***Fitting ideal*** of X.

Remarks 4.30.
(i) $\mathfrak{F}(X)$ does not depend on the chosen representation of X (see Corollary 20.4 in [Ei 95]).
(ii) We may write $\mathfrak{F}(X) = (f)\cdot J$, where the ideal $J \subseteq \Lambda_d$ is not contained in any non-trivial principal ideal (i.e., ideal of height one) of Λ_d.
(iii) If X can be generated over Λ_d by l elements, then

$$\mathrm{Ann}(X)^l \;\subseteq\; \mathfrak{F}(X) \;\subseteq\; \mathrm{Ann}(X)\;,$$

where $\mathrm{Ann}(X) \subseteq \Lambda_d$ denotes the annihilator ideal of X (compare Proposition 20.7 in [Ei 95]). In particular, $\mathfrak{F}(X) \neq (0)$, since X is Λ_d-torsion.
(iv) If $d = 1$, then the Weierstraß Preparation Theorem 1.14 implies that the characteristic power series $f \in \Lambda_1$ of X may be written as $f = U \cdot p^m \cdot \tilde{f}$, where $U \in \Lambda^*$ is a unit, $m = \mu(X) \in \mathbb{N}_0$, and where $\tilde{f} \in \mathbb{Z}_p[X]$ is a distinguished polynomial. Actually $\tilde{f} = F_X$ is the characteristic polynomial of X introduced in Definition 1.29.

Definition 4.31. Let $d \in \mathbb{N}$ and $0 \neq f \in \Lambda_d \cong \mathbb{Z}_p[[\Gamma^d]]$, with $\Gamma^d \cong \mathbb{Z}_p^d$. Write $f = p^\mu \cdot g$ with $p \nmid g$. Then $m_0(f) := \mu$.
Let further $\overline{g}$ denote the reduction of g modulo p, i.e., $\overline{g} \in \overline{\Lambda}_d := \Lambda_d/p\Lambda_d$. Then we define $l_0(f) := \sum v_{\mathcal{P}}(\overline{g})$, where the sum is taken over all prime ideals of

$\overline{\Lambda}_d$ of the form $\mathcal{P} = (\overline{\gamma - 1})$, with $\gamma \in \Gamma^d \setminus (\Gamma^d)^p$. Here $v_\mathcal{P}$ denotes the $\mathcal{P}$-adic valuation, respectively. Note that the sum $\sum v_\mathcal{P}(\overline{g})$ is always finite, because $\overline{\Lambda}_d$ is a unique factorisation domain.

Let $\mathcal{E}^{\subseteq \mathbb{K}}(K)$ be the set of $\mathbb{Z}_p$-extensions L/K such that $L \subseteq \mathbb{K}$. Monsky proved the following criterion for the global boundedness of λ-invariants (in the case of $d = 2$):

Theorem 4.32 (Monsky)**.** *Let $\mathbb{K}/K$ denote a $\mathbb{Z}_p^2$-extension with characteristic power series $f \in \Lambda_2$. Then the λ-invariants $\lambda(L/K)$, $L \in \mathcal{E}^{\subseteq \mathbb{K}}(K)$, are bounded if and only if $l_0(f) = 0$.*

Proof. See Theorem IV in [Mo 81]. □

We will prove the following result:

Theorem 4.33. *Let $d \in \mathbb{N}$, let $\mathbb{K}/K$ be a $\mathbb{Z}_p^d$-extension, $X = \mathrm{Gal}(H(\mathbb{K})/\mathbb{K})$, and let $f \in \Lambda_d$ denote the characteristic power series of $\mathbb{K}/K$.*
We write $f = p^{m_0} \cdot g$, with $p \nmid g$.

(i) λ is unbounded on the set $\mathcal{E}^{\subseteq \mathbb{K}}(K)$ if there exists a $\mathbb{Z}_p$-extension $M \subseteq \mathbb{K}$ of K such that only finitely many primes of M ramify in $\mathbb{K}$ and such that $p \mid \pi_M(g)$, where π_M corresponds to M via Lemma 2.7.

(ii) λ is bounded on $\mathcal{E}^{\subseteq \mathbb{K}}(K)$ if for every $\pi \in \varepsilon_{d-1}^0$, the quotient module $X_\pi = X/(\ker(\pi) \cdot X)$ is $\Lambda_\pi = \Lambda_d/(\ker \pi)$-torsion and satisfies $\mu(X_\pi) = m_0$.

(iii) If $d = 2$, then λ is unbounded if and only if $p \mid \pi(g)$ for some $\pi \in \varepsilon_{d-1}^0$.

Before starting with the proof, we state a fact which will be useful several times.

Proposition 4.34.

(i) Suppose that $\pi \in \varepsilon_{d-1}^0 \setminus V(X)$, let $f \in \Lambda_d$. Then $m_0(\pi(f)) \leq \mu(X_\pi)$.

(ii) If $\pi(f) = p^x \cdot h$ with $x \in \mathbb{N}_0$ and $p \nmid h$, then $\deg_p(h) \leq \lambda(X_\pi)$.

Proof. (i) We will use the notation from the proofs of Theorem 4.25 and Lemma 4.26 (with $M = X$). If $f_1, \ldots, f_r \in \Lambda_d$ denote the minors of order l of the matrix A, then $f = \mathrm{ggT}(f_1, \ldots, f_r)$ and therefore

$$\begin{aligned} m_0(\pi(f)) &= m_0(\pi(\mathrm{ggT}(f_1, \ldots, f_r))) \\ &\leq m_0(\mathrm{ggT}(\pi(f_1), \ldots, \pi(f_r))) \overset{4.26}{=} \mu(X_\pi)\,, \end{aligned}$$

since $\pi(\mathrm{ggT}(f_1, \ldots, f_r))$ divides $\mathrm{ggT}(\pi(f_1), \ldots, \pi(f_r))$, because π is a homomorphism.

(ii) Suppose first that $\mu(X_\pi) = 0$. Analogously to (i), we have

$$\deg_p(\pi(f)) \leq \deg_p(\mathrm{ggT}(\pi(f_1), \ldots, \pi(f_r))) = \lambda(X_\pi)\,,$$

where the last equality may be proved similarly to Lemma 4.26 by considering modules over localisations $\Lambda/(g_i)$ for the irreducible divisors of the characteristic polynomial of the Λ-module X_π.
In the general case, we extract suitable powers of p and concentrate on the remaining distinguished polynomials in $\Lambda_\pi = \Lambda_d/(\ker(\pi))$.

□

We now start with the proof of Theorem 4.33.

Proof. (i) We assume that for some $\pi \in \varepsilon_{d-1}^0$, we have $p \mid \pi(g)$ (note that this includes the possibility that $\pi(f) = 0$). Then Lemma 4.23 implies that for any given integer $C \in \mathbb{N}$, we may choose a neighbourhood $U = U(C)$ of π such that for every $\pi \neq \tilde{\pi} \in U$, we have $p \nmid \tilde{\pi}(g)$ and $\deg_p(\tilde{\pi}(g)) > C$. Via Lemma 2.7, this yields a neighbourhood $\tilde{U}$ of the $\mathbb{Z}_p$-extension M of K corresponding to π.
Let $\mathcal{E}'(K)$ denote the set of $\mathbb{Z}_p$-extensions N of K such that only finitely many primes of N divide p (i.e., no prime of K dividing p is completely split in N). The set $\mathcal{E}'(K)$ is dense in $\mathcal{E}(K)$ (compare Remark 4.4).
We therefore may choose a sequence of $\mathbb{Z}_p$-extensions $M^{(n)} \in \mathcal{E}'(K) \cap \tilde{U}$ such that for the corresponding homomorphisms π_n of $M^{(n)}$, we have $\deg_p(\pi_n(g)) \geq n$, respectively. Moreover, we may assume that

$$[(M^{(n)} \cap M) : K] \ \geq \ p^n$$

for every n.
For $M^{(n)} \in \mathcal{E}'(K)$, the module X_{π_n} is a torsion $\Lambda_{M^{(n)}}$-module, by Lemma 4.3. Proposition 4.34, (ii) therefore implies that $\lambda(X_{\pi_n}) \geq n$ for each n. Now

$$\lambda(X_{\pi_n}) \ \leq \ \lambda(M^{(n)}/K) + \frac{(d-1)(d-2)}{2} + j(\mathbb{K}/M^{(n)}) \, ,$$

where $j(\mathbb{K}/M^{(n)})$ denotes the sum of the $\mathbb{Z}_p$-ranks of the inertia subgroups of $\mathrm{Gal}(H(\mathbb{K})^{\mathrm{ab}^{(n)}}/M^{(n)})$, by Lemma 4.3, (ii). Here $H(\mathbb{K})^{\mathrm{ab}^{(n)}}$ denotes the maximal subextension of $H(\mathbb{K})$ that is abelian over $M^{(n)}$, respectively.
For every $n \in \mathbb{N}_0$, we let M_n denote the intermediate field of M/K that has degree p^n over K. Let s_n denote the number of primes of M_n that are divisible by some prime of M ramifying in $\mathbb{K}/M$. Since only finitely many primes of M are ramified in $\mathbb{K}/M$, by assumption, we may conclude that there exists an integer $m \in \mathbb{N}$ such that $s_n = s_m$ for every $n \geq m$. We assume that $m \geq e(M/K) + 1$. Let t_m denote the number of primes of M_m that are ramified in M_{m+1}.
By construction, $M^{(n)} \cap M \supseteq M_n$ for every $n \in \mathbb{N}_0$. If $\mathfrak{p}$ denotes a prime of $M^{(n)}$ that ramifies in $\mathbb{K}/M^{(n)}$, and if $\underline{\mathfrak{p}} := \mathfrak{p} \cap M_n$, then either $\underline{\mathfrak{p}}$ ramifies in M/M_n, or $\underline{\mathfrak{p}}$ is divisible by some prime of M ramifying in $\mathbb{K}/M$. If $n > m$, then $\underline{\mathfrak{p}}$ is the unique prime of $M_n \subseteq M^{(n)}$ dividing the prime $\underline{\mathfrak{p}} \cap M_{n-1}$, respectively, and therefore $\underline{\mathfrak{p}}$ is the unique prime of M_n dividing $\mathfrak{p}$. This shows that the number of primes $\mathfrak{p}$ of $M^{(n)}$ ramifying in $\mathbb{K}/M^{(n)}$ is bounded by $C := s_m + t_m$ for every $n > m$.
Since $H(\mathbb{K})/\mathbb{K}$ is unramified, the $\mathbb{Z}_p$-rank of each inertia subgroup of $\mathrm{Gal}(H(\mathbb{K})^{\mathrm{ab}^{(n)}}/M^{(n)})$ is at most $d-1 = \mathrm{rank}_{\mathbb{Z}_p}(\mathrm{Gal}(\mathbb{K}/M^{(n)})$. Therefore we have proved the bound

$$j(\mathbb{K}/M^{(n)}) \leq C \cdot (d-1) \, ,$$

which holds for every $n \geq m$.
This implies that the $\lambda(M^{(n)}/K)$ are unbounded.

(ii) Now we assume that for every $\pi \in \varepsilon_{d-1}^0$, X_π is a torsion Λ_π-module satisfying $\mu(X_\pi) = m_0$. Let π be arbitrary, let $M \in \mathcal{E}^{\subseteq \mathbb{K}}(K)$ correspond to π. Let $\mathfrak{F}(X)$ denote the Fitting ideal of X (compare Definition 4.29, (2)). We write $\mathfrak{F}(X) = (f) \cdot J$, as in Remarks 4.30, (2).

Lemma 4.35. $\pi(\mathfrak{F}(X)) = \mathfrak{F}(X_\pi)$.

Proof. Let r denote the number of generators of the Λ_d-module X. By definition, $\mathfrak{F}(X)$ is the ideal generated by the $r \times r$-minors of the matrix A describing the presentation of X. Since $\pi(A)$ describes a presentation of the Λ-module $X_\pi = X/(\ker \pi \cdot X)$ (compare the proof of Lemma 4.26), we see that $\mathfrak{F}(X_\pi) = \pi(\mathfrak{F}(X))$. □

Since $\mu(X_\pi) = m_0$ by assumption, Lemma 4.35 implies that there exists an element $h = f \cdot j \in \mathfrak{F}(X)$ such that $\pi(h) \not\equiv 0 \bmod p^{m_0+1}$. More precisely, if $h = p^{m_0} \cdot \tilde{h}$ with $\tilde{h} = g \cdot j$, then $\pi(\tilde{h}) \not\equiv 0 \mod p$. This means that we can choose a neighbourhood U_π of π such that for every $\tilde{\pi} \in U_\pi$, we have $\tilde{\pi}(\tilde{h}) \not\equiv 0 \bmod p$ and moreover $\deg_p(\tilde{\pi}(\tilde{h})) = \deg_p(\pi(\tilde{h}))$ (compare Proposition 4.18).
Let $C_\pi := \deg_p(\pi(\tilde{h})) < \infty$. Since $\tilde{\pi}(h) \in \mathfrak{F}(X_{\tilde{\pi}})$, we have

$$\lambda(X_{\tilde{\pi}}) \;\leq\; C_\pi < \infty$$

for every $\tilde{\pi} \in U_\pi$. Since ε_{d-1}^0 is compact and therefore can be covered by finitely many neighbourhoods U_π, we may conclude that there exists a constant $C < \infty$ such that $\lambda(X_\pi) \leq C$ for every $\pi \in \varepsilon_{d-1}^0$.
If $M \in \mathcal{E}^{\subseteq \mathbb{K}}(K)$ corresponds to $\pi \in \varepsilon_{d-1}^0$, then Lemma 4.3, (ii) implies that

$$\lambda(M/K) \;\leq\; \lambda(X_\pi) + d - 1$$

(note that this inequality holds for every $M \in \mathcal{E}^{\subseteq \mathbb{K}}(K) \cap \mathcal{E}(X)$, as we have seen in the proof of Lemma 4.3, (ii); moreover, we have $\mathcal{E}^{\subseteq \mathbb{K}}(K) = \mathcal{E}(X)$, by assumption). This shows that

$$\lambda(M/K) \;\leq\; C + d - 1$$

for every $M \in \mathcal{E}^{\subseteq \mathbb{K}}(K)$.

(iii) Finally, let us assume that $d = 2$. In this case, λ is unbounded whenever there exists some $\pi \in \varepsilon_{d-1}^0 = \varepsilon_1^0$ such that $p \mid \pi(g)$, i.e., we do not need to ensure that the corresponding $\mathbb{Z}_p$-extension M of K satisfies the additional condition from (i). Indeed, in the proof of (i), the condition that only finitely many primes of M ramify in $\mathbb{K}$ was only needed in order to bound the number of primes that could possibly ramify in $\mathbb{K}/M^{(n)}$, where $M^{(n)}$ runs through a sequence of $\mathbb{Z}_p$-extensions of K contained in a suitable neighbourhood $\mathcal{E}'(K) \cap \tilde{U}$ of M.
In [Mo 81], Monsky proved that in the case $d = 2$, there exists actually a global constant C such that for every $N \in \mathcal{E}'(K) \cap \mathcal{E}^{\subseteq \mathbb{K}}(K)$, the number of primes ramifying in $\mathbb{K}/N$ is smaller than or equal to C. Namely, let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ denote the primes of K that ramify in $\mathbb{K}$ and that are divisible

by only finitely many primes of $\mathbb{K}$, respectively. Let c_i denote this finite number, $1 \leq i \leq r$, and let $C := \sum_{i=1}^{r} c_i$.
Let now $N \in \mathcal{E}'(K) \cap \mathcal{E}^{\subseteq \mathbb{K}}(K)$ be arbitrary. If $\mathfrak{p}$ denotes a prime of N ramifying in $\mathbb{K}$, then only finitely many primes of $\mathbb{K}$ divide $\mathfrak{p}$, since $\mathrm{Gal}(\mathbb{K}/N) \cong \mathbb{Z}_p$. Moreover, $\mathfrak{p}$ is only finitely decomposed in N/K, because $N \in \mathcal{E}'(K)$. Therefore $\mathfrak{p} \cap K \in \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$, proving that the number of primes ramifying in $\mathbb{K}/N$ is bounded by C.
In the notation from (i), this means that $j(\mathbb{K}/M^{(n)}) \leq C \cdot (d-1)$ for every $n \in \mathbb{N}_0$. Therefore λ is unbounded if $p \mid \pi(g)$ for any $\pi \in \varepsilon_1^0$.
It remains to show that λ is bounded on $\mathcal{E}^{\subseteq \mathbb{K}}(K)$ if $p \nmid \pi(g)$ for every $\pi \in \varepsilon_1^0$.
Let $\mathfrak{F}(X) = (f) \cdot J$ be the Fitting ideal of X. Fix some $\pi \in \varepsilon_1^0$. We will use the following fact.

Lemma 4.36. *There exists an element $H \in \Lambda_2$ such that $\pi(H) \not\equiv 0 \bmod p$ and $p^s \cdot H \in J$ for some $s \in \mathbb{N}_0$.*

Proof. The proof follows an idea of Monsky (compare the proof of Theorem 3.3 in [Mo 81]). We consider the ideal

$$J^* := \{z \in \Lambda_2 \mid p^s \cdot z \in J \text{ for some } s \in \mathbb{N}_0\} .$$

Then multiplication by p is an injective operation on the quotient module Λ_2/J^*. We will now use the following terminology:

Definition 4.37. Let R denote a Noetherian ring, let M be a finitely generated R-module. Then a prime ideal $\mathfrak{p} \subseteq R$ is called ***associated*** to M if and only if $\mathfrak{p}$ is equal to the annihilator ideal of some element $x \in M$.

Lemma 4.38. *Let R denote a Noetherian ring, let $M \neq \{0\}$ be a finitely generated R-module.*

(i) Let $a \in R$. The map $m_a : M \longrightarrow M$, $m \mapsto a \cdot m$, is injective if and only if a is not contained in any associated prime ideal of M.

(ii) Assume that $\mathfrak{p}$ is a prime ideal of R that contains the annihilator ideal of M and is minimal concerning inclusion with this property. Then $\mathfrak{p}$ is associated to M.

Proof. (i) See [La 93], Chapter X, Proposition 2.9.
(ii) See [Ei 95], Theorem 3.1, a.

□

If we apply Lemma 4.38 to the finitely generated Λ_2-module Λ_2/J^*, then we may conclude that p is not contained in any prime ideal containing J^* and being minimal with this property.
Choose generators γ_1, γ_2, respectively, δ, of $\Gamma^2 = \mathrm{Gal}(\mathbb{K}/K)$, respectively, $\Gamma = \mathrm{Gal}(M/K)$ such that with respect to the corresponding variables $X_i = \gamma_i - 1$ and $T = \delta - 1$, we have $\pi(X_1) = 0$, whereas $\pi(X_2) = T$.

Lemma 4.39. *Fix $i \in \{1, 2\}$. There does not exist a prime ideal $\mathfrak{p}$ such that $J^* \subseteq \mathfrak{p} \subseteq (p, X_i)$. In particular, $J^* \not\subseteq (p, X_i)$.*

Proof. Assume that there exists a prime ideal $\mathfrak{p}$ such that $J^* \subseteq \mathfrak{p} \subseteq (p, X_i)$, and that $\mathfrak{p}$ is minimal with respect to inclusion. We will show that in this situation, $\mathfrak{p}$ will necessarily be equal to (p, X_i). But $p \notin \mathfrak{p}$, by the above, yielding a contradiction.
Since Λ_2 is a Noetherian ring (compare Proposition 2.17, (v)), a maximal descending chain of prime ideals

$$(p, X_i) =: \mathfrak{p}_r \supsetneq \mathfrak{p}_{r-1} \supsetneq \ldots \supsetneq \mathfrak{p}_0 = (0)$$

has length $r = 2$ (see Corollary 10.3 in [Ei 95]).
Since $J \subseteq J^*$ is not contained in any prime ideal of Λ_2 of height one, we may conclude that the minimal number of elements generating $\mathfrak{p} \supseteq J^*$ is at least two, i.e., $\mathfrak{p}$ is not principal.
Since $(0) \neq J \subseteq \mathfrak{p}$, there exists an element $0 \neq g \in \mathfrak{p}$. We may assume that g is irreducible, using the fact that $\mathfrak{p}$ is a prime ideal (g has a decomposition into irreducible elements in the unique factorisation domain Λ_2). But then the principal ideal (g) is prime, again using the fact that Λ_2 is a unique factorisation domain. Moreover, $(g) \neq \mathfrak{p}$, since $\mathfrak{p}$ is not principal. Therefore

$$(p, X_i) \supseteq \mathfrak{p} \supsetneq (g) \supsetneq (0)\,,$$

so that the above descending chain condition implies that we must have $(p, X_i) = \mathfrak{p}$, yielding the desired contradiction.

□

But this means that we may choose an element $H \in J^* \subseteq \Lambda_2$ such that $\pi(H) = H(0, T) \not\equiv 0 \bmod p$, proving Lemma 4.36. □

Now we may finish the proof of Theorem 4.33, (iii). We may simply copy the proof of the boundedness of λ for arbitrary d, given in (ii), replacing the element $\tilde{h}$ used there by $f \cdot H$. Indeed, $p \nmid \pi(f \cdot H)$, by assumption, and $0 \neq p^s \cdot \pi(f \cdot H) \in \mathfrak{F}(X_\pi)$ for some $s \in \mathbb{N}$, implying that each X_π is a torsion Λ_π-module, respectively (compare Lemma 4.2, (i)). Moreover, $\lambda(X_{\tilde{\pi}}) \leq \deg_p(f \cdot H)$ for every $\tilde{\pi}$ contained in a suitable neighbourhood of π, respectively, as in the proof of (ii).

□

If $d = 2$, then the conditions in our criterion (Theorem 4.33) and Monsky's Theorem 4.32 are equivalent, so that our theorem generalises Monsky's result to the case of arbitrary $d \geq 2$:

Proposition 4.40. *Let $2 \leq d \in \mathbb{N}$. Assume that $g \in \Lambda_d$ satisfies $p \nmid g$. If $l_0(g) \neq 0$, then there exists a homomorphism $\pi \in \varepsilon_{d-1}^0$ such that $p \mid \pi(g)$.*
If, on the other hand, there exists $\pi \in \varepsilon_{d-1}^0$ with $p \mid \pi(g)$, then we can choose generators $\gamma_1, \ldots, \gamma_d$ of Γ^d such that with respect to the corresponding variables $X_j = \gamma_j - 1$, $1 \leq j \leq d$, we have $g \equiv 0 \bmod (p, X_1, \ldots, X_{d-1})$. In particular, if $d = 2$, then $l_0(g) > 0$.

Proof. Assume that $l_0(g) \neq 0$. Then there exists an element $\gamma \in \Gamma^d \setminus (\Gamma^d)^p$ such that $\overline{g}$ is divisible by $\overline{\gamma - 1}$ in $\overline{\Lambda}_d$. Letting $X := \gamma - 1 \in \Lambda_d$, we may conclude

that $g \in (p, X)$. Since $\gamma \notin (\Gamma^d)^p$, we may extend γ to a basis $\{\gamma, \gamma_2, \ldots, \gamma_d\}$ of Γ^d. Now define $\pi : \Gamma^d \longrightarrow \Gamma$ by $\pi(\gamma_d) := \delta$ (a generator of Γ), $\pi(\gamma_i) = 1$ for every $i < d$. Let $T := \delta - 1$. Then $\pi(g) = g(0, \ldots, 0, T) \equiv 0 \bmod p$, by construction.

If, on the other hand, a homomorphism $\pi \in \varepsilon_{d-1}^0$ is given such that $p \mid \pi(g)$, then we choose generators $\gamma_1, \ldots, \gamma_d$ and δ of Γ^d and Γ, respectively, such that $\pi(\gamma_i) = 1$ for $i < d$ and $\pi(\gamma_d) = \delta$. Then $p \mid \pi(g) = g(0, \ldots, 0, T)$, and therefore $\overline{g}$ is contained in the ideal of $\overline{\Lambda}_d$ generated by the elements $\overline{\gamma_i - 1}$, $i = 1, \ldots, d-1$. □

It seems natural to conjecture that our condition that $\pi(g) \equiv 0 \bmod p$, i.e., $\pi(f) \equiv 0 \bmod p^{m_0(\mathbb{K}/K)+1}$, for some $\pi \in \varepsilon_{d-1}^0$ is tightly connected to the fact that $\mu(M/K) > m_0(\mathbb{K}/K)$ for some $M \in \mathcal{E}^{\subseteq \mathbb{K}}(K)$. We are able to make this precise for $d = 2$ if the Fitting ideal $\mathfrak{F}(X)$ of $X = \mathrm{Gal}(H(\mathbb{K})/\mathbb{K})$ satisfies the following technical condition.

Definition 4.41. Let $\mathbb{K}/K$ denote a $\mathbb{Z}_p^2$-extension, and let $X = \mathrm{Gal}(H(\mathbb{K})/\mathbb{K})$. We write the Fitting ideal of X in the form $\mathfrak{F}(X) = (f) \cdot J$, as in Remarks 4.30, (2).
We call $\mathbb{K}/K$ ***regular*** if there exist elements $g, h \in J$ such that the greatest common divisor $\overline{G}$ of their reductions $\overline{g}, \overline{h} \in \overline{\Lambda}_2 = \Lambda_2/p\Lambda_2$ is the reduction modulo p of a series $G \in \Lambda_2$ with $l_0(G) = 0$, and $\overline{G} \neq \overline{0}$.
Note that this is the case, for example, if there exists an element $h \in J$ such that $p \nmid h$ and $l_0(h) = 0$. This is equivalent to saying that for any choice of generators $\gamma_1, \gamma_2 \in \Gamma^2$, $h \in J$ is regular with respect to the variables $X_1 = \gamma_1 - 1$ *and* $X_2 = \gamma_2 - 1$ of Λ_2 in the sense of Definition 4.9 (compare Remarks 4.10, (3) and the proof of Proposition 4.40).

Remarks 4.42.

(1) Note that not every irreducible element of $\overline{\Lambda}_d$ is of the form $\overline{\gamma - 1}$ for some $\gamma \in \Gamma^d \setminus (\Gamma^d)^p$. Therefore an element $h \in J$ with $p \nmid h$ and $l_0(h) = 0$ will not have to be a unit.
Indeed, assume that $p \neq 2$, and let $X_1 = \gamma_1 - 1$ and $X_2 = \gamma_2 - 1$ for two multiplicatively independent elements $\gamma_1, \gamma_2 \in \Gamma^2 \setminus (\Gamma^2)^p$. We consider the element $X_1 + X_2 \in \Lambda_2$, and we will show that $l_0(X_1 + X_2) = 0$. Note that, on the contrary, $l_0(X_1 - X_2) > 0$, because

$$X_1 - X_2 \;=\; (X_2 + 1) \cdot ((X_1 + 1)(X_2 + 1)^\alpha - 1)\;,$$

where $\alpha \in \mathbb{Z}_p$ is chosen such that $\alpha + 1 = 0$.
By Proposition 4.40, $l_0(X_1 + X_2) > 0$ if and only if there exists a homomorphism $\pi \in \varepsilon_1^0$ such that $\pi(X_1 + X_2) \equiv 0 \bmod p$. We will show that such a homomorphism cannot exist (note that, on the contrary, $\pi(X_1 - X_2) = 0$ for $\pi : X_1 \mapsto T$, $X_2 \mapsto T$).
We know that

$$\pi(X_1) \;=\; (T+1)^{a_1} - 1\;, \quad \pi(X_2) \;=\; (T+1)^{a_2} - 1$$

for suitable $a_1, a_2 \in \mathbb{Z}_p$. Since $\pi : \mathbb{Z}_p[[X_1, X_2]] \longrightarrow \mathbb{Z}_p[[T]]$ is surjective, we may assume that $a_1 \not\equiv 0 \mod p$. Since π is a homomorphism, π maps $X_1 + X_2$ to

$$(T+1)^{a_1} - 1 + (T+1)^{a_2} - 1 \equiv a_1 T + 1 - 1 + a_2 T + 1 - 1 \mod (p, T^2),$$

using Lemma 2 of [Ba 76]. If $\pi(X_1+X_2) \equiv 0 \mod p$, then we may conclude that $a_1 + a_2 \equiv 0 \mod p$.
Now we consider the coefficient of T^2, obtaining

$$\left(\binom{a_1}{2} + \binom{a_2}{2}\right) \cdot T^2 = \left[\frac{a_1(a_1-1)}{2} + \frac{a_2(a_2-1)}{2}\right] \cdot T^2 .$$

Since $p \neq 2$, this term is congruent to zero modulo p if and only if

$$a_1(a_1-1) + a_2(a_2-1) \equiv 0 \mod p .$$

Inserting $a_2 \equiv -a_1 \mod p$, this yields

$$a_1^2 - a_1 + a_1^2 + a_1 \equiv 0 \mod p ,$$

i.e., $a_1 \equiv 0 \mod p$. But this contradicts our choice $a_1 \not\equiv 0 \mod p$.

(2) Since J is not contained in any prime ideal of Λ_d of height one, there do always exist two coprime elements $g, h \in J$. In fact, if $0 \neq g \in J$ is arbitrary, then there exists an element $h \in J$ coprime to g (compare Remarks 2.20, (3)).
Moreover, we may assume that $p \nmid g \cdot h$. Indeed, since $J \not\subseteq (p)$, we may choose some $g \in J$ such that $p \nmid g$. Then we choose an element $h \in J$ coprime to $p \cdot g \in J$.
However, it is well possible that $\overline{g}$ and $\overline{h}$ are not longer coprime. For example, if $g = X_1$ and $h = X_1 + pX_2$, then $\overline{g} = \overline{h}$.

(3) In order to motivate our definition of regularity, we consider the following example. Suppose that $J = (X_1 + p, X_1^2)$. Then $\mathbb{K}/K$ is not regular, since $\overline{X_1} = \overline{\gamma_1 - 1}$ divides every residue class $\overline{h}$, $h \in J$. We make the following observation. If $\pi \in \varepsilon_1^0$ satisfies $\pi(X_1) = 0$, then $\pi(J) \subseteq (p)$, and therefore

$$\mu(X_\pi) > m_0(\pi(f))$$

(compare the proof of Proposition 4.34). This is exactly the phenomenon we want to get rid of by our regularity constraint (see the proof of Theorem 4.43 below).

Theorem 4.43. *Let $\mathbb{K}/K$ denote a* regular $\mathbb{Z}_p^2$*-extension. If there exists some $M \in \mathcal{E}^{\subseteq \mathbb{K}}(K)$ such that $\mu(M/K) > m_0 := m_0(\mathbb{K}/K)$, then λ is unbounded on $\mathcal{E}^{\subseteq \mathbb{K}}(K)$.*

Proof. We will first prove a general result which shows that we may assume that for every $\pi \in \varepsilon_1^0$, the module $X_\pi = X/(\ker(\pi) \cdot X)$ is a torsion Λ_{M_π}-module, with $M_\pi \in \mathcal{E}^{\subseteq \mathbb{K}}(K)$ corresponding to π via Lemma 2.7.

Lemma 4.44. *Let $\mathbb{K}/K$ denote a $\mathbb{Z}_p^2$-extension with corresponding Greenberg-module $X = \mathrm{Gal}(H(\mathbb{K})/\mathbb{K})$. If there exists a homomorphism $\pi \in \varepsilon_1^0$, with corresponding field $M_\pi \in \mathcal{E}^{\subseteq\mathbb{K}}(K)$, such that $X_\pi = X/(\ker(\pi)\cdot X)$ is no torsion Λ_{M_π}-module, then λ is unbounded on $\mathcal{E}^{\subseteq\mathbb{K}}(K)$.*

Proof. Let $f \in \Lambda_d$ denote the characteristic power series of X. Write $f = p^{m_0}\cdot g$, $p \nmid g$, with $m_0 = m_0(\mathbb{K}/K)$. Let $\pi \in \varepsilon_1^0$ be such that X_π is no torsion Λ_{M_π}-module. Then $\pi(g) = 0$. Indeed, we may use Lemma 4.36 in order to find an element $H \in \Lambda_2$ such that $\pi(H) \not\equiv 0 \bmod p$ and such that $p^s \cdot f \cdot H \in \mathfrak{F}(X)$ for some $s \in \mathbb{N}_0$. But then

$$p^s \cdot \pi(f) \cdot \pi(H) \;=\; p^{s+m_0} \cdot \pi(g) \cdot \pi(H) \;\in \mathfrak{F}(X_\pi)\;,$$

and this element is different from zero if $\pi(g) \neq 0$. Lemma 4.2, (i) then would imply that X_π was Λ_{M_π}-torsion.

We therefore assume that $\pi(g) = 0$. Then Lemma 4.23 implies that for every $C \in \mathbb{N}$ we may find a neighbourhood U_C of π such that $\tilde{\pi}(g) \not\equiv 0 \bmod p$ and $\deg_p(\tilde{\pi})(g) > C$ for every $\pi \neq \tilde{\pi} \in U_C$.

Let $\mathcal{E}'(K)$ denote the set of $\mathbb{Z}_p$-extensions of K in which no prime dividing p splits into infinitely many primes. We have shown in Lemma 4.3, (i) that the module $X_{\pi_{\tilde{M}}}$ is $\Lambda_{\tilde{M}}$-torsion for every homomorphism $\pi_{\tilde{M}} \in \varepsilon_1^0$ corresponding to some $\tilde{M} \in \mathcal{E}'(K)$. $\mathcal{E}'(K)$ is dense in $\mathcal{E}^{\subseteq\mathbb{K}}(K)$, see Remark 4.4. Moreover, there exists a constant $C_1 \in \mathbb{N}$ such that for every $\tilde{M} \in \mathcal{E}'(K)$ and corresponding $\pi_{\tilde{M}}$, we have

$$\lambda(X_{\pi_{\tilde{M}}}) \;\leq\; \lambda(\tilde{M}/K) + C_1$$

(compare the proof of Theorem 4.33, (iii)).

Now assume that λ is bounded on $\mathcal{E}^{\subseteq\mathbb{K}}(K)$, i.e., let $X \in \mathbb{N}$ be such that $\lambda(N/K) \leq X$ for every $N \in \mathcal{E}^{\subseteq\mathbb{K}}(K)$. Let $C := X + C_1$. Choose some $\tilde{M} \in \mathcal{E}'(K) \cap U_C$. The corresponding homomorphism $\tilde{\pi} \in \varepsilon_1^0$ then satisfies $\tilde{\pi}(g) \not\equiv 0 \bmod p$ and $\deg_p(\tilde{\pi}(g)) > X + C_1$. Since $\deg_p(\tilde{\pi}(g)) \leq \lambda(X_{\tilde{\pi}})$ (compare Proposition 4.34, (ii)), it follows that

$$\lambda(\tilde{M}/K) \;\geq\; \lambda(X_{\tilde{\pi}}) - C_1 \;>\; X\;,$$

yielding a contradiction. □

Now we return to the proof of Theorem 4.43. Let $\pi \in \varepsilon_1^0$ correspond to the element $M \in \mathcal{E}^{\subseteq\mathbb{K}}(K)$ with $\mu(M/K) > m_0$. In view of Lemma 4.44, we may assume that X_π is a torsion Λ_M-module. Then

$$\mu(X_\pi) \;\geq\; \mu(M/K) \;>\; m_0\;,$$

by Corollary 4.5.

We have seen in Proposition 4.34, (i) that $m_0(\pi(f)) \leq \mu(X_\pi)$ whenever $\pi \in \mathcal{E}(X)$. We will prove now that the assumed regularity of $\mathbb{K}/K$ implies that we actually have $m_0(\pi(f)) = \mu(X_\pi)$ for every π (compare Remarks 4.42, (3)):

Proof. Suppose first that there exists $h \in J$ such that $p \nmid h$ and $l_0(h) = 0$. Then $\pi(h) \not\equiv 0 \bmod p$ for every $\pi \in \varepsilon_1^0$, by Proposition 4.40. But $\pi(f) \cdot \pi(h) \in \mathfrak{F}(X_\pi)$ for each π, implying that

$$\mu(X_\pi) \;\leq\; m_0(\pi(f)) + m_0(\pi(h)) \;=\; m_0(\pi(f)) \;.$$

Let now $g, h \in J$ denote two elements such that the greatest common divisor $\overline{G}$ of their reductions $\overline{g}$ and $\overline{h}$ modulo p is not divisible by any irreducible element of the form $\overline{\gamma - 1}$, $\gamma \in \Gamma^2 \setminus (\Gamma^2)^p$.

We may assume that $p \nmid g \cdot h$ (otherwise our condition on $\overline{G}$ implies that $l_0(g) = 0$ or $l_0(h) = 0$, and we are done because of the special case discussed above).

If $\pi \in \varepsilon_1^0$ satisfies $m_0(\pi(f)) < \mu(X_\pi)$, then $\pi(H) \equiv 0 \bmod p$ for every $H \in J$. In particular, $\pi(g) \equiv 0 \bmod p$ and $\pi(h) \equiv 0 \bmod p$. If γ_1, γ_2 denote topological generators of Γ^2 such that $\pi(\gamma_1) = 1$ and such that $\pi(\gamma_2) = \delta$ generates the image $\Gamma = \pi(\Gamma^2)$, then this means that the reductions $\overline{g}$ and $\overline{h}$ of g and h are divisible by $\overline{\gamma_1 - 1}$ in $\overline{\Lambda_d}$ (compare the proof of Proposition 4.40). But then $\overline{\gamma_1 - 1}$ divides the greatest common divisor $\overline{G}$ of $\overline{g}$ and $\overline{h}$, in contradiction to our regularity constraints.

This shows that for every $\pi \in \varepsilon_1^0$, we have either $\pi(g) \not\equiv 0 \bmod p$ or $\pi(h) \not\equiv 0 \bmod p$, proving that $m_0(\pi(f)) = \mu(X_\pi)$. □

But this implies that for the homomorphism $\pi \in \varepsilon_1^0$ corresponding to our fixed $M \in \mathcal{E}^{\subseteq \mathbb{K}}(K)$, we have $m_0(\pi(f)) = \mu(X_\pi) > m_0$, i.e., $f = p^{m_0} \cdot g$ and $p \mid \pi(g)$. Therefore Theorem 4.33, (iii) implies that λ is unbounded on $\mathcal{E}^{\subseteq \mathbb{K}}(K)$. □

Definition 4.45. Let $d \in \mathbb{N}$, let $f \in \Lambda_d = \mathbb{Z}_p[[\Gamma^d]]$, $f \neq 0$. We write $f = p^{m_0} \cdot g$, with $p \nmid g$. Then we define $\delta_0(f)$ to be the number of pairwise coprime irreducible elements $\overline{\gamma - 1}$, $\gamma \in \Gamma^d \setminus (\Gamma^d)^p$ dividing $\overline{g}$ in $\overline{\Lambda}_d = \Lambda_d / p\Lambda_d$. In particular, $\delta_0(f) = 0$ if and only if $l_0(f) = 0$.

Corollary 4.46. *Let $\mathbb{K}/K$ denote a $\mathbb{Z}_p^2$-extension. Let $\mathfrak{F}(X) = (f) \cdot J$, let*

$$m \;:=\; \min(\{\delta_0(h) \mid h \in J,\, p \nmid h\}) \;.$$

If there exist at least $m + 1$ different $\mathbb{Z}_p$-extensions $M_1, \ldots, M_{m+1} \in \mathcal{E}^{\subseteq \mathbb{K}}(K)$ such that $\mu(M_i/K) > m_0(\mathbb{K}/K)$ for every $i \in \{1, \ldots, m+1\}$, then λ is unbounded on $\mathcal{E}^{\subseteq \mathbb{K}}(K)$.

Proof. First note that m is well-defined, since not every element of J can be divisible by p. Let $h \in J$, $p \nmid h$, be an element such that $\delta_0(h) = m$. For every $\pi \in \varepsilon_1^0$, we have $\pi(h) \equiv 0 \bmod p$ if and only if $\pi(\gamma_i) = 1$ for some $\gamma_i \in \Gamma^2 \setminus (\Gamma^2)^p$ satisfying $\overline{\gamma_i - 1} \mid \overline{h}$ (compare the proof of Proposition 4.40). This means that there exist exactly m homomorphisms $\pi_1, \ldots, \pi_m$ such that $\pi_j(h) \equiv 0 \bmod p$, because every $\pi \in \varepsilon_1^0$ is uniquely determined by its (rank one) kernel. Indeed, if the kernel of π is generated by $\gamma \in \Gamma^2 \setminus (\Gamma^2)^p$, then we extend γ to a basis $\{\gamma, \gamma_2\}$ of Γ^2, and π has to map γ_2 to a generator of Γ. Since we do not distinguish between the homomorphisms π and π^u, $u \in \mathbb{Z}_p^*$, in ε_1^0, γ uniquely determines π.

This means that $\pi(h) \not\equiv 0 \bmod p$ and therefore $m_0(\pi(f)) = \mu(X_\pi)$ for every π different from $\pi_1, \ldots, \pi_m$. Write $f = p^{m_0(\mathbb{K}/K)} \cdot g$. If there exist more than m $\mathbb{Z}_p$-extensions whose μ-invariant is greater than $m_0(\mathbb{K}/K)$, then there exists $\pi \in \varepsilon_1^0$ such that $p \mid \pi(g)$, and therefore λ is unbounded. □

Corollary 4.47. *Suppose that K is an abelian number field. Let $\mathbb{K}/K$ denote a $\mathbb{Z}_p^2$-extension containing the cyclotomic $\mathbb{Z}_p$-extension K_∞ of K. We write $\mathfrak{F}(X) = (f) \cdot J$. Let*

$$m := \min(\{\delta_0(h) \mid h \in J,\, p \nmid h\}) .$$

If there exist at least $m+1$ different $\mathbb{Z}_p$-extensions $M_1, \ldots, M_{m+1} \in \mathcal{E}^{\subseteq \mathbb{K}}(K)$ such that $\mu(M_i/K) > 0$ for every $i \in \{1, \ldots, m+1\}$, then λ is unbounded on $\mathcal{E}^{\subseteq \mathbb{K}}(K)$.

Proof. If K is an abelian extension of $\mathbb{Q}$ and if K_∞ denotes the cyclotomic $\mathbb{Z}_p$-extension of K, then it is known that $\mu(K_\infty/K) = 0$ (compare [FW 79]). Moreover, every prime of K dividing p ramifies in K_∞/K (compare Lemma 3.18, (ii)), and therefore $K_\infty \in \mathcal{E}'(K)$ and $\mu(X_\pi) = \mu(K_\infty/K)$ for the corresponding homomorphism $\pi \in \varepsilon_1^0$. Since $\mu(X_\pi) \geq m_0(\mathbb{K}/K)$ (see Proposition 4.34, (i)), it follows that $m_0(\mathbb{K}/K) = 0$. Now apply the previous corollary. □

Remarks 4.48.

(1) If $m = 0$ in Corollary 4.46, then we are in the special case of regularity mentioned in Definition 4.41, and therefore the statement of the corollary follows from Theorem 4.43.

(2) We already know that the existence of some

$$L \in \mathcal{E}^{\subseteq \mathbb{K}}(K) \cap \mathcal{E}'(K)$$

with $\mu(L/K) = 0$ implies that the $\mathbb{Z}_p$-extensions $M \subseteq \mathbb{K}$ of K satisfying $\mu(M/K) = 0$ are dense in $\mathcal{E}^{\subseteq \mathbb{K}}(K)$ (compare Theorem 4.15).
In the case of $d = 2$, there can exist only finitely many $\mathbb{Z}_p$-extensions $M_1, \ldots, M_r \subseteq \mathbb{K}$ of K such that $\mu(M_i/K) \neq m_0(\mathbb{K}/K)$ (compare Theorem 5 in [Ba 76] and Lemma 5.10 below). In this notation, the Corollaries 4.46 and 4.47 show that $r \leq m$.

(3) The proof of Theorem 4.43 may be used in order to prove the following generalisation. Let $d \in \mathbb{N}$, $d \geq 2$.
Let $\mathbb{K}/K$ be a $\mathbb{Z}_p^d$-extension having a Fitting ideal $\mathfrak{F}(X) = (f) \cdot J$ such that J contains an element h with the following property: For every choice of topological generators of $\mathrm{Gal}(\mathbb{K}/K)$, h is regular with respect to each of the variables $X_i = \gamma_i - 1$ of Λ_d in the sense of Definition 4.9 (this generalises the special case of regularity mentioned in Definition 4.41). Let $M \in \mathcal{E}^{\subseteq \mathbb{K}}(K)$ be such that every prime of K that ramifies in $\mathbb{K}$ is also ramified in M. If $\mu(M/K) > m_0(\mathbb{K}/K)$, then λ is unbounded on $\mathcal{E}^{\subseteq \mathbb{K}}(K)$.
Indeed, the existence of h implies that

$$m_0(\pi(f)) \;=\; \mu(X_\pi) \;>\; m_0(\mathbb{K}/K)$$

for the homomorphism $\pi \in \varepsilon_{d-1}^0$ corresponding to M (compare Remarks 4.10, (3) and the proof of Proposition 4.40). Moreover, the ramification condition ensures that for some $C_1 \in \mathbb{N}$, we have

$$\lambda(X_{\pi_{\tilde{M}}}) \;\leq\; \lambda(\tilde{M}/K) + C_1$$

for each $\tilde{M}$ contained in a suitable neighbourhood $U(M,n)$ of M, for some $n \geq e(M/K)+1$ (compare the proof of Theorem 4.33).

Corollary 4.49. *Let K be an abelian number field, let $\mathbb{K}/K$ denote a regular $\mathbb{Z}_p^2$-extension containing the cyclotomic $\mathbb{Z}_p$-extension of K. Assume that K contains only one prime dividing p. Then λ is unbounded on $\mathcal{E}^{\subseteq\mathbb{K}}(K)$ if and only if there exists $M \in \mathcal{E}^{\subseteq\mathbb{K}}(K)$ such that $\mu(M/K) > 0$.*

Proof. If $\mu(M/K) > 0$ for some $M \in \mathcal{E}^{\subseteq\mathbb{K}}(K)$, then λ is unbounded by Theorem 4.43 (compare the proof of Corollary 4.47). If, on the other hand, $\mu(M/K) = 0$ for every $M \in \mathcal{E}^{\subseteq\mathbb{K}}(K)$, then λ is bounded by Corollary 3.60. Note that this has been reproved in Theorem 4.33, (iii), since $\mu(M/K) = \mu(X_\pi)$ for every M, because each M is ramified at the single prime $\mathfrak{p}$ of K dividing p (compare Corollary 4.5). □

Remark 4.50. Note that instead of assuming that K contains only one prime dividing p, it would be sufficient if every $M \in \mathcal{E}^{\subseteq\mathbb{K}}(K)$ had the same ramification set (compare Corollary 3.60).

Chapter 5

Local behaviour of generalised Iwasawa invariants

Let K denote a fixed number field. In Chapter 3, we studied the local behaviour of Iwasawa invariants on the set $\mathcal{E}(K)$ of $\mathbb{Z}_p$-extensions of K, with respect to suitable topologies. We will now, more generally, consider the sets of $\mathbb{Z}_p^d$-extensions $\mathcal{E}^d(K)$ of K, $d \in \mathbb{N}$. Note that $\mathcal{E}^d(K) = \emptyset$ if d is too large (compare Theorem 1.7).

In analogy with the theory developed in Chapter 3, we will study the local behaviour of so-called *generalised Iwasawa invariants*, which are natural analogues of Iwasawa's classical μ- and λ-invariants. In the first section, we will define the Greenberg- and Greenberg-R-topologies on the sets $\mathcal{E}^d(K)$. Then we start the investigation of local properties of generalised Iwasawa invariants, using a descent-ascent method and applying our one-dimensional results from Chapter 3.

In order to obtain stronger results, we will then work out a generalisation of our method to the higher-dimensional setting. In Section 5.4, we introduce a suitable concept of Fukuda modules and prove some basic properties. Section 5.5 is devoted to a study of ramification. As in the one-dimensional case, a good understanding of ramification is fundamental for our method. We will see that, although sufficient for the study of $\mathbb{Z}_p$-extensions, the Greenberg-R-topology has to be refined further in order to control the ramification in neighbourhoods of $\mathbb{Z}_p^d$-extensions.

In Section 5.6, we introduce a notion of ranks of Λ_d-modules generalising the f-ranks, $f \in \Lambda$, studied in Chapter 3. In comparison to the one-dimensional case, it is much more difficult to handle pseudo-isomorphisms of Λ_d-modules, because for $d > 1$ the kernels and cokernels of these maps in general will not be finite. In fact, we typically only know an upper bound for their Krull dimension, and therefore it is usually a difficult task to relate the ranks of two pseudo-isomorphic Λ_d-modules.

The main theorem is stated in Section 5.7. We have to make several technical assumptions in order to be able to apply our method. In particular, we have to presume the validity of a certain inequality concerning the ranks of cyclic torsion Λ_d-modules. Under these assumptions, we are able to prove a generalisation of

Theorem 3.57 (the main result of Chapter 3).

Section 5.8 is dedicated to a proof of a technical lemma that has been used in the proof of the main theorem. In Section 5.9, we prove the rank inequality needed for Section 5.7 in certain special cases.

Finally, Section 5.10 contains some results concerning the special case of a $\mathbb{Z}_p^2$-extension $\mathbb{K}/K$ of a number field K which contains only one prime above p. We will use the results of the preceding chapters in order to obtain a criterion for the Greenberg module of $\mathbb{K}/K$ to be pseudo-null.

5.1 Introduction

In generalisation of Iwasawa's Theorem 1.32, A. Cuoco and P. Monsky proved the following result (compare Theorem I in [CM 81]):

Theorem 5.1 (Cuoco, Monsky)**.** *Let $\mathbb{K}/K$ denote a $\mathbb{Z}_p^d$-extension, let further $\Gamma^d := \mathrm{Gal}(\mathbb{K}/K) \cong \mathbb{Z}_p^d$. For every $n \in \mathbb{N}_0$, we let $\mathbb{K}_n \subseteq \mathbb{K}$ denote the subfield that is fixed by $(\Gamma^d)^{p^n}$, and we let A_n denote the p-primary part of the ideal class group of $\mathbb{K}_n$, respectively.*
Then there exist integers $m_0, l_0 \in \mathbb{N}_0$ such that for every $n \in \mathbb{N}_0$, we have $|A_n| = p^{e_n}$ with

$$e_n \;=\; (m_0 p^n + l_0 n + \mathcal{O}(1)) p^{(d-1)n}\,.$$

We call m_0 and l_0 the **generalised Iwasawa invariants** *of $\mathbb{K}/K$.*

Remark 5.2. If $d = 1$, then this result gives a weak version of Theorem 1.32 (compare also Theorem 5.3 below); while Theorem 1.32 gives an explicit formula for the e_n (for n sufficiently large), Theorem 5.1 only includes an upper bound for the 'constant contribution'. Cuoco and Monsky conjectured that Theorem 5.1 in general cannot be improved in order to obtain an explicit polynomial

$$(m_0 p^n + l_0 n + n_0) \cdot p^{(d-1)n}$$

for some $n_0 \in \mathbb{Z}$, and they gave module-theoretic evidence for their conjecture (compare Section 7 in [CM 81]).

In [CM 81], Cuoco and Monsky also proved that m_0 and l_0 only depend on $\mathbb{K}/K$, in the following sense.

In Section 4.3, we introduced the notion of the *characteristic power series* $f \in \Lambda_d = \mathbb{Z}_p[[T_1, \ldots, T_d]]$ of a given $\mathbb{Z}_p^d$-extension $\mathbb{K}/K$ (compare Definition 4.29, (1)): If $H(\mathbb{K})$ denotes the maximal p-abelian unramified extension of $\mathbb{K}$, then one can show that $X := \mathrm{Gal}(H(\mathbb{K})/\mathbb{K})$ is a finitely generated torsion Λ_d-module, using the isomorphism $\Lambda_d \cong \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{K}/K)]]$. By the Structure Theorem 2.23, X is pseudo-isomorphic to an elementary torsion module $\bigoplus_{j=1}^{s} \Lambda_d/\mathfrak{p}_j^{n_j}$, with $\mathfrak{p}_j = (f_j)$ and $f_j \in \Lambda_d$ irreducible for every j. Then $f := \prod_{j=1}^{s} f_j^{n_j}$.

Moreover, f is equal to the greatest common divisor of the generators of the *Fitting ideal* $\mathfrak{F}(X)$ of X (compare Definition 4.29, (2)). We refer to Remarks 4.30 for some basic properties of $\mathfrak{F}(X)$.

In Definition 4.31, we defined integers $m_0(f)$ and $l_0(f)$ attached to the power series $0 \neq f \in \Lambda_d$.

Theorem 5.3 (Cuoco, Monsky)**.** *Let $\mathbb{K}/K$ denote a $\mathbb{Z}_p^d$-extension with generalised Iwasawa invariants m_0 and l_0. Then $m_0 = m_0(f)$ and $l_0 = l_0(f)$, where $f \in \Lambda_d$ denotes the characteristic power series of $\mathbb{K}/K$. In particular, if $d = 1$, then $m_0 = \mu$ and $l_0 = \lambda$ coincide with Iwasawa's classical invariants.*

Proof. Compare the proof of Theorem I in [CM 81]. □

We will now define two topologies on the sets $\mathcal{E}^d(K)$ of $\mathbb{Z}_p^d$-extensions of K, $d \in \mathbb{N}$.

Definition 5.4. Let $d \in \mathbb{N}$, and assume that the set $\mathcal{E}^d(K)$ is non-empty. Let $\mathbb{K} \in \mathcal{E}^d(K)$. For every $n \in \mathbb{N}_0$, we let

$$\mathcal{E}(\mathbb{K}, n) := \{\mathbb{L} \in \mathcal{E}^d(K) \mid \mathbb{L}_n = \mathbb{K}_n\} .$$

Here $\mathbb{L}_n$, respectively, $\mathbb{K}_n$, denote the subfield of $\mathbb{L}$ fixed by $\mathrm{Gal}(\mathbb{L}/K)^{p^n}$, respectively, the subfield of $\mathbb{K}$ fixed by $\mathrm{Gal}(\mathbb{K}/K)^{p^n}$.

Note that this generalises Greenberg's topology on $\mathcal{E}(K) = \mathcal{E}^1(K)$ (compare Section 2.3). We will therefore speak of the *Greenberg topology* on $\mathcal{E}^d(K)$.

Remark 5.5. *The sets $\mathcal{E}(\mathbb{K}, n)$, together with $\emptyset$, generate a topology on $\mathcal{E}^d(K)$ with regard to which $\mathcal{E}^d(K)$ is compact.*

Proof. It is easy to see that the intersection of two sets $\mathcal{E}(\mathbb{K}, n_1)$ and $\mathcal{E}(\tilde{\mathbb{K}}, n_2)$ is either empty or equal to one of the two sets. Therefore the $\mathcal{E}(\mathbb{K}, n)$, $n \in \mathbb{N}_0$, and $\emptyset$, can be taken as a basis of neighbourhoods of $\mathbb{K} \in \mathcal{E}^d(K)$, respectively. The compactness may be proved analogously to Greenberg's proof for $d = 1$ (compare [Gr 73], p. 208): For each m, let $\mathcal{E}_m$ denote the set of abelian extensions of K of degree p^{dm} which are the m-th intermediate field for some $\mathbb{K} \in \mathcal{E}^d(K)$ (i.e., equal to the subfield of $\mathbb{K}$ fixed by $\mathrm{Gal}(\mathbb{K}/K)^{p^m}$). Then every $\mathcal{E}_m$ is a finite set because each $L \in \mathcal{E}_m$ is the composite of d cyclic extensions of degree p^m over K contained in some $\mathbb{Z}_p$-extension of K, respectively; it is well-known that there exist only finitely many cyclic extensions of this shape. Moreover, $\mathcal{E}^d(K) \cong \varprojlim \mathcal{E}_m$, where the inverse limit is taken with respect to the following maps: if $m' \geq m$, then an element $L \in \mathcal{E}_{m'}$ is mapped to the unique subfield that is fixed by $\mathrm{Gal}(L/K)^{p^m}$ (which is an element of $\mathcal{E}_m$). Since every set $\mathcal{E}_m$ is finite and therefore a discrete compact topological space, it follows that $\mathcal{E}^d(K)$ is compact. □

Definition 5.6. Let $\mathbb{K}/K$ denote a $\mathbb{Z}_p^d$-extension, $d \in \mathbb{N}$.
Then we denote by $\mathcal{P}(\mathbb{K})$ the ***ramification set*** of $\mathbb{K}$, i.e., the set of primes of K that ramify in $\mathbb{K}/K$. Note that $\mathcal{P}(\mathbb{K})$ is a subset of the set $\mathcal{I}$ of primes of K dividing p.

The following lemma will be used below.

Lemma 5.7. *Let $\mathbb{K}/K$ denote a $\mathbb{Z}_p^d$-extension.*

(i) The set of $\mathbb{Z}_p$-extensions $L \subseteq \mathbb{K}$ of K satisfying $\mathcal{P}(L) = \mathcal{P}(\mathbb{K})$ is dense in $\mathcal{E}^{\subseteq\mathbb{K}}(K) \subseteq \mathcal{E}(K)$ with respect to Greenberg's topology.

(ii) More generally, for $i \leq d$, we denote by $\mathcal{E}^{i,\subseteq\mathbb{K}}(K)$ the set of $\mathbb{Z}_p^i$-extensions $\mathbb{L} \subseteq \mathbb{K}$ of K. Then the set of $\mathbb{Z}_p^i$-extensions $\mathbb{L} \subseteq \mathbb{K}$ of K satisfying $\mathcal{P}(\mathbb{L}) = \mathcal{P}(\mathbb{K})$ is dense in $\mathcal{E}^{i,\subseteq\mathbb{K}}(K) \subseteq \mathcal{E}^i(K)$ with respect to Greenberg's topology on $\mathcal{E}^i(K)$, as introduced in Definition 5.4.

Proof. (i) Write $\mathcal{P}(\mathbb{K}) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$. For every $\mathfrak{p}_i \in \mathcal{P}(\mathbb{K})$, there exists a $\mathbb{Z}_p$-extension $L_i \in \mathcal{E}^{\subseteq\mathbb{K}}(K)$ such that $\mathfrak{p}_i \in \mathcal{P}(L_i)$, because a prime $\mathfrak{p}_i$ that is unramified in every $L_i \in \mathcal{E}^{\subseteq\mathbb{K}}(K)$ will also be unramified in their composite $\mathbb{K}$. Therefore, we may choose suitable $L_1, \ldots, L_s \in \mathcal{E}^{\subseteq\mathbb{K}}(K)$ such that

$$\mathcal{P}(L_1) \cup \cdots \cup \mathcal{P}(L_s) \;=\; \mathcal{P}(\mathbb{K})\,.$$

Note that we have $\mathcal{P}(\tilde{L}) = \mathcal{P}(L_1) \cup \mathcal{P}(L_2)$ for almost every $\mathbb{Z}_p$-extension

$$\tilde{L} \;\subseteq\; L_1 \cdot L_2 \;\subseteq\; \mathbb{K}$$

of K (i.e., there exist only finitely many $\tilde{L}$ contained in this composite such that $\mathcal{P}(\tilde{L}) \subsetneqq \mathcal{P}(L_1) \cup \mathcal{P}(L_2)$), by Lemma 3.19, (ii). We choose an extension $\tilde{L} \in \mathcal{E}^{\subseteq\mathbb{K}}(K)$ with $\mathcal{P}(\tilde{L}) = \mathcal{P}(L_1) \cup \mathcal{P}(L_2)$ and continue with $\tilde{L}$ and L_3. Inductively, we obtain some $L \in \mathcal{E}^{\subseteq\mathbb{K}}(K)$ satisfying $\mathcal{P}(L) = \mathcal{P}(\mathbb{K})$.
Now let $M \in \mathcal{E}^{\subseteq\mathbb{K}}(K)$ be arbitrary. Then $\mathcal{P}(\tilde{L}) = \mathcal{P}(\mathbb{K})$ for almost every $\tilde{L} \subseteq L \cdot M$, again using Lemma 3.19, (ii). In particular, every neighbourhood U of M contains an element $\tilde{L}$ with the desired property.

(ii) Suppose that $\mathbb{L} \subseteq \mathbb{K}$ is a $\mathbb{Z}_p^i$-extension of K; let $L^1, \ldots, L^i$ denote $\mathbb{Z}_p$-extensions of K such that $\mathbb{L} = L^1 \cdot \ldots \cdot L^i$. We may assume that

$$L^k \cap \prod_{j \neq k} L^j \;=\; K$$

for every $k \in \{1, \ldots, i\}$.
Let $n \in \mathbb{N}_0$ be given. We will construct an element $\tilde{\mathbb{L}} \in \mathcal{E}(\mathbb{L}, n)$ such that $\mathcal{P}(\tilde{\mathbb{L}}) = \mathcal{P}(\mathbb{K})$.
If $\mathcal{P}(\mathbb{L}) \subsetneqq \mathcal{P}(\mathbb{K})$, then $\mathcal{P}(L^j) \subsetneqq \mathcal{P}(\mathbb{K})$ for every j. By (i), there exists a $\mathbb{Z}_p$-extension $\tilde{L}^1 \subseteq \mathbb{K}$ of K contained in $\mathcal{E}(L^1, n)$ such that $\mathcal{P}(\tilde{L}^1) = \mathcal{P}(\mathbb{K})$. We let $\tilde{\mathbb{L}} := \tilde{L}^1 \cdot L^2 \cdot \ldots \cdot L^i$. Then $\tilde{\mathbb{L}} \subseteq \mathbb{K}$ is a $\mathbb{Z}_p^i$-extension of K (note that $\tilde{L}^1 \cap \prod_{j \neq 1} L^j = K$, since the n-th intermediate field $(\tilde{L}^1)_n$ of $\tilde{L}^1/K$ is contained in L^1), and $\mathcal{P}(\tilde{\mathbb{L}}) = \mathcal{P}(\mathbb{K})$. Moreover, $\tilde{\mathbb{L}} \in \mathcal{E}(\mathbb{L}, n)$, because $(\tilde{L}^1)_n = (L^1)_n$ and therefore

$$\tilde{\mathbb{L}}_n \;=\; (\tilde{L}^1)_n \cdot (L^2)_n \cdot \ldots \cdot (L^i)_n \;=\; (L^1)_n \cdot \ldots \cdot (L^i)_n \;=\; \mathbb{L}_n\,.$$

□

In Chapter 3, we observed that the use of Fukuda's Theorem and its generalisations make it necessary to take care of the ramification of primes in the

corresponding $\mathbb{Z}_p$-extensions. We therefore introduced a new topology on $\mathcal{E}(K)$, which we called the *Greenberg-R-topology*, and which we want to define on arbitrary $\mathcal{E}^d(K)$ now.

Definition 5.8. Let $\mathbb{K}/K$ denote a $\mathbb{Z}_p^d$-extension, $d \in \mathbb{N}$. For every $n \in \mathbb{N}_0$, we define

$$U(\mathbb{K}, n) := \{\mathbb{L} \in \mathcal{E}(\mathbb{K}, n) \mid \mathcal{P}(\mathbb{L}) \subseteq \mathcal{P}(\mathbb{K})\} .$$

Remark 5.9. The $U(\mathbb{K}, n)$, together with $\emptyset$, generate a topology on $\mathcal{E}^d(K)$.

Proof. The intersection of two sets $U(\mathbb{K}, n_1)$ and $U(\tilde{\mathbb{K}}, n_2)$ is a finite union of sets of this type, or empty (compare the proof of Lemma 3.25, (i)):

Without loss of generality, we may assume that $n_1 \geq n_2$. Then

$$U(\mathbb{K}, n_1) \cap U(\tilde{\mathbb{K}}, n_2) = \{\mathbb{L} \in \mathcal{E}(\mathbb{K}, n_1) \mid \mathcal{P}(\mathbb{L}) \subseteq \mathcal{P}(\mathbb{K}) \cap \mathcal{P}(\tilde{\mathbb{K}})\} .$$

This set might be empty. Otherwise, we choose sets $I_1, \ldots, I_r \subseteq \mathcal{P}(\mathbb{K}) \cap \mathcal{P}(\tilde{\mathbb{K}})$ such that

- for every $i = 1, \ldots, r$, there exists an element $\mathbb{L}_i \in \mathcal{E}(\mathbb{K}, n_1)$ such that $\mathcal{P}(\mathbb{L}_i) = I_i$, and
- for every $\mathbb{M} \in \mathcal{E}(\mathbb{K}, n_1)$ with $\mathcal{P}(\mathbb{M}) \subseteq \mathcal{P}(\mathbb{K}) \cap \mathcal{P}(\tilde{\mathbb{K}})$, we have $\mathcal{P}(\mathbb{M}) \subseteq I_i$ for some $i \in \{1, \ldots, r\}$.

Then

$$U(\mathbb{K}, n_1) \cap U(\tilde{\mathbb{K}}, n_2) = \bigcup_{i=1}^{r} U(\mathbb{L}_i, n_1) .$$

□

We will see in Section 5.5 that, in contrast to the one-dimensional case, a full use of Fukuda theory for $\mathbb{Z}_p^d$-extensions requires a finer control on the ramification than is provided by the Greenberg-R-topology. In fact, it will not be enough to simply control which primes of K do ramify at all. We will moreover have to fix the rank of the maximal 'torsion' unramified subextension of our $\mathbb{Z}_p^d$-extension (compare Definition 5.38 for details).

The Greenberg-R-topology, however, is fine enough in order to allow the application of the one-dimensional Fukuda method developed in Chapter 3 to suitable $\mathbb{Z}_p$-extensions of K that are contained in our $\mathbb{Z}_p^d$-extensions. This will be exploited in the next two sections, yielding the first results concerning the local behaviour of generalised Iwasawa invariants.

5.2 m_0 is locally maximal

We will now start to study the local behaviour of generalised Iwasawa invariants with respect to the topologies introduced above. Before formulating the first result, we prove a technical lemma.

Lemma 5.10. *Let $d \in \mathbb{N}$, $d \geq 2$. Let $\mathbb{K}/K$ denote a $\mathbb{Z}_p^d$-extension, and let $m_0 := m_0(\mathbb{K}/K) \in \mathbb{N}_0$. Then there exist only finitely many $\mathbb{Z}_p^{d-1}$-extensions $M \subseteq \mathbb{K}$ of K such that*

$$m_0(M/K) > m_0 .$$

If $d = 2$, then there exist only finitely many $\mathbb{Z}_p$-extensions $M \subseteq \mathbb{K}$ of K such that $\mu(M/K) \neq m_0(\mathbb{K}/K)$.

Proof. We first note that there exist only finitely many $\mathbb{Z}_p^{d-1}$-extensions $M \subseteq \mathbb{K}$ of K such that $\mathcal{P}(M) \subsetneqq \mathcal{P}(\mathbb{K})$. Indeed, each such M has to be contained in the inertia subfield of a prime of K ramifying in $\mathbb{K}$ whose inertia group is a subgroup of $\mathrm{Gal}(\mathbb{K}/K)$ of $\mathbb{Z}_p$-rank 1.

Therefore, we will from now on assume that $\mathcal{P}(M) = \mathcal{P}(\mathbb{K})$.

Let $f \in \Lambda_d$ denote the characteristic power series of $\mathbb{K}/K$, and let us write $f = p^{m_0} \cdot g$, with $p \nmid g$. Consider the Fitting ideal $(0) \neq \mathfrak{F}(X) = (p^{m_0} g) \cdot J$ of $X := \mathrm{Gal}(H(\mathbb{K})/\mathbb{K})$, where $H(\mathbb{K})$ denotes the maximal unramified p-abelian extension of $\mathbb{K}$. Suppose that $0 \neq h \in J$ is not divisible by p (such an element exists because J is not contained in the prime ideal $(p) \subseteq \Lambda_d$ of height one).

By Lemma 4.20, the subset $C \subset \varepsilon_{d-1}^{d-2}$ of homomorphisms π such that either $\pi(g) \equiv 0 \bmod p$ or $\pi(h) \equiv 0 \bmod p$ is finite. For every $\pi \in \varepsilon_{d-1}^{d-2} \backslash C$, the module $X_\pi = X/(\ker(\pi) \cdot X)$ is a finitely generated torsion Λ_{d-1}-module (annihilated, for example, by $p^{m_0} \cdot \pi(g \cdot h) \neq 0$), and

$$p^{m_0} \cdot \pi(g \cdot h) \in \mathfrak{F}(X_\pi)$$

(compare Lemma 4.35). Therefore

$$m_0(X_\pi) = m_0 .$$

If $d = 2$, then Lemma 4.3, (ii) implies that $\mu(M/K) = m_0(X_\pi)$ for the $\mathbb{Z}_p$-extension M/K that corresponds to π, provided that $\mathcal{P}(M) = \mathcal{P}(\mathbb{K})$.

In order to handle the case $d > 2$, we generalise Lemma 4.3, (ii) and show that $m_0(M/K) \leq m_0(X_\pi)$ if M corresponds to some $\pi \in \varepsilon_{d-1}^{d-2} \setminus C$.

Proposition 5.11. *Let $j, r \in \mathbb{N}$, $2 \leq j \leq r-1$. Let $\mathbb{K}/K$ denote a $\mathbb{Z}_p^r$-extension, and let $M \in \mathcal{E}^{j,\subseteq\mathbb{K}}(K)$ denote a $\mathbb{Z}_p^j$-extension of K contained in $\mathbb{K}$. Let $X := \mathrm{Gal}(H(\mathbb{K})/\mathbb{K})$, and suppose that $\pi \in \varepsilon_{r-1}^{j-1}$ corresponds to the restriction map $\mathrm{Gal}(\mathbb{K}/K) \twoheadrightarrow \mathrm{Gal}(M/K)$. We assume that $X_\pi := X/(\ker(\pi) \cdot X)$ is a torsion Λ_j-module. Then*

$$m_0(M/K) \leq m_0(X_\pi) \quad \text{and} \quad l_0(M/K) \leq l_0(X_\pi) .$$

If only finitely many primes of M ramify in $\mathbb{K}$, then we have equalities.

Proof. We adapt the proof of Lemma 4.3, (ii). If $H(M)$ denotes the maximal unramified p-abelian extension of M, then $m_0(M/K) = m_0(\mathrm{Gal}(H(M)/M))$, by definition. The inclusion $H(M) \cdot \mathbb{K} \subseteq H(\mathbb{K})$ implies that we have a surjective homomorphism

$$X = \mathrm{Gal}(H(\mathbb{K})/\mathbb{K}) \longrightarrow\!\!\!\!\!\rightarrow \mathrm{Gal}((H(M) \cdot \mathbb{K})/\mathbb{K}) .$$

Note that $\ker \pi = \{\sigma - 1 \mid \sigma \in \mathrm{Gal}(\mathbb{K}/M)\}$. Since

$$(\sigma - 1) \cdot \tau = \tilde{\sigma} \circ \tau \circ \tilde{\sigma}^{-1} \circ \tau^{-1} = \tau \circ \tau^{-1} = 1$$

for every $\tau \in \mathrm{Gal}((H(M)\cdot\mathbb{K})/\mathbb{K})$ and every $\sigma \in \mathrm{Gal}(\mathbb{K}/M)$, it follows that $\ker(\pi)\cdot\mathrm{Gal}((H(M)\cdot\mathbb{K})/\mathbb{K}) = \{1\}$ (here $\tilde{\sigma} \in \mathrm{Gal}((H(M)\cdot\mathbb{K})/M)$ denotes any lift of σ, respectively). We therefore obtain a surjective $\mathbb{Z}_p[[\mathrm{Gal}(M/K)]] \cong \Lambda_j$-module homomorphism

$$X_\pi = X/(\ker(\pi)\cdot X) \longrightarrow\!\!\!\!\!\rightarrow \mathrm{Gal}((H(M)\cdot\mathbb{K})/\mathbb{K}) \cong \mathrm{Gal}(H(M)/(H(M)\cap\mathbb{K}))\ .$$

In particular,

$$m_0(\mathrm{Gal}(H(M)/(H(M)\cap\mathbb{K}))) \ \leq\ m_0(X_\pi)$$

and

$$l_0(\mathrm{Gal}(H(M)/(H(M)\cap\mathbb{K}))) \ \leq\ l_0(X_\pi)\ .$$

We will show that the Λ_j-module $\mathrm{Gal}(H(M)/(H(M)\cap\mathbb{K}))$ is pseudo-isomorphic to $\mathrm{Gal}(H(M)/M)$ and therefore

$$m_0(\mathrm{Gal}(H(M)/(H(M)\cap\mathbb{K}))) \ =\ m_0(M/K)$$

and

$$l_0(\mathrm{Gal}(H(M)/(H(M)\cap\mathbb{K}))) \ =\ l_0(M/K)\ .$$

The reason for this is the fact that

$$\mathrm{Gal}(H(M)/M)\,/\,\mathrm{Gal}(H(M)/(H(M)\cap\mathbb{K})) \ \cong\ \mathrm{Gal}((H(M)\cap\mathbb{K})/M)$$

is a finitely generated $\mathbb{Z}_p$-module and therefore is pseudo-null as a Λ_j-module. Indeed, we may assume that $Z := \mathrm{Gal}((H(M)\cap\mathbb{K})/M)$ is in fact $\mathbb{Z}_p$-free, because the torsion subgroup of Z is finite. We write $\Lambda_j = \mathbb{Z}_p[[T_1,\ldots,T_j]]$. Recall that $j \geq 2$, by assumption. There exist distinguished polynomials in $\mathbb{Z}_p[T_1]$ as well as in $\mathbb{Z}_p[T_2]$ that annihilate the finitely generated $\mathbb{Z}_p$-module Z, using the Weierstraß Preparation Theorem 1.14 and the assumption that Z is torsion-free. In particular, these two polynomials are coprime when regarded as elements of Λ_j, and therefore Z is Λ_j-pseudo-null.

Now suppose that only finitely many primes of M ramify in $\mathbb{K}$. Then the proof of the first inequality of Lemma 4.3, (ii) shows that

$$m_0(X_\pi) \ \leq\ m_0(M/K) \quad \text{and} \quad l_0(X_\pi) \ \leq\ l_0(M/K)\ .$$

Indeed, if the $\mathbb{Z}_p$-extension L of K in Greenberg's original approach is replaced by the $\mathbb{Z}_p^j$-extension M/K, then the proof goes through without changes. In particular, the two groups D and T remain finitely generated over $\mathbb{Z}_p$. By the above, D and T therefore are pseudo-null as Λ_j-modules. □

This also concludes the proof of Lemma 5.10. □

We are now ready to state the main result of this section.

Theorem 5.12. *Let $\mathbb{K}/K$ denote a $\mathbb{Z}_p^d$-extension. Then $m_0 := m_0(\mathbb{K}/K)$ is* **locally maximal** *with respect to the Greenberg-R-topology, i.e., there exists an integer $n \in \mathbb{N}_0$ such that $m_0(\mathbb{L}/K) \leq m_0(\mathbb{K}/K)$ for every $\mathbb{L} \in U(\mathbb{K},n)$.*

Proof. If $d = 1$, then the statement has been proved in Lemma 3.56 (recall that in this case, $m_0(\mathbb{K}/K) = \mu(\mathbb{K}/K)$, by Theorem 5.3).

Let us now assume that $d = 2$. Then there exist only finitely many $\mathbb{Z}_p$-extensions $M \subseteq \mathbb{K}$ of K with $\mu(M/K) \neq m_0(\mathbb{K}/K)$, by Lemma 5.10. In view of Lemma 5.7, (i), we may choose $M \in \mathcal{E}^{\subseteq\mathbb{K}}(K)$ such that $\mu(M/K) = m_0(\mathbb{K}/K)$ and $\mathcal{P}(M) = \mathcal{P}(\mathbb{K})$. Let $n \in \mathbb{N}$ be large enough to ensure that in the one-dimensional neighbourhood $U(M,n)$ of $M \in \mathcal{E}(K)$, $\mu(M/K)$ is locally maximal. We may assume that every prime ramifying in the $\mathbb{Z}_p$-extension M/K has already started ramifying in the n-th intermediate field M_n.

Now consider the neighbourhood $U := U(\mathbb{K},n)$ of $\mathbb{K} \in \mathcal{E}^d(K)$. Let $\tilde{\mathbb{K}} \in U$. Then $M_n \subseteq \mathbb{K}_n = \tilde{\mathbb{K}}_n \subseteq \tilde{\mathbb{K}}$, where $\tilde{\mathbb{K}}_n$ denotes the subfield of $\tilde{\mathbb{K}}$ that is fixed by $\mathrm{Gal}(\tilde{\mathbb{K}}/K)^{p^n}$. Since $\mathrm{Gal}(\tilde{\mathbb{K}}/K) \cong \mathbb{Z}_p^d$ is torsion-free, we may choose a $\mathbb{Z}_p$-extension $\tilde{M} \subseteq \tilde{\mathbb{K}}$ of K containing M_n. In view of Lemma 5.7, (i), we may assume that $\mathcal{P}(\tilde{M}) = \mathcal{P}(\tilde{\mathbb{K}})$. Then $\tilde{M} \in U(M,n) \subseteq \mathcal{E}(K)$, because

$$\mathcal{P}(\tilde{M}) \,=\, \mathcal{P}(\tilde{\mathbb{K}}) \,\subseteq\, \mathcal{P}(\mathbb{K}) \,=\, \mathcal{P}(M)\,.$$

Therefore $\mu(\tilde{M}/K) \leq \mu(M/K)$.

We let $\tilde{X} := \mathrm{Gal}(H(\tilde{\mathbb{K}})/\tilde{\mathbb{K}})$. Let $\tilde{f} \in \Lambda_2$ denote the characteristic power series of $\tilde{\mathbb{K}}/K$, and let $\tilde{\pi} \in \varepsilon_1^0$ denote the homomorphism corresponding to $\tilde{M} \subseteq \tilde{\mathbb{K}}$ via Lemma 2.7. Then

$$\mu(\tilde{M}/K) \,=\, \mu(\tilde{X}_{\tilde{\pi}}) < \infty\,,$$

by Lemma 4.3, (ii), and $\mu(\tilde{X}_{\tilde{\pi}}) \geq m_0(\tilde{\pi}(\tilde{f}))$, by Proposition 4.34, (i). But then

$$m_0(\tilde{\mathbb{K}}/K) \,=\, m_0(\tilde{f}) \,\leq\, \mu(\tilde{M}/K) \,\leq\, \mu(M/K) \,=\, m_0(\mathbb{K}/K)\,.$$

Assume now that $3 \leq d$ is arbitrary. First note that all but finitely many $\mathbb{Z}_p^{d-1}$-extensions $\mathbb{K}^{(d-1)} \subseteq \mathbb{K}$ of K satisfy $\mathcal{P}(\mathbb{K}^{(d-1)}) = \mathcal{P}(\mathbb{K})$ (compare the proof of Lemma 5.10). Moreover, Lemma 5.10 implies that we may choose $\mathbb{K}^{(d-1)}$ such that $m_0(\mathbb{K}^{(d-1)}/K) \leq m_0(\mathbb{K}/K)$.

Inductively, we obtain a $\mathbb{Z}_p$-extension $M \subseteq \mathbb{K}$ of K such that

$$\mu(M/K) \,\leq\, m_0(\mathbb{K}/K) \quad \text{and} \quad \mathcal{P}(M) \,=\, \mathcal{P}(\mathbb{K})\,.$$

Let $n \in \mathbb{N}$ be large enough to ensure that in the one-dimensional neighbourhood $U(M,n)$ of $M \in \mathcal{E}(K)$, $\mu(M/K)$ is locally maximal, and such that every prime ramifying in M/K has already started ramifying in the n-th intermediate field M_n of M/K.

Let $U := U(\mathbb{K},n) \subseteq \mathcal{E}^d(K)$. Suppose that $\tilde{\mathbb{K}} \in U$. As in the proof of $d = 2$, we can choose a $\mathbb{Z}_p$-extension

$$\tilde{M} \,\in\, U(M,n) \cap \mathcal{E}^{\subseteq\tilde{\mathbb{K}}}(K)$$

such that $\mathcal{P}(\tilde{M}) = \mathcal{P}(\tilde{\mathbb{K}})$. Again, Lemma 4.3, (ii) implies that

$$m_0(\tilde{\mathbb{K}}/K) \,\leq\, \mu(\tilde{M}/K) \,\leq\, \mu(M/K) \,\leq\, m_0(\mathbb{K}/K)\,.$$

□

We may draw some conclusions from this theorem.

Corollary 5.13. *Suppose that $\mathbb{K}/K$ denotes a $\mathbb{Z}_p^d$-extension such that every prime of K dividing p ramifies in $\mathbb{K}/K$ (this is the case, for example, if $\mathbb{K}$ contains the cyclotomic $\mathbb{Z}_p$-extension of K). Then $m_0 := m_0(\mathbb{K}/K)$ is locally maximal with respect to* Greenberg's topology*, i.e., there exists some $n \in \mathbb{N}_0$ such that $m_0(\mathbb{L}/K) \leq m_0$ for every $\mathbb{L} \in \mathcal{E}(\mathbb{K}, n)$.*

Proof. If every prime of K dividing p ramifies in $\mathbb{K}/K$, then there exists an integer $e \in \mathbb{N}$ such that every such prime is ramified in the e-th intermediate field $\mathbb{K}_e$, since $\mathbb{K} = \bigcup_{n\geq 0} \mathbb{K}_n$. Therefore $\mathcal{E}(\mathbb{K}, n) = U(\mathbb{K}, n)$ for every $n \geq e$. □

Corollary 5.14. *Suppose that $\mathbb{K}/K$ denotes a $\mathbb{Z}_p^d$-extension. If $m_0(\mathbb{K}/K) = 0$, then there exists some integer $n \in \mathbb{N}_0$ such that $m_0(\mathbb{L}/K) = 0$ for every $\mathbb{L} \in U(\mathbb{K}, n)$.*

Proof. This is obvious from Theorem 5.12. □

5.3 l_0 is locally bounded

We will now turn to the consideration of l_0 invariants. We will see below that these are more difficult to handle, so that several arguments used in the proof of Theorem 5.12 will have to be made more precise. The statement that we obtain by a more or less direct adaption of the above proof will therefore be weaker, namely, we will only prove local boundedness instead of local maximality.

Theorem 5.15. *Let $\mathbb{K}/K$ denote a $\mathbb{Z}_p^d$-extension, let $m_0 := m_0(\mathbb{K}/K) \in \mathbb{N}_0$. In the following, we restrict to $\mathbb{Z}_p^d$-extensions $\mathbb{L}/K$ satisfying $m_0(\mathbb{L}/K) = m_0$. Then l_0 is* **locally bounded** *with respect to the Greenberg-R-topology, i.e., there exist an integer $n \in \mathbb{N}_0$ and a fixed constant $C < \infty$ such that $l_0(\mathbb{L}/K) \leq C$ for every $\mathbb{L} \in U(\mathbb{K}, n)$ satisfying $m_0(\mathbb{L}/K) = m_0$.*

Proof. As in the proof of Theorem 5.12, there exists a $\mathbb{Z}_p$-extension $M \subseteq \mathbb{K}$ of K such that $\mu(M/K) \leq m_0(\mathbb{K}/K)$ and $\mathcal{P}(M) = \mathcal{P}(\mathbb{K})$. By Theorem 3.57, there exists an integer $n \in \mathbb{N}$ such that for every element $\tilde{M}$ contained in the neighbourhood $U(M, n)$ of the $\mathbb{Z}_p$-extension $M \in \mathcal{E}(K)$, we have

$$\mu(\tilde{M}/K) \;\leq\; \mu(M/K)\,,$$

and

$$\lambda(\tilde{M}/K) \;\leq\; \lambda(M/K)$$

if $\mu(\tilde{M}/K) = \mu(M/K)$.

We assume that n is large enough to make the statement of Theorem 5.12 hold for $U(\mathbb{K}, n) \subseteq \mathcal{E}^d(K)$. Let $U := U(\mathbb{K}, n)$, and suppose that $\tilde{\mathbb{K}} \in U$. Using Lemma 5.7, (i), we may choose some

$$\tilde{M} \;\in\; \mathcal{E}^{\subseteq \tilde{\mathbb{K}}}(K) \cap \mathcal{E}(M, n)$$

such that $\mathcal{P}(\tilde{M}) = \mathcal{P}(\tilde{\mathbb{K}}) \subseteq \mathcal{P}(\mathbb{K})$. Then $\tilde{M} \in U(M, n)$. Moreover, Lemma 4.3, (ii) implies that for the homomorphism $\tilde{\pi} \in \varepsilon_{d-1}^0$ corresponding to $\tilde{M} \subseteq \tilde{\mathbb{K}}$,

the quotient $\tilde{X}_{\tilde{\pi}} = \tilde{X}/(\ker(\tilde{\pi}) \cdot \tilde{X})$ of $\tilde{X} = \mathrm{Gal}(H(\tilde{\mathbb{K}})/\tilde{\mathbb{K}})$ is a finitely generated torsion Λ-module, and $\mu(\tilde{X}_{\tilde{\pi}}) = \mu(\tilde{M}/K)$.

We have a chain of inequalitites

$$m_0(\tilde{\mathbb{K}}/K) \;\leq\; \mu(\tilde{M}/K) \;\leq\; \mu(M/K) \;\leq\; m_0 \;,$$

as in the proof of Theorem 5.12.

We will now assume that $m_0(\tilde{\mathbb{K}}/K) = m_0$. Then the above actually is a chain of equalities. In particular, we have $\mu(\tilde{M}/K) = \mu(M/K)$ and therefore $\lambda(\tilde{M}/K) \leq \lambda(M/K)$.

Moreover, if $\tilde{f} \in \Lambda_d$ denotes the characteristic polynomial of $\tilde{\mathbb{K}}/K$, then

$$\begin{aligned} m_0(\tilde{f}) &= m_0(\tilde{\mathbb{K}}/K) \\ &= \mu(\tilde{M}/K) \\ &= \mu(\tilde{X}_{\tilde{\pi}}) \\ &\geq m_0(\tilde{\pi}(\tilde{f})) \;, \end{aligned}$$

using Proposition 4.34, (i). Therefore

$$m_0(\tilde{f}) \;=\; m_0(\tilde{\pi}(\tilde{f})) \;.$$

We will now apply the following fact:

Lemma 5.16. *Let $d \in \mathbb{N}$, let $0 \neq f \in \Lambda_d \cong \mathbb{Z}_p[[\Gamma^d]]$, with $\Gamma^d \cong \mathbb{Z}_p^d$. Suppose that $\pi \in \varepsilon_{d-1}^0$ satisfies $m_0(\pi(f)) = m_0(f)$. Then*

$$l_0(\pi(f)) \;\geq\; l_0(f) \;.$$

Proof. Write $f = p^{m_0(f)} \cdot g$, $p \nmid g$. Suppose that in $\overline{\Lambda}_d = \Lambda_d/p\Lambda_d$, we have

$$\overline{g} \;=\; (\overline{\gamma_1 - 1}) \cdot \ldots \cdot (\overline{\gamma_{l_0} - 1}) \cdot \overline{h} \;,$$

with $l_0 := l_0(f)$, $\gamma_1, \ldots, \gamma_{l_0} \in \Gamma^d \setminus (\Gamma^d)^p$, and $l_0(h) = 0$ (note that the γ_j will not necessarily be pairwise independent). Then $\pi(h) \neq 0$ and $\pi(\gamma_j - 1) \neq 0$ for every j, because $m_0(\pi(f)) = m_0(f)$ by assumption.

Fix $j \in \{1, \ldots, l_0\}$. If δ denotes a topological generator of $\Gamma := \pi(\Gamma^d) \cong \mathbb{Z}_p$, then

$$\pi(\gamma_j - 1) \;=\; ((\delta - 1) + 1)^{x_j} - 1$$

for some $x_j \in \mathbb{Z}_p$. Moreover, $x_j \neq 0$, because $\pi(\gamma_j - 1) \neq 0$. But

$$0 \;\neq\; \pi(\gamma_j - 1) \;\equiv\; 0 \mod (\delta - 1) \;,$$

i.e., $l_0(\pi(\gamma_j - 1)) \geq 1$. This shows that $l_0(\pi(f)) \geq l_0(f)$. □

Using this lemma, we may conclude that

$$l_0(\tilde{\mathbb{K}}/K) \;=\; l_0(\tilde{f}) \;\leq\; l_0(\tilde{\pi}(\tilde{f})) \;\leq\; \lambda(\tilde{X}_{\tilde{\pi}}) \;,$$

where the last inequality follows from Proposition 4.34, (ii). Moreover, there exist constants $C_1, C_2 \in \mathbb{N}$ such that

$$\lambda(\tilde{X}_{\tilde{\pi}}) \;\leq\; \lambda(\tilde{M}/K) + C_1 \qquad \text{and} \qquad \lambda(\tilde{M}/K) \;\leq\; \lambda(\tilde{X}_{\tilde{\pi}}) + C_2$$

for every $\tilde{M} \in \mathcal{E}^{\subseteq \tilde{\mathbb{K}}}(K) \cap \mathcal{E}(M,n)$, provided that $n \geq e(M/K)+1$ (compare Lemma 4.3, (ii)). Note that analogous inequalities (containing the same constants) are also valid for the invariants of the Λ-torsion module X_π attached to our fixed $M \in \mathcal{E}^{\subseteq \mathbb{K}}(K)$. Therefore

$$\begin{aligned} l_0(\tilde{\mathbb{K}}/K) &\leq \lambda(\tilde{M}/K) + C_1 \\ &\leq \lambda(M/K) + C_1 \\ &\leq \lambda(X_\pi) + C_1 + C_2 \\ &= l_0(f) + C_1 + C_2 + (\lambda(X_\pi) - l_0(f)) \ =: \ l_0(\mathbb{K}/K) + C \end{aligned}$$

for every $\tilde{\mathbb{K}} \in U$, where f denotes the characteristic power series of $\mathbb{K}/K$, and where $C := C_1 + C_2 + \lambda(X_\pi) - l_0(f) < \infty$; note that $\lambda(X_\pi) - l_0(f)$ only depends on the fixed $\mathbb{Z}_p$-extension $M \subseteq \mathbb{K}$ of K. □

5.4 Generalised Fukuda theory

In Chapter 3, we studied the classical Iwasawa invariants of $\mathbb{Z}_p$-extensions, and we proved that the λ-invariants actually are not only locally bounded, but in fact locally maximal. In order to obtain results which are stronger than Theorem 5.15, we will now start to work out a generalisation of the method that we have used in Chapter 3. The first step will be to prove a generalisation of Fukuda's Theorem in the higher-dimensional setting. We therefore look for a Fukuda module containing the necessary information about the class numbers of the intermediate fields in a given $\mathbb{Z}_p^d$-extension. In particular, we will have to find a suitable index barrier attached to this module. In fact, we will see that a slight generalisation of the notion of Fukuda modules used in Chapter 3 (compare Definitions 3.3 and 5.24) will be appropriate for obtaining a variant of Fukuda's Theorem. This will take into account the fact that we are not longer dealing with Λ-modules, but with modules over Λ_d for some $d \in \mathbb{N}$.

Suppose that $\mathbb{K}/K$ denotes a $\mathbb{Z}_p^d$-extension, $d \in \mathbb{N}$, and let $\Gamma := \mathrm{Gal}(\mathbb{K}/K)$. Then $\mathbb{K}$ is the union of the finite field extensions $\mathbb{K}_n := \mathbb{K}^{\Gamma^{p^n}}$ of K, $n \geq 0$, and each $\mathbb{K}_n$ is galois over K with $\mathrm{Gal}(\mathbb{K}_n/K) \cong (\mathbb{Z}/p^n\mathbb{Z})^d$. For each n, we let $A_n = A_n^{(\mathbb{K})}$ denote the p-Sylow subgroup of the ideal class group of $\mathbb{K}_n$, respectively, and we define $A := \varprojlim A_n$, where the projective limit is taken with respect to the norm maps.

From now on, we will make the following assumption:

Assumption 5.17. There exists a prime $\mathfrak{p}$ of K that is totally ramified in $\mathbb{K}/K$.

Of course the prime $\mathfrak{p}$ has to divide p. Assumption 5.17 implies that the norm maps $N_{m,n} : A_m \longrightarrow A_n$ are surjective for every $m \geq n \geq 0$ (compare [Wa 97], Theorem 10.1).

Let $H(\mathbb{K})$ denote the maximal p-abelian unramified extension of $\mathbb{K}$. Then $X := \mathrm{Gal}(H(\mathbb{K})/\mathbb{K})$ is isomorphic to A, via Artin's isomorphism from class field theory (this can be proved as in the case $d = 1$ – compare Section 1.3). X is called the *Greenberg module* attached to the $\mathbb{Z}_p^d$-extension $\mathbb{K}/K$.

Note that because of its maximality property, $H(\mathbb{K})$ is in fact a Galois extension of K. We let $G := \mathrm{Gal}(H(\mathbb{K})/K)$. Suppose that $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ denote the primes of K ramifying in $H(\mathbb{K})/K$. Then $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\} = \mathcal{P}(\mathbb{K})$. Assume that $\mathfrak{p}_1$ is totally ramified in $\mathbb{K}/K$. For each $j \in \{1, \ldots, s\}$, we choose a prime $\mathfrak{P}_j$ of $H(\mathbb{K})$ dividing $\mathfrak{p}_j$, respectively, and we denote by $I_j = I_{\mathfrak{P}_j/\mathfrak{p}_j}(H(\mathbb{K})/K) \subseteq G$ the inertia group of $\mathfrak{P}_j$ over $\mathfrak{p}_j$ in the extension $H(\mathbb{K})/K$.

Since $H(\mathbb{K})/\mathbb{K}$ is unramified, we have $I_j \cap X = \{1\}$ for every j. Moreover, since $\mathfrak{p}_1$ is totally ramified in $\mathbb{K}/K$, the induced injection $I_1 \hookrightarrow G/X \cong \Gamma$ is surjective, so that G is isomorphic to the semi-direct product $X \rtimes I_1$. In particular, identifying G with $X \rtimes I_1$, we may conclude that

$$I_j \subseteq X \rtimes I_1$$

for every $j \in \{2, \ldots, s\}$.

Since each I_j bijectively maps to a submodule of the (multiplicative) free $\mathbb{Z}_p$-module

$$G/X \cong \Gamma ,$$

we see that every I_j is a finitely generated free $\mathbb{Z}_p$-module of rank smaller or equal to d. We denote this rank by r_j, and we choose topological generators $\sigma_{j,1}, \ldots, \sigma_{j,r_j}$ of I_j, respectively.

Definition 5.18. There exist elements $a_{2,1}, \ldots, a_{2,r_2}, \ldots, a_{s,1}, \ldots, a_{s,r_s} \in X$ such that

$$\sigma_{j,k} = a_{j,k} \cdot \sigma_{j,k}^{(1)}$$

for suitable elements $\sigma_{j,k}^{(1)} \in I_1$, $2 \leq j \leq s$, $1 \leq k \leq r_j$, respectively.

Let us fix a set of topological generators $\gamma_1, \ldots, \gamma_d$ of Γ. Analogously to the classical one-dimensional case which has been described in Section 1.3, Γ acts on X by conjugation: For $x \in X$, $\gamma \in \Gamma = \mathrm{Gal}(\mathbb{K}/K)$, we let

$$\gamma \cdot x := \tilde{\gamma} \circ x \circ \tilde{\gamma}^{-1} ,$$

where $\tilde{\gamma}$ denotes any lift of γ to $G = \mathrm{Gal}(H(\mathbb{K})/K)$. This is well-defined (i.e., independent of the choice of $\tilde{\gamma}$) because $\mathrm{Gal}(H(\mathbb{K})/\mathbb{K})$ is abelian. Moreover, we may identify I_1 and Γ, using the bijection mentioned above, in order to 'fix' the lifts.

Letting $T_j := \gamma_j - 1$, $1 \leq j \leq d$, we obtain an action of the module

$$\Lambda_d = \mathbb{Z}_p[[T_1, \ldots, T_d]] \cong \mathbb{Z}_p[[\Gamma]]$$

on X.

Lemma 5.19. *Let G' denote the closure of the commutator subgroup of G. Then $G' = (T_1, \ldots, T_d) \cdot X$, where $(T_1, \ldots, T_d)$ is considered as an ideal of Λ_d.*

Proof. This can be proved analogously to the case of $d = 1$, see Lemma 13.14 in [Wa 97]. In order to clarify the notation, we will for the moment write the action of Γ on X multiplicatively. In what follows, we will identify I_1 with Γ.

Let $a, b \in G$. Since the map

$$X \times I_1 \longrightarrow X \times I_1 \,, \quad (x, \gamma) \longmapsto (x^\gamma, \gamma) \,,$$

is a bijection, we have an equality of sets $G = X \cdot I_1 = I_1 \cdot X$. We thus write $a = \alpha x$, $b = \beta y$, with $\alpha, \beta \in \Gamma = I_1$ and $x, y \in X$. It is shown in the proof of Lemma 13.14 in [Wa 97] that

$$aba^{-1}b^{-1} \;=\; (x^\alpha)^{1-\beta} \,\cdot\, (y^\beta)^{\alpha-1} \,.$$

Indeed, we have

$$\begin{aligned} aba^{-1}b^{-1} &= \alpha x \beta y x^{-1} \alpha^{-1} y^{-1} \beta^{-1} \\ &= x^\alpha \alpha \beta y x^{-1} \alpha^{-1} y^{-1} \beta^{-1} \\ &= x^\alpha (yx^{-1})^{\alpha\beta} \underbrace{\alpha\beta\alpha^{-1}}_{=\beta} y^{-1} \beta^{-1} \\ &= x^\alpha (yx^{-1})^{\alpha\beta} (y^{-1})^\beta \\ &= x^\alpha (x^{-1}y)^{\alpha\beta} (y^{-1})^\beta \\ &= x^{\alpha - \alpha\beta} \cdot y^{\alpha\beta - \beta} \,, \end{aligned}$$

using the commutativity of X and Γ, respectively.

In particular, letting $\beta = 1$ and $\alpha \in \{\gamma_1, \ldots, \gamma_d\}$, we see that $y^{\gamma_i - 1} \in G'$ for every $y \in X$ and each $i \in \{1, \ldots, d\}$, so that $(T_1, \ldots, T_d) \cdot X \subseteq G'$.

On the other hand, an arbitrary element $\beta \in \Gamma$ may be written in the form $\beta = \gamma_1^{c_1} \cdot \ldots \cdot \gamma_d^{c_d}$, with $c_1, \ldots, c_d \in \mathbb{Z}_p$. Then

$$\begin{aligned} 1 - \beta &= 1 - (T_1 + 1)^{c_1} \cdot \ldots \cdot (T_d + 1)^{c_d} \\ &= 1 - \left(\sum_{n=0}^{\infty} \binom{c_1}{n} \cdot T_1^n \right) \cdot \ldots \cdot \left(\sum_{n=0}^{\infty} \binom{c_d}{n} \cdot T_d^n \right) \;\in\; (T_1, \ldots, T_d) \cdot \Lambda_d \,, \end{aligned}$$

and therefore $(x^\alpha)^{1-\beta} \in (T_1, \ldots, T_d) \cdot X$ for every $x \in X$ and $\alpha, \beta \in \Gamma$. Analogously, $(y^\beta)^{1-\alpha} \in (T_1, \ldots, T_d) \cdot X$ for every $y \in X$ and $\alpha, \beta \in \Gamma$. Therefore $G' \subseteq (T_1, \ldots, T_d) \cdot X$, because $(T_1, \ldots, T_d) \cdot X$ is closed as being the image of the compact set X^d under the continuous map

$$\phi : X^d \longrightarrow X \,, \quad (x_1, \ldots, x_d) \mapsto T_1 \cdot x_1 + \ldots + T_d \cdot x_d \;\; .$$

□

Now we return to the study of $A = \varprojlim A_n$. In order to define a suitable index barrier for a Fukuda module structure on A, we will use the following invariant introduced by A. Cuoco and P. Monsky in [CM 81]:

Definition 5.20. For every $j \in \{1, \ldots, s\}$, we denote by $\overline{I}_j$ the image of I_j in $G/X \cong \Gamma$. Then we let $e(\mathbb{K}/K) \in \mathbb{N}_0$ denote the smallest integer k such that p^k annihilates the torsion subgroup of every quotient $\Gamma/\overline{I}_j$, $1 \leq j \leq s$.

In particular, if $d = 1$, then $e(\mathbb{K}/K)$ coincides with the integer defined in Proposition 1.3.

We will show below that $e(\mathbb{K}/K)$ may indeed serve as a kind of index barrier for A. The first step in this direction is the next lemma. For each $n \in \mathbb{N}_0$, we let $G^{(n)} := \mathrm{Gal}(H(\mathbb{K})/\mathbb{K}_n) \subseteq G$, and we define $I_j^{(n)} := I_j \cap G^{(n)}$, respectively.

Lemma 5.21. *$I_j^{(n+1)} = (I_j^{(n)})^p$ for every $n \geq e(\mathbb{K}/K)$ and each $j \in \{1, \ldots, s\}$.*

Proof. This is Lemma 5.1 in [CM 81]. □

Definition 5.22.

(1) We first assume that $e(\mathbb{K}/K) = 0$. We define Y_0 to be the submodule of X generated by $(T_1, \ldots, T_d) \cdot X$ and by the $\mathbb{Z}_p$-span of the elements $a_{j,k}$, $2 \leq j \leq s$, $1 \leq k \leq r_j$, introduced in Definition 5.18.

(2) More generally, let $n \in \mathbb{N}$. Let $\nu_{(n,0)}(T) \in \mathbb{Z}_p[T]$ denote the distinguished polynomial

$$\nu_{(n,0)}(T) \;=\; \frac{(T+1)^{p^n} - 1}{(T+1)^{p^0} - 1} \;=\; (T+1)^{p^n - 1} + \ldots + (T+1)^1 + 1 \,.$$

Then we define $Y_n \subseteq X$ to be the submodule generated by

$$(\nu_{(n,0)}(T_1) \cdot T_1, \ldots, \nu_{(n,0)}(T_d) \cdot T_d) \cdot X$$

and by the $\mathbb{Z}_p$-span of the elements $\nu_{(n,0)}(T_{j,k}) \cdot a_{j,k}$, where

$$T_{j,k} \;=\; \sigma_{j,k}^{(1)} - 1 \in \Lambda_d \cong \mathbb{Z}_p[[\Gamma]] \,, \quad 2 \leq j \leq s \,, \quad 1 \leq k \leq r_j \,,$$

respectively. Here we use the notation introduced in Definition 5.18, and we recall that Γ has been identified with I_1.

(3) Finally, suppose that $e = e(\mathbb{K}/K) \in \mathbb{N}_0$ is arbitrary. Then $\mathbb{K}/\mathbb{K}_e$ is a $\mathbb{Z}_p^d$-extension satisfying $e(\mathbb{K}/\mathbb{K}_e) = 0$, and we let Y_e denote the module 'Y_0 attached to $\mathbb{K}/\mathbb{K}_e$', as defined in (1). Note that $X = \mathrm{Gal}(H(\mathbb{K})/\mathbb{K})$ remains the same if we replace K by $\mathbb{K}_e$. Moreover, $\mathrm{Gal}(\mathbb{K}/\mathbb{K}_e)$ is generated topologically by $\gamma_1^{p^e}, \ldots, \gamma_d^{p^e}$. Therefore $Y_e \subseteq X$ is the submodule generated by $(\nu_{(e,0)}(T_1) \cdot T_1, \ldots, \nu_{(e,0)}(T_d) \cdot T_d) \cdot X$ and by the $\mathbb{Z}_p$-span of the corresponding elements $a_{j,k}$ attached to the inertia subgroups in $\mathrm{Gal}(\mathbb{K}/\mathbb{K}_e)$. For $n \geq e$, we define $Y_n \subseteq X$ to be the submodule generated by

$$(\nu_{(n,e)}(T_1) \cdot \nu_{(e,0)}(T_1) \cdot T_1, \ldots, \nu_{(n,e)}(T_d) \cdot \nu_{(e,0)}(T_d) \cdot T_d) \cdot X$$

and by the $\mathbb{Z}_p$-span of the elements $\nu_{(n,e)}(T_{j,k}) \cdot a_{j,k}$, where $\nu_{(n,e)}(T) \in \mathbb{Z}_p[T]$ denotes the distinguished polynomial

$$\nu_{(n,e)}(T) \;=\; \frac{(T+1)^{p^n} - 1}{(T+1)^{p^e} - 1} \;=\; (T+1)^{p^n - p^e} + \ldots + (T+1)^{p^e} + 1 \,,$$

respectively.

Let $n \in \mathbb{N}_0$. Then $A_n \cong \mathrm{Gal}(H_n/\mathbb{K}_n)$ by Artin's isomorphism, where $H_n := H(\mathbb{K}_n)$ denotes the maximal unramified p-abelian extension of $\mathbb{K}_n$. Since $\mathfrak{p}_1$ is totally ramified in $\mathbb{K}/K$, we have $\mathbb{K} \cap H_n = \mathbb{K}_n$, and thus

$$\mathrm{Gal}(H_n/\mathbb{K}_n) \cong \mathrm{Gal}((\mathbb{K} \cdot H_n)/\mathbb{K}) =: X_n .$$

Letting $\overline{H_n} := \mathbb{K} \cdot H_n$, we conclude that

$$X = \varprojlim \mathrm{Gal}(\overline{H_n}/\mathbb{K}) ,$$

using the fact that $H(\mathbb{K}) = \bigcup_{n=0}^{\infty} H_n = \bigcup_{n=0}^{\infty} \overline{H_n}$, which may be proved analogously to Proposition 1.33. Let $\varphi : A \xrightarrow{\sim} X$ denote the isomorphism induced by Artin's maps $\varphi_n : A_n \xrightarrow{\sim} X_n$, $n \in \mathbb{N}_0$.

Lemma 5.23. *For each integer $n \in \mathbb{N}_0$, we define Y_n^X to be the kernel of the projection $\mathrm{pr}_n : X = \varprojlim X_n \longrightarrow X_n$ (this map is induced by the restriction from $H(\mathbb{K})$ to $\overline{H_n}$). Then $Y_n^X = Y_n$ for every $n \geq 0$.*

Proof. Let us first assume that $e(\mathbb{K}/K) = 0$. We will adapt the proof of Lemma 1.37, which is divided into three steps.

1. *Let $n \in \mathbb{N}_0$ be arbitrary, but fixed. Then Y_n^X is the set of $y \in X$ satisfying $y|_{\overline{H_n}} = 1$.*

   Proof. $X = \varprojlim \mathrm{Gal}(\overline{H_n}/\mathbb{K})$. Therefore $y \in Y_n^X$ if and only if $y|_{\overline{H_n}} = 1$. □

2. *We have $Y_0 = Y_0^X$.*

   Proof. Since H_0 by definition is the maximal abelian unramified p-extension of $\mathbb{K}_0 = K$, and since $H(\mathbb{K})/K$ is a pro-p-extension, it follows that H_0 is the maximal abelian unramified subextension of $H(\mathbb{K})/K$. Therefore

   $$\mathrm{Gal}(H(\mathbb{K})/H_0) \subseteq \mathrm{Gal}(H(\mathbb{K})/K) = G$$

   is the closed subgroup generated by the commutator subgroup of G together with all the inertia subgroups I_j, $1 \leq j \leq s$.
   This means that $\mathrm{Gal}(H(\mathbb{K})/H_0)$ is the closure of the subgroup of G generated by G', I_1 and the elements $a_{j,k}$, $2 \leq j \leq s$, $1 \leq k \leq r_j$, respectively. Therefore

   $$\begin{aligned} \mathrm{Gal}(H_0/K) &\cong \mathrm{Gal}(H(\mathbb{K})/K)/\mathrm{Gal}(H(\mathbb{K})/H_0) = G/\mathrm{Gal}(H(\mathbb{K})/H_0) \\ &= X \cdot I_1 \,/\, \overline{<G', I_1, \{a_{j,k}\}>} \\ &\cong X/<(T_1, \ldots, T_d) \cdot X, \{a_{j,k}\}>_{\mathbb{Z}_p} , \end{aligned}$$

   since Lemma 5.19 implies that $G' = (T_1, \ldots, T_d) \cdot X$. But $X = \mathrm{Gal}(H(\mathbb{K})/\mathbb{K})$, so that

   $$X/\mathrm{Gal}(H(\mathbb{K})/\overline{H_0}) \cong \mathrm{Gal}(\overline{H_0}/\mathbb{K}) \cong \mathrm{Gal}(H_0/K) ,$$

   and therefore the subset of elements of X fixing $\overline{H_0}$ is exactly

   $$Y_0 = <(T_1, \ldots, T_d) \cdot X, \{a_{j,k}\}>_{\mathbb{Z}_p} .$$

   By the first part of the proof, it follows that $Y_0 = Y_0^X$, as claimed. □

3. *Now consider an arbitrary $n \in \mathbb{N}_0$. Then $Y_n = Y_n^X$.*

Proof. This can be proved analogously to the second step. Simply replace the ground field K by $\mathbb{K}_n$. Then H_n and $\overline{H_n}$ correspond to the fields H_0 and $\overline{H_0}$ in step 2, and the topological generators $\sigma_{j,k}$, $2 \leq j \leq s$, $1 \leq k \leq r_j$, are replaced by their p^n-th powers, respectively (note that $\mathrm{Gal}(\mathbb{K}/K) \,/\, \overline{I}_j$ is torsion-free for every j, since $e(\mathbb{K}/K) = 0$). Now

$$\begin{aligned}
\sigma_{j,k}^{p^n} &= (a_{j,k} \cdot \sigma_{j,k}^{(1)})^{p^n} \\
&= a_{j,k} \cdot \sigma_{j,k}^{(1)} \cdot a_{j,k} \cdot (\sigma_{j,k}^{(1)})^{-1} (\sigma_{j,k}^{(1)})^2 \cdot \ldots \cdot a_{j,k} \cdot (\sigma_{j,k}^{(1)})^{-(p^n-1)} (\sigma_{j,k}^{(1)})^{p^n} \\
&= (1 + \sigma_{j,k}^{(1)} + \ldots + (\sigma_{j,k}^{(1)})^{p^n-1}) \cdot a_{j,k} \cdot (\sigma_{j,k}^{(1)})^{p^n} \\
&= \nu_{(n,0)}(T_{j,k}) \cdot a_{j,k} \cdot (\sigma_{j,k}^{(1)})^{p^n} \ ,
\end{aligned}$$

compare p. 280 in [Wa 97]. Therefore each $a_{j,k} \in X$ has to be replaced by $\nu_{(n,0)}(T_{j,k}) \cdot a_{j,k}$, respectively. Moreover, $(T_1, \ldots, T_d) \cdot X$ has to be replaced by $(\nu_{(n,0)}(T_1) \cdot T_1, \ldots, \nu_{(n,0)}(T_d) \cdot T_d) \cdot X$, because

$$\gamma_j^{p^n} - 1 \ = \ \nu_{(n,0)}(T_j) \cdot (\gamma_j - 1)$$

for every $j = 1, \ldots, d$, respectively.
By the argument used in step 2, and in view of Definition 5.22, $Y_n \subseteq X$ is the subgroup fixing $\overline{H_n}$, and so $Y_n = Y_n^X$ by step 1. □

If $e(\mathbb{K}/K) \in \mathbb{N}_0$ is arbitrary, then $\mathbb{K}/\mathbb{K}_e$ is a $\mathbb{Z}_p^d$-extension with $e(\mathbb{K}/\mathbb{K}_e) = 0$. By definition, Y_e is 'Y_0 for $\mathbb{K}/\mathbb{K}_e$' and X_n corresponds to 'X_{n-e} for $\mathbb{K}/\mathbb{K}_e$', $n \geq e$. Therefore Y_e^X corresponds to 'Y_0^X for $\mathbb{K}/\mathbb{K}_e$', so that $Y_e^X = Y_e$, by step 2.

The proof of $Y_n^X = Y_n$ for arbitrary $n \geq e$ is now analogous to step 3 above, replacing the distinguished polynomial $\nu_{(n,0)}$ by $\nu_{(n,e)}$ (compare Definition 5.22). □

This lemma shows that we will have to modify the notion of Fukuda modules introduced in the third chapter. The following definition introduces a concept of Fukuda modules that will be sufficient for our purposes.

Definition 5.24. Let R denote a local domain with maximal ideal $\mathfrak{m}$. Suppose that R is Hausdorff and complete with respect to the $\mathfrak{m}$-adic topology, and that the residue field $R/\mathfrak{m}$ is finite.
Let $B = \varprojlim B_n$ denote the projective limit of finite R-modules B_n, $n \in \mathbb{N}_0$, each of which we assume to be an abelian p-group.
Furthermore, we assume that $B = \varprojlim B_n$ satisfies the following two properties: Suppose that there exists an integer $e \geq 0$ such that:
(1) For every $n \geq e$, the n-th projection $\mathrm{pr}_n : B \longrightarrow B_n$ is surjective.
(2) If $Y_n := \ker(\mathrm{pr}_n)$, $n \in \mathbb{N}_0$, then $Y_{n+1} \subseteq \mathfrak{m} \cdot Y_n$ for every $n \geq e$.
Then B is called a ***Fukuda-R-module*** (or simply ***Fukuda module***) with ***index barrier*** e.

Proposition 5.25. *Every Fukuda-R-module B is finitely generated over R.*

Proof. Since $B/Y_e \cong B_e$ is finite, B is finitely generated over R if and only if Y_e is finitely generated. Our assumptions on R imply that R is a compact topological ring (compare the proof of Lemma 2.15, (ii)). Using Nakayama's Lemma 1.42, (ii), it will be sufficient to prove that $Y_e/(\mathfrak{m} \cdot Y_e)$ is finite, because $B = \varprojlim B_n$ and therefore also $Y_e = \ker(\mathrm{pr}_e) \subseteq B$ are compact R-modules. But

$$|Y_e/(\mathfrak{m} \cdot Y_e)| \;\leq\; |Y_e/Y_{e+1}| \;\leq\; |B/Y_{e+1}| \;=\; |B_{e+1}| \,.$$

□

Corollary 5.26. *Let $\mathbb{K}/K$ denote a $\mathbb{Z}_p^d$-extension, and let $e := e(\mathbb{K}/K)$, as in Definition 5.20. Then the Greenberg-module $X = \mathrm{Gal}(H(\mathbb{K})/\mathbb{K})$ is a Fukuda-Λ_d-module with index barrier e.*

Proof. First note that Λ_d satisfies the properties of the ring R in Definition 5.24, by Proposition 2.17.

Recall that $X = \varprojlim X_n$ with $X_n = \mathrm{Gal}((\mathbb{K} \cdot H_n)/\mathbb{K})$. Since $\mathfrak{p}_1$ is totally ramified in $\mathbb{K}/K$ by Assumption 5.17, $X_n \cong \mathrm{Gal}(H_n/\mathbb{K}_n) \cong A_n$ for every n, using Artin's isomorphism. Therefore each X_n is a finite abelian p-group. Moreover, $H_n \subseteq H(\mathbb{K})$ for every n, by Proposition 1.34, and therefore the restriction maps

$$X \;=\; \mathrm{Gal}(H(\mathbb{K})/\mathbb{K}) \;\longrightarrow\!\!\!\!\!\rightarrow\; \mathrm{Gal}((H_n \cdot \mathbb{K})/\mathbb{K}) \;\cong\; X_n$$

are surjective for each $n \geq e$.

Let Y_n^X denote the kernel of the projection map $\mathrm{pr}_n : X \longrightarrow X_n$, respectively. Then we have shown in Lemma 5.23 that $Y_n^X = Y_n$ for every $n \geq e$, with the modules $Y_n \subseteq X$ that have been introduced in Definition 5.22. But this means that $Y_{n+1}^X \subseteq I \cdot Y_n^X$ for every such n, where the ideal $I \subseteq \Lambda_d$ is generated by a finite set of elements $\nu_{(n+1,n)}(T_{j,k}) = \frac{\nu_{(n+1,e)}(T_{j,k})}{\nu_{(n,e)}(T_{j,k})}$, with certain $T_{j,k} \in \Lambda_d$ satisfying $T_{j,k} \in (T_1, \ldots, T_d)$. In particular, $I \subseteq (p, T_1, \ldots, T_d) = \mathfrak{m}$. □

Lemma 5.27 (Isomorphisms of Fukuda-modules)**.** *Let $A = \varprojlim A_n$ be a Fukuda-R-module, let $\varphi : A \longrightarrow B$ be an R-module isomorphism, $B = \varprojlim B_n$. Assume that φ is induced by R-module isomorphisms $\varphi_n : A_n \longrightarrow B_n$ such that the diagrams*

$$\begin{array}{ccc} A & \xrightarrow{\;\varphi\;} & B \\ {\scriptstyle \mathrm{pr}_n}\downarrow & & \downarrow{\scriptstyle \mathrm{pr}_n} \\ A_n & \xrightarrow{\;\varphi_n\;} & B_n \end{array} \qquad (\star)$$

are commutative for all $n \geq e$, where $e := e(A)$ denotes the index barrier of A. Then $B = \varphi(A)$ is a Fukuda-R-module with index barrier e.

Proof. This may be proved analogously to Lemma 3.8: The commutativity of the diagrams $(\star)$ implies that $Y_n^B = \varphi(Y_n^A)$ for every $n \geq e$, and therefore

$$Y_{n+1}^B \;=\; \varphi(Y_{n+1}^A) \;\subseteq\; \varphi(\mathfrak{m} \cdot Y_n^A) \;=\; \mathfrak{m} \cdot Y_n^B$$

for every $n \geq e$. □

Corollary 5.28. *Let $\mathbb{K}/K$ denote a $\mathbb{Z}_p^d$-extension, $e := e(\mathbb{K}/K)$. Recall that we assume that there exists a prime $\mathfrak{p}_1$ of K that is totally ramified in $\mathbb{K}/K$. Then $A = \varprojlim A_n$ is a Fukuda-Λ_d-module with index barrier e.*

Proof. Use Artin's isomorphisms $\varphi : X_n \xrightarrow{\sim} A_n$ from class field theory, and apply Corollary 5.26 and Lemma 5.27 (compare the proof of Corollary 3.9). □

Lemma 5.29 (Quotients of Fukuda modules)**.** *Let $A = \varprojlim A_n$ denote a Fukuda-R-module with index barrier e. Let $M \subseteq A$ be a submodule, i.e., $M = \varprojlim M_n$ with R-submodules $M_n \subseteq A_n$, $n \geq 0$. We assume that the projection maps $\mathrm{pr}_n : M \longrightarrow M_n$ are surjective for every $n \geq e$.*

Then $A/M := \varprojlim A_n/M_n$ is a Fukuda-R-module with index barrier e.

Proof. This can be proved analogously to Lemma 3.10 by showing that the canonical projection $\pi : A \longrightarrow A/M$ maps Y_n^A onto $Y_n^{A/M}$ for every $n \geq e$. □

We will now prove a generalisation of Fukuda's Theorem that will be fundamental for our method.

Theorem 5.30. *Let $A = \varprojlim A_n$ denote a Fukuda-R-module with index barrier e.*

(i) If there exists an integer $n \geq e$ such that $|A_{n+1}| = |A_n|$, then $|A_m| = |A_n|$ for every $m \geq n$, and therefore $|A_n| = |A|$.

(ii) Let $j \in \mathbb{N}$, let $f_1, \ldots, f_j \in R$. If there exists an integer $n \geq e$ such that

$$|A_{n+1}/((f_1, \ldots, f_j) \cdot A_{n+1})| \;=\; |A_n/((f_1, \ldots, f_j) \cdot A_n)| \,,$$

then $|A_m/((f_1, \ldots, f_j) \cdot A_m)| = |A_n/((f_1, \ldots, f_j) \cdot A_n)|$ for every $m \geq n$, and in fact $|A_n/((f_1, \ldots, f_j) \cdot A_n)| = |A/((f_1, \ldots, f_j) \cdot A)|$.

Proof. (i) Since $n \geq e$, the projections $\mathrm{pr}_n : A \longrightarrow A_n$, $\mathrm{pr}_{n+1} : A \longrightarrow A_{n+1}$ and the map $f_{n+1,n} : A_{n+1} \longrightarrow A_n$ are surjective (the latter is part of the projective system corresponding to the inverse limit $A = \varprojlim A_n$, compare the introduction to inverse limits given prior to Definition 3.3). Note that $\mathrm{pr}_n = f_{n+1,n} \circ \mathrm{pr}_{n+1}$, by definition.
Since $|A_{n+1}| = |A_n|$ by assumption, the map $f_{n+1,n}$ actually is an isomorphism, so that

$$A/Y_{n+1} \;\cong\; A_{n+1} \;\cong\; A_n \;\cong\; A/Y_n \,.$$

Since $Y_{n+1} \subseteq \mathfrak{m} \cdot Y_n \subseteq Y_n$, and as both quotients A/Y_{n+1} and A/Y_n are finite, it follows that $Y_{n+1} = Y_n$. In particular, $Y_n = \mathfrak{m} \cdot Y_n$, and Nakayama's Lemma 1.41 (with $E = Y_n$ and $F = \{0\}$) implies that $Y_n = \{0\}$. Therefore $Y_m \subseteq \mathfrak{m}^{m-n} \cdot Y_n = \{0\}$ for every $m \geq n$, so that $|A_m| = |A_n|$ for each $m \geq n$.

(ii) Letting $M := \varprojlim M_n$ with $M_n := (f_1, \ldots, f_j) \cdot A_n$, $n \geq 0$, the quotient module $A/M = \varprojlim A_n/M_n$ is a Fukuda-R-module with index barrier e, by Lemma 5.29. Now apply (i).

□

5.5 Ramification and the index barrier

Let $\mathbb{K}/K$ denote a $\mathbb{Z}_p^d$-extension. We have seen in the last section that the inverse limit $A = \varprojlim A_n$ is a Fukuda-Λ_d-module with index barrier $e(\mathbb{K}/K)$. The generalised Iwasawa invariants attached to $\mathbb{K}/K$ describe the asymptotic growth of the class groups A_n, $n \in \mathbb{N}_0$. In order to study the local behaviour of these invariants, we therefore want to transform information about the A_n, coded into the finiteness of certain quotients (the details will be given in the next section), into information about the class groups $A_n^{(\mathbb{L})}$ attached to $\mathbb{Z}_p^d$-extensions $\mathbb{L}/K$ that are contained in some neighbourhood of $\mathbb{K}$. The main tool for performing this transfer will be Theorem 5.30. Since the statements in this theorem are only valid for integers $n \geq e$, respectively, it is necessary to obtain control on the index barriers of the modules $A^{(\mathbb{L})} = \varprojlim A_n^{(\mathbb{L})}$.

In Chapter 3, we have seen that Greenberg's topology is not suitable for this purpose, since the index barriers $e(L/K)$, $L \in \mathcal{E}(K)$, in general will not be locally bounded with respect to this topology (compare Lemma 3.18, (vi)). We therefore introduced the Greenberg-R-topology, with respect to which the $e(L/K)$ in fact even are locally constant (see Corollary 3.22).

In the present section, we will define a topology on the set $\mathcal{E}^d(K)$ of $\mathbb{Z}_p^d$-extensions of K that will be sufficient for our purposes. In Section 5.1, we introduced the Greenberg-R-topology on $\mathcal{E}^d(K)$. A typical neighbourhood of an element $\mathbb{K} \in \mathcal{E}^d(K)$ with respect to this topology is given by

$$U(\mathbb{K}, n) \;=\; \{\mathbb{L} \in \mathcal{E}(\mathbb{K}, n) \mid \mathcal{P}(\mathbb{L}) \subseteq \mathcal{P}(\mathbb{K})\} \; .$$

Therefore this topology – in contrast to Greenberg's topology – depends on the set of primes of K ramifying in $\mathbb{K}$. In the case $d = 1$, this was enough. However, we will now see that it might not be sufficient if $d > 1$. We first seek for a better understanding of the invariant $e(\mathbb{K}/K)$.

Proposition 5.31. *Let $\mathbb{K}/K$ denote a $\mathbb{Z}_p^d$-extension, let $e := e(\mathbb{K}/K)$. We consider the set $\mathcal{E}^{\subseteq \mathbb{K}}(K)$ of $\mathbb{Z}_p$-extensions of K that are contained in $\mathbb{K}$. If $\mathcal{P}(\mathbb{K}) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$, then*

$$\max_{\mathfrak{p}_j \in \mathcal{P}(\mathbb{K})} \inf_{\substack{L \in \mathcal{E}^{\subseteq \mathbb{K}}(K) \\ \mathfrak{p}_j \in \mathcal{P}(L)}} e_j(L/K) \;\leq\; e \;\leq \sup_{L \in \mathcal{E}^{\subseteq \mathbb{K}}(K)} e(L/K) \; .$$

Here $e_j(L/K)$ denotes the largest integer $k \in \mathbb{N}_0$ such that $\mathfrak{p}_j$ is unramified in the k-th intermediate field L_k of L/K, respectively.

Remarks 5.32.

(1) The supremum of the $e(L/K)$ is finite if and only if $\mathcal{P}(L) = P$ for some fixed set $P \subseteq \mathcal{I}$ of primes and every $L \in \mathcal{E}^{\subseteq \mathbb{K}}(K)$ (compare Lemma 3.18). In view of Lemma 5.7, (i), this is equivalent to the condition that $\mathcal{P}(L) = \mathcal{P}(\mathbb{K})$ for every $L \in \mathcal{E}^{\subseteq \mathbb{K}}(K)$. Therefore the upper bound for e given in Proposition 5.31 is non-trivial only in this special case.

(2) In general, the first inequality will be strict. Suppose, for example, that $\mathcal{P}(\mathbb{K}) = \{\mathfrak{p}\}$ contains only one element, and let $\overline{I} \subseteq \mathrm{Gal}(\mathbb{K}/K)$ denote the

inertia subgroup of $\mathfrak{p}$ in $\mathbb{K}/K$. Then $\Gamma/\overline{I}$ is a finite group, since the prime $\mathfrak{p}$ has to ramify in each $\mathbb{Z}_p$-extension $L \subseteq \mathbb{K}$ of K. We assume that the torsion group $\Gamma/\overline{I}$ is not cyclic, i.e.,

$$\Gamma/\overline{I} \;\cong\; \bigoplus_{i=1}^{s} \mathbb{Z}/p^{n_i}\mathbb{Z}$$

with $s > 1$. Assume further that not all the n_i are equal. Then

$$e \;=\; \max_i n_i \;>\; \min_i n_i \;\geq\; \inf_{L \in \mathcal{E}^{\subseteq \mathbb{K}}(K)} e(L/K)\;.$$

Here the last inequality follows from Proposition 5.33, (i) below.

We now turn to the proof of Proposition 5.31.

Proof. For every $1 \leq j \leq s$, we let H_j denote the subfield of $\mathbb{K}$ that is fixed by $\overline{I_j} \subseteq \Gamma$ (compare Definition 5.20), i.e., H_j is the maximal subextension of $\mathbb{K}$ that is unramified at $\mathfrak{p}_j$. Let T_j denote the $\mathbb{Z}_p$-torsion subgroup of $\mathrm{Gal}(H_j/K)$, and let furthermore

$$B_j \;\subseteq\; \mathrm{Gal}(H_j/K) \;\cong\; \Gamma \,/\, \overline{I_j}$$

denote some torsion-free submodule such that $\mathrm{Gal}(H_j/K) = B_j \oplus T_j$. Finally, let $F_j \subseteq H_j$ be the subfield fixed by B_j, respectively. Then F_j is a finite abelian extension of K, and $\mathrm{Gal}(F_j/K)$ is isomorphic to the torsion subgroup T_j of the $\mathbb{Z}_p$-module $\mathrm{Gal}(H_j/K)$. Note that the 'maximal free subgroup' B_j of $\mathrm{Gal}(H_j/K)$ and therefore the field F_j are not unique; but $\mathrm{Gal}(F_j/K)$ is unique up to isomorphism. Every cyclic subextension M/K of F_j is contained in some $\mathbb{Z}_p$-extension of K that ramifies at $\mathfrak{p}_j$ (note that every finite subfield of $\mathbb{K}$, cyclic over K, is contained in some $\mathbb{Z}_p$-extension of K). Moreover, we have the following fact.

Proposition 5.33.

(i) *Let $k \in \mathbb{N}$. If $M \subseteq F_j$ is maximal cyclic of degree p^k over K and if $L \in \mathcal{E}^{\subseteq \mathbb{K}}(K)$ contains M, then $\mathfrak{p}_j$ ramifies in $L_{k+1}/L_k = M$.*

(ii) *If $M \subseteq F_j$ denotes any cyclic extension of K, $M \neq K$, and if some $L \in \mathcal{E}^{\subseteq \mathbb{K}}(K)$ contains M, then $\mathfrak{p}_j$ ramifies in L_{e+1}/K, where $e = e(\mathbb{K}/K)$.*

Proof. (i) If $\mathfrak{p}_j$ was unramified in L_{k+1}, then $L_{k+1} \subseteq H_j$. F_j is the subfield of H_j fixed by some torsion-free subgroup $B_j \subseteq \mathrm{Gal}(H_j/K)$. Write the torsion subgroup of $\mathrm{Gal}(H_j/K)$ as

$$T_j \;=\; \bigoplus_{i=1}^{t} V_i\;, \quad V_i \;\cong\; \mathbb{Z}/p^{n_i}\mathbb{Z}\;,$$

for suitable $n_i \in \mathbb{N}$, respectively. Then $n_i = k$ for some i, because of our assumptions on $M \subseteq F_j$. We may without loss of generality assume that $n_1 = k$, and that $M \subseteq F_j$ is the subfield of H_j fixed by $B_j \oplus V_2 \oplus \cdots \oplus V_t$. If $M \subseteq L_{k+1} \subseteq H_j$, then the subgroup of $\mathrm{Gal}(H_j/K)$ fixing L_{k+1} has to be a proper subgroup of $B_j \oplus V_2 \oplus \cdots \oplus V_t$ of index p. But then

$$\mathrm{Gal}(L_{k+1}/K) \;\cong\; \mathrm{Gal}(H_j/K) \,/\, \mathrm{Gal}(H_j/L_{k+1})$$

cannot be cyclic, yielding a contradiction.

(ii) If $M \subseteq F_j$ denotes any subextension that is cyclic over K, then we may choose the $V_i \subseteq T_j$ such that the subgroup $\mathrm{Fix}(M) \subseteq \mathrm{Gal}(H_j/K)$ fixing M is given by

$$\mathrm{Fix}(M) \;=\; B_j \oplus \tilde{V}_1 \oplus V_2 \oplus \cdots \oplus V_t \;,$$

where $\tilde{V}_1 \subseteq V_1$ is a subgroup of index $[M : K]$. Assume that $\mathfrak{p}_j$ is unramified in L_{e+1}/K for some $\mathbb{Z}_p$-extension $L \in \mathcal{E}^{\subseteq \mathbb{K}}(K)$ containing M. Then $M \subseteq L_{e+1} \subseteq H_j$, and therefore $\mathrm{Fix}(L_{e+1}) \subseteq \mathrm{Fix}(M)$. Moreover, $\mathrm{Fix}(L_{e+1}) + T_j \neq \mathrm{Gal}(H_j/K)$, since otherwise, $\mathrm{Fix}(L_{e+1})$ would have to contain a torsion-free subgroup C_j such that $C_j + T_j = \mathrm{Gal}(H_j/K)$; but then L_{e+1} would be contained in the fixed field $\tilde{F}_j := H_j^{C_j}$. Since the exponent of $\mathrm{Gal}(\tilde{F}_j/K) \cong T_j$ would be bounded by e, this would contradict the fact that L_{e+1}/K is cyclic of degree p^{e+1}.
We therefore may choose an element $g \in \mathrm{Gal}(H_j/K)$ such that

$$g \;\notin\; \mathrm{Fix}(L_{e+1}) + T_j \;.$$

Moreover, $g \in \mathrm{Gal}(H_j/K) \setminus T_j$ has infinite order, and we may assume that g is contained in the fixed torsion-free subgroup $B_j \subseteq \mathrm{Gal}(H_j/K)$ satisfying $B_j + T_j = \mathrm{Gal}(H_j/K)$ (indeed, if $g = \tilde{g} + t$ with $\tilde{g} \in B_j$ and $t \in T_j$, then we may replace g by $\tilde{g} \notin \mathrm{Fix}(L_{e+1}) + T_j$.) Let further $v \in V_1 \setminus \tilde{V}_1$ denote any fixed element. Then the cosets of g and v in

$$\mathrm{Gal}(L_{e+1}/K) \;\cong\; \mathrm{Gal}(H_j/K) \,/\, \mathrm{Fix}(L_{e+1})$$

are non-trivial. Moreover, we claim that these cosets in fact generate a group having p-rank two. This contradicts the fact that L_{e+1}/K is cyclic, proving the proposition.
Indeed, assume that $g = \lambda \cdot v + z$, with $\lambda \in \mathbb{Z}_p$ and $z \in \mathrm{Fix}(L_{e+1})$. Then $g \in \mathrm{Fix}(L_{e+1}) + T_j$, contradiction. Assume, on the other hand, that $v = \lambda \cdot g + z$, with λ and z as above. Then $v - \lambda \cdot g \in \mathrm{Fix}(L_{e+1}) \subseteq \mathrm{Fix}(M)$, and therefore $v \in \mathrm{Fix}(M)$, because $B_j \subseteq \mathrm{Fix}(M)$ and $g \in B_j$, by our choice of g. This again yields a contradiction.

□

Now we return to the proof of Proposition 5.31. Fix $j \in \{1, \ldots, s\}$. Then $e \geq \exp(\Gamma/\overline{I_j}) = \exp(\mathrm{Gal}(F_j/K))$, by definition. We let $k \leq e$ denote the largest integer such that there exists an extension $M \subseteq F_j$ that is cyclic of degree p^k over K. By the above, there exists some $L \in \mathcal{E}^{\subseteq \mathbb{K}}(K)$ such that $M \subseteq L$ and such that $\mathfrak{p}_j$ ramifies in L_{k+1}/L_k. Therefore $k = e_j(L/K)$, and thus

$$\inf_{\substack{L \in \mathcal{E}^{\subseteq \mathbb{K}}(K) \\ \mathfrak{p}_j \in \mathcal{P}(L)}} e_j(L/K) \;\leq e \;.$$

Since this holds for every $j \in \{1, \ldots, s\}$, the first inequality of Proposition 5.31 follows.

Now suppose that $\mathcal{P}(L) = P$ for some $P \subseteq \mathcal{I}$ and every $L \in \mathcal{E}^{\subseteq \mathbb{K}}(K)$. Let $C \in \mathbb{N}$ be the smallest integer such that $e(L/K) \leq C$ for each $L \in \mathcal{E}^{\subseteq \mathbb{K}}(K)$

(compare Remarks 5.32, (1)). If $e > C$, then there exists $j \in \{1, \ldots, s\}$ such that the exponent of the Galois group $\mathrm{Gal}(F_j/K)$ is strictly larger than C. But this means that there exists an extension $M \subseteq \mathbb{K}$, cyclic of degree p^{C+1} over K, such that $\mathfrak{p}_j$ is unramified in M, and such that M is contained in some $L \in \mathcal{E}^{\subseteq \mathbb{K}}(K)$ with $\mathfrak{p}_j \in \mathcal{P}(L)$. Therefore $e(L/K) \geq C + 1$, yielding a contradiction. □

Lemma 5.34. *Let $e := e(\mathbb{K}/K)$, let $\mathbb{L} \in U(\mathbb{K}, e+1)$. Then*
(i) $\mathcal{P}(\mathbb{L}) = \mathcal{P}(\mathbb{K})$, *and*
(ii) $e(\mathbb{L}/K) \geq e(\mathbb{K}/K)$.

Proof. (i) We have $\mathcal{P}(\mathbb{L}) \subseteq \mathcal{P}(\mathbb{K})$ by definition of $U(\mathbb{K}, e+1)$. If $\mathfrak{p} \in \mathcal{P}(\mathbb{K})$, then there exists some $M \in \mathcal{E}^{\subseteq \mathbb{K}}(K)$ such that $\mathfrak{p} \in \mathcal{P}(M)$. Let $e_{\mathfrak{p}}(M/K)$ denote the largest integer $k \in \mathbb{N}_0$ such that $\mathfrak{p}$ is unramified in the intermediate field M_k/K. We may assume that M/K has been chosen such that $e_{\mathfrak{p}}(M/K)$ is minimal among the $\mathbb{Z}_p$-extensions in $\mathcal{E}^{\subseteq \mathbb{K}}(K)$ which ramify at $\mathfrak{p}$. Then $e_{\mathfrak{p}}(M/K) \leq e$, by Proposition 5.31, and $\mathfrak{p}$ ramifies in

$$M_{e_{\mathfrak{p}}(M/K)+1} \subseteq \mathbb{K}_{e+1} = \mathbb{L}_{e+1} \subseteq \mathbb{L}\,.$$

Therefore $\mathfrak{p} \in \mathcal{P}(\mathbb{L})$.

(ii) Write $\mathcal{P}(\mathbb{L}) = \mathcal{P}(\mathbb{K}) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$, and fix some $j \in \{1, \ldots, s\}$. Let H_j denote the subfield of $\mathbb{K}$ fixed by $\overline{I_j}$, and let $F_j \subseteq H_j$ denote the field fixed by some free subgroup B_j of $\mathrm{Gal}(H_j/K) \cong \Gamma / \overline{I_j}$ satisfying $B_j \oplus T_j = \mathrm{Gal}(H_j/K)$, as in the proof of Proposition 5.31. We will denote by $H_j^{(\mathbb{L})}$, respectively, $F_j^{(\mathbb{L})}$, subfields of $\mathbb{L}$ that are obtained in an analogous way (again, we remark that F_j and $F_j^{(\mathbb{L})}$ in general are not unique).

Then $F_j \subseteq \mathbb{K}_e = \mathbb{L}_e \subseteq \mathbb{L}$, and in fact $F_j^{(\mathbb{L})}$ can be chosen such that $F_j \subseteq F_j^{(\mathbb{L})}$. This will be shown below (compare Proposition 5.35 and Corollary 5.36). Before stating these results, we will finish the proof of Lemma 5.34:

Note that there exists some $j \in \{1, \ldots, s\}$ such that $e = \exp(\mathrm{Gal}(F_j/K))$ (for every choice of F_j). If $N \subseteq F_j$ denotes a cyclic extension of K of degree p^e, then $N \subseteq F_j \subseteq F_j^{(\mathbb{L})}$, by the results announced above. Therefore

$$e(\mathbb{L}/K) = \max_j \exp(\mathrm{Gal}(F_j^{(\mathbb{L})}/K)) \geq \exp(\mathrm{Gal}(N/K)) = e\,.$$

Proposition 5.35. *Let $K \neq M \subseteq H_j$. Then M is contained in F_j for some choice of B_j if and only if no subfield $N \neq K$ of M, cyclic over K, is contained in a $\mathbb{Z}_p$-extension $L \in \mathcal{E}^{\subseteq \mathbb{K}}(K)$ that is unramified at $\mathfrak{p}_j$.*

Proof. Let $\tilde{H}_j \subseteq H_j$ denote the subfield fixed by the torsion subgroup T_j of $G := \mathrm{Gal}(H_j/K)$. Then $\mathrm{Gal}(\tilde{H}_j/K)$ is torsion-free, and every finite cyclic subextension of $\tilde{H}_j$ is contained in some $\mathbb{Z}_p$-extension of K that is unramified at $\mathfrak{p}_j$. Moreover, every $\mathbb{Z}_p$-extension $L \in \mathcal{E}^{\subseteq \mathbb{K}}(K)$ that is unramified at $\mathfrak{p}_j$ is contained in $\tilde{H}_j$, since $\tilde{H}_j \subseteq H_j$ is of finite index $|T_j|$.

This shows that the latter condition in the lemma is satisfied if and only if $M \cap \tilde{H}_j = K$.
Let now $N := M \cap \tilde{H}_j$. Then the subgroup $\mathrm{Fix}(N) \subseteq G$ fixing N contains the torsion group $T_j = \mathrm{Fix}(\tilde{H}_j)$. Moreover, if M is contained in some F_j, then also $N \subseteq F_j$, and $\mathrm{Fix}(N)$ contains the $\mathbb{Z}_p$-free group B_j fixing F_j. Since $B_j \oplus T_j = G$, we conclude that $N = K$.
If, on the other hand, $M \cap \tilde{H}_j = K$, then

$$\mathrm{Fix}(M) + T_j \;=\; G \;=\; \mathrm{Gal}(H_j/K)\;.$$

Since $\mathrm{Fix}(M) \subseteq G$ is of finite index, there exists a torsion-free subgroup $C \subseteq \mathrm{Fix}(M)$ such that $\mathrm{rank}_{\mathbb{Z}_p}(C) = \mathrm{rank}_{\mathbb{Z}_p}(G/T_j)$ and $\mathrm{Fix}(M) \subseteq C + T_j$. Then $C + T_j = G$, and therefore M is contained in the subfield $F_j := H_j^C$ of H_j that is fixed by C. □

Corollary 5.36. *Suppose that $\mathbb{L} \in U(\mathbb{K}, e(\mathbb{K}/K) + 1)$. For every choice of $F_j \subseteq \mathbb{K}$, we have $F_j \subseteq F_j^{(\mathbb{L})}$ for some choice of $F_j^{(\mathbb{L})} \subseteq \mathbb{L}$.*

Proof. Let $e := e(\mathbb{K}/K)$. We will apply the previous proposition to $M = F_j$. Suppose that $K \neq N$ denotes any subfield of M. We will show that there cannot exist a $\mathbb{Z}_p$-extension $W \in \mathcal{E}^{\subseteq \mathbb{L}}(K)$ that contains N and at the same time is unramified at $\mathfrak{p}_j$. Otherwise, the intermediate field $W_{e+1} \subseteq \mathbb{L}_{e+1} = \mathbb{K}_{e+1}$ was unramified at $\mathfrak{p}_j$. But then there would exist a $\mathbb{Z}_p$-extension in $\mathcal{E}^{\subseteq \mathbb{K}}(K)$ containing $W_{e+1} \supseteq N$, in contradiction to Proposition 5.33, (ii).
Now Proposition 5.35 implies that $M = F_j$ is contained in some choice of $F_j^{(\mathbb{L})}$. This concludes the proof of Corollary 5.36, and also the proof of Lemma 5.34. □

□

Note that it is well possible that $e(\mathbb{L}/K) > e(\mathbb{K}/K)$: This will happen if the rank of the torsion submodule of the quotient of $\mathrm{Gal}(\mathbb{L}/K)$ by the inertia subgroup of some $\mathfrak{p}_j \in \mathcal{P}(\mathbb{L})$ is strictly larger than the rank of the corresponding quotient of $\mathrm{Gal}(\mathbb{K}/K)$ by the inertia subgroup $\overline{I}_j^{(\mathbb{K})} \subseteq \mathrm{Gal}(\mathbb{K}/K)$, by the next result.

For any $\mathbb{Z}_p$-module M, we will denote by M° the torsion submodule of M.

Lemma 5.37. *Let $\mathbb{K}/K$ denote a $\mathbb{Z}_p^d$-extension, let $U := U(\mathbb{K}, e(\mathbb{K}/K) + 1)$. For $\mathbb{L} \in U$ and $\mathfrak{p}_j \in \mathcal{I} =: \{\mathfrak{p}_1, \ldots, \mathfrak{p}_t\}$, we denote by*

$$\overline{I}_j^{(\mathbb{L})} \;\subseteq\; \Gamma^{(\mathbb{L})} \;:=\; \mathrm{Gal}(\mathbb{L}/K)$$

the inertia subgroup of $\mathfrak{p}_j$ in $\mathbb{L}/K$, and we let $G_j^{(\mathbb{L})} := \Gamma^{(\mathbb{L})}/\overline{I}_j^{(\mathbb{L})}$, $1 \leq j \leq t$. In particular, $G_j^{(\mathbb{L})} = \Gamma^{(\mathbb{L})}$ if $\mathfrak{p}_j \notin \mathcal{P}(\mathbb{L}) = \mathcal{P}(\mathbb{K})$.

(i) Then $\mathrm{rank}_p((G_j^{(\mathbb{L})})^\circ) \geq \mathrm{rank}_p((G_j^{(\mathbb{K})})^\circ)$ for every $j \in \{1, \ldots, t\}$.

(ii) If $\mathrm{rank}_p((G_j^{(\mathbb{L})})^\circ) = \mathrm{rank}_p((G_j^{(\mathbb{K})})^\circ)$ for every $j \in \{1, \ldots, t\}$, then $e(\mathbb{L}/K) = e(\mathbb{K}/K)$.

(iii) *If on the other hand* $\mathrm{rank}_p((G_j^{(\mathbb{L})})^\circ) > \mathrm{rank}_p((G_j^{(\mathbb{K})})^\circ)$ *for some* j*, then* $e(\mathbb{L}/K) > e(\mathbb{K}/K)$.
More generally, if $U = U(\mathbb{K}, n+1)$ *for any* $n \geq e(\mathbb{K}/K)$, $\mathbb{L} \in U$ *and if* $\mathrm{rank}_p((G_j^{(\mathbb{L})})^\circ) > \mathrm{rank}_p((G_j^{(\mathbb{K})})^\circ)$ *for some* j*, then* $e(\mathbb{L}/K) > n$.

Proof. (i) Let $\mathfrak{p}_j \in \mathcal{P}(\mathbb{K}) = \mathcal{P}(\mathbb{L})$. Let H_j and F_j, respectively, $H_j^{(\mathbb{L})}$ and $F_j^{(\mathbb{L})}$, denote the fields introduced in the proofs of Proposition 5.31 and Lemma 5.34, (ii). Then

$$\mathrm{rank}_p((G_j^{(\mathbb{K})})^\circ) \;=\; \mathrm{rank}_p(\mathrm{Gal}(F_j/K)) \;,$$

since $\mathrm{Gal}(F_j/K)$ is isomorphic to the torsion subgroup of the finitely generated $\mathbb{Z}_p$-module $\mathrm{Gal}(H_j/K) \cong G_j^{(\mathbb{K})}$. Analogously,

$$\mathrm{rank}_p((G_j^{(\mathbb{L})})^\circ) \;=\; \mathrm{rank}_p(\mathrm{Gal}(F_j^{(\mathbb{L})}/K)) \;.$$

Since we have shown in Corollary 5.36 that $F_j \subseteq F_j^{(\mathbb{L})}$ for a suitably chosen $F_j^{(\mathbb{L})}$, it follows that

$$\mathrm{rank}_p((G_j^{(\mathbb{L})})^\circ) \;\geq\; \mathrm{rank}_p((G_j^{(\mathbb{K})})^\circ) \;,$$

proving (i).

(ii) If $\mathrm{rank}_p((G_j^{(\mathbb{L})})^\circ) = \mathrm{rank}_p((G_j^{(\mathbb{K})})^\circ)$, then

$$\mathrm{rank}_p(\mathrm{Gal}(F_j^{(\mathbb{L})}/K)) \;=\; \mathrm{rank}_p(\mathrm{Gal}(F_j/K)) \;.$$

But $F_j \subseteq F_j^{(\mathbb{L})}$, and each maximal cyclic subextension of F_j of degree p^k over K is contained in some $\mathbb{Z}_p$-extension M that ramifies in N_{k+1}/N_k (compare Proposition 5.33, (i)). Therefore $F_j = F_j^{(\mathbb{L})}$, since otherwise, there would exist a maximal cyclic subextension M of F_j that is contained in some extension $M^{(\mathbb{L})} \subseteq F_j^{(\mathbb{L})}$ of degree p over M. If $[M:K] = p^k$, then $k \leq e := e(\mathbb{K}/K)$, and therefore $M^{(\mathbb{L})} \subseteq \mathbb{L}_{e+1} = \mathbb{K}_{e+1}$. Then there exists a $\mathbb{Z}_p$-extension $N \in \mathcal{E}^{\subseteq \mathbb{K}}(K)$ of K such that $M \subseteq M^{(\mathbb{L})} \subseteq N$ and such that $\mathfrak{p}_j$ is unramified in $M^{(\mathbb{L})} = N_{k+1}$, in contradiction to Proposition 5.33.

(iii) Suppose that $U = U(\mathbb{K}, n+1)$ for some $n \geq e(\mathbb{K}/K)$, and that

$$\begin{aligned} \mathrm{rank}_p(\mathrm{Gal}(F_j^{(\mathbb{L})}/K)) \;&=\; \mathrm{rank}_p((G_j^{(\mathbb{L})})^\circ) \\ &>\; \mathrm{rank}_p((G_j^{(\mathbb{K})})^\circ) \;=\; \mathrm{rank}_p(\mathrm{Gal}(F_j/K)) \end{aligned}$$

for some $\mathbb{L} \in U$ and some $j \in \{1, \ldots, t\}$.
Since $n \geq e(\mathbb{K}/K)$, we have $\mathcal{P}(\mathbb{L}) = \mathcal{P}(\mathbb{K})$, by Lemma 5.34, (i). Therefore $\mathbb{K} \in U(\mathbb{L}, n+1)$. If $e(\mathbb{L}/K) \leq n$, then (i) implies that

$$\mathrm{rank}_p((G_j^{(\mathbb{K})})^\circ) \;\geq\; \mathrm{rank}_p((G_j^{(\mathbb{L})})^\circ) \;,$$

yielding a contradiction. This shows that $e(\mathbb{L}/K) > n$.

□

Definition 5.38. Let $d \in \mathbb{N}$. Let $\mathcal{E}^d(K)$ denote the set of $\mathbb{Z}_p^d$-extensions of K, and let $\mathbb{K} \in \mathcal{E}^d(K)$. We use the notation introduced in the previous lemma, i.e., we write $\mathcal{I} = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_t\}$ and $G_j^{(\mathbb{K})} := \Gamma^{(\mathbb{K})}/\overline{I_j}^{(\mathbb{K})}$, $1 \leq j \leq t$.
For $n \in \mathbb{N}$, we define

$$\mathcal{U}(\mathbb{K}, n) := \left\{ \mathbb{L} \in \mathcal{E}(\mathbb{K}, n) \mid \operatorname{rank}_p((G_j^{(\mathbb{L})})^\circ) \leq \operatorname{rank}_p((G_j^{(\mathbb{K})})^\circ)\ ,\ 1 \leq j \leq t \right\}.$$

Then the $\mathcal{U}(\mathbb{K}, n)$ define a topology on $\mathcal{E}^d(K)$ (see Proposition 5.39 below), which we call the ***R*-topology** on $\mathcal{E}^d(K)$.

Proposition 5.39. *$\mathcal{U}(\mathbb{K}, n) \subseteq U(\mathbb{K}, n)$ for every $\mathbb{K} \in \mathcal{E}^d(K)$ and every $n \in \mathbb{N}$. The $\mathcal{U}(\mathbb{K}, n)$, together with $\emptyset$ and $\mathcal{E}^d(K)$, generate a topology on $\mathcal{E}^d(K)$. $e(\mathbb{L}/K)$ is locally constant with respect to this topology.*

Proof. If $\mathbb{L} \in \mathcal{U}(\mathbb{K}, n)$ and $\mathfrak{p}_j \in \mathcal{I}$ is unramified in $\mathbb{K}/K$, then

$$\operatorname{rank}_p((G_j^{(\mathbb{L})})^\circ) \leq \operatorname{rank}_p((G_j^{(\mathbb{K})})^\circ) = 0\,.$$

If $\mathfrak{p}_j$ was ramified in $\mathbb{L}/K$, then $\mathbb{L}$ would have to contain a $\mathbb{Z}_p$-extension M of K such that $\mathfrak{p}_j \in \mathcal{P}(M)$. Since $\operatorname{rank}_p((G_j^{(\mathbb{L})})^\circ) = 0$, the Galois group $\operatorname{Gal}(H_j^{(\mathbb{L})}/K)$ of the maximal subextension $H_j^{(\mathbb{L})} \subseteq \mathbb{L}$ which is unramified at $\mathfrak{p}_j$ (compare the proof of Proposition 5.31) is $\mathbb{Z}_p$-free of rank $d_j \leq d$. If $\mathfrak{p}_j \in \mathcal{P}(\mathbb{L})$, then $d_j < d$. This means that M could be chosen such that $M \cap H_j^{(\mathbb{L})} = K$, i.e., such that $\mathfrak{p}_j$ was totally ramified in M/K. However, since $M_n \subseteq \mathbb{L}_n = \mathbb{K}_n$, $\mathfrak{p}_j$ cannot ramify in M_n/K, yielding a contradiction. Therefore $\mathcal{P}(\mathbb{L}) \subseteq \mathcal{P}(\mathbb{K})$, i.e., $\mathbb{L} \in U(\mathbb{K}, n)$.

The intersection of two sets $\mathcal{U}(\mathbb{K}, n_1)$ and $\mathcal{U}(\tilde{\mathbb{K}}, n_2)$ is a finite union of sets of this type (compare the proof of Lemma 3.25, (i), and the proof of Remark 5.9). Indeed, we may assume that $n_1 \geq n_2$. Then $\mathcal{U}(\mathbb{K}, n_1) \cap \mathcal{U}(\tilde{\mathbb{K}}, n_2)$ is the set of $\mathbb{Z}_p$-extensions $\mathbb{L} \in \mathcal{E}(\mathbb{K}, n_1)$ satisfying

$$\operatorname{rank}_p((G_j^{(\mathbb{L})})^\circ) \leq m_j := \min(\{\operatorname{rank}_p((G_j^{(\mathbb{K})})^\circ), \operatorname{rank}_p((G_j^{(\tilde{\mathbb{K}})})^\circ)\})$$

for every $j \in \{1, \ldots, t\}$. This set might be empty. Otherwise, we can choose a set $I \subseteq \mathbb{N}_0^t$ of tuples $(n_1, \ldots, n_t)$ such that $n_j \leq m_j$ for every $1 \leq j \leq t$, and such that

- for every $(\underline{n}) = (n_1, \ldots, n_t) \in I$, there exists some $\mathbb{L}^{(\underline{n})} \in \mathcal{E}(\mathbb{K}, n_1)$ such that $\operatorname{rank}_p((G_j^{(\mathbb{L}^{(\underline{n})})})^\circ) = n_j$, $1 \leq j \leq t$, and
- for every $\mathbb{M} \in \mathcal{U}(\mathbb{K}, n_1) \cap \mathcal{U}(\tilde{\mathbb{K}}, n_2)$, there exists some tuple

$$(\underline{n}) = (n_1, \ldots, n_t) \in I$$

such that $\operatorname{rank}_p((G_j^{(\mathbb{M})})^\circ) \leq n_j$, $1 \leq j \leq t$.

Note that $|I| \leq \prod_{j=1}^{t} (m_j + 1) < \infty$.

Then $\mathcal{U}(\mathbb{K}, n_1) \cap \mathcal{U}(\tilde{\mathbb{K}}, n_2) = \bigcup_{(\underline{n}) \in I} \mathcal{U}(\mathbb{L}^{(\underline{n})}, n_1)$.

Finally, the last statement follows from Lemma 5.37, (i) and (ii). □

Since $e(\mathbb{L}/K)$ is locally constant with respect to the R-topology, this topology allows a full use of Theorem 5.30 and therefore is suitable for our Fukuda-theoretic method. We will conclude the present section by pointing out one disadvantage of the R-topology. Namely, the space $\mathcal{E}^d(K)$ usually will not be compact with respect to this topology.

Lemma 5.40. *Let $d, i \in \mathbb{N}$, and suppose that $d \geq 2i$. For every $\mathbb{Z}_p^d$-extension $\mathbb{L}$ of K, we let $\mathcal{E}^{i,\subseteq\mathbb{L}}(K)$ denote the subset of $\mathbb{Z}_p^i$-extensions of K contained in $\mathbb{L}$.*
Then $\mathcal{E}^{i,\subseteq\mathbb{L}}(K)$ is compact with respect to the R-topology if and only if there exists a set P of primes of K such that $\mathcal{P}(M) = P$ for every $\mathbb{Z}_p$-extension $M \subseteq \mathbb{L}$ of K.

Proof. Let us first assume that $\mathcal{P}(M) = P$ for a suitable set P and every $M \in \mathcal{E}^{\subseteq\mathbb{L}}(K)$. We will show that in this case, the Greenberg, Greenberg-R and R-topologies on $\mathcal{E}^{i,\subseteq\mathbb{L}}(K)$ coincide.

Indeed, it is obvious that the assumption implies that $\mathcal{E}(\mathbb{K}, n) = U(\mathbb{K}, n)$ for each $\mathbb{K} \in \mathcal{E}^{i,\subseteq\mathbb{L}}(K)$ and every $n \in \mathbb{N}_0$. Moreover, Proposition 5.35 implies that $U(\mathbb{K}, n) = \mathcal{U}(\mathbb{K}, n)$ for each $\mathbb{K} \in \mathcal{E}^{i,\subseteq\mathbb{L}}(K)$ and every $n \geq e(\mathbb{K}/K) + 1$, since either every $\tilde{\mathbb{K}} \in U(\mathbb{K}, n) = \mathcal{E}(\mathbb{K}, n)$ is unramified at $\mathfrak{p}_j$, or $\mathfrak{p}_j \in \mathcal{P}(\mathbb{K}) = P$ and

$$H_j^{(\tilde{\mathbb{K}})} \;=\; F_j^{(\tilde{\mathbb{K}})} \;=\; F_j^{(\mathbb{K})} \;=\; H_j^{(\mathbb{K})}$$

for every $\tilde{\mathbb{K}} \in U(\mathbb{K}, n)$.

Therefore, under this assumption, $\mathcal{E}^{i,\subseteq\mathbb{L}}(K)$ is compact by Remark 5.5 (note that the proof of this remark goes through for $\mathcal{E}^{i,\subseteq\mathbb{L}}(K)$ instead of $\mathcal{E}^i(K)$).

Now we assume that there exist two $\mathbb{Z}_p$-extensions $M, N \subseteq \mathbb{L}$ of K such that $\mathcal{P}(M) \neq \mathcal{P}(N)$. In view of Lemma 5.7, (i), we may assume that

$$\mathcal{P}(M) \;=\; \mathcal{P}(\mathbb{L}) \;=:\; P \quad \text{and} \quad \mathcal{P}(N) \;\subsetneqq\; P\;.$$

We will show that in this case, $e(\mathbb{M}/K)$ is unbounded on $\mathcal{E}^{i,\subseteq\mathbb{L}}(K)$. Since $e(\mathbb{M}/K)$ is locally constant with respect to the R-topology, this will show that $\mathcal{E}^{i,\subseteq\mathbb{L}}(K)$ cannot be compact with regard to this topology.

We will make use of the following result.

Proposition 5.41. *Suppose that $\mathbb{L}/K$ denotes a $\mathbb{Z}_p^d$-extension, let $i < d$. Let $\mathfrak{p}_j \in \mathcal{P}(\mathbb{L})$. Let $\mathbb{K} \in \mathcal{E}^{i,\subseteq\mathbb{L}}(K)$ be such that $\mathfrak{p}_j$ is unramified in $\mathbb{K}$ (so that in particular, $\mathrm{rank}_p((G_j^{(\mathbb{K})})^\circ) = 0$, where $G_j^{(\mathbb{K})} = \Gamma^{(\mathbb{K})}/\overline{I_j}^{(\mathbb{K})}$, as above).*
If $n_j \in \mathbb{N}_0$ denotes the largest integer such that there exists some $\tilde{\mathbb{K}} \in \mathcal{E}^{i,\subseteq\mathbb{L}}(K)$ satisfying $\mathrm{rank}_p((G_j^{(\tilde{\mathbb{K}})})^\circ) = n_j$, then $n_j > 0$. Moreover, define

$$\mathcal{A}_j^{n_j} \;:=\; \{\tilde{\mathbb{K}} \in \mathcal{E}^{i,\subseteq\mathbb{L}}(K) \mid \mathrm{rank}_p((G_j^{(\tilde{\mathbb{K}})})^\circ) = n_j\}\;.$$

Then for every $n \in \mathbb{N}$, there exists some $\tilde{\mathbb{K}} \in \mathcal{E}(\mathbb{K}, n) \cap \mathcal{A}_j^{n_j}$.

Proof. Let $\tilde{\mathbb{L}} \subseteq \mathbb{L}$ denote the composite of all $\mathbb{Z}_p$-extensions in $\mathcal{E}^{\subseteq\mathbb{L}}(K)$ that are unramified at $\mathfrak{p}_j$. If $\tilde{\mathbb{L}}/K$ is a $\mathbb{Z}_p^t$-extension, then $n_j \leq \min(i, d-t)$. Note that

every $M \in \mathcal{E}^{\subseteq \mathbb{L}}(K)$ unramified at $\mathfrak{p}_j$ is contained in $\tilde{\mathbb{L}}$. In particular, $\mathbb{K} \subseteq \tilde{\mathbb{L}}$, by assumption.

We choose $\mathbb{Z}_p$-extensions $M^1, \ldots, M^i \in \mathcal{E}^{\subseteq \mathbb{L}}(K)$ such that $\mathbb{K} = M^1 \cdot \ldots \cdot M^i$. We may assume that $M^l \cap \prod_{k \neq l} M^k = K$ for each l, respectively.

Let $n \in \mathbb{N}$ be arbitrary. We consider the composite $M^i \cdot L$, where $L \subseteq \mathbb{L}$ denotes any $\mathbb{Z}_p$-extension of K that is ramified at $\mathfrak{p}_j$. Every $\mathbb{Z}_p$-extension $V \subseteq M^i \cdot L$ of K, $V \neq M^i$, is ramified at $\mathfrak{p}_j$ (compare Lemma 3.19, (ii)). We choose some $V \subseteq M^i \cdot L$ such that $V \in \mathcal{E}(M^i, n)$. Then

$$\mathbb{V} := M^1 \cdot \ldots \cdot M^{i-1} \cdot V$$

is a $\mathbb{Z}_p^i$-extension of K contained in $\mathcal{E}(\mathbb{K}, n)$, and $\mathrm{rank}_p((G_j^{(\mathbb{V})})^\circ) = 1$. In particular, this shows that $n_j \geq 1$.

Inductively, suppose that we have obtained a $\mathbb{Z}_p^i$-extension

$$\tilde{\mathbb{K}} \;=\; M^1 \cdot \ldots \cdot M^{i-r} \cdot V^{i-r+1} \cdot \ldots \cdot V^i \;\in\; \mathcal{E}(\mathbb{K}, n)$$

such that $\mathrm{rank}_p((G_j^{(\tilde{\mathbb{K}})})^\circ) = r \geq 1$, $(M^1 \cdot \ldots \cdot M^{i-r}) \cap (V^{i-r+1} \cdot \ldots \cdot V^i) = K$, and such that $(V^{i-r+1} \cdot \ldots \cdot V^i) \cap \tilde{\mathbb{L}}$ is finite over K. Recall that $\mathfrak{p}_j$ is unramified in $M^1 \cdot \ldots \cdot M^{i-r}$.

If $r < n_j \leq d - t$, then we may choose some $L \in \mathcal{E}^{\subseteq \mathbb{L}}(K)$, ramified at $\mathfrak{p}_j$, such that

$$(L \cdot M^{i-r}) \cap (M^1 \cdot \ldots \cdot M^{i-r-1} \cdot V^{i-r+1} \cdot \ldots \cdot V^i) \;=\; K$$

and such that

$$(M^{i-r} \cdot L \cdot V^{i-r+1} \cdot \ldots \cdot V^i) \cap \tilde{\mathbb{L}}$$

is a finite extension of M^{i-r}.

Let $M^{i-r} \neq V \subseteq M^{i-r} \cdot L$ denote any $\mathbb{Z}_p$-extension of K contained in $\mathcal{E}(M^{i-r}, n)$. Then $(V \cdot V^{i-r+1} \cdot \ldots \cdot V^i)$ does not contain any $\mathbb{Z}_p$-extension of K which is unramified at $\mathfrak{p}_j$. Therefore Proposition 5.35 implies that the Galois group of the maximal abelian extension of K contained in $V \cdot V^{i-r+1} \cdot \ldots \cdot V^i$ and unramified at $\mathfrak{p}_j$ is finite of rank $r+1$, by our induction hypothesis and the choice of V.

Therefore

$$\mathbb{V} := M^1 \cdot \ldots \cdot M^{i-r-1} \cdot V \cdot V^{i-r+1} \cdot \ldots \cdot V^i \;\in\; \mathcal{E}(\tilde{\mathbb{K}}, n) \;=\; \mathcal{E}(\mathbb{K}, n)$$

satisfies $\mathrm{rank}_p((G_j^{(\mathbb{V})})^\circ) = r + 1$.

Inductively, we construct a $\mathbb{Z}_p^i$-extension $\mathbb{W} \in \mathcal{E}(\mathbb{K}, n)$ such that

$$\mathrm{rank}_p((G_j^{(\mathbb{W})})^\circ) = n_j \; .$$

□

We will now conclude the proof of Lemma 5.40. Fix a prime $\mathfrak{p}_j \in \mathcal{P}(\mathbb{L})$ such that there exists some $N \in \mathcal{E}^{\subseteq \mathbb{L}}(K)$ unramified at $\mathfrak{p}_j$. We want to show that $e(\mathbb{M}/K)$ is unbounded on $\mathcal{E}^{i, \subseteq \mathbb{L}}(K)$.

Suppose that $d \geq 2i$. As in the proof of Proposition 5.41, we let

$$\tilde{\mathbb{L}} \;:=\; L^1 \cdot \ldots \cdot L^t \;\subseteq\; \mathbb{L}$$

denote the composite of all $\mathbb{Z}_p$-extensions in $\mathcal{E}^{\subseteq \mathbb{L}}(K)$ that are unramified at $\mathfrak{p}_j$. We distinguish two cases.

If $t \geq i$, then we may apply Proposition 5.41 to $\mathbb{K} := L^1 \cdot \ldots \cdot L^i \subseteq \mathbb{L}$. Lemma 5.37, (iii) then implies that $e(\mathbb{M}/K)$ is unbounded in any neighbourhood of $\mathbb{K}$.

If $1 \leq t < i$, then we let $\mathbb{K} \in \mathcal{E}^{i,\subseteq \mathbb{L}}(K)$ denote any $\mathbb{Z}_p^i$-extension of K which contains the $\mathbb{Z}_p$-extension N of K that is unramified at $\mathfrak{p}_j$. We claim that in every given neighbourhood $\mathcal{E}(\mathbb{K}, n)$, $n \geq e(\mathbb{K}/K) + 1$, we find some $\mathbb{W} \in \mathcal{E}^{i,\subseteq \mathbb{L}}(K)$ such that

$$\mathrm{rank}_p((G_j^{(\mathbb{W})})^\circ) \;>\; \mathrm{rank}_p((G_j^{(\mathbb{K})})^\circ) \;=:\; m_j \;.$$

Indeed, we write $\mathbb{K} = M^1 \cdot \ldots \cdot M^i$, with $M^1, \ldots, M^r$ ramified at $\mathfrak{p}_j$ for some $r \in \mathbb{N}$, $r \geq m_j$, and with $M^{r+1} \cdot \ldots \cdot M^i$ unramified at $\mathfrak{p}_j$. Suppose that $(M^1 \cdot \ldots \cdot M^{m_j}) \cap \tilde{\mathbb{L}}$ is a finite extension of K.

We proceed as in the proof of Proposition 5.41: Since $d - t > i$, there exists a $\mathbb{Z}_p$-extension $L \subseteq \mathbb{L}$ of K, ramified at $\mathfrak{p}_j$, such that

$$(L \cdot M^i) \cap (M^1 \cdot \ldots \cdot M^{i-1}) \;=\; K$$

and such that

$$(M^1 \cdot \ldots \cdot M^{m_j} \cdot L \cdot M^i) \;\cap\; \tilde{\mathbb{L}}$$

is a finite extension of M^i.

Let $V \subseteq L \cdot M^i$, $V \neq M^i$, denote a $\mathbb{Z}_p$-extension of K contained in $\mathcal{E}(M^i, n)$. Then $V \cdot M^1 \cdot \ldots \cdot M^{m_j}$ does not contain any $\mathbb{Z}_p$-extension of K which is unramified at $\mathfrak{p}_j$.

Letting

$$\mathbb{W} \;:=\; V \cdot M^1 \cdot \ldots \cdot M^{i-1} \;,$$

we may conclude that $\mathbb{W} \in \mathcal{E}(\mathbb{K}, n)$ satisfies $\mathrm{rank}_p((G_j^{(\mathbb{W})})^\circ) > m_j$, as in the proof of Proposition 5.41.

Therefore $e(\mathbb{W}/K) \geq n + 1$, by Lemma 5.37, (iii). Since $n \geq e(\mathbb{K}/K) + 1$ was arbitrary, the statement follows. □

Remark 5.42. Lemma 5.40 shows that, as in the case $d = 1$, we will usually not be able to gather global information (such as global boundedness on $\mathcal{E}^d(K)$) about the generalised Iwasawa invariants (compare Remarks 3.26, (1)).

5.6 Finiteness of ranks

In our approach for the study of classical Iwasawa invariants, developed in the third chapter, the following observation provided a link between characteristic polynomials of Greenberg modules and the f-ranks which then could be studied via Fukuda's Theorem:

Let L/K denote a $\mathbb{Z}_p$-extension, $A = \varprojlim A_n^{(L)}$, and let $F_A(T) \in \mathbb{Z}_p[T]$ denote the characteristic polynomial of A (compare Definition 1.29). Then $F_A(T)$ has degree $\lambda(L/K)$. If $f(T) \in \mathbb{Z}_p[T]$ denotes any irreducible distinguished polynomial, then

$$\operatorname{rank}_f(A) := v_p(|A/(f \cdot A)|) < \infty \quad \Longleftrightarrow \quad f \nmid F_A \, .$$

This property of f-ranks is based on the following two facts:
(1) $\operatorname{rank}_f(A) < \infty \quad \Longleftrightarrow \quad \operatorname{rank}_f(E_A) < \infty$, where

$$E_A \, = \, \bigoplus_{i=1}^{s} \Lambda/(p^{n_i}) \, \oplus \, \bigoplus_{j=1}^{t} \Lambda/(f_j(T)^{l_j})$$

denotes the elementary Λ-module attached to A (this follows from Proposition 3.41).
(2) If $f \in \Lambda$ is irreducible, then $|\Lambda/(f)| = \infty$. If $g, h \in \Lambda$ are coprime, then $|\Lambda/(g,h)| < \infty$ (compare Lemma 1.17).

In order to adapt our method for the case of $d > 1$, we will have to study whether our ranks of Λ_d-modules (to be defined below) satisfy analogous properties.

We immediately see that it will not be sufficient to simply consider, for some element $f \in \Lambda_d = \mathbb{Z}_p[[T_1, \ldots, T_d]]$ and a given finitely generated torsion Λ_d-module A, the quotient $A/(f \cdot A)$. Indeed, this quotient will in general be an infinite group. Suppose, for example, that $A = \Lambda_d/(T_1)$. If $d \geq 2$, then $T_2 \in \Lambda_d$ is an irreducible element coprime to the characteristic power series T_1 of A, but

$$A/(T_2 \cdot A) \, = \, \Lambda_d/(T_1, T_2) \, \cong \, \mathbb{Z}_p[[T_3, \ldots, T_d]]$$

is infinite.

This example already hints at how to define an appropriate rank: the quotient

$$A/((T_2, \ldots, T_d, p) \cdot A) \, \cong \, \mathbb{Z}_p/p\mathbb{Z}_p \, \cong \, \mathbb{Z}/p\mathbb{Z} \, ,$$

for example, is finite. The ranks that we will introduce below will be the orders of quotients $A/(I \cdot A)$, where $I \subseteq \Lambda_d$ denotes an ideal having d suitably chosen generators. Note that this obviously generalises the case $d = 1$.

If A denotes an arbitrary finitely generated torsion Λ_d-module, then Theorem 2.23 implies that A is pseudo-isomorphic to some elementary Λ_d-module

$$E_A \, = \, \bigoplus_{i=1}^{s} \Lambda_d/\mathfrak{p}_i^{n_i} \, ,$$

where $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ denote prime ideals of Λ_d of height one, i.e., principal prime ideals $\mathfrak{p}_i = (g_i)$, respectively. $F_A := \prod_{i=1}^{s} g_i^{n_i}$ is called the characteristic power series of A (compare Section 4.3).

We start with several technical results.

Proposition 5.43. *Let $d \in \mathbb{N}$, and suppose that $g, h \in \Lambda_d$ are relatively prime. Then there exist pseudo-isomorphisms*

$$\varphi : \Lambda_d/(gh) \xrightarrow{\sim} \Lambda_d/(g) \oplus \Lambda_d/(h)$$

and

$$\psi : \Lambda_d/(g) \oplus \Lambda_d/(h) \xrightarrow{\sim} \Lambda_d/(gh) \ .$$

Proof. This generalises Example 1.21. We give an adaption of the corresponding proof given in [Wa 97], Lemma 13.8.

Let

$$\varphi : \Lambda_d/(gh) \longrightarrow \Lambda_d/(g) \oplus \Lambda_d/(h)$$

be the Λ_d-module homomorphism mapping the coset of an element $x \in \Lambda_d$ in $\Lambda_d/(gh)$ to the tuple $(\overline{x}, \overline{x})$ of the corresponding cosets in the quotients $\Lambda_d/(g)$ and $\Lambda_d/(h)$, respectively. This is well-defined, and moreover injective because Λ_d is a unique factorisation domain by Proposition 2.17, (iv).

Let $(\overline{a}, \overline{b}) \in \Lambda_d/(g) \oplus \Lambda_d/(h)$ be arbitrary, but fixed. We choose representatives $a, b \in \Lambda_d$ of $\overline{a}$ and $\overline{b}$, respectively. If $a - b \in (g, h)$, then $a - b = \alpha \cdot g + \beta \cdot h$ for suitable elements $\alpha, \beta \in \Lambda_d$. Let

$$c \ := \ a - \alpha \cdot g \ = \ b + \beta \cdot h \ .$$

Then we may conclude that

$$(\overline{a}, \overline{b}) \ = \ \varphi(\overline{c}) \ \in \ \mathrm{Im}(\varphi) \ .$$

If $(\overline{a}, \overline{b}) \in \Lambda_d/(g) \oplus \Lambda_d/(h)$ is arbitrary, then $\lambda \cdot (\overline{a}, \overline{b}) = (\overline{\lambda a}, \overline{\lambda b}) \in \mathrm{Im}(\varphi)$ for every $\lambda \in (g, h)$, by the above. But this means that the cokernel of φ is annihilated by every element $\lambda \in (g, h)$. Since g and h are relatively prime, Remarks 2.20, (2) and (3) imply that $\mathrm{coker}(\varphi)$ is a pseudo-null Λ_d-module. Since also $\ker(\varphi) = \{\overline{0}\}$ is pseudo-null, this proves that φ is a pseudo-isomorphism.

Since both $\Lambda_d/(gh)$ and $\Lambda_d/(g) \oplus \Lambda_d/(h)$ are finitely generated torsion Λ_d-modules, the existence of φ implies that there exists also a pseudo-isomorphism

$$\psi : \Lambda_d/(g) \oplus \Lambda_d/(h) \xrightarrow{\sim} \Lambda_d/(gh)$$

(compare Remarks 2.22, (1)). This fact may also easily be proved directly:

By the above, $\Lambda_d/(gh)$ is isomorphic to a submodule $M \subseteq \Lambda_d/(g) \oplus \Lambda_d/(h)$ such that the quotient

$$(\Lambda_d/(g) \oplus \Lambda_d/(h)) \,/\, M$$

is a pseudo-null Λ_d-module. This means that there exists an element $P \in \Lambda_d$, coprime to $g \cdot h$, such that $P \cdot (\overline{x}, \overline{y}) \in M$ for each $(\overline{x}, \overline{y}) \in \Lambda_d/(g) \oplus \Lambda_d/(h)$ (compare Remarks 2.20, (3)).

Moreover, if

$$P \cdot (\overline{x}, \overline{y}) \ = \ (\overline{Px}, \overline{Py}) \ = \ (\overline{0}, \overline{0})$$

in $\Lambda_d/(g) \oplus \Lambda_d/(h)$, then $(\overline{x}, \overline{y}) = (\overline{0}, \overline{0})$ since Λ_d is a unique factorisation domain and P is coprime to $g \cdot h$. This shows that the composite map

$$\psi : \Lambda_d/(g) \oplus \Lambda_d/(h) \xrightarrow{\cdot P} M \xrightarrow{\varphi^{-1}} \Lambda_d/(gh)$$

induced by multiplication by P is injective.

Moreover, the image of $\Lambda_d/(g) \oplus \Lambda_d/(h)$ under this map contains

$$\varphi^{-1}(P \cdot (\overline{1}, \overline{1})) \;=\; \varphi^{-1}(\overline{P}, \overline{P}) \;=\; \overline{P}\;.$$

Since $\Lambda_d/(gh, P)$ is pseudo-null, this proves that the cokernel of ψ is pseudo-null, and therefore ψ is a pseudo-isomorphism. □

Proposition 5.44. *If $\varphi_1 : A \xrightarrow{\sim} E_A$ and $\varphi_2 : B \xrightarrow{\sim} E_B$ denote two pseudo-isomorphisms of Λ_d-modules, then*

$$\varphi : A \oplus B \;\longrightarrow\; E_A \oplus E_B\;, \quad (a, b) \;\longmapsto\; (\varphi_1(a), \varphi_2(b))\;,$$

is a pseudo-isomorphism. In particular, the direct sum of two pseudo-null Λ_d-modules is pseudo-null.

Proof. The map φ obviously is a Λ_d-module homomorphism. We have to show that the kernel and the cokernel of φ are pseudo-null Λ_d-modules. Recall that a finitely generated Λ_d-module M is called pseudo-null if and only if the localisation $M_\mathfrak{p}$ is trivial for every prime ideal $\mathfrak{p} \subseteq \Lambda_d$ of height at most one. Now $\ker(\varphi) = \ker(\varphi_1) \oplus \ker(\varphi_2)$ and

$$\operatorname{coker}(\varphi) \;=\; (E_A \oplus E_B)/(\operatorname{im}(\varphi_1) \oplus \operatorname{im}(\varphi_2)) \;\cong\; E_A/\operatorname{im}(\varphi_1) \oplus E_B/\operatorname{im}(\varphi_2)\;.$$

Therefore both $\ker(\varphi)$ and $\operatorname{coker}(\varphi)$ are finitely generated over Λ_d, and the statement follows from the general fact that for a Λ_d-module $M = M_1 \oplus M_2$ and a prime $\mathfrak{p} \subseteq \Lambda_d$, we have $M_\mathfrak{p} \cong (M_1)_\mathfrak{p} \oplus (M_2)_\mathfrak{p}$. This can be proved by using, for example, Lemma 2.4 in [Ei 95].

In particular, if A and B are pseudo-null, then

$$(A \oplus B)_\mathfrak{p} \;\cong\; A_\mathfrak{p} \oplus B_\mathfrak{p} \;=\; \{0\}$$

for every prime $\mathfrak{p} \subseteq \Lambda_d$ of height ≤ 1. □

Proposition 5.45. *Let A be a finitely generated torsion Λ_d-module, let*

$$E_A \;=\; \bigoplus_{i=1}^{s} \Lambda_d/(g_i^{n_i})$$

be the elementary Λ_d-module of A, and let $F_A \in \Lambda_d$ denote the characteristic power series attached to A. Suppose that $f \in \Lambda_d$ is irreducible.
Then f is coprime to F_A if and only if $E_A/(f \cdot E_A)$ is a pseudo-null Λ_d-module.

Proof. A finitely generated Λ_d-module M is pseudo-null if and only if it is annihilated by two relatively prime elements of Λ_d (compare Remarks 2.20, (2) and (3)). $E_A/(f \cdot E_A)$ is pseudo-null if and only if each summand $\Lambda_d/(g_i^{n_i}, f)$ is pseudo-null, by the previous proposition. This completes the proof. □

This result proves part of an analogon of the property mentioned at the beginning of the current section. The main difference when compared to the one-dimensional case concerns the observation that a Λ_1-module is pseudo-null if and only if it is finite (compare Remarks 2.20, (4)). Since this is not longer true if $d > 1$, our method gets much more involved in the higher-dimensional setting.

More precisely, whereas in the one-dimensional case, $E_A/(f \cdot E_A)$ will be finite for every $f \in \Lambda$ coprime to F_A, it is in general a non-trivial task to find elements $f_1, \ldots, f_d \in \Lambda_d$ such that, as in the above example,

$$E_A/((f_1, \ldots, f_d) \cdot E_A)$$

is finite, even if some $f \in \Lambda_d$ coprime to F_A is already known (of course we want to exclude the trivial case where one of the f_j is a unit, i.e., $(f_1, \ldots, f_d) = \Lambda_d$).

The following lemma shows that this is (at least in principle) always possible. Therefore this result is one of the main motivations for our method.

Lemma 5.46. *Let E_A denote an elementary Λ_d-module with characteristic power series F_A. Then we may choose $f_1, \ldots, f_d \in \Lambda_d$ such that*

- *$(f_1, \ldots, f_d)$ does not contain a unit of Λ_d,*
- *$E_A/((f_1, \ldots, f_d) \cdot E_A)$ is finite, and*
- *$\Lambda_d/(f_1, \ldots, f_d)$ is isomorphic to a finitely generated free $\mathbb{Z}_p$-module.*

Proof. Let $F_A = \mathfrak{p}_1^{n_1} \cdot \ldots \cdot \mathfrak{p}_s^{n_s}$ denote the characteristic power series of A, with irreducible elements $\mathfrak{p}_1, \ldots, \mathfrak{p}_s \in \Lambda_d$. If $f \in \Lambda_d$ denotes an irreducible element, then f is coprime to F_A if and only if the image of each $\mathfrak{p}_j$ in $\Lambda_d/(f)$ is different from zero.

We will use an inductive argument. First choose $f_1 \in \mathbb{Z}_p[T_1]$ distinguished with respect to T_1 (which is the same as being regular in $\mathbb{Z}_p[[T_1]]$ with respect to T_1 in the sense of Definition 4.9), and coprime to F_A. This is possible since there exist only finitely many irreducible divisors $\mathfrak{p}_j$ of F_A, whereas there exist infinitely many irreducible distinguished polynomials in $\mathbb{Z}_p[T_1]$.

Now we choose $f_2 \in \mathbb{Z}_p[T_2]$ distinguished with respect to T_2, and such that the image of each $\mathfrak{p}_j$ in $\Lambda_d/(f_1, f_2)$ is different from zero. Inductively, choose $f_3, \ldots, f_d \in \Lambda_d$ such that $f_i \in \mathbb{Z}_p[T_i]$ is regular with respect to T_i, and such that the residue classes $\overline{\mathfrak{p}_j}$ of $\mathfrak{p}_j$ are non-trivial in $\Lambda_d/(f_1, \ldots, f_i)$, $3 \leq i \leq d$. Again, this is possible since $\mathbb{Z}_p[T_i]$ contains infinitely many prime elements and since $f_1, \ldots, f_{i-1}$ do not affect the variable T_i, respectively.

Then

$$\Lambda_d/(f_1, \ldots, f_d) \;\cong\; \mathbb{Z}_p[T_1, \ldots, T_d]/(f_1, \ldots, f_d)$$

is isomorphic to $\mathbb{Z}_p^r$, with r being the sum of the degrees of the f_i with respect to T_i, respectively.

Indeed, we will prove that for every $i \leq d$, the quotient ring

$$\mathbb{Z}_p[[T_1, \ldots, T_i]]/(f_1, \ldots, f_i)\ ,$$

with $f_i \in \mathbb{Z}_p[T_i]$ distinguished, respectively, is $\mathbb{Z}_p$-free of rank equal to the sum of the degrees of the f_i. This is certainly true for $i = 1$, since we can divide with

remainder by the monic polynomial f_1 in the ring $\mathbb{Z}_p[[T_1]]$ (compare Lemma 1.10). Inductively, assume that

$$R \;:=\; \mathbb{Z}_p[[T_1,\ldots,T_i]]/(f_1,\ldots,f_i)$$

is isomorphic to $\mathbb{Z}_p^{\deg(f_1)+\ldots+\deg(f_i)}$.

The isomorphism

$$\mathbb{Z}_p[[T_1,\ldots,T_{i+1}]] \;\cong\; (\mathbb{Z}_p[[T_1,\ldots,T_i]])[[T_{i+1}]]$$

induces an isomorphism between $\mathbb{Z}_p[[T_1,\ldots,T_{i+1}]]/(f_1,\ldots,f_{i+1})$ and

$$((\mathbb{Z}_p[[T_1,\ldots,T_i]]/(f_1,\ldots,f_i))[[T_{i+1}]])/(f_{i+1}) \;=\; (R[[T_{i+1}]])/(f_{i+1})\;.$$

Again, since $f_{i+1} \in \mathbb{Z}_p[T_{i+1}] \subseteq R[[T_{i+1}]]$ is monic, we may divide with remainder by f_{i+1} in this ring. Therefore $R[[T_{i+1}]]/(f_{i+1})$ is isomorphic to $R^{\deg(f_{i+1})}$ as $\mathbb{Z}_p$-module (note that division with remainder in $R[[T_{i+1}]]$ is 'R-linear'). Using our induction hypothesis, the claim follows.

Remarks 5.47.

(1) The same proof works if each f_i is a monic polynomial in T_i with coefficients in $\mathbb{Z}_p[[T_1,\ldots,T_{i-1}]]$, respectively.

(2) In the case $f_i \in \mathbb{Z}_p[T_i]$, $1 \le i \le d$, a basis of the free $\mathbb{Z}_p$-module

$$Q \;:=\; \Lambda_d/(f_1.\ldots,f_d)$$

is given by the residue classes of the elements

$$T_1^{s_1}\cdot\ldots\cdot T_d^{s_d}\;,\quad 0 \le s_i < \deg(f_i)\;,\quad 1 \le i \le d\;.$$

Indeed, it is obvious that these elements generate Q. Moreover, the corresponding residue classes are $\mathbb{Z}_p$-linearly independent: Suppose that there exist elements

$$\lambda_{(s_1,\ldots,s_d)} \in \mathbb{Z}_p\;,\quad 0 \le s_i < \deg(f_i)\;,\quad 1 \le i \le d\;,$$

such that $\sum \lambda_{(s_1,\ldots,s_d)} \cdot T_1^{s_1}\cdot\ldots\cdot T_d^{s_d}$ yields the zero class in Q. Since Q is $\mathbb{Z}_p$-torsionfree, we may assume that at least one $\lambda_{(s_1,\ldots,s_d)}$ is not divisible by p. Then this coefficient is a unit in $\mathbb{Z}_p$, and therefore

$$T_1^{s_1}\cdot\ldots\cdot T_d^{s_d} \;=\; \sum_{(t_1,\ldots,t_d)\,\neq\,(s_1,\ldots,s_d)} \tilde{\lambda}_{(t_1,\ldots,t_d)} \cdot T_1^{t_1}\cdot\ldots\cdot T_d^{t_d} \;+\; \sum_{j=1}^{d} \mu_j f_j$$

for suitable elements $\tilde{\lambda}_{(t_1,\ldots,t_d)} \in \mathbb{Z}_p$, $\mu_j \in \Lambda_d$, respectively. We consider the coefficient of $T_1^{s_1}\cdot\ldots\cdot T_d^{s_d}$ on the right hand side. The fact that the $f_j \in \mathbb{Z}_p[T_j]$ are distinguished polynomials of degree $\deg(f_j) > t_j$, respectively, implies that this coefficient is divisible by p, yielding a contradiction.

We will now prove that $f_1,\ldots,f_d$ may be chosen such that furthermore,

$$E_A/((f_1,\ldots,f_d)\cdot E_A)$$

is finite. We will make use of the following fact.

Proposition 5.48. *Let $f_1, \ldots, f_d \in \Lambda_d$ be such that $Q := \Lambda_d/(f_1, \ldots, f_d)$ is isomorphic to a finitely generated free $\mathbb{Z}_p$-module. Let $\mathfrak{p} \in \Lambda_d$. Then the following statements are equivalent:*
(i) $\Lambda_d/(f_1, \ldots, f_d, \mathfrak{p}^n)$ is finite for some $n \in \mathbb{N}$,
(ii) the residue class of $\mathfrak{p}^n$ is no zero divisor in Q for some $n \in \mathbb{N}$,
(iii) multiplication by (the residue class of) $\mathfrak{p}$ is injective on Q.

Proof. We first note that statements (ii) and (iii) are obviously equivalent: If $\overline{\mathfrak{p}^n} \cdot \overline{x} = \overline{0}$ for some $\overline{x} \in Q$, then $\overline{\mathfrak{p}} \cdot \overline{\mathfrak{p}^{n-1}x} = \overline{0}$, so that either (iii) is false or $\overline{\mathfrak{p}^{n-1}x} = \overline{0}$. Inductively, we see that (iii) implies (ii). If, on the other hand, multiplication by $\mathfrak{p}$ is not injective on Q, then this also holds for multiplication by $\mathfrak{p}^n$, implying that (ii) is not true.

We will now show that (i) implies (iii). To this purpose, suppose that $\overline{x} \in Q$ denotes an element such that $\overline{\mathfrak{p}} \cdot \overline{x} = \overline{0}$. Then the annihilator ideal $\mathrm{Ann}(\overline{x}) \subseteq \Lambda_d$ of $\overline{x}$ contains $\mathfrak{p}, f_1, \ldots, f_d$. Since $|\Lambda_d/(f_1, \ldots, f_d, \mathfrak{p}^n)|$ is finite, by (i), the ideal $(f_1, \ldots, f_d, \mathfrak{p}^n) \subseteq \Lambda_d$ is of finite index. Then also $|\Lambda_d/(f_1, \ldots, f_d, \mathfrak{p})|$ is finite. This means that there exists an integer $r \in \mathbb{N}$ such that $\mathfrak{m}^r \subseteq \mathrm{Ann}(\overline{x})$, where $\mathfrak{m} = (p, T_1, \ldots, T_d)$ denotes the maximal ideal of Λ_d. In particular, this implies that $p^r \cdot \overline{x} = \overline{0}$. However, Q is $\mathbb{Z}_p$-torsionfree, and therefore $\overline{x} = \overline{0}$, proving (iii).

Finally, we will show that (iii) implies (i). We let $x := \mathfrak{p}^n$. Then $\overline{x} \neq \overline{0}$ in Q. Moreover, multiplication by $\overline{x}$ is a $\mathbb{Z}_p$-linear map $Q \longrightarrow Q$, and this map is injective by (iii). This means that the image $\overline{x} \cdot Q \subseteq Q$ is a $\mathbb{Z}_p$-module of rank equal to $\mathrm{rank}_{\mathbb{Z}_p}(Q)$, and therefore the quotient

$$Q/(\overline{x}) \cong \Lambda_d/(f_1, \ldots, f_d, \mathfrak{p}^n)$$

is finite. □

We return to the proof of Lemma 5.46. We want to show that the polynomials $f_1, \ldots, f_d$ may be chosen such that $\Lambda_d/(f_1, \ldots, f_d, \mathfrak{p}_i^{n_i})$ is finite for every $i \in \{1, \ldots, s\}$, where $F_A = \mathfrak{p}_1^{n_1} \cdot \ldots \cdot \mathfrak{p}_s^{n_s}$. This will follow from the following fact.

Claim 5.49. *$f_1, \ldots, f_d \in \Lambda_d$ as above may be chosen such that*

$$(f_1, \ldots, f_d) \subseteq \Lambda_d$$

is a prime ideal.

If we have shown this claim, then the lemma will follow at once, since by construction of the f_j, $\mathfrak{p}_i^{n_i} \notin (f_1, \ldots, f_d)$ for every i. This implies that none of the $\overline{\mathfrak{p}_i}$ is a zero divisor in the domain Q, and therefore each $\Lambda_d/(f_1, \ldots, f_d, \mathfrak{p}_i^{n_i})$ is finite, by the preceding proposition.

In order to prove Claim 5.49, we assume that the $f_j \in \mathbb{Z}_p[T_j]$ have been chosen in the special form

$$f_j = T_j + p^{k_j} ,$$

with suitable integers $k_j \in \mathbb{N}_0$, $1 \leq j \leq d$. Note that this is possible since on the one hand, the family $\{T_j + p^{k_j} \mid k_j \in \mathbb{N}_0\} \subseteq \mathbb{Z}_p[T_j]$ contains infinitely many pairwise coprime irreducible elements, yielding infinitely many different residue

classes in $\Lambda_d/(f_1,\ldots,f_{j-1})$, respectively. On the other hand, we only have to exclude that $\overline{f_j}$ divides one of the finitely many residue classes $\overline{\mathfrak{p}_1^{n_1}},\ldots,\overline{\mathfrak{p}_s^{n_s}}$ in $\Lambda_d/(f_1,\ldots,f_{j-1})$.

It is now easy to see that the ideal $(f_1,\ldots,f_j)\subseteq\Lambda_d$ is a prime ideal for every $1\leq j\leq d$. Indeed, the ring isomorphism

$$\Lambda_d/(f_1,\ldots,f_j)\ \longrightarrow\ \mathbb{Z}_p[[T_{j+1},\ldots,T_d]]$$

mapping T_i to $-p^{k_i}$, $1\leq i\leq j$, is a bijection between $\Lambda_d/(f_1,\ldots,f_j)$ and the domain $\mathbb{Z}_p[[T_{j+1},\ldots,T_d]]$. This may be seen via induction on j, using the isomorphism

$$\Lambda_d/(f_1,\ldots,f_j)\ \cong\ R/(f_j)\ ,$$

where $R:=\Lambda_d/(f_1,\ldots,f_{j-1})\cong\mathbb{Z}_p[[T_j,\ldots,T_d]]$ is a domain because of the induction hypothesis.

This concludes the proof of Lemma 5.46.

□

The following result considers, more generally, arbitrary finitely generated torsion Λ_d-modules. It moreover proves the plausible fact that for a pseudo-null Λ_d-module A, $d-1$ suitably chosen f_j are enough in order to make $A/((f_1,\ldots,f_{d-1})\cdot A)$ finite. We want to exclude the trivial solution of choosing f_j to be a unit in Λ_d for some j. Therefore we assume that each f_j is contained in the maximal ideal $\mathfrak{m}=(p,T_1,\ldots,T_d)$ of the local ring Λ_d, respectively.

Proposition 5.50. *Let A denote a finitely generated torsion Λ_d-module.*

(i) There exist elements $f_1,\ldots,f_d\in\mathfrak{m}$ such that $A/((f_1,\ldots,f_d)\cdot A)$ is finite.

(ii) If A is pseudo-null, then we may find $d-1$ elements $f_1,\ldots,f_{d-1}\in\mathfrak{m}$ such that $A/((f_1,\ldots,f_{d-1})\cdot A)$ is finite.

(iii) More generally, if $s\in\mathbb{N}$, and if $A_1,\ldots,A_s$ denote pseudo-null Λ_d-modules, then there exist $d-1$ elements $f_1,\ldots,f_{d-1}\in\mathfrak{m}$ such that

$$A_i/((f_1,\ldots,f_{d-1})\cdot A_i)$$

is finite for every $1\leq i\leq s$.

Proof. (i) Let $f_A\in\Lambda_d$ denote a non-trivial annihilator of the torsion-module A. The proof of Lemma 5.46 implies that we may choose $f_1,\ldots,f_d\in\mathfrak{m}$ such that $\Lambda_d/(f_A,f_1,\ldots,f_d)$ is finite.

If $c_1,\ldots,c_r$ denote generators of A over Λ_d, then

$$A/((f_1,\ldots,f_d)\cdot A)\ =\ A/((f_A,f_1,\ldots,f_d)\cdot A)$$

may be imbedded into

$$\Lambda_d/(f_A,f_1,\ldots,f_d)\cdot c_1\ +\ \ldots\ +\ \Lambda_d/(f_A,f_1,\ldots,f_d)\cdot c_r\ ,$$

and therefore is finite.

(ii) This is a special case of (iii).

(iii) $M := A_1 \oplus \ldots \oplus A_s$ is a pseudo-null Λ_d-module (compare Proposition 5.44). This means that the annihilator ideal $I := \mathrm{Ann}(M) \subseteq \Lambda_d$ of M is not contained in any prime ideal of Λ_d of height one.
We claim that the *Krull dimension* (compare Definition 2.11) of $R := \Lambda_d/I$ is at most $d-1$.
Indeed, suppose that $\dim(R) \geq d$. Then there exists a chain of prime ideals

$$\overline{\mathfrak{p}_d} \supsetneqq \overline{\mathfrak{p}_{d-1}} \supsetneqq \ldots \supsetneqq \overline{\mathfrak{p}_0}$$

in R. This yields a chain of primes

$$\mathfrak{p}_d \supsetneqq \mathfrak{p}_{d-1} \supsetneqq \ldots \supsetneqq \mathfrak{p}_0 \supseteq I$$

in Λ_d. Since we have seen in Proposition 2.17, (ii) that the Krull dimension of Λ_d is equal to $d+1$, it follows that the height of $\mathfrak{p}_0$ is at most one. But this contradicts the fact that M is pseudo-null. Therefore we may conclude that $\dim(R) \leq d-1$.
Let now $\overline{\mathfrak{m}}$ denote the maximal ideal of the local ring $R = \Lambda_d/I$. Then Corollary 10.7 in [Ei 95] implies that there exist $d-1 \geq \dim(R)$ elements $\overline{f_1}, \ldots, \overline{f_{d-1}} \in \overline{\mathfrak{m}}$ such that

$$\overline{\mathfrak{m}}^n \subseteq (\overline{f_1}, \ldots, \overline{f_{d-1}})$$

for sufficiently large n. If $f_1, \ldots, f_{d-1} \in \mathfrak{m}$ denote lifts of $\overline{f_1}, \ldots, \overline{f_{d-1}}$, respectively, then this means that there exists an integer $n_0 \in \mathbb{N}$ such that

$$\mathfrak{m}^n \subseteq I + (f_1, \ldots, f_{d-1})$$

for every $n \geq n_0$, and therefore

$$|\Lambda_d/(I + (f_1, \ldots, f_{d-1}))| \leq |\Lambda_d/\mathfrak{m}^{n_0}| = p^{dn_0} < \infty .$$

Since M is finitely generated over Λ_d, this means that also

$$M/((f_1, \ldots, f_{d-1}) \cdot M) = M/((I + (f_1, \ldots, f_{d-1})) \cdot M)$$

is finite, as in the proof of (i). This proves (iii).

□

Definition 5.51. Let A denote a finitely generated torsion Λ_d-module. Suppose that $f_1, \ldots, f_d \in \Lambda_d$. Then we define

$$\mathrm{rank}_{(f_1,\ldots,f_d)}(A) := v_p(|A/((f_1, \ldots, f_d) \cdot A)|) ,$$

whenever this is finite. Otherwise, we let $\mathrm{rank}_{(f_1,\ldots,f_d)}(A) := \infty$.

This generalises the f-rank of Λ-modules introduced in Chapter 3 (compare Definition 3.40). We would like to carry over the properties of the f-rank (in particular Proposition 3.41 and the property (1) mentioned at the beginning of the current section) to this multi-dimensional version. In particular, we want to relate the rank of a finitely generated torsion Λ_d-module A to the rank of

the corresponding elementary Λ_d-module E_A. We will, however, see that not all of the results from Chapter 3 remain valid if $d > 1$.

We will start with the proof of some easy properties of the ranks introduced in Definition 5.51 (compare Proposition 3.41):

Proposition 5.52. *Let $f_1, \dots, f_d \in \Lambda_d$.*

(i) Suppose that A denotes a finitely generated torsion Λ_d-module. Let $\tilde{A} \subseteq A$ be a Λ_d-submodule. If $\operatorname{rank}_{(f_1,\dots,f_d)}(\tilde{A})$ and $\operatorname{rank}_{(f_1,\dots,f_d)}(A/\tilde{A})$ are finite, then so is $\operatorname{rank}_{(f_1,\dots,f_d)}(A)$, and in fact

$$\operatorname{rank}_{(f_1,\dots,f_d)}(A) \;\leq\; \operatorname{rank}_{(f_1,\dots,f_d)}(\tilde{A}) + \operatorname{rank}_{(f_1,\dots,f_d)}(A/\tilde{A}) \;.$$

(ii) Let A, B denote Λ_d-modules such that at least one of the ranks $\operatorname{rank}_{(f_1,\dots,f_d)}(A)$, $\operatorname{rank}_{(f_1,\dots,f_d)}(B)$ is defined. Assume that there exists a Λ_d-module isomorphism

$$\varphi : A \;\xrightarrow{\sim}\; B \;.$$

Then both $\operatorname{rank}_{(f_1,\dots,f_d)}(A)$ and $\operatorname{rank}_{(f_1,\dots,f_d)}(B)$ are defined, and

$$\operatorname{rank}_{(f_1,\dots,f_d)}(A) \;=\; \operatorname{rank}_{(f_1,\dots,f_d)}(B) \;.$$

(iii) Let A denote a Λ_d-module such that $\operatorname{rank}_{(f_1,\dots,f_d)}(A)$ is finite. Then

$$\operatorname{rank}_{(f_1,\dots,f_d)}(A/M) \;\leq\; \operatorname{rank}_{(f_1,\dots,f_d)}(A)$$

for every Λ_d-submodule M of A.

(iv) If a Λ_d-module A is isomorphic to the direct sum of two Λ_d-modules B_1 and B_2, and if $\operatorname{rank}_{(f_1,\dots,f_d)}(B_1)$ and $\operatorname{rank}_{(f_1,\dots,f_d)}(B_2)$ are finite, then $\operatorname{rank}_{(f_1,\dots,f_d)}(A)$ is also finite, and

$$\operatorname{rank}_{(f_1,\dots,f_d)}(A) \;=\; \operatorname{rank}_{(f_1,\dots,f_d)}(B_1) \;+\; \operatorname{rank}_{(f_1,\dots,f_d)}(B_2) \;.$$

Proof. (i) Fix some set M of representatives for $A/\tilde{A}$. Then every element $a \in A$ may in a unique way be written as $a = b + \alpha$ with $b \in \tilde{A}$ and $\alpha \in M$. Since

$$(f_1, \dots, f_d) \cdot \tilde{A} \;\subseteq\; (f_1, \dots, f_d) \cdot A \cap \tilde{A} \;,$$

the assertion follows.

(ii) Since

$$\varphi((f_1, \dots, f_d) \cdot A) \;=\; (f_1, \dots, f_d) \cdot \varphi(A) \;=\; (f_1, \dots, f_d) \cdot B \;,$$

we obtain a well-defined Λ_d-module isomophism

$$\overline{\varphi} : A/((f_1, \dots, f_d) \cdot A) \;\xrightarrow{\sim}\; B/((f_1, \dots, f_d) \cdot B) \;.$$

(iii) For every submodule M of A, the order of

$$(A/M)/((f_1, \dots, f_d) \cdot (A/M)) \;=\; A/(M + (f_1, \dots, f_d) \cdot A)$$

is less or equal to the order of $A/((f_1, \dots, f_d) \cdot A)$.

(iv) Using (ii), we may assume that $A = B_1 \oplus B_2$. Then

$$A/((f_1,\ldots,f_d)\cdot A) \;\cong\; B_1/((f_1,\ldots,f_d)\cdot B_1) \,\oplus\, B_2/((f_1,\ldots,f_d)\cdot B_2)\;.$$

□

In Proposition 3.41, (i), we proved the following statement, which is considerably stronger than assertion (i) above: If $A = \Lambda/(\mathfrak{p}^n)$ for some irreducible element $\mathfrak{p} \in \Lambda$ and some $n \in \mathbb{N}$, and if $\tilde{A} \subseteq A$ is a submodule of finite index (i.e., $A/\tilde{A}$ is a pseudo-null Λ-module), then $\mathrm{rank}_f(A) = \mathrm{rank}_f(\tilde{A})$ for every distinguished polynomial $f \in \Lambda$ that is coprime to $\mathfrak{p}$.

The proof was based on properties of a cohomological invariant $Q_f(A)$ which is defined as $Q_f(A) = \frac{|A[f]|}{|A/(f\cdot A)|}$, whenever both orders are finite. Here $A[f]$ denotes the submodule of A that is annihilated by the element $f \in \Lambda$. In Proposition 3.43, we proved that Q_f is 'multiplicative in short exact sequences', and that $Q_f(M) = 1$ for a pseudo-null (i.e., finite) Λ-module M.

Let $f_1,\ldots,f_d \in \Lambda_d$, let A denote a finitely generated torsion Λ_d-module. We will now see that the canonical generalisation

$$Q_{(f_1,\ldots,f_d)}(A) \;:=\; \frac{|A[f_1] \cap \ldots \cap A[f_d]|}{|A/((f_1,\ldots,f_d)\cdot A)|}$$

of the above invariant in general does not share analogous properties.

Example 5.53.

(1) Let $d = 2$. Then $A := \Lambda_2/(T_1, p)$ is a pseudo-null Λ_2-module. However, we will see that $Q_{(T_1,T_2)}(A) \neq 1$:
First, $A[T_1] \cap A[T_2] = A[T_2] = \{\overline{0}\}$, since $A = \Lambda_2/(T_1,p) \cong (\mathbb{Z}/p\mathbb{Z})[[T_2]]$ is a domain and $T_2 \notin (T_1, p)$. Moreover,

$$A/((T_1,T_2)\cdot A) \;=\; \Lambda_2/(p,T_1,T_2) \;\cong\; \mathbb{Z}/p\mathbb{Z}$$

contains p elements, and therefore $Q_{(T_1,T_2)}(A) = \frac{1}{p}$.

(2) Let $d = 2$, $A = \Lambda_2/(T_1)$, and let $\tilde{A} := (T_1,T_2)/(T_1)$, so that $\tilde{A}$ is a Λ_2-submodule of A. Then we have a short exact sequence

$$0 \longrightarrow \tilde{A} \longrightarrow A \longrightarrow A/\tilde{A} \longrightarrow 0\;.$$

We will see that $Q_{(p,T_2)}(A) \neq Q_{(p,T_2)}(\tilde{A}) \cdot Q_{(p,T_2)}(A/\tilde{A})$. Indeed, on the one hand,

$$A[p] \;=\; \tilde{A}[p] \;=\; (A/\tilde{A})[p] \;=\; \{\overline{0}\}\;,$$

using the fact that $A/\tilde{A} \cong \Lambda_2/(T_1,T_2) \cong \mathbb{Z}_p$ is $\mathbb{Z}_p$-torsionfree.
On the other hand, $A/((p,T_2)\cdot A) \cong \mathbb{Z}/p\mathbb{Z}$,

$$\tilde{A}/((p,T_2)\cdot\tilde{A}) \;\cong\; T_2\cdot\Lambda_2/(pT_2, T_2^2, T_2\cdot T_1) \;\cong\; \mathbb{Z}/p\mathbb{Z}$$

and $(A/\tilde{A})/((p,T_2)\cdot(A/\tilde{A})) \;\cong\; \mathbb{Z}/p\mathbb{Z}$. Thus

$$Q_{(p,T_2)}(A) \;=\; \frac{1}{p} \;\neq\; \frac{1}{p}\cdot\frac{1}{p} \;=\; Q_{(p,T_2)}(\tilde{A})\cdot Q_{(p,T_2)}(A/\tilde{A})\;.$$

Remark 5.54. Although the above examples show that the quantity $Q_{(f_1,\ldots,f_d)}(A)$ is not a suitable generalisation of the invariant $Q_f(A)$ defined in the third chapter, one might hope that nevertheless

$$\mathrm{rank}_{(f_1,\ldots,f_d)}(A) \;=\; \mathrm{rank}_{(f_1,\ldots,f_d)}(\tilde{A})$$

for submodules $\tilde{A} \subseteq A$ such that $A/\tilde{A}$ is pseudo-null – at least in the case where $A = E$ is elementary, as in Proposition 3.41, (i) and (ii). The next example shows, however, that this in general is not even true for cyclic torsion Λ_d-modules.

Example 5.55. Let $d = 3$, $E := \Lambda_3/(p)$, and $\tilde{E} := (T_1, T_2, p)/(p) \subseteq E$. Then $E/\tilde{E} \cong \Lambda_3/(T_1, T_2, p)$ is pseudo-null. Moreover, $\mathrm{rank}_{(T_1,T_2,T_3)}(E) = 1$. But

$$\begin{aligned}\mathrm{rank}_{(T_1,T_2,T_3)}(\tilde{E}) &= v_p(|\tilde{E}/((T_1,T_2,T_3)\cdot\tilde{E})|)\\ &= v_p(|<T_1,T_2> / <pT_1,pT_2,T_1^2,T_1T_2,T_2^2,T_1T_3,T_2T_3>|)\\ &= 2 \;>\; 1\,.\end{aligned}$$

Every submodule $\tilde{E}$ of a cyclic Λ_d-module $E = \Lambda_d/(g)$, where $g \in \Lambda_d$ denotes an arbitrary non-unit, is of the form $\tilde{E} = C/(g)$, where $C \subseteq \Lambda_d$ is an ideal containing g. Since Λ_d is Noetherian, C is finitely generated. We choose generators $c_1, \ldots, c_k$ of C such that c_1 is a divisor of g in Λ_d. We may assume that k has been chosen as small as possible.

Lemma 5.56. *Let $E = \Lambda_d/(g)$ and $\tilde{E} = C/(g)$ be as above. We assume that $k = 2$. Let first $g = \mathfrak{p}^r$ be a power of an irreducible element $\mathfrak{p} \in \Lambda_d$.*
Suppose that $\mathrm{rank}_{(f_1,\ldots,f_d)}(E) < \infty$ for suitable elements $f_1, \ldots, f_d \in \Lambda_d$, and that $\Lambda_d/(f_1, \ldots, f_d)$ is a finitely generated free $\mathbb{Z}_p$-module.
Then also $\mathrm{rank}_{(f_1,\ldots,f_d)}(\tilde{E}) < \infty$. Moreover,

$$\mathrm{rank}_{(f_1,\ldots,f_d)}(\tilde{E}) \;=\; \mathrm{rank}_{(f_1,\ldots,f_d)}(E)$$

if and only if the two generators of C are coprime. Note that this is the case if and only if $E/\tilde{E}$ is pseudo-null.
More generally, if $f_1, \ldots, f_d \in \Lambda_d$ are as above, $g \in \Lambda_d$ is an arbitrary non-unit, and if $E/\tilde{E}$ is pseudo-null, then

$$\mathrm{rank}_{(f_1,\ldots,f_d)}(\tilde{E}) \;=\; \mathrm{rank}_{(f_1,\ldots,f_d)}(E)\,.$$

Proof. We will make use of the following property of ranks of elementary Λ_d-modules:

Proposition 5.57. *Let $\mathfrak{p} \in \Lambda_d$. Suppose that we have chosen $f_1, \ldots, f_d \in \Lambda_d$ such that $Q := \Lambda_d/(f_1, \ldots, f_d)$ is a finitely generated free $\mathbb{Z}_p$-module, and such that $R := \mathrm{rank}_{(f_1,\ldots,f_d)}(\Lambda_d/(\mathfrak{p})) < \infty$. Then*
(i) multiplication by $\mathfrak{p}$ is an injective operation on Q,
(ii) we have an equality of ideals $(f_1, \ldots, f_d) \cap (\mathfrak{p}) \;=\; (\mathfrak{p}) \cdot (f_1, \ldots, f_d)$, and
(iii) $\mathrm{rank}_{(f_1,\ldots,f_d)}(\Lambda_d/(\mathfrak{p}^i)) \;=\; i \cdot R$ for every $i \in \mathbb{N}$.

(iv) More generally, suppose that $\mathfrak{p} = \mathfrak{p}_1 \cdot \mathfrak{p}_2$ *in* Λ_d.
Then both $\mathrm{rank}_{(f_1,\ldots,f_d)}(\Lambda_d/(\mathfrak{p}_1))$ *and* $\mathrm{rank}_{(f_1,\ldots,f_d)}(\Lambda_d/(\mathfrak{p}_2))$ *are finite, and*

$$\mathrm{rank}_{(f_1,\ldots,f_d)}(\Lambda_d/(\mathfrak{p})) \;=\; \mathrm{rank}_{(f_1,\ldots,f_d)}(\Lambda_d/(\mathfrak{p}_1)) + \mathrm{rank}_{(f_1,\ldots,f_d)}(\Lambda_d/(\mathfrak{p}_2)) \;.$$

Proof. (i) This follows from Proposition 5.48.

(ii) It is clear that $(\mathfrak{p}) \cdot (f_1,\ldots,f_d) \subseteq (\mathfrak{p}) \cap (f_1,\ldots,f_d)$. Suppose now that $x \in (f_1,\ldots,f_d) \cap (\mathfrak{p})$. Then $x = \mathfrak{p} \cdot y$ in Λ_d, and we want to prove that $y \in (f_1,\ldots,f_d)$. Otherwise, $\overline{y} \neq \overline{0}$ in $Q = \Lambda_d/(f_1,\ldots,f_d)$, and $\mathfrak{p} \cdot \overline{y} = \overline{0}$. But this contradicts (i).

(iii) We first note that multiplication by $\mathfrak{p}^j$, $j \in \mathbb{N}$, induces a Λ_d-module isomorphism

$$Q/(\mathfrak{p} \cdot Q) \;\cong\; (\mathfrak{p}^j \cdot Q)/(\mathfrak{p}^{j+1} \cdot Q) \qquad (\star)$$

(here the injectivity follows from (i)). In particular,

$$|(\mathfrak{p}^j \cdot Q)/(\mathfrak{p}^{j+1} \cdot Q)| \;=\; |Q/(\mathfrak{p} \cdot Q)| \;=\; p^R$$

for every $j \in \mathbb{N}$.
Let now $i \in \mathbb{N}$ be given. Then the isomorphisms $(\star)$ imply that

$$\begin{aligned} |Q/(\mathfrak{p}^i \cdot Q)| &= |Q/(\mathfrak{p} \cdot Q)| \cdot |(\mathfrak{p} \cdot Q)/(\mathfrak{p}^2 \cdot Q)| \cdot \ldots \cdot |(\mathfrak{p}^{i-1} \cdot Q)/(\mathfrak{p}^i \cdot Q)| \\ &= |Q/(\mathfrak{p} \cdot Q)|^i \;, \end{aligned}$$

and therefore $\mathrm{rank}_{(f_1,\ldots,f_d)}(\Lambda_d/(\mathfrak{p}^i)) = i \cdot R$.

(iv) Since $(f_1,\ldots,f_d,\mathfrak{p})$ is contained in each of the ideals $(f_1,\ldots,f_d,\mathfrak{p}_1)$ and $(f_1,\ldots,f_d,\mathfrak{p}_2)$, it follows that both

$$\mathrm{rank}_{(f_1,\ldots,f_d)}(\Lambda_d/(\mathfrak{p}_1)) \quad \text{and} \quad \mathrm{rank}_{(f_1,\ldots,f_d)}(\Lambda_d/(\mathfrak{p}_2))$$

are bounded by R. Therefore multiplication by $\mathfrak{p}_1$ and by $\mathfrak{p}_2$ on Q is injective by (i). In particular, multiplication by $\mathfrak{p}_1$ induces a Λ_d-module isomorphism

$$Q/(\mathfrak{p}_2 \cdot Q) \;\cong\; (\mathfrak{p}_1 \cdot Q)/(\mathfrak{p} \cdot Q) \;,$$

since $\mathfrak{p} = \mathfrak{p}_1 \cdot \mathfrak{p}_2$.
This means that

$$\begin{aligned} |Q/(\mathfrak{p} \cdot Q)| &= |Q/(\mathfrak{p}_1 \cdot Q)| \cdot |(\mathfrak{p}_1 \cdot Q)/(\mathfrak{p} \cdot Q)| \\ &= |Q/(\mathfrak{p}_1 \cdot Q)| \cdot |Q/(\mathfrak{p}_2 \cdot Q)| \;. \end{aligned}$$

□

We return to the proof of Lemma 5.56. Suppose first that $g = \mathfrak{p}^r$, where $\mathfrak{p} \in \Lambda_d$ is irreducible. Write $C = <c_1, c_2>_{\Lambda_d}$, with $c_1 = \mathfrak{p}^s$, $s \leq r$, and with $c_2 =: \mathfrak{p}^t \cdot \tilde{\mathfrak{p}}$, where $\tilde{\mathfrak{p}}$ is coprime to $\mathfrak{p}$.

Since $\mathrm{rank}_{(f_1,\ldots,f_d)}(E) < \infty$ by assumption, the ideal $(\mathfrak{p}^r, f_1,\ldots,f_d) \subseteq \Lambda_d$ is of finite index, and therefore also $(\mathfrak{p}, f_1,\ldots,f_d) \subseteq \Lambda_d$ is of finite index, i.e., $R := \mathrm{rank}_{(f_1,\ldots,f_d)}(\Lambda_d/(\mathfrak{p})) < \infty$.

In Lemma 5.59 below, we will give a general proof for the finiteness of $\mathrm{rank}_{(f_1,\ldots,f_d)}(\tilde{E})$. In what follows, we will actually compute this value explicitely.

Suppose first that $t = 0$. We have $\tilde{E}/((f_1, \ldots, f_d) \cdot \tilde{E}) = <\mathfrak{p}^s, \tilde{\mathfrak{p}}>/N$, with

$$N \ = \ <\mathfrak{p}^r, \mathfrak{p}^s f_1, \ldots, \mathfrak{p}^s f_d, \tilde{\mathfrak{p}} f_1, \ldots, \tilde{\mathfrak{p}} f_d> \ .$$

Suppose that $\lambda_1, \lambda_2 \in \Lambda_d$ are elements such that $\lambda_1 \cdot \mathfrak{p}^s + \lambda_2 \cdot \tilde{\mathfrak{p}} \in N$. Then

$$\lambda_1 \cdot \mathfrak{p}^s + \lambda_2 \cdot \tilde{\mathfrak{p}} \ = \ \mu_0 \cdot \mathfrak{p}^r + \mu_1 \cdot \mathfrak{p}^s + \mu_2 \cdot \tilde{\mathfrak{p}}$$

with suitable elements $\mu_0 \in \Lambda_d$ and $\mu_1, \mu_2 \in (f_1, \ldots, f_d)$.

In particular, $(\lambda_2 - \mu_2) \cdot \tilde{\mathfrak{p}} \in (\mathfrak{p}^s)$, and therefore $\lambda_2 - \mu_2 \in (\mathfrak{p}^s)$, since $\mathfrak{p}$ and $\tilde{\mathfrak{p}}$ are coprime. This means that $\lambda_2 \in (\mathfrak{p}^s, f_1, \ldots, f_d)$. In other words, $\lambda_1 \cdot \mathfrak{p}^s + \lambda_2 \cdot \tilde{\mathfrak{p}} \notin N$ whenever $\overline{\lambda_2} \neq \overline{0}$ in $\Lambda_d/(\mathfrak{p}^s, f_1, \ldots, f_d)$.

This holds for every $\lambda_1 \in \Lambda_d$. We will now determine the elements λ_1' which yield the same class $\overline{\lambda_1' \cdot \mathfrak{p}^s + \lambda_2 \cdot \tilde{\mathfrak{p}}} = \overline{\lambda_1 \cdot \mathfrak{p}^s + \lambda_2 \cdot \tilde{\mathfrak{p}}}$ modulo N. Let therefore λ_2 be fixed. Without loss of generality, we may assume that $\lambda_2 = 0$. If $\lambda_1' \cdot \mathfrak{p}^s \in N$, then

$$\lambda_1' \cdot \mathfrak{p}^s \ = \ \mu_0 \cdot \mathfrak{p}^r + \mu_1 \cdot \mathfrak{p}^s + \mu_2 \cdot \tilde{\mathfrak{p}} \ ,$$

as above. Since $\tilde{\mathfrak{p}}$ is coprime to $\mathfrak{p}^s$, we may conclude that $\mu_2 \equiv 0 \bmod \mathfrak{p}^s$. Proposition 5.57, (ii) then implies that $\mu_2 = \mathfrak{p}^s \cdot \tilde{\mu_2}$ for some $\tilde{\mu_2} \in (f_1, \ldots, f_d)$. Dividing by $\mathfrak{p}^s$ in the unique factorisation domain Λ_d, we therefore see that an equation as above is equivalent to the fact that $\lambda_1' \in (\mathfrak{p}^{r-s}, f_1, \ldots, f_d)$.

Summarising, for each $\lambda_2 \in \Lambda_d \setminus (\mathfrak{p}^s, f_1, \ldots, f_d)$, we obtain exactly

$$|\Lambda_d/(\mathfrak{p}^{r-s}, f_1, \ldots, f_d)|$$

many pairwise distinct equivalence classes $\overline{\lambda_1 \cdot \mathfrak{p}^s + \lambda_2 \cdot \tilde{\mathfrak{p}}}$ in the quotient module $\tilde{E}/((f_1, \ldots, f_d) \cdot \tilde{E})$.

Suppose now that $\lambda_2 \in (\mathfrak{p}^s, f_1, \ldots, f_d)$. Then we write

$$\lambda_2 \ = \ x \cdot \mathfrak{p}^s + \mu \ ,$$

with $x \in \Lambda_d$ and $\mu \in (f_1, \ldots, f_d)$. Considering congruence classes in

$$<\mathfrak{p}^s, \tilde{\mathfrak{p}}>/N \ ,$$

we may conclude that

$$\overline{\lambda_1 \cdot \mathfrak{p}^s + \lambda_2 \cdot \tilde{\mathfrak{p}}} \ = \ \overline{\lambda_1 \cdot \mathfrak{p}^s + x \cdot \mathfrak{p}^s \tilde{\mathfrak{p}}} \ = \ \overline{\mathfrak{p}^s(\lambda_1 + x\tilde{\mathfrak{p}})} \ .$$

As we have seen above, this yields

$$|\Lambda_d/(\mathfrak{p}^{r-s}, f_1, \ldots, f_d)|$$

many pairwise distinct equivalence classes.

We may conclude that

$$\operatorname{rank}_{(f_1,\ldots,f_d)}(\tilde{E}) \ = \ \operatorname{rank}_{(f_1,\ldots,f_d)}(\Lambda_d/(\mathfrak{p}^s)) \ + \ \operatorname{rank}_{(f_1,\ldots,f_d)}(\Lambda_d/(\mathfrak{p}^{r-s})) \ .$$

Now we apply Proposition 5.57, (iii). It follows that

$$\begin{aligned} \operatorname{rank}_{(f_1,\ldots,f_d)}(\tilde{E}) \ &= \ \operatorname{rank}_{(f_1,\ldots,f_d)}(\Lambda_d/(\mathfrak{p}^s)) \ + \ \operatorname{rank}_{(f_1,\ldots,f_d)}(\Lambda_d/(\mathfrak{p}^{r-s})) \\ &= \ s \cdot R + (r-s) \cdot R \ = \ r \cdot R \\ &= \ \operatorname{rank}_{(f_1,\ldots,f_d)}(\Lambda_d/(\mathfrak{p}^r)) \ = \ \operatorname{rank}_{(f_1,\ldots,f_d)}(E) \ . \end{aligned}$$

If $t > 0$, then

$$\tilde{E} \;= <\mathfrak{p}^s, \mathfrak{p}^t \cdot \tilde{\mathfrak{p}}> / <\mathfrak{p}^r> \;\cong\; <\mathfrak{p}^{s-t}, \tilde{\mathfrak{p}}> / <\mathfrak{p}^{r-t}> ,$$

where we note that $t < s \leq r$, since we assume that C is not a principal ideal ($k = 2$). Now the first part of the proof implies that

$$\begin{aligned} \mathrm{rank}_{(f_1,\ldots,f_d)}(\tilde{E}) &= \mathrm{rank}_{(f_1,\ldots,f_d)}(\Lambda_d/(\mathfrak{p}^{s-t})) + \mathrm{rank}_{(f_1,\ldots,f_d)}(\Lambda_d/(\mathfrak{p}^{(r-t)-(s-t)})) \\ &= \mathrm{rank}_{(f_1,\ldots,f_d)}(\Lambda_d/(\mathfrak{p}^{r-t})) \\ &< \mathrm{rank}_{(f_1,\ldots,f_d)}(\Lambda_d/(\mathfrak{p}^r)) \\ &= \mathrm{rank}_{(f_1,\ldots,f_d)}(E) \; . \end{aligned}$$

Finally, let $g \in \Lambda_d$ be arbitrary. By our assumptions, the ideal C has generators $c_1 =: \mathfrak{p}_1$ dividing g and $c_2 = \tilde{\mathfrak{p}}$ coprime to g. Then the proof of the case '$t = 0$' above goes through literally. Indeed,

$$\lambda_1 \cdot \mathfrak{p}_1 + \lambda_2 \cdot \tilde{\mathfrak{p}} \;\in\; N \;:=\; <g, \mathfrak{p}_1 f_1, \ldots, \mathfrak{p}_1 f_d, \tilde{\mathfrak{p}} f_1, \ldots, \tilde{\mathfrak{p}} f_d>$$

only if $\lambda_2 \in (\mathfrak{p}_1, f_1, \ldots, f_d)$, since $\mathfrak{p}_1$ and $\tilde{\mathfrak{p}}$ are coprime.

Moreover, since

$$\mathrm{rank}_{(f_1,\ldots,f_d)}(\Lambda_d/(\mathfrak{p}_1)) \;\leq\; \mathrm{rank}_{(f_1,\ldots,f_d)}(\Lambda_d/(\mathfrak{p})) \;<\; \infty \; ,$$

Proposition 5.57, (ii) implies that $\lambda_1 \cdot \mathfrak{p}_1 \in N$ if and only if $\lambda_1 \in (\mathfrak{p}_2, f_1, \ldots, f_d)$, where $\mathfrak{p}_2 := \frac{g}{\mathfrak{p}_1}$. Finally, Proposition 5.57, (iv) implies that

$$\begin{aligned} \mathrm{rank}_{(f_1,\ldots,f_d)}(\tilde{E}) &= \mathrm{rank}_{(f_1,\ldots,f_d)}(\Lambda_d/(\mathfrak{p}_1)) + \mathrm{rank}_{(f_1,\ldots,f_d)}(\Lambda_d/(\mathfrak{p}_2)) \\ &= \mathrm{rank}_{(f_1,\ldots,f_d)}(E) \; . \end{aligned}$$

□

Remark 5.58. If $E = \Lambda_d/(\mathfrak{p}^r)$, $\mathfrak{p}$ irreducible, and if $C = <\mathfrak{p}^s>$ is a principal ideal for some $s \geq 1$, then

$$\begin{aligned} \mathrm{rank}_{(f_1,\ldots,f_d)}(\tilde{E}) &= (r-s) \cdot \mathrm{rank}_{(f_1,\ldots,f_d)}(\Lambda_d/(\mathfrak{p})) \\ &< r \cdot \mathrm{rank}_{(f_1,\ldots,f_d)}(\Lambda_d/(\mathfrak{p})) \;=\; \mathrm{rank}_{(f_1,\ldots,f_d)}(E) \; . \end{aligned}$$

In this case, $E/\tilde{E}$ is not pseudo-null, of course.

Lemma 5.59. *Let $\mathfrak{p} \in \Lambda_d$ be a not necessarily irreducible element. Suppose that $E = \Lambda_d/(\mathfrak{p})$, and let $\tilde{E}$ denote a Λ_d-submodule of E. If $\mathrm{rank}_{(f_1,\ldots,f_d)}(E) < \infty$ for suitable elements $f_1, \ldots, f_d \in \Lambda_d$, then $\mathrm{rank}_{(f_1,\ldots,f_d)}(\tilde{E}) < \infty$.*
If $E/\tilde{E}$ is pseudo-null, then the converse also holds.

Proof. As above, $\tilde{E} = C/(\mathfrak{p})$, where $C \subseteq \Lambda_d$ denotes an ideal containing $\mathfrak{p}$. Since Λ_d is Noetherian, C can be generated over Λ_d by a finite set $\{c_1, \ldots, c_k\}$.

Let $M := \Lambda_d/(\mathfrak{p}, f_1, \ldots, f_d)$, and let $R := \mathrm{rank}_{(f_1,\ldots,f_d)}(E) < \infty$. Then $|M| = p^R$. Moreover,

$$|\tilde{E}/((f_1, \ldots, f_d) \cdot \tilde{E})| \;\leq\; | <c_1>_M | \cdot \ldots \cdot | <c_k>_M | \; ,$$

and therefore $\mathrm{rank}_{(f_1,\ldots,f_d)}(\tilde{E}) \leq k \cdot R < \infty$.

Now suppose, to the contrary, that $\mathrm{rank}_{(f_1,\ldots,f_d)}(\tilde{E}) < \infty$, and assume that $E/\tilde{E}$ is pseudo-null. We will make use of the following concepts.

Definition 5.60.
(1) If R is a ring and M is an R-module, then the ***length*** of M over R denotes the least length of a maximal chain of submodules decreasing from M – or infinity, if there exists no finite maximal chain.
(2) Let R denote a local ring with maximal ideal $\mathfrak{m}$. Suppose that M is a finitely generated R-module, and let $I \subseteq \mathfrak{m}$ be an ideal of R. Then we say that I is ***an ideal of finite colength on*** M if the quotient module $M/(I \cdot M)$ has finite length.

Proposition 5.61. *If R is a local ring with maximal ideal $\mathfrak{m}$, then an ideal $I \subseteq \mathfrak{m}$ has finite colength on a finitely generated R-module M if and only if*

$$\mathfrak{m}^n \subseteq I + \mathrm{Ann}(M)$$

for every sufficiently large $n \in \mathbb{N}$. Here $\mathrm{Ann}(M) \subseteq R$ denotes the annihilator ideal of M, i.e., $\mathrm{Ann}(M) = \{0\}$ if M is not R-torsion.

Proof. See Proposition 10.8.a in [Ei 95]. □

We return to the proof of Lemma 5.59. Since $\mathrm{rank}_{(f_1,\ldots,f_d)}(\tilde{E}) < \infty$, the length of $\tilde{E}/((f_1,\ldots,f_d)\cdot\tilde{E})$ is finite. Proposition 5.61 therefore implies that

$$\mathfrak{m}^n \subseteq (f_1,\ldots,f_d) + \mathrm{Ann}(\tilde{E}) ,$$

provided that $n \in \mathbb{N}$ is sufficiently large.

Since $\tilde{E} \subseteq E$ is a Λ_d-submodule and $E/\tilde{E}$ is pseudo-null, we have a pseudo-isomorphism $\varphi : \tilde{E} \xrightarrow{\sim} E$. Moreover, since both E and $\tilde{E}$ are finitely generated and Λ_d-torsion, there exists also a pseudo-isomorphism $\psi : E \xrightarrow{\sim} \tilde{E}$ (compare Remarks 2.22, (1)). ψ is actually an injection, because the cyclic Λ_d-module $E = \Lambda_d/(\mathfrak{p})$ does not contain any non-trivial pseudo-null submodules (this may be proved analogously to Remarks 2.25, (2)).

But then the annihilator ideal $\mathrm{Ann}(E)$ of E contains $\mathrm{Ann}(\tilde{E})$, and therefore

$$\mathfrak{m}^n \subseteq (f_1,\ldots,f_d) + \mathrm{Ann}(E)$$

for every sufficiently large $n \in \mathbb{N}$. Since $\mathrm{Ann}(E) = (\mathfrak{p})$, this means that

$$\Lambda_d/(f_1,\ldots,f_d,\mathfrak{p})$$

is finite, i.e., $\mathrm{rank}_{(f_1,\ldots,f_d)}(E) < \infty$. □

Corollary 5.62. *Let A be a finitely generated torsion Λ_d-module, let E_A denote the elementary Λ_d-module attached to A, and let $C_A := \Lambda_d/(F_A)$, where F_A denotes the characteristic power series of A. Suppose that $f_1,\ldots,f_d \in \Lambda_d$. If $\mathrm{rank}_{(f_1,\ldots,f_d)}(A) < \infty$, then $\mathrm{rank}_{(f_1,\ldots,f_d)}(C_A) < \infty$ and $\mathrm{rank}_{(f_1,\ldots,f_d)}(E_A) < \infty$.*

Proof. Let $\varphi : A \longrightarrow E_A$ denote a pseudo-isomorphism, let $M_1 := \ker(\varphi)$. Then φ induces an isomorphism $A/M_1 \cong \tilde{E}_A \subseteq E_A$, and the cokernel $M_2 := E_A/\tilde{E}_A$ is pseudo-null. Proposition 5.43 implies that there exists a pseudo-isomorphism $\varphi_2 : E_A \longrightarrow C_A$, which is in fact injective in view of Remarks 2.25, (2). Let

$\psi : A \longrightarrow C_A$ be the pseudo-isomorphism $\psi := \varphi_2 \circ \varphi$. Then $\ker(\psi) = M_1$, and $\mathrm{im}(\psi) =: \tilde{C}_A \subseteq C_A$ is a submodule such that $C_A/\tilde{C}_A$ is pseudo-null.

Proposition 5.52, (ii) and (iii) therefore imply that

$$\begin{aligned} \mathrm{rank}_{(f_1,\ldots,f_d)}(\tilde{C}_A) &= \mathrm{rank}_{(f_1,\ldots,f_d)}(A/M_1) \\ &\leq \mathrm{rank}_{(f_1,\ldots,f_d)}(A) \ < \ \infty \, . \end{aligned}$$

Therefore $\mathrm{rank}_{(f_1,\ldots,f_d)}(C_A) < \infty$, by Lemma 5.59. Now consider the injective pseudo-isomorphism $\varphi_2 : E_A \longrightarrow C_A$. Since the cokernel of φ_2 is pseudo-null, Lemma 5.59 implies that $\mathrm{rank}_{(f_1,\ldots,f_d)}(\varphi_2(E_A)) < \infty$. But

$$\mathrm{rank}_{(f_1,\ldots,f_d)}(\varphi_2(E_A)) \ = \ \mathrm{rank}_{(f_1,\ldots,f_d)}(E_A) \, ,$$

by Proposition 5.52, (ii). □

Remarks 5.63.

(1) The assumption in the second part of Lemma 5.59 that $E/\tilde{E}$ is pseudo-null is necessary, which follows from Example 5.64, (2) below. Moreover, Example 5.64, (1) will show that an analogous result is wrong in general for non-elementary torsion Λ_d-modules.

(2) At the beginning of the current section, we mentioned two facts that have been fundamental prerequisites for the one-dimensional Fukuda method. The first statement was that $\mathrm{rank}_f(A) < \infty$ if and only if $\mathrm{rank}_f(E_A) < \infty$, where $f \in \Lambda$, and where E_A denotes the elementary Λ-module attached to a finitely generated torsion Λ-module A. In Corollary 5.62, we proved one direction of an analogous statement for finitely generated torsion Λ_d-modules. The following example, however, shows that the reverse implication will not be true in general for arbitrary $d > 1$.

Example 5.64.

(1) Suppose that $d = 3$. Let $A := \Lambda_3/(T_1, T_2)$. Then A is a pseudo-null Λ_3-module, and therefore $E_A = \{0\}$. If we consider $f_1 = T_1$, $f_2 = T_2$ and $f_3 = T_3$, then $\mathrm{rank}_{(f_1,f_2,f_3)}(A) = |\Lambda_3/(T_1, T_2, T_3)| = \infty$. But of course $\mathrm{rank}_{(f_1,f_2,f_3)}(E_A) = 0 < \infty$. Note that $\tilde{A} := \{\overline{0}\} \subseteq A$ is a submodule such that $A/\tilde{A}$ is pseudo-null.

(2) Suppose now that $E = \Lambda_2/(T_1)$, so that E is a Λ_2-elementary module. Then $\mathrm{rank}_{(T_1,T_2)}(E) = \infty$, but of course $\mathrm{rank}_{(T_1,T_2)}(\{0\}) < \infty$, where $\tilde{E} := \{0\}$ is a submodule of E such that $E/\tilde{E}$ is not pseudo-null.

As we pointed out in Remark 5.54, one could hope that

$$\mathrm{rank}_{(f_1,\ldots,f_d)}(\tilde{E}) \ = \ \mathrm{rank}_{(f_1,\ldots,f_d)}(E)$$

for every submodule of an elementary torsion Λ_d-module E such that $E/\tilde{E}$ is pseudo-null, provided that the two ranks are finite. However, Example 5.55 showed that in this situation, $\mathrm{rank}_{(f_1,\ldots,f_d)}(\tilde{E})$ can be strictly larger than $\mathrm{rank}_{(f_1,\ldots,f_d)}(E)$.

In what follows, we will consider cyclic Λ_d-modules in place of elementary Λ_d-modules, using the pseudo-isomorphisms from Proposition 5.43: Instead

of considering a pseudo-isomorphism between a finitely generated torsion Λ_d-module A and the corresponding elementary Λ_d-module, we will from now on usually consider the induced map from A to $\Lambda_d/(F_A)$, where $F_A \in \Lambda_d$ denotes the characteristic power series of A. This will make it easier to relate information about F_A to the size of suitable ranks of A.

In view of Example 5.55, we state the following conjecture.

Conjecture 5.65 (Rank inequality)**.** *Suppose that $E = \Lambda_d/(\mathfrak{p})$ denotes a cyclic torsion Λ_d-module, with $\mathfrak{p} \in \Lambda_d \setminus \Lambda_d^*$ arbitrary, and let $\tilde{E} \subseteq E$ be a submodule such that $M := E/\tilde{E}$ is pseudo-null. Let $f_1, \ldots, f_d \in \Lambda_d$ be such that $\operatorname{rank}_{(f_1,\ldots,f_d)}(E)$ and $\operatorname{rank}_{(f_1,\ldots,f_d)}(\tilde{E})$ are finite. Then*

$$\operatorname{rank}_{(f_1,\ldots,f_d)}(\tilde{E}) \;\geq\; \operatorname{rank}_{(f_1,\ldots,f_d)}(E)\;.$$

Remarks 5.66.

(1) We have shown in Lemma 5.59 that under the assumptions of the conjecture, $\operatorname{rank}_{(f_1,\ldots,f_d)}(E)$ is finite if and only if $\operatorname{rank}_{(f_1,\ldots,f_d)}(\tilde{E})$ is finite.

(2) It follows from Lemma 5.56 that Conjecture 5.65 holds if $\tilde{E}$ can be generated by the residue classes of exactly two elements of Λ_d, provided that $\Lambda_d/(f_1, \ldots, f_d)$ is a finitely generated free $\mathbb{Z}_p$-module.

(3) Let A be a finitely generated torsion Λ_d-module, and let $E_A := \Lambda_d/(F_A)$, where $F_A \in \Lambda_d$ denotes the characteristic power series of A.
If the Rank Inequality Conjecture 5.65 holds for $f_1, \ldots, f_d \in \Lambda_d$ and E_A, and if $\operatorname{rank}_{(f_1,\ldots,f_d)}(A) < \infty$, then

$$\operatorname{rank}_{(f_1,\ldots,f_d)}(E_A) \;\leq\; \operatorname{rank}_{(f_1,\ldots,f_d)}(A)\;.$$

Proof. We have seen in the proof of Corollary 5.62 that

$$\operatorname{rank}_{(f_1,\ldots,f_d)}(\tilde{E}_A) \;\leq\; \operatorname{rank}_{(f_1,\ldots,f_d)}(A)\;,$$

where $\tilde{E}_A \subseteq E_A$ denotes a submodule such that $E_A/\tilde{E}_A$ is pseudo-null. Therefore the statement follows from Lemma 5.59 and from the validity of the conjecture. □

We have not found any example violating Conjecture 5.65, but we also have not been able to prove this conjecture in general. In Section 5.9, we will state several results proving the conjecture in some special cases.

We will conclude the present section by giving an important example of a situation where finite ranks naturally occur.

Lemma 5.67. *Let $\mathbb{K}/K$ denote a $\mathbb{Z}_p^d$-extension, let $e := e(\mathbb{K}/K)$. We consider the Greenberg module $X := \operatorname{Gal}(H(\mathbb{K})/\mathbb{K})$. For every $n > m$ and $1 \leq i \leq d$, we let $\nu_{(n,m)}(T_i) \in \mathbb{Z}_p[T_i]$ denote the distinguished polynomial*

$$\nu_{(n,m)}(T_i) := \frac{(T_i+1)^{p^n} - 1}{(T_i+1)^{p^m} - 1}$$

(compare Definition 5.22). Then

$$\operatorname{rank}_{(\nu_{(n_1,m_1)}(T_1),\ldots,\nu_{(n_d,m_d)}(T_d))}(X) < \infty$$

for each pair of tuples $(n_1,\ldots,n_d),(m_1,\ldots,m_d) \in \mathbb{N}_0^d$ *such that* $n_j > m_j \geq e$ *for every* $j = 1,\ldots,d$.

Proof. We will first consider the case $n_1 = \ldots = n_d > m_1 = \ldots = m_d$.

For every $n \geq 0$, we let $Y_n \subseteq X$ denote the kernel of the projection map $\mathrm{pr}_n : X = \varprojlim X_n \longrightarrow X_n$, with $X_n = \mathrm{Gal}(H_n/K_n)$, as in Section 5.4. Then $X/Y_n \cong X_n$ is finite for every $n \geq 0$.

Let us first assume that there exists only one prime of K that ramifies in $\mathbb{K}$. We have shown in the proof of Lemma 5.23 that

$$Y_n \;\subseteq\; (\nu_{(n,m)}(T_1),\ldots,\nu_{(n,m)}(T_d)) \cdot Y_m$$

for every $n > m \geq e$. Indeed, our assumption implies that

$$Y_m \;=\; (\nu_{(m,e)}(T_1)\cdot\nu_{(e,0)}(T_1)\cdot T_1,\ldots,\nu_{(m,e)}(T_d)\cdot\nu_{(e,0)}(T_d)\cdot T_d)\cdot X$$

for every $m \geq e$ (compare Definition 5.22); further note that

$$\nu_{(n,e)}(T_i) \;=\; \nu_{(n,m)}(T_i)\cdot\nu_{(m,e)}(T_i)$$

for every $1 \leq i \leq d$ and every $n > m \geq e$.

Since $Y_m/Y_n \subseteq X/Y_n \cong X_n$ is finite, it follows that

$$Y_m/((\nu_{(n,m)}(T_1),\ldots,\nu_{(n,m)}(T_d))\cdot Y_m)$$

is finite, i.e., $\mathrm{rank}_{(\nu_{(n,m)}(T_1),\ldots,\nu_{(n,m)}(T_d))}(Y_m) < \infty$. But $Y_m \subseteq X$ is of finite index, and therefore

$$\begin{aligned}
\mathrm{rank}_{(\nu_{(n,m)}(T_1),\ldots,\nu_{(n,m)}(T_d))}(X) \;&\leq\; \mathrm{rank}_{(\nu_{(n,m)}(T_1),\ldots,\nu_{(n,m)}(T_d))}(Y_m) \\
&\qquad +\; \mathrm{rank}_{(\nu_{(n,m)}(T_1),\ldots,\nu_{(n,m)}(T_d))}(X/Y_m) \\
&\leq\; \mathrm{rank}_{(\nu_{(n,m)}(T_1),\ldots,\nu_{(n,m)}(T_d))}(Y_m) \;+\; |X/Y_m| \\
&<\; \infty\,,
\end{aligned}$$

using Proposition 5.52, (i).

Now we drop the assumption that only one prime ramifies in $\mathbb{K}/K$. In the general case, Lemma 5.23 shows that for every $n > m \geq e$,

$$Y_n \;\subseteq\; \underbrace{(\nu_{(n,m)}(T_1),\ldots,\nu_{(n,m)}(T_d),\{\nu_{(n,m)}(T_{j,k})_{j,k}\})}_{=:\,I_{n,m}}\cdot Y_m\,,$$

where $\{T_{j,k}\}_{j,k}$ denotes a certain set of elements in $(T_1,\ldots,T_d) \subseteq \Lambda_d$ such that for each j and k, $T_{j,k}+1$ is a product $\prod_{i=1}^{d}(T_i+1)^{b_i}$ with suitable elements $b_i \in \mathbb{Z}_p$ (compare the Definitions 5.18 and 5.22).

We want to show that $(\nu_{(n,m)}(T_1),\ldots,\nu_{(n,m)}(T_d)) \subseteq I_{n,m}$ is of finite index. Since $Y_m \subseteq X$ is a finitely generated Λ_d-module (recall that Λ_d is Noetherian), this will imply that

$$Y_m/((\nu_{(n,m)}(T_1),\ldots,\nu_{(n,m)}(T_d))\cdot Y_m)$$

is finite if and only if $Y_m/(I_{n,m} \cdot Y_m)$ is finite. Since $Y_n \subseteq I_{n,m} \cdot Y_m$, and as $Y_m/Y_n \subseteq X/Y_n$ is finite, it will then follow that

$$\mathrm{rank}_{(\nu_{(n,m)}(T_1),\ldots,\nu_{(n,m)}(T_d))}(Y_m) < \infty \,,$$

and therefore $\mathrm{rank}_{(\nu_{(n,m)}(T_1),\ldots,\nu_{(n,m)}(T_d))}(X) < \infty$, as in the above special case.

In order to prove our claim, we observe that $\Lambda_d/(\nu_{(n,m)}(T_1),\ldots,\nu_{(n,m)}(T_d))$ is a finitely generated free $\mathbb{Z}_p$-module (compare the proof of Lemma 5.46).

Moreover, the rank of the free $\mathbb{Z}_p$-module $\Lambda_d/(\nu_{(n,m)}(T_1),\ldots,\nu_{(n,m)}(T_d))$ is equal to $(p^n - p^m)^d$, because every $\nu_{(n,m)}(T_i)$ has degree $p^n - p^m$ in T_i, respectively. It therefore will suffice to show that the $\mathbb{Z}_p$-rank of $\Lambda_d/I_{n,m}$ is equal to $(p^n - p^m)^d$. To this purpose, we will show that the residue classes in $\Lambda_d/I_{n,m}$ of the elements $T_1^{s_1} \cdot \ldots \cdot T_d^{s_d} \in \Lambda_d$, $0 \leq s_1, \ldots, s_d < p^n - p^m$, are $\mathbb{Z}_p$-linearly independent. The proof will be a variant of an argument used in the proof of Remarks 5.47, (2).

Assume, to the contrary, that there exist elements

$$\lambda_{(s_1,\ldots,s_d)} \in \mathbb{Z}_p \,, \quad 0 \,\leq\, s_1, \ldots, s_d \,<\, p^n - p^m \,,$$

not all of which equal zero, such that $\sum \lambda_{(s_1,\ldots,s_d)} \cdot T_1^{s_1} \cdot \ldots \cdot T_d^{s_d} \in I_{n,m}$. Since we do not care about torsion elements in the $\mathbb{Z}_p$-module $\Lambda_d/I_{n,m}$, we may assume that at least one of the $\lambda_{(s_1,\ldots,s_d)}$ is not divisible by p. Then this coefficient is a unit in $\mathbb{Z}_p$, so we may assume that there exists a tuple $(s_1, \ldots, s_d)$ such that

$$T_1^{s_1} \cdot \ldots \cdot T_d^{s_d} \,=\, \sum_{(t_1,\ldots,t_d) \neq (s_1,\ldots,s_d)} \tilde{\lambda}_{(t_1,\ldots,t_d)} T_1^{t_1} \cdot \ldots \cdot T_d^{t_d} \,+\, \sum_{\substack{1 \leq j \leq d \\ 1 \leq k \leq r_j}} \mu_{j,k} \cdot \nu_{(n,m)}(T_{j,k})$$

for suitable elements $\tilde{\lambda}_{(t_1,\ldots,t_d)} \in \mathbb{Z}_p$ and $\mu_{j,k} \in \Lambda_d$, where $r_2, \ldots, r_d$ have been introduced in Definition 5.18, and where we let $r_1 := d$ and $T_{1,k} := T_k$, respectively.

Now reduce modulo $(T_1^{p^n - p^m}, \ldots, T_d^{p^n - p^m})$. The degree of each $\nu_{(n,m)}(T_{j,k})$, with respect to a single variable T_i that occurs in $T_{j,k}$ (i.e., $b_i \neq 0$ in the above representation of $T_{j,k} + 1$), is at least equal to $\deg(\nu_{(n,m)}(T_i)) = p^n - p^m$. Since $\nu_{(n,m)}(T_i) \in \mathbb{Z}_p[T_i]$ is distinguished with respect to the variable T_i, we may conclude that the latter sum is congruent to some multiple of p modulo $(T_1^{p^n - p^m}, \ldots, T_d^{p^n - p^m})$. But the first sum does not contain a term $T_1^{s_1} \cdot \ldots \cdot T_d^{s_d}$. Comparing coefficients of $T_1^{s_1} \cdot \ldots \cdot T_d^{s_d}$ on both sides of the equation therefore yields the contradiction $1 \equiv 0 \bmod p$.

This shows that $(\nu_{(n,m)}(T_1), \ldots, \nu_{(n,m)}(T_d)) \subseteq I_{n,m}$ is of finite index, and concludes the proof of the lemma in the case where we have $n_1 = \ldots = n_d$ and $m_1 = \ldots = m_d$.

Finally, if $(n_1, \ldots, n_d)$ and $(m_1, \ldots, m_d) \in \mathbb{N}_0^d$ denote any tuples such that $n_i > m_i \geq e$ for every $1 \leq i \leq d$, then we define $n := \max(n_1, \ldots, n_d)$ and $m := \min(m_1, \ldots, m_d)$. Then each $\nu_{(n_i,m_i)}(T_i)$ divides $\nu_{(n,m)}(T_i)$, respectively, and therefore

$$(\nu_{(n,m)}(T_1), \ldots, \nu_{(n,m)}(T_d)) \,\subseteq\, (\nu_{(n_1,m_1)}(T_1), \ldots, \nu_{(n_d,m_d)}(T_d)) \,.$$

This proves that

$$\mathrm{rank}_{(\nu_{(n_1,m_1)}(T_1),\ldots,\nu_{(n_d,m_d)}(T_d))}(X) \;\leq\; \mathrm{rank}_{(\nu_{(n,m)}(T_1),\ldots,\nu_{(n,m)}(T_d))}(X) < \infty\,.$$

□

Corollary 5.68. *In the situation of the previous lemma, we consider the Λ_d-module $A = \varprojlim A_n^{(\mathbb{K})}$. Then*

$$\mathrm{rank}_{(\nu_{(n_1,m_1)}(T_1),\ldots,\nu_{(n_d,m_d)}(T_d))}(A) \;<\; \infty$$

for each pair of tuples $(n_1,\ldots,n_d),(m_1,\ldots,m_d) \in \mathbb{N}_0^d$ such that $n_j > m_j \geq e$ for every $j = 1,\ldots,d$.

Corollary 5.69. *Let $E_A := \Lambda_d/(F_A)$, where F_A denotes the characteristic power series of A. Then*

$$\mathrm{rank}_{(\nu_{(n_1,m_1)}(T_1),\ldots,\nu_{(n_d,m_d)}(T_d))}(E_A) \;<\; \infty$$

for each pair of tuples $(n_1,\ldots,n_d),(m_1,\ldots,m_d) \in \mathbb{N}_0^d$ such that $n_j > m_j \geq e$ for every $j = 1,\ldots,d$.
Moreover, if the Rank Inequality Conjecture 5.65 holds for the tuple

$$(\nu_{(n_1,m_1)}(T_1),\ldots,\nu_{(n_d,m_d)}(T_d))$$

and the module E_A, then

$$\mathrm{rank}_{(\nu_{(n_1,m_1)}(T_1),\ldots,\nu_{(n_d,m_d)}(T_d))}(E_A) \;\leq\; \mathrm{rank}_{(\nu_{(n_1,m_1)}(T_1),\ldots,\nu_{(n_d,m_d)}(T_d))}(A)\,.$$

Proof. This follows from Lemma 5.67 together with Corollary 5.62 and Remarks 5.66, (3), respectively. □

5.7 Local maximality of l_0

In this section, we want to use the methods developed in the preceding paragraphs in order to obtain results concerning l_0 invariants. We want to do better than Theorem 5.15 (i.e., local boundedness of l_0). In order to prove local maximality, we will have to put a technical assumption on the power series F_A attached to the Fukuda module A under consideration. We want to motivate this by the following observation.

If L/K denotes a $\mathbb{Z}_p$-extension, $A = \varprojlim A_n^{(L)}$ and $F_A \in \Lambda = \mathbb{Z}_p[[T]]$ are defined as usual, then $\lambda(L/K)$ equals the degree of the distinguished polynomial $F_A(T)$. However, there is no direct analogon of this fact in the higher-dimensional setting:

Suppose that $\mathbb{K}/K$ denotes a $\mathbb{Z}_p^d$-extension, $d > 1$. Then we may write the characteristic power series $F_A \in \Lambda_d$ of $A^{(\mathbb{K})} = \varprojlim A_n^{(\mathbb{K})}$ as $F_A = p^{m_0(\mathbb{K}/K)} \cdot f$, with $f \in \Lambda_d = \mathbb{Z}_p[[T_1,\ldots,T_d]]$ being coprime to p. Suppose that $f \notin \Lambda_d^*$. Then Lemma 4.7 implies that we may choose elements $\tilde{\gamma}_1,\ldots,\tilde{\gamma}_{d-1} \in \Gamma = \mathrm{Gal}(\mathbb{K}/K)$

such that Γ is generated by $\tilde{\gamma}_1, \ldots, \tilde{\gamma}_{d-1}$ and $\gamma_d = T_d + 1$, and such that (up to multiplication by a unit)

$$f \;=\; T_d^k + h_{k-1} \cdot T_d^{k-1} + \ldots + h_0 \;, \qquad (\star)$$

where $k \in \mathbb{N}$, $h_0, \ldots, h_{k-1} \in (p, \tilde{T}_1, \ldots, \tilde{T}_{d-1})$ and $\tilde{T}_i = \tilde{\gamma}_i - 1$, respectively.

Lemma 5.70. $l_0(f) \leq k$.

Proof. Suppose that $\overline{f} = \overline{g} \cdot \overline{h}$ in the quotient $\overline{\Lambda_d} = \Lambda_d / p\Lambda_d$. Then

$$\overline{g} \cdot \overline{h} \;\equiv\; \overline{T_d}^k \mod (\overline{T_1}, \ldots, \overline{T_{d-1}}) \;,$$

where $\overline{T_1}, \ldots, \overline{T_{d-1}}$ denote the residue classes of $\tilde{T}_1, \ldots, \tilde{T}_{d-1}$ in $\overline{\Lambda_d}$, respectively.

Since $\Lambda_d/(p, \tilde{T}_1, \ldots, \tilde{T}_{d-1}) \cong (\mathbb{Z}/p\mathbb{Z})[[T_d]]$ is a unique factorisation domain, it follows that $\overline{g} \equiv \overline{T_d}^i \mod (\overline{T_1}, \ldots, \overline{T_{d-1}})$ for some $i \in \{0, \ldots, k\}$. If $i = 0$ or $i = k$, then $\overline{g}$, respectively, $\overline{h}$, will be a unit in $\overline{\Lambda_d}$. This shows that $\overline{f}$ can have at most k irreducible divisors in the unique factorisation domain $\overline{\Lambda_d}$. □

More generally, if $\gamma \in \Gamma = \mathrm{Gal}(\mathbb{K}/K)$, $\gamma \notin (\Gamma)^p$, is arbitrary, then we may choose a set $\{\gamma_1, \ldots, \gamma_{d-1}, \gamma\}$ of topological generators of Γ containing γ (if $\{b_1, \ldots, b_d\}$ denotes any $\mathbb{Z}_p$-basis of Γ, and if $\gamma = b_1^{\lambda_1} \cdot \ldots \cdot b_d^{\lambda_d}$, then at least one of the coefficients $\lambda_i \in \mathbb{Z}_p$ is not divisible by p; we then may replace the corresponding b_i by γ).

Moreover, Lemma 4.7 implies that we may change this basis into a basis $\{\tilde{\gamma}_1, \ldots, \tilde{\gamma}_{d-1}, \gamma\}$ of Γ such that f has a representation as in $(\star)$ with respect to $T_d := \gamma - 1$, and with $\tilde{T}_i := \tilde{\gamma}_i - 1$ for $1 \leq i \leq d-1$.

An inequality analogous to that of Lemma 5.70 then holds for every integer $k = k(T_d)$ attached to some variable T_d with respect to which a representation of f as in $(\star)$ is valid.

Remark 5.71. It is possible that $l_0(f) < k$. Consider, for example, the element $f = T_1 + T_2 \in \Lambda_2$. Then $f = T_1 + T_1^0 \cdot T_2 = T_2 + T_2^0 \cdot T_1$ is represented as in $(\star)$, with $k = 1$ in both variants. However, we have seen in Remarks 4.42, (1) that $l_0(f) = 0$.

In what follows, we will sometimes not consider f, but in fact an appropriate multiple of f which will be constructed now. Let $E_A := \Lambda_d/(F_A)$ denote the cyclic Λ_d-module attached to the finitely generated torsion Λ_d-module $A := \varprojlim A_n^{(\mathbb{K})}$. Let further $\varphi : E_A \longrightarrow A$ denote a pseudo-isomorphism. If $\tilde{A} \subseteq A$ denotes the image of φ, then the cokernel $M := A/\tilde{A}$ of φ is a pseudo-null Λ_d-module. This means that there exists an annihilator $h \in \Lambda_d$ of M such that h is not divisible by p, since otherwise the annihilator ideal of M was contained in the height one prime ideal $(p) \subseteq \Lambda_d$ (compare Remarks 2.20).

In fact, it is possible to choose h as a multiple of f because we may simply replace h by the least common multiple g of h and f in the unique factorisation domain Λ_d. Then g is still coprime to p, and we can choose generators of Γ in order to obtain a representation of g as in $(\star)$. Summarising, we obtain the following result:

Lemma 5.72. *We may choose a set of generators of* $\Gamma = \mathrm{Gal}(\mathbb{K}/K)$ *(corresponding to variables* $T_1, \ldots, T_d$ *of* Λ_d*) such that there exists an element* $g \in \Lambda_d$ *which has the following properties:*
(1) g *is divisible by* $f = f_A$*,*
(2) g *annihilates* $M := A/\tilde{A}$ *(where* $\tilde{A}$ *has been defined above), and*
(3) we have a representation of g *as in* $(\star)$*, so that in particular* $p \nmid g$*.*

Remark 5.73. In the situation of Lemma 5.72, f automatically has also a representation as in $(\star)$ with respect to these variables $T_1, \ldots, T_d$. Indeed, otherwise f was not regular with respect to T_d, i.e., $f \in (p, T_1, \ldots, T_{d-1})$ (compare Remarks 4.10, (3)). But then also the multiple g of f was contained in $(p, T_1, \ldots, T_{d-1})$, in contradiction to $(\star)$.

From now on, we will make the following assumption:

Assumption 5.74. We may choose a set of variables $T_1, \ldots, T_d$ of Λ_d such that $l_0(f) = k$, where k is defined by the corresponding representation of f as in $(\star)$.

Remark 5.75. In particular, the special case $l_0(\mathbb{K}/K) = l_0(f) = 0$ has to be treated separately, since $k \geq 1$ in our representations of f.

We will prove our main result by considering $(f_1, \ldots, f_d)$-ranks with

$$f_i \;=\; \nu_{(n_i,m_i)}(T_i)\;, \quad 1 \leq i \leq d\;,$$

where the tuples $(n_1, \ldots, n_d), (m_1, \ldots, m_d) \in \mathbb{N}_0^d$ have been chosen such that $n_j > m_j \geq e = e(\mathbb{K}/K)$ for every j. Then the Corollaries 5.68 and 5.69 imply that $\mathrm{rank}_{(f_1,\ldots,f_d)}(A) < \infty$ and $\mathrm{rank}_{(f_1,\ldots,f_d)}(E_A) < \infty$.

We will now prove an explicit formula for $\mathrm{rank}_{(f_1,\ldots,f_d)}(E_A)$ that will give us a link to the generalised Iwasawa invariants of A. This connection will then be used in order to bound these invariants in terms of our ranks. The following result is the generalisation of an argument used in the proof of Theorem 3.57.

Lemma 5.76. *Let* $f \in \Lambda_d$*,* $f \neq 0$*, let* $E = \Lambda_d/(f)$*. We assume that* $(n_1, \ldots, n_d)$ *and* $(m_1, \ldots, m_d)$ *denote tuples of integers such that*

$$\mathrm{rank}_{(\nu_{(n_1,m_1)}(T_1),\ldots,\nu_{(n_d,m_d)}(T_d))}(E) < \infty\;.$$

Then $f(\zeta_{p^{l_1}} - 1, \ldots, \zeta_{p^{l_d}} - 1) \neq 0$ *for every tuple* $(l_1, \ldots, l_d) \in \mathbb{N}^d$ *such that* $m_j < l_j \leq n_j$*,* $1 \leq j \leq d$*. Here* $\zeta_{p^{l_j}}$ *denotes a primitive* p^{l_j}*-th root of unity contained in a fixed algebraic closure of* $\mathbb{Q}_p$*, respectively.*
Moreover,

$$\mathrm{rank}_{(\nu_{(n_1,m_1)}(T_1),\ldots,\nu_{(n_d,m_d)}(T_d))}(E) \;=\; \sum v_p(f(\zeta_{p^{l_1}} - 1, \ldots, \zeta_{p^{l_d}} - 1))\;,$$

where the sum is taken over the same set of tuples $(l_1, \ldots, l_d)$*.*

Proof. $X := \Lambda_d/(\nu_{(n_1,m_1)}(T_1),\ldots,\nu_{(n_d,m_d)}(T_d))$ is a free $\mathbb{Z}_p$-module of rank $(p^{n_1}-p^{m_1})\cdot\ldots\cdot(p^{n_d}-p^{m_d})$ (compare the proof of Lemma 5.46). A basis over $\mathbb{Z}_p$ is given by the products $T_1^{s_1}\cdot\ldots\cdot T_d^{s_d}$, with $s_j < \deg(\nu_{(n_j,m_j)}(T_j)) = p^{n_j}-p^{m_j}$, respectively.

Multiplication by T_1 in Λ_d induces a $\mathbb{Z}_p$-linear map $T_1 : X \longrightarrow X$. The matrix corresponding to this map with regard to the above basis, ordered properly, is a block matrix

$$\begin{pmatrix} \boxed{A_1} & 0 & \cdots & \cdots & 0 \\ 0 & \boxed{A_1} & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & \boxed{A_1} \end{pmatrix},$$

where

$$A_1 = \begin{pmatrix} 0 & \cdots & \cdots & 0 & -c_0 \\ 1 & 0 & \cdots & 0 & -c_1 \\ & 1 & \ddots & \vdots & \vdots \\ & & \ddots & 0 & -c_{p^{n_1}-p^{m_1}-2} \\ & & & 1 & -c_{p^{n_1}-p^{m_1}-1} \end{pmatrix}$$

is the *companion matrix* of

$$\nu_{(n_1,m_1)}(T_1) \;=\; T_1^{p^{n_1}-p^{m_1}} + c_{p^{n_1}-p^{m_1}-1} + \ldots + c_0 \;.$$

The number of blocks is equal to $(p^{n_2}-p^{m_2})\cdot\ldots\cdot(p^{n_d}-p^{m_d})$. In particular, the characteristic polynomial of the linear map T_1 is equal to

$$\nu_{(n_1,m_1)}(T_1)^{(p^{n_2}-p^{m_2})\cdot\ldots\cdot(p^{n_d}-p^{m_d})} \;.$$

This shows that the eigenvalues of this map are exactly the roots

$$\zeta_{p^{l_1}} - 1 \;, \quad m_1 < l_1 \leq n_1 \;,$$

of $\nu_{(n_1,m_1)}(T_1)$.

Analogously, the eigenvalues of the $\mathbb{Z}_p$-linear maps on X induced by multiplication by T_i, $2 \leq i \leq d$, are equal to the roots of $\nu_{(n_i,m_i)}(T_i)$, respectively.

Consider a direct sum decomposition of the free $\mathbb{Z}_p$-module X into submodules corresponding to the block decomposition of the matrix representing the map T_1. The representation matrix of the restriction of T_1 to one of the corresponding submodules is equal to A_1, and therefore the characteristic polynomial is given by $\nu_{(n_1,m_1)}(T_1)$, respectively. Since this polynomial has pairwise different roots, we may conclude that T_1 is diagonalisable on X (over an algebraic extension of $\mathbb{Q}_p$ containing the eigenvalues).

The same is true for the maps $T_2,\ldots,T_d$. Moreover, since Λ_d is a commutative ring, these maps actually are simultaneously diagonalisable. We fix a basis of X with respect to which $T_1,\ldots,T_d$ are diagonalised.

Now we consider the given element $f \in \Lambda_d$ such that

$$\mathrm{rank}_{(\nu_{(n_1,m_1)}(T_1),\ldots,\nu_{(n_d,m_d)}(T_d))}(\Lambda_d/(f)) < \infty \ .$$

Since $X = \Lambda_d/(\nu_{(n_1,m_1)}(T_1),\ldots,\nu_{(n_d,m_d)}(T_d))$ is isomorphic to

$$\mathbb{Z}_p[T_1,\ldots,T_d]/(\nu_{(n_1,m_1)}(T_1),\ldots,\nu_{(n_d,m_d)}(T_d)) \ ,$$

we may conclude that

$$E/((\nu_{(n_1,m_1)}(T_1),\ldots,\nu_{(n_d,m_d)}(T_d))\cdot E) \ = \ \Lambda_d/(f,\nu_{(n_1,m_1)}(T_1),\ldots,\nu_{(n_d,m_d)}(T_d))$$

is isomorphic to $X/(\overline{f}\cdot X)$, where $\overline{f} \in \mathbb{Z}_p[T_1,\ldots,T_d]$ denotes a representative of the residue class of f in $\mathbb{Z}_p[T_1,\ldots,T_d]/(\nu_{(n_1,m_1)}(T_1),\ldots,\nu_{(n_d,m_d)}(T_d))$ which has degree less than $p^{n_i}-p^{m_i}$ in T_i, respectively.

Now we observe that $X/(\overline{f}\cdot X)$ is the cokernel of the map on X given by multiplication by $\overline{f}$. By the above, the eigenvalues of this map are equal to

$$\overline{f}(\zeta_{p^{l_1}}-1,\ldots,\zeta_{p^{l_d}}-1) \ ,$$

where $(l_1,\ldots,l_d) \in \mathbb{N}^d$ runs through the tuples such that $m_j < l_j \leq n_j$ for every $1 \leq j \leq d$.

Moreover, if 0 is an eigenvalue of the $\mathbb{Z}_p$-linear map $\overline{f} : X \longrightarrow X$ (equivalently, if $\overline{f}(\zeta_{p^{l_1}}-1,\ldots,\zeta_{p^{l_d}}-1) = 0$ for some choice of $(l_1,\ldots,l_d)$), then $X/(\overline{f}\cdot X)$ is infinite, since X is a free $\mathbb{Z}_p$-module. Therefore our assumption that $\mathrm{rank}_{(\nu_{(n_1,m_1)}(T_1),\ldots,\nu_{(n_d,m_d)}(T_d))}(E) < \infty$ implies that $\overline{f}(\zeta_{p^{l_1}}-1,\ldots,\zeta_{p^{l_d}}-1) \neq 0$ for each tuple $(l_1,\ldots,l_d)$.

Finally, if $X/(\overline{f}\cdot X)$ is finite, then its order is equal to $p^{v_p(\det(\overline{f}))}$, and the determinant of $\overline{f}$ is given by the product of the eigenvalues. Therefore

$$\begin{aligned}
\mathrm{rank}_{(\nu_{(n_1,m_1)}(T_1),\ldots,\nu_{(n_d,m_d)}(T_d))}(E) &= v_p(|X/(\overline{f}\cdot X)|) \\
&= \sum v_p(\overline{f}(\zeta_{p^{l_1}}-1,\ldots,\zeta_{p^{l_d}}-1)) \\
&= \sum v_p(f(\zeta_{p^{l_1}}-1,\ldots,\zeta_{p^{l_d}}-1)) \ ,
\end{aligned}$$

as claimed.

Note that the sum always runs over all tuples $(l_1,\ldots,l_d) \in \mathbb{N}^d$ such that $m_i < l_i \leq n_i$ for every i. This means that if, for example, T_d does not occur in f (i.e., if $f \in \mathbb{Z}_p[[T_1,\ldots,T_{d-1}]]$), then each eigenvalue $\overline{f}(\zeta_{p^{l_1}}-1,\ldots,\zeta_{p^{l_{d-1}}}-1)$ will be counted with multiplicity $p^{n_d}-p^{m_d}$ (overall, the sum has

$$(p^{n_1}-p^{m_1})\cdot\ldots\cdot(p^{n_d}-p^{m_d}) \ = \ \mathrm{rank}_{\mathbb{Z}_p}(X)$$

terms). □

We now may formulate our main result.

Theorem 5.77. *Let $\mathbb{K}/K$ denote a $\mathbb{Z}_p^d$-extension, and let moreover $A = A^{(\mathbb{K})}$ and $E_A := \Lambda_d/(F_A)$ be defined as above. We assume that*

- *there exists a prime of K that is totally ramified in $\mathbb{K}/K$, and*
- *Conjecture 5.65 holds for the tuples*

$$(\nu_{(n_1,m_1)}(T_1),\dots,\nu_{(n_d,m_d)}(T_d))\ ,\quad n_j > m_j \geq e(\mathbb{K}/K)\ \textit{for each } j\ ,$$

for the cyclic modules $E_{A^{(\mathbb{L})}} = \Lambda_d/(F_{A^{(\mathbb{L})}})$ attached to the $\mathbb{Z}_p^d$-extensions $\mathbb{L}/K$ contained in a suitable neighbourhood $\mathcal{U}(\mathbb{K},r_0)$ of $\mathbb{K}$, with respect to the R-topology (compare Definition 5.38).

Then

(i) there exists a neighbourhood $\tilde{U} = \mathcal{U}(\mathbb{K},r)$ of $\mathbb{K}$ such that

$$m_0(\mathbb{L}/K)\ \leq\ m_0(\mathbb{K}/K)$$

for each $\mathbb{L} \in \tilde{U}$, and

(ii) there exist a neighbourhood $\mathcal{U}(\mathbb{K},r_2) =: U \subseteq \tilde{U}$ and an integer $k \in \mathbb{N}$ such that

$$l_0(\mathbb{L}/K)\ \leq\ k$$

for every $\mathbb{L} \in U$ satisfying $m_0(\mathbb{L}/K) = m_0(\mathbb{K}/K)$.

If Assumption 5.74 holds for $\mathbb{K}/K$, i.e., if we may choose variables $T_1,\dots,T_d$ of Λ_d (corresponding to generators of $\mathrm{Gal}(\mathbb{K}/K)$) such that $l_0(f) = k$ in the representation $(\star)$ derived at the beginning of the current section, then there exists a neighbourhood $U = \mathcal{U}(\mathbb{K},r_2) \subseteq \tilde{U}$ such that

$$l_0(\mathbb{L}/K)\ \leq\ l_0(\mathbb{K}/K)$$

for every $\mathbb{L} \in U$ satisfying $m_0(\mathbb{L}/K) = m_0(\mathbb{K}/K)$.

Proof. • Let $\mathfrak{p}_1$ denote a prime of K that is totally ramified in $\mathbb{K}/K$. If $\tilde{U} = \mathcal{U}(\mathbb{K},n_0)$ denotes some neighbourhood of $\mathbb{K}$ and if $n_0 > 0$, then $\mathfrak{p}_1$ is totally ramified in every $\mathbb{Z}_p^d$-extension $\mathbb{L}/K$, $\mathbb{L} \in \tilde{U}$, since there does not exist an extension of K of degree p that is contained in $\mathbb{L}$ (and therefore also in $\mathbb{K}$) and unramified at $\mathfrak{p}_1$.

- We will consider the modules $A^{(\mathbb{L})} = \varprojlim A_n^{(\mathbb{L})}$ for $\mathbb{Z}_p^d$-extensions $\mathbb{L} \in \tilde{U}$. These are Fukuda modules with index barrier $e(\mathbb{L}/K)$, respectively, by Corollary 5.28.
- Let $e := e(\mathbb{K}/K)$. Corollary 5.68 implies that for every pair of tuples $(n_1,\dots,n_d),(m_1,\dots,m_d) \in \mathbb{N}_0^d$ such that $n_j > m_j \geq e$, $1 \leq j \leq d$, we have

$$\mathrm{rank}_{(\nu_{(n_1,m_1)}(T_1),\dots,\nu_{(n_d,m_d)}(T_d))}(A^{(\mathbb{K})}) < \infty\ .$$

- We fix tuples $(n_1,\dots,n_d)$ and $(m_1,\dots,m_d)$ with the above properties. Theorem 5.30 implies that there exists a neighbourhood $\mathcal{U}(\mathbb{K},r)$ such that

$$\mathrm{rank}_{(\nu_{(n_1,m_1)}(T_1),\dots,\nu_{(n_d,m_d)}(T_d))}(A^{(\mathbb{L})})\ =\ \mathrm{rank}_{(\nu_{(n_1,m_1)}(T_1),\dots,\nu_{(n_d,m_d)}(T_d))}(A^{(\mathbb{K})})$$

is finite for every $\mathbb{L} \in \mathcal{U}(\mathbb{K},r)$: just choose $r \geq e+1$ large enough to ensure that

$$\mathrm{rank}_{(\nu_{(n_1,m_1)}(T_1),\dots,\nu_{(n_d,m_d)}(T_d))}(A_{r-1}^{(\mathbb{K})})$$

is equal to

$$\mathrm{rank}_{(\nu_{(n_1,m_1)}(T_1),\ldots,\nu_{(n_d,m_d)}(T_d))}(A_r^{(\mathbb{K})}) \ .$$

Note that such a stabilisation index exists because we have surjective maps

$$\begin{array}{c} A_j^{(\mathbb{K})}/((\nu_{(n_1,m_1)}(T_1),\ldots,\nu_{(n_d,m_d)}(T_d))\cdot A_j^{(\mathbb{K})}) \\ \big\downarrow \\ A_i^{(\mathbb{K})}/((\nu_{(n_1,m_1)}(T_1),\ldots,\nu_{(n_d,m_d)}(T_d))\cdot A_i^{(\mathbb{K})}) \end{array}$$

for every $j \geq i \geq e$, induced by the norm maps, and therefore the rank of $A_i^{(\mathbb{K})}$ increases for $i \geq e$. Note that Lemma 5.37, (i) and (ii) imply that $e(\mathbb{L}/K) = e$ for every $\mathbb{L} \in \mathcal{U}(\mathbb{K}, r)$, since $r \geq e+1$. Therefore Theorem 5.30 indeed applies to $\mathbb{L} \in \mathcal{U}(\mathbb{K}, r)$.

- In what follows, the rank of a module M will always denote

$$\mathrm{rank}_{(\nu_{(n_1,m_1)}(T_1),\ldots,\nu_{(n_d,m_d)}(T_d))}(M) \ .$$

Suppose that $r \geq r_0$, and let $\mathbb{L} \in \mathcal{U}(\mathbb{K}, r)$. If $E_{A^{(\mathbb{L})}} = \Lambda_d/(F_{A^{(\mathbb{L})}})$ denotes the cyclic Λ_d-module corresponding to $A^{(\mathbb{L})}$, then

$$\mathrm{rank}(E_{A^{(\mathbb{L})}}) \ \leq \ \mathrm{rank}(A^{(\mathbb{L})}) \ = \ \mathrm{rank}(A^{(\mathbb{K})}) \ ,$$

by Corollary 5.69, since we assume that Conjecture 5.65 holds for $E_{A^{(\mathbb{L})}}$ and $(\nu_{(n_1,m_1)}(T_1),\ldots,\nu_{(n_d,m_d)}(T_d))$.
On the other hand, we let $\varphi : E_{A^{(\mathbb{K})}} \longrightarrow A^{(\mathbb{K})} = A$ denote a pseudo-isomorphism. Then φ is an injection because the Λ_d-module $E_{A^{(\mathbb{K})}}$ does not contain any non-trivial pseudo-null submodules (this may be proved analogous to Remarks 2.25, (2)).
Writing $\tilde{A} := \mathrm{im}(\varphi)$, we may conclude that $\mathrm{rank}(E_{A^{(\mathbb{K})}}) = \mathrm{rank}(\tilde{A})$, using Proposition 5.52, (ii). Moreover, Proposition 5.52, (i) implies that

$$\mathrm{rank}(A) \ \leq \ \mathrm{rank}(\tilde{A}) + \mathrm{rank}(A/\tilde{A}) \ .$$

This shows that

$$\mathrm{rank}(E_{A^{(\mathbb{L})}}) \ \leq \ \mathrm{rank}(E_{A^{(\mathbb{K})}}) + \mathrm{rank}(A/\tilde{A}) \tag{5.1}$$

for every $\mathbb{L} \in \mathcal{U}(\mathbb{K}, r)$.

- The following result shows that $\mathrm{rank}_{(\nu_{(n_1,m_1)}(T_1),\ldots,\nu_{(n_d,m_d)}(T_d))}(A/\tilde{A})$ may be bounded linearly with respect to the (difference of the) two indices n_d and m_d.
We will assume from now on that

$$m_1 = \ldots = m_{d-1} =: m \quad \text{and} \quad n_1 = \ldots = n_{d-1} =: n \ ,$$

and that $m_d > n$ (this will be sufficient for our applications). Moreover, $m \geq e$ will be thought of as being fixed.

Lemma 5.78. *There exists a constant $C \in \mathbb{N}$ such that for each tuple $(n, n, \ldots, n, n_d) \in \mathbb{N}^d$ and every $m_d \in \mathbb{N}$ such that $n > m \geq e$ and $n_d > m_d > n$, we have*

$$\operatorname{rank}_{(f_1,\ldots,f_d)}(A/\tilde{A}) \;\leq\; C \cdot [(p^n - p^m)^{d-1} + (n_d - m_d)(p^n - p^m)^{d-2}] \,,$$

where $f_j := \nu_{(n,m)}(T_j)$, $1 \leq j \leq d-1$, and $f_d := \nu_{(n_d,m_d)}(T_d)$.

Proof. As we have shown in Lemma 5.72, there exists an annihilator $g \in \Lambda_d$ of the pseudo-null Λ_d-module $M := A/\tilde{A}$ such that g is regular with respect to T_d, i.e., such that

$$T_d^l \;\equiv\; 0 \mod (p, T_1, \ldots, T_{d-1}, g)$$

for some integer $l \in \mathbb{N}$.
We let $\operatorname{Ann}(M) \subseteq \Lambda_d$ denote the annihilator ideal of M, and we define $\overline{M} := M/pM$ and $R := \Lambda_d/(p\Lambda_d + \operatorname{Ann}(M))$. Then R is a local ring, and the Krull dimension of R is at most $d-1$, since M is pseudo-null (compare the proof of Proposition 5.50, (iii)).
If $\overline{\mathfrak{m}}$ denotes the maximal ideal of R and if $\overline{T_1}, \ldots, \overline{T_{d-1}}$ denote the residue classes of $T_1, \ldots, T_{d-1}$, respectively, then

$$\overline{\mathfrak{m}}^l \subseteq (\overline{T_1}, \ldots, \overline{T_{d-1}}) \,,$$

because $g \in \operatorname{Ann}(M)$ and therefore $T_d^l \in (T_1, \ldots, T_{d-1}) + \operatorname{Ann}(M)$. This means that

$$\overline{\mathfrak{m}}^{l(d-1)(p^n-p^m)} \;\subseteq\; (\overline{\nu_{(n,m)}(T_1)}, \ldots, \overline{\nu_{(n,m)}(T_{d-1})}) \,.$$

Therefore

$$\operatorname{rank}_{(\nu_{(n,m)}(T_1),\ldots,\nu_{(n_d,m_d)}(T_d))}(\overline{M}) \;\leq\; v_p(|\overline{M}/(\overline{\mathfrak{m}}^{l(d-1)(p^n-p^m)} \cdot \overline{M})|) \,.$$

Now we apply the theory of *Hilbert polynomials* (compare Section 12.1 in [Ei 95]). Recall the notions introduced in Definition 5.60.

Lemma 5.79 (Hilbert polynomials)**.**

(i) Let R be a Noetherian ring, let M be a finitely generated R-module. Suppose that $I \subseteq R$ is an ideal of finite colength on M. If

$$H_{I,M}(n) \;:=\; \textit{length of } (I^n \cdot M)/(I^{n-1} \cdot M) \,,$$

$n \in \mathbb{N}$, then there exists a polynomial $P_{I,M} \in \mathbb{Z}[T]$ of degree smaller than the number of generators of I such that

$$P_{I,M}(n) \;=\; H_{I,M}(n)$$

for every sufficiently large n.

(ii) If $L_{I,M}(n) := \textit{length of } M/(I^n \cdot M)$, $n \in \mathbb{N}$, then there exists a polynomial $\tilde{P}_{I,M}$ of degree at most $1 + \deg P_{I,M}$ such that

$$\tilde{P}_{I,M}(n) \;=\; L_{I,M}(n)$$

for every sufficiently large n.

(iii) If R is a local ring, then $\tilde{P}_{I,M}$ may be chosen of degree at most equal to the Krull dimension of $R/\mathrm{Ann}(M)$, where $\mathrm{Ann}(M) \subseteq R$ denotes the annihilator ideal of M (i.e., $\mathrm{Ann}(M) = \{0\}$ if M is not R-torsion).

Proof. (i) Compare Proposition 11.2 of [Ei 95].
(ii) See page 277 in [Ei 95].
(iii) Compare Theorem 12.4 in [Ei 95].

□

We apply Lemma 5.79, (iii) to $R = \Lambda_d/(p\Lambda_d + \mathrm{Ann}(M))$ and $I = \overline{\mathfrak{m}}$. Since

$$R/\overline{\mathfrak{m}} \;\cong\; \Lambda_d/\mathfrak{m} \;\cong\; \mathbb{Z}/p\mathbb{Z}\,,$$

the length of $(\overline{\mathfrak{m}}^k \cdot \overline{M}/(\overline{\mathfrak{m}}^{k+1} \cdot \overline{M})$ corresponds to the dimension over the field $R/\overline{\mathfrak{m}}$ for every $k \in \mathbb{N}$. Since the Krull dimension of $R/\mathrm{Ann}(\overline{M})$ is smaller than or equal to the Krull dimension of R, which is at most $d-1$ by the above, we may conclude that

$$\begin{aligned} v_p(|\overline{M}/(\overline{\mathfrak{m}}^{l(d-1)(p^n-p^m)} \cdot \overline{M})|) &= \mathcal{O}(l^{(d-1)}(d-1)^{d-1} \cdot (p^n-p^m)^{(d-1)}) \\ &= \mathcal{O}((p^n-p^m)^{(d-1)})\,. \end{aligned}$$

Letting $N := M/((\nu_{(n,m)}(T_1), \ldots, \nu_{(n_d,m_d)}(T_d)) \cdot M)$, we may conclude that

$$\begin{aligned} \mathrm{rank}_p(N) &= v_p(|\overline{M}/((\nu_{(n,m)}(T_1), \ldots, \nu_{(n_d,m_d)}(T_d)) \cdot \overline{M})|) \\ &\leq v_p(|\overline{M}/(\overline{\mathfrak{m}}^{l(d-1)(p^n-p^m)} \cdot \overline{M})|) \\ &= \mathcal{O}((p^n-p^m)^{(d-1)})\,, \end{aligned}$$

and it remains to estimate the exponent of N. To this purpose, we refer to results of A. Cuoco and P. Monsky. The idea is as follows (compare the proof of Theorem 3.2 in [CM 81]).
We define $M' := \{x \in M \mid p^j \cdot x = 0 \text{ for some } j \in \mathbb{N}\}$ and $M'' := M/M'$. Then there exists a fixed integer j, depending only on M, such that $p^j \cdot M' = 0$ (recall that M is finitely generated over Λ_d and therefore Noetherian). Using the above approach, we obtain

$$\mathrm{rank}_{(\nu_{(n,m)}(T_1),\ldots,\nu_{(n_d,m_d)}(T_d))}(M') \;=\; \mathcal{O}((p^n-p^m)^{(d-1)})\,.$$

It will therefore be enough to bound $\mathrm{rank}_{(\nu_{(n,m)}(T_1),\ldots,\nu_{(n_d,m_d)}(T_d))}(M'')$, since

$$\mathrm{rank}(M) \;\leq\; \mathrm{rank}(M') + \mathrm{rank}(M'')$$

by Proposition 5.52, (i). We will first show that we can actually find a better bound for the p-rank of M''.
If $J := \mathrm{Ann}(M'') \subseteq \Lambda_d$ denotes the annihilator ideal of M'', then we let $\overline{J}$ denote the image of J in $\overline{\Lambda_d} := \Lambda_d/p\Lambda_d$. Note that p is not a zero divisor on M'', by definition. Since M and therefore also M'' are pseudo-null Λ_d-modules, the quotient ring $\overline{\Lambda_d}/\overline{J}$ has Krull dimension at most $d-2$ (compare the proof of Lemma 3.1 in [CM 81]).

Let $\overline{\mathfrak{m}}$ denote the maximal ideal of the local ring $\overline{\Lambda_d}/\overline{J}$. If $\overline{M''} := M''/pM''$, then

$$\overline{\mathfrak{m}}^{\,l(d-1)(p^n-p^m)} \cdot \overline{M''} \;\subseteq\; (\nu_{(n,m)}(T_1), \ldots, \nu_{(n_d,m_d)}(T_d)) \cdot \overline{M''}$$

because

$$T_d^l \cdot \overline{M''} \;\subseteq\; (p, T_1, \ldots, T_{d-1}, g) \cdot \overline{M''} \;=\; (T_1, \ldots, T_{d-1}) \cdot \overline{M''}\,,$$

as in the case of $\overline{M}$.
Therefore

$$\operatorname{rank}_p(M''/((\nu_{(n,m)}(T_1), \ldots, \nu_{(n_d,m_d)}(T_d)) \cdot M'')) \;=\; \mathcal{O}((p^n - p^m)^{d-2})\,,$$

using Lemma 5.79, (iii) and the fact that the Krull dimension of $\overline{\Lambda_d}/\overline{J}$ is at most $d-2$.
Finally, we use the following bound on the exponent of M'':

Lemma 5.80. *Let N denote a finitely generated Λ_d-module. Then there exists a constant $c = c(N)$ such that*

$$p^{n_1+\ldots+n_{d-1}+(n_d-m_d)+c}$$

annihilates the torsion subgroup of

$$N/((\nu_{(n_1,m_1)}(T_1), \ldots, \nu_{(n_d,m_d)}(T_d)) \cdot N)$$

for each pair $(n_1, \ldots, n_d), (m_1, \ldots, m_d) \in \mathbb{N}^d$ satisfying $n_i > m_i$ for every i and $m_d > \max(n_1, \ldots, n_{d-1})$.

Proof. This is a modification of Theorem 2.8 in [CM 81]; in that article, the result is proved with $\nu_{(n_i,m_i)}(T_i)$ replaced by $\nu_{(n_i,0)}(T_i)\cdot T_i$, respectively, and assuming that all the n_i are equal. We will give a proof of a slightly more general version of this lemma in the next section. □

Summarising, we obtain that

$$\begin{aligned}\operatorname{rank}(M'') &= \mathcal{O}([(d-1)\cdot n + (n_d - m_d) + c] \cdot (p^n - p^m)^{d-2}) \\ &= \mathcal{O}(n(p^n - p^m)^{d-2} + (n_d - m_d)(p^n - p^m)^{d-2})\,,\end{aligned}$$

and therefore

$$\operatorname{rank}(M) \;=\; \mathcal{O}((p^n - p^m)^{d-1} + (n_d - m_d)(p^n - p^m)^{d-2})\,,$$

since $n \leq p^n - p^m = p^m(p^{n-m} - 1)$ for large n. □

Remark 5.81. We want to stress the fact that the bound in Lemma 5.78 is linear in n_d and m_d. This will be one main ingredient making our proof work.

- We will now compute $\mathrm{rank}(E_{A^{(\mathbb{K})}})$. Let $F_A = p^{m_0(\mathbb{K}/K)} \cdot f \in \Lambda_d$ denote the characteristic power series of $A = A^{(\mathbb{K})}$, so that $E_{A^{(\mathbb{K})}} = \Lambda_d/(F_A)$. Recall that $\mathrm{rank}(E_{A^{(\mathbb{K})}}) < \infty$, by our choice of $(n_1, \ldots, n_d)$ and $(m_1, \ldots, m_d)$. Therefore Lemma 5.76 implies that

$$\mathrm{rank}_{(\nu_{(n_1,m_1)}(T_1),\ldots,\nu_{(n_d,m_d)}(T_d))}(E_A) \;=\; \sum v_p(\overline{F_A}(\zeta_{p^{l_1}} - 1, \ldots, \zeta_{p^{l_d}} - 1)) \;,$$

where the sum is taken over all tuples $(l_1, \ldots, l_d) \in \mathbb{N}^d$ such that we have $m_j < l_j \leq n_j$, $1 \leq j \leq d$. Here $\overline{F_A} \in \mathbb{Z}_p[T_1, \ldots, T_d]$ denotes, without loss of generality, a representative of the class of F_A in

$$\Lambda_d/(\nu_{(n_1,m_1)}(T_1), \ldots, \nu_{(n_d,m_d)}(T_d))$$

having degree less than $p^{n_i} - p^{m_i}$ in each variable T_i, respectively. Consider the representation

$$F_A \;=\; p^{m_0} \cdot (T_d^k + h_{k-1} \cdot T_d^{k-1} + \ldots + h_0) \;, \qquad (\star)$$

with $m_0 = m_0(\mathbb{K}/K)$. Suppose that

$$n \;=\; n_1 \;=\; \ldots \;=\; n_{d-1} \;>\; m \;=\; m_1 \;=\; \ldots \;=\; m_{d-1} \;\geq\; e$$

are fixed, and that $m_d > n$ has been chosen large enough to ensure that

$$\frac{k}{p^{m_d}(p-1)} \;<\; \frac{1}{p^n(p-1)} \;. \qquad (5.2)$$

Then

$$v_p(\overline{F_A}(\zeta_{p^{l_1}} - 1, \ldots, \zeta_{p^{l_d}} - 1)) \;=\; m_0 + \frac{k}{p^{l_d - 1}(p-1)}$$

for every tuple $(l_1, \ldots, l_d)$. Indeed, $h_0, \ldots, h_{k-1} \in (p, T_1, \ldots, T_{d-1})$ and therefore

$$v_p(h_i(\zeta_{p^{l_1}} - 1, \ldots, \zeta_{p^{l_d}} - 1)) \;\geq\; \frac{1}{p^{n-1}(p-1)}$$

for every i, provided that $h_i(\zeta_{p^{l_1}} - 1, \ldots, \zeta_{p^{l_d}} - 1) \neq 0$. But this implies that

$$\begin{aligned} v_p(\zeta_{p^{l_d}}^k) \;&=\; \frac{k}{p^{l_d-1}(p-1)} \\ &<\; \frac{k}{p^{m_d-1}(p-1)} \\ &<\; v_p(\zeta_{p^{l_d}}^i \cdot h_i(\zeta_{p^{l_1}} - 1, \ldots, \zeta_{p^{l_d}} - 1)) \end{aligned}$$

for every $0 \leq i \leq d-1$ such that $h_i(\zeta_{p^{l_1}} - 1, \ldots, \zeta_{p^{l_d}} - 1) \neq 0$. Note that vanishing h_i do not contribute to $v_p(\overline{F_A}(\zeta_{p^{l_1}} - 1, \ldots, \zeta_{p^{l_d}} - 1)$. This shows that

$$\begin{aligned} \mathrm{rank}(E_{A^{(\mathbb{K})}}) \;&=\; m_0 \cdot (p^n - p^m)^{d-1} \cdot (p^{n_d} - p^{m_d}) \\ &\quad + (n_d - m_d) \cdot k \cdot (p^n - p^m)^{d-1} \;. \end{aligned} \qquad (5.3)$$

We will now study $\mathrm{rank}(E_{A^{(\mathbb{L})}})$ for arbitrary $\mathbb{L} \in \mathcal{U}(\mathbb{K}, r)$ (the neighbourhood corresponding to the tuples $(n, \ldots, n, n_d)$ and $(m, \ldots, m, m_d)$, respectively, as defined at the beginning of the proof), turning to the proofs of (i) and (ii).

(i) Let $F_{A^{(\mathbb{L})}}$ denote the characteristic power series of $A^{(\mathbb{L})}$. Then $p^{m_0(\mathbb{L}/K)}$ divides $F_{A^{(\mathbb{L})}}$, and therefore Lemma 5.76 implies that

$$\operatorname{rank}(E_{A^{(\mathbb{L})}}) \;\geq\; m_0(\mathbb{L}/K)\cdot(p^n-p^m)^{d-1}\cdot(p^{n_d}-p^{m_d})\;.$$

Choose an integer $i\in\mathbb{N}$ such that

$$p^i \;>\; i\cdot(k+C)+C\;, \tag{5.4}$$

where C denotes the constant defined in Lemma 5.78. Now suppose that $m_d > n+i$ is large enough to make (5.2) valid. Furthermore, we define $n_d := m_d + i$.
If $\mathcal{U}(\mathbb{K},r)$ denotes a neighbourhood of $\mathbb{K}$ such that

$$\operatorname{rank}_{(\nu_{(n,m)}(T_1),\ldots,\nu_{(n_d,m_d)}(T_d))}(A^{(\mathbb{L})}) \;=\; \operatorname{rank}_{(\nu_{(n,m)}(T_1),\ldots,\nu_{(n_d,m_d)}(T_d))}(A^{(\mathbb{K})})$$

for every $\mathbb{L}\in\mathcal{U}(\mathbb{K},r)$, then (5.1) and (5.3) imply that $m_0(\mathbb{L}/K)\leq m_0$ for every such $\mathbb{L}$.

(ii) From now on, we will restrict to those $\mathbb{L}\in\mathcal{U}(\mathbb{K},r)$ satisfying

$$m_0(\mathbb{L}/K) \;=\; m_0(\mathbb{K}/K)\;.$$

We will bound l_0 invariants by using (5.1) and (5.3). First we subtract $m_0(\mathbb{K}/K)\cdot(p^n-p^m)^{d-1}\cdot(p^{n_d}-p^{m_d})$ on both sides of the inequality (5.1). This means that we may without loss of generality assume that $m_0(\mathbb{L}/K)=m_0(\mathbb{K}/K)=0$.
By Lemma 5.76, we have

$$\operatorname{rank}_{(\nu_{(n_1,m_1)}(T_1),\ldots,\nu_{(n_d,m_d)}(T_d))}(E_{A^{(\mathbb{L})}}) \;=\; \sum v_p(f^{(\mathbb{L})}(\zeta_{p^{l_1}}-1,\ldots,\zeta_{p^{l_d}}-1))\;,$$

where $f^{(\mathbb{L})}=F_{A^{(\mathbb{L})}}$ denotes the characteristic power series of $A^{(\mathbb{L})}$, and where the sum is taken over all $(l_1,\ldots,l_d)\in\mathbb{N}^d$ such that $m_j<l_j\leq n_j$, $1\leq j\leq d$.
We will now estimate $v_p(f^{(\mathbb{L})}(\zeta_{p^{l_1}}-1,\ldots,\zeta_{p^{l_d}}-1))$. Choose generators $\gamma_1',\ldots,\gamma_d'$ of $\Gamma':=\operatorname{Gal}(\mathbb{L}/K)$ such that each γ_i' coincides with the generator $\gamma_i\in\Gamma=\operatorname{Gal}(\mathbb{K}/K)$ on $\mathbb{K}\cap\mathbb{L}$, respectively. Let $T_i':=\gamma_i'-1$, $1\leq i\leq d$, so that $f^{(\mathbb{L})}\in\Lambda_d'=\mathbb{Z}_p[[T_1',\ldots,T_d']]$.
We want to show that $f^{(\mathbb{L})}$ is regular with respect to the variable T_d' in the sense of Definition 4.9. Then we can write (after multiplication by a suitable unit of Λ_d')

$$f^{(\mathbb{L})} \;=\; T_d'^{k'}+T_d'^{k'-1}\cdot h_{k'-1}'+\ldots+h_0'\;,$$

with $k'\in\mathbb{N}$ and $h_0',\ldots,h_{k'-1}'\in(p,T_1',\ldots,T_{d-1}')\subseteq\Lambda_d'$. Note that

$$v_p(f^{(\mathbb{L})}(\zeta_{p^{l_1}}-1,\ldots,\zeta_{p^{l_d}}-1)) \;=\; v_p(\overline{f^{(\mathbb{L})}}(\zeta_{p^{l_1}}-1,\ldots,\zeta_{p^{l_d}}-1))\;,$$

where, as usual, $\overline{f^{(\mathbb{L})}}\in\mathbb{Z}_p[T_1',\ldots,T_d']$ denotes a representative of the residue class of $f^{(\mathbb{L})}$ in $\Lambda_d'/(\nu_{(n_1,m_1)}(T_1'),\ldots,\nu_{(n_d,m_d)}(T_d'))$ having degree

less than $p^{n_i} - p^{m_i}$ in each variable T_i', respectively. We therefore may assume that each h_i' is of finite total degree.
Since $\mathrm{rank}(E_{A^{(\mathbb{L})}}) < \infty$, we know that $\overline{f^{(\mathbb{L})}}(\zeta_{p^{l_1}} - 1, \ldots, \zeta_{p^{l_d}} - 1) \neq 0$ for every choice of $(l_1, \ldots, l_d)$, by Lemma 5.76.
If $f^{(\mathbb{L})}$ is not regular with respect to T_d', then $f^{(\mathbb{L})} \in (p, T_1', \ldots, T_{d-1}')$ and

$$v_p(\overline{f^{(\mathbb{L})}}(\zeta_{p^{l_1}} - 1, \ldots, \zeta_{p^{l_d}} - 1)) \geq \frac{1}{p^{n-1}(p-1)}$$

for each tuple $(l_1, \ldots, l_d)$. If $f^{(\mathbb{L})}$ is regular in T_d', but $\frac{k'}{p^{l_d-1}(p-1)} \geq \frac{1}{p^{n-1}(p-1)}$ for some $m_d < l_d \leq n_d$, then the same estimate holds for every $l_1, \ldots, l_{d-1}$ (for this fixed l_d). Otherwise,

$$v_p(\overline{f^{(\mathbb{L})}}(\zeta_{p^{l_1}} - 1, \ldots, \zeta_{p^{l_d}} - 1)) = \frac{k'}{p^{l_d-1}(p-1)} .$$

If $k_1, \ldots, k_s$ denote the values of l_d for which only the 'bad' estimate $v_p(\overline{f^{(\mathbb{L})}}(\zeta_{p^{l_1}} - 1, \ldots, \zeta_{p^{l_d}} - 1)) \geq \frac{1}{p^{n-1}(p-1)}$ holds, then

$$\{k_1, \ldots, k_s\} = \{m_d + 1, \ldots, m_d + s\} ,$$

since $\frac{k'}{p^{l_d-1}(p-1)}$ becomes smaller for growing l_d and therefore the 'bad' l_d are the small ones, as in the proof of Theorem 3.57. Note that up to now, we have not excluded the possibility that $m_d + s = n_d$ (and this will happen, for example, if $f^{(\mathbb{L})}$ is not regular in T_d').
Summarising, we obtain that

$$\begin{aligned} & \frac{1}{p^{n-1}(p-1)} \cdot (p^n - p^m)^{d-1} \cdot (p^{m_d+s} - p^{m_d}) \\ & \quad + k' \cdot (p^n - p^m)^{d-1} \cdot (n_d - m_d - s) \\ \leq\ & \mathrm{rank}(E_{A^{(\mathbb{L})}}) \\ \leq\ & k \cdot (p^n - p^m)^{d-1} \cdot (n_d - m_d) + C \cdot (p^n - p^m)^{d-1} \\ & \quad + C \cdot (n_d - m_d) \cdot (p^n - p^m)^{d-2} , \end{aligned} \tag{5.5}$$

using (5.1), (5.3) and Lemma 5.78.
Recall that $m_d > n + i$ is large enough in order to make (5.2) valid, and that $n_d = m_d + i$, where $p^i > i \cdot (k + C) + C$ by (5.4). In particular,

$$\begin{aligned} (p^{m_d+s} - p^{m_d}) \cdot \frac{1}{p^{n-1}(p-1)} &= p^{m_d} \cdot (p^s - 1) \cdot \frac{1}{p^{n-1}(p-1)} \\ &> p^{m_d-n} \\ &> p^i \\ &> (n_d - m_d) \cdot (k + C) + C \end{aligned}$$

whenever $s > 0$. Since this contradicts (5.5), we may conclude that $s = 0$ in $\mathcal{U}(\mathbb{K}, r)$. In particular, this shows that every $\mathbb{L} \in \mathcal{U}(\mathbb{K}, r)$ satisfying $m_0(\mathbb{L}/K) = m_0(\mathbb{K}/K)$ has (up to powers of p) a characteristic power series which is regular with respect to the variable T_d', respectively.

Therefore (5.5) reduces to

$$\begin{aligned} k'(p^n-p^m)^{d-1}(n_d-m_d) \;\leq\; & k(p^n-p^m)^{d-1}(n_d-m_d)+C(p^n-p^m)^{d-1} \\ & +C(n_d-m_d)(p^n-p^m)^{d-2}\,, \end{aligned}$$

or equivalently

$$k'(n_d-m_d)(p^n-p^m) \;\leq\; k(n_d-m_d)(p^n-p^m)+C(p^n-p^m)+C(n_d-m_d)\,.$$

Now we assume that $n-m$ (which still is a free parameter) is greater than or equal to $\log_p(i+1)$, $i=n_d-m_d$. Letting $i\longrightarrow\infty$ (this does not affect C!), we may conclude that there exists a neighbourhood $U=\mathcal{U}(\mathbb{K},r)$ of $\mathbb{K}$ such that

$$k'\leq k$$

for every $\mathbb{L}\in U$ satisfying $m_0(\mathbb{L}/K)=m_0(\mathbb{K}/K)$. In particular,

$$l_0(f^{(\mathbb{L})}) \;\leq\; k' \;\leq\; k$$

for each $\mathbb{L}\in U$, by Lemma 5.70.
Finally, if Assumption 5.74 holds for $\mathbb{K}/K$, then

$$l_0(\mathbb{L}/K) \;=\; l_0(f^{(\mathbb{L})}) \;\leq\; k \;=\; l_0(f) \;=\; l_0(\mathbb{K}/K)$$

for all such $\mathbb{L}$.

□

As we have already observed earlier (compare Remark 5.75), the case of $l_0(\mathbb{K}/K)=0$ has to be treated seperately.

Theorem 5.82. *Let $\mathbb{K}/K$ denote a $\mathbb{Z}_p^d$-extension such that there exists a prime $\mathfrak{p}$ of K that is totally ramified in $\mathbb{K}/K$. Suppose that Conjecture 5.65 holds for the tuples*

$$(\nu_{(n_1,m_1)}(T_1),\ldots,\nu_{(n_d,m_d)}(T_d))\,,\quad n_j>m_j\geq e(\mathbb{K}/K) \text{ for each } j\,,$$

for the cyclic modules $E_{A^{(\mathbb{L})}}=\Lambda_d/(F_{A^{(\mathbb{L})}})$ attached to the $\mathbb{Z}_p^d$-extensions $\mathbb{L}/K$ contained in a suitable neighbourhood $\mathcal{U}(\mathbb{K},r_0)$ of $\mathbb{K}$.
If the characteristic power series $f^{(\mathbb{K})}$ of $\mathbb{K}/K$ is associated to a power of p (so that in particular $l_0(\mathbb{K}/K)=0$), then there exists a neighbourhood $\mathcal{U}=\mathcal{U}(\mathbb{K},r)$ of $\mathbb{K}$ such that

$$l_0(\mathbb{L}/K) \;=\; 0$$

for every $\mathbb{L}\in\mathcal{U}$ satisfying $m_0(\mathbb{L}/K)=m_0(\mathbb{K}/K)$. In fact, $f^{(\mathbb{L})}=p^{m_0(\mathbb{K}/K)}$ for $\mathbb{L}\in\mathcal{U}$.

Proof. We will use the notation from the proof of Theorem 5.77, in particular applying the inequalities (5.1) and (5.5).

As in the proof of Theorem 5.77, (ii), we subtract on both sides of the inequality (5.1) the term $m_0(\mathbb{K}/K)\cdot(p^n-p^m)^{d-1}\cdot(p^{n_d}-p^{m_d})$ and therefore may assume that, without loss of generality, $m_0(\mathbb{K}/K)=0$.

Then the fact that $f^{(\mathbb{K})} = 1$ implies that $E_{A^{(\mathbb{K})}} = \{0\}$. Therefore (5.1) implies that

$$\operatorname{rank}(E_{A^{(\mathbb{L})}}) \leq \operatorname{rank}(A/\tilde{A}) \leq C \cdot [(p^n - p^m)^{d-1} + (n_d - m_d)(p^n - p^m)^{d-2}]$$

for some constant $C \in \mathbb{N}$ and every $\mathbb{L} \in \mathcal{U}(\mathbb{K}, r)$, provided that r is large enough.

If $f^{(\mathbb{L})} \neq 1$, then $v_p(\overline{f^{(\mathbb{L})}}(\zeta_{p^{l_1}} - 1, \ldots, \zeta_{p^{l_d}} - 1)) \geq \frac{1}{p^{l_d - 1}(p-1)}$ for each of the corresponding tuples of p-power roots of unity (recall that $l_d > m_d > n + i$ for some large integer $i \in \mathbb{N}$).

But then $\operatorname{rank}(E_{A^{(\mathbb{L})}}) \geq (n_d - m_d) \cdot (p^n - p^m)^{d-1}$, which is strictly larger than $C \cdot [(p^n - p^m)^{d-1} + (n_d - m_d)(p^n - p^m)^{d-2}]$ if the parameters are large enough. This proves that $f^{(\mathbb{L})} = 1$ and therefore $l_0(\mathbb{L}/K) = 0$ for every $\mathbb{L} \in \mathcal{U}$. □

Corollary 5.83. *Let $\mathbb{K}/K$ denote a $\mathbb{Z}_p^d$-extension such that there exists a prime $\mathfrak{p}$ of K that is totally ramified in $\mathbb{K}/K$. Suppose that Conjecture 5.65 holds for the tuples*

$$(\nu_{(n_1,m_1)}(T_1), \ldots, \nu_{(n_d,m_d)}(T_d)) \,, \quad n_j > m_j \geq e(\mathbb{K}/K) \text{ for each } j \,,$$

for the cyclic modules $E_{A^{(\mathbb{L})}} = \Lambda_d/(F_{A^{(\mathbb{L})}})$ attached to the $\mathbb{Z}_p^d$-extensions $\mathbb{L}/K$ contained in a suitable neighbourhood $\mathcal{U}(\mathbb{K}, r_0)$ of $\mathbb{K}$.
If $A^{(\mathbb{K})}$ is pseudo-null, then there exists a neighbourhood $\mathcal{U} = \mathcal{U}(\mathbb{K}, r)$ of $\mathbb{K}$ such that $A^{(\mathbb{L})}$ is pseudo-null for every $\mathbb{L} \in \mathcal{U}$.

Proof. If $A^{(\mathbb{K})}$ is pseudo-null, then $m_0(\mathbb{K}/K) = 0$ and $f^{(\mathbb{K})} = 1$. Since m_0 is locally maximal by Theorem 5.12 (note that $\mathcal{U}(\mathbb{K}, r) \subseteq U(\mathbb{K}, r)$ for every $r \in \mathbb{N}$, by Proposition 5.39), the claim follows from the previous theorem. □

Remarks 5.84.

(1) Let $\mathbb{K}/K$ denote a $\mathbb{Z}_p^d$-extension such that there exists a prime of K that is totally ramified in $\mathbb{K}/K$. Then the statements of Theorem 5.77, respectively, Theorem 5.82 and Corollary 5.83, hold for all $\mathbb{Z}_p^d$-extensions $\mathbb{L}$ of K that are contained in a suitable neighbourhood $\mathcal{U}(\mathbb{K}, r)$ of $\mathbb{K}$ and satisfy the following condition:
The module $A^{(\mathbb{L})} = \varprojlim A_n^{(\mathbb{L})}$ is generated over Λ_d by at most two elements.

Proof. If $\mathbb{L} \in \mathcal{U}(\mathbb{K}, r)$ satisfies the above condition, then the image

$$\tilde{E}_{A^{(\mathbb{L})}} := \varphi^{(\mathbb{L})}(A^{(\mathbb{L})}) \subseteq E_{A^{(\mathbb{L})}} := \Lambda_d/(F_{A^{(\mathbb{L})}})$$

under the corresponding pseudo-isomorphism $\varphi^{(\mathbb{L})} : A^{(\mathbb{L})} \xrightarrow{\sim} E_{A^{(\mathbb{L})}}$ is generated by at most two elements.
We have to show that this implies that inequality (5.1) holds, since this is the only step of the proof of Theorem 5.77 which depends on Conjecture 5.65.
In other words, it suffices to show that

$$\operatorname{rank}(E_{A^{(\mathbb{L})}}) \leq \operatorname{rank}(A^{(\mathbb{L})})$$

for these $\mathbb{L}$, where rank always denotes $\mathrm{rank}_{(\nu_{(n_1,m_1)}(T_1),\ldots,\nu_{(n_d,m_d)}(T_d))}$, and where $n_j > m_j \geq e(\mathbb{K}/K)$ for every $j \in \{1,\ldots,d\}$.
If $A^{(\mathbb{L})}$ and therefore also $\tilde{E}_{A^{(\mathbb{L})}} = \varphi^{(\mathbb{L})}(A^{(\mathbb{L})})$ are cyclic Λ_d-modules (i.e., generated by a single element), then we have in fact

$$A^{(\mathbb{L})} \cong E_{A^{(\mathbb{L})}} = \Lambda_d/(F_{A^{(\mathbb{L})}}) ,$$

and therefore

$$\mathrm{rank}(E_{A^{(\mathbb{L})}}) = \mathrm{rank}(A^{(\mathbb{L})}) .$$

Now suppose that $\tilde{E}_{A^{(\mathbb{L})}} \subseteq E_{A^{(\mathbb{L})}}$ is generated by exactly two elements. Since $\Lambda_d/(\nu_{(n_1,m_1)}(T_1),\ldots,\nu_{(n_d,m_d)}(T_d))$ is isomorphic to a finitely generated free $\mathbb{Z}_p$-module, Lemma 5.56 and Proposition 5.52, (ii) and (iii) imply that

$$\begin{aligned} \mathrm{rank}(E_{A^{(\mathbb{L})}}) &= \mathrm{rank}(\tilde{E}_{A^{(\mathbb{L})}}) = \mathrm{rank}(A^{(\mathbb{L})}/M_1^{(\mathbb{L})}) \\ &\leq \mathrm{rank}(A^{(\mathbb{L})}) , \end{aligned}$$

where $M_1^{(\mathbb{L})} \subseteq A^{(\mathbb{L})}$ denotes the kernel of the pseudo-isomorphism $\varphi^{(\mathbb{L})}$, respectively. □

(2) In Section 5.9, we will prove Conjecture 5.65 in several further special cases, thus obtaining more unconditional variants of Theorem 5.77.

5.8 Bounding the exponents of torsion modules

This section is devoted to a proof of Lemma 5.80, which has been used in the proof of Theorem 5.77. We will actually prove a slightly more general statement which will be needed in the next section. In order to state this result in an elegant way, we introduce some ad hoc notation.

For every $i \in \{1,\ldots,d\}$ and each $n \in \mathbb{N}_0$, we define

$$\nu_{(0,-1)}(T_i) := T_i$$

and

$$\nu_{(n,-1)}(T_i) := \nu_{(n,0)}(T_i) \cdot \nu_{(0,-1)}(T_i) = T_i \cdot \nu_{(n,0)}(T_i) .$$

Lemma 5.80. *Let N denote a finitely generated Λ_d-module. Then there exists a constant $c = c(N)$ such that*

$$p^{n_1+\ldots+n_{d-1}+(n_d-m_d)+c}$$

annihilates the $\mathbb{Z}_p$-torsion subgroup of

$$N/((\nu_{(n_1,m_1)}(T_1),\ldots,\nu_{(n_d,m_d)}(T_d)) \cdot N)$$

for each pair $(n_1,\ldots,n_d),(m_1,\ldots,m_d) \in \mathbb{Z}^d$ satisfying $n_j > m_j \geq -1$ for every $1 \leq j \leq d$, provided that $m_d > \max(n_1,\ldots,n_{d-1})$.

Our proof is a slight modification of the proof of Theorem 2.8 in [CM 81]. This theorem bounds the exponent of the torsion submodule of

$$N/((T_1 \cdot \nu_{(n,0)}(T_1), \ldots, T_d \cdot \nu_{(n,0)}(T_d)) \cdot N) \;=\; N/((\nu_{(n,-1)}(T_1), \ldots, \nu_{(n,-1)}(T_d)) \cdot N)$$

for $n \in \mathbb{N}$.

Let $I := (\nu_{(n_1,m_1)}(T_1), \ldots, \nu_{(n_d,m_d)}(T_d)) \subseteq \Lambda_d$. The first step will be to construct an embedding of Λ_d/I into a direct sum of cyclotomic rings $\mathbb{Z}_p[\underline{\zeta}]$ generated by suitable p^l-th roots of unity.

More precisely, we consider the set W of tuples $\underline{\zeta} = (\zeta_{p^{l_1}}, \ldots, \zeta_{p^{l_d}})$ of primitive p^{l_j}-th roots of unity, contained in a fixed algebraic closure $\overline{\mathbb{Q}_p}$ of $\mathbb{Q}_p$, where $m_j < l_j \leq n_j$, respectively. Here 1 is the only primitive p^0-th root of unity. Note that $\zeta_{p^{l_j}} - 1$ is a root of $\nu_{(n_j,m_j)}(T_j)$ for every $m_j < l_j \leq n_j$, respectively.

Each cyclotomic ring $\mathbb{Z}_p[\underline{\zeta}]$ is a free $\mathbb{Z}_p$-module of rank $\varphi(p^{l_i})$, where

$$l_i \;=\; \max(l_1, \ldots, l_d) \; .$$

Two tuples $\underline{\zeta}$ and $\underline{\zeta}'$ are called conjugate if and only if there exists an automorphism $\psi \in \mathrm{Aut}_{\mathbb{Q}_p}(\overline{\mathbb{Q}_p})$ such that $\psi(\underline{\zeta}) = \underline{\zeta}'$, where we let ψ act componentwise. Note that this is the case if and only if $\underline{\zeta}' = \underline{\zeta}^u$ for some integer $u \in \{1, \ldots, p^{\max(l_1,\ldots,l_d)}\}$ coprime to p, i.e., if $\underline{\zeta}$ and $\underline{\zeta}'$ generate the same cyclotomic ring.

We choose one $\underline{\zeta}$ of each conjugacy class of W, and we consider the direct sum

$$Z \;:=\; \bigoplus \mathbb{Z}_p[\underline{\zeta}]$$

over this set of representatives.

Suppose that $k \in \{0, \ldots, d\}$ is chosen such that $m_1 = \ldots = m_k = -1$ and $m_i \geq 0$ for every $i > k$ (if necessary, we permute some of the indices). Then Z is a free $\mathbb{Z}_p$-module of rank

$$p^{n_1} \cdot \ldots \cdot p^{n_k} \cdot (p^{n_{k+1}} - p^{m_{k+1}}) \cdot \ldots \cdot (p^{n_d} - p^{m_d}) \; .$$

Moreover, we obtain a surjective map

$$\varphi \;=\; \varphi_{(n_1,\ldots,n_d),(m_1,\ldots,m_d)} \;:\; \Lambda_d/I \;\longrightarrow\!\!\!\!\!\rightarrow\; Z \;\; ,$$

induced by the maps

$$\Lambda_d/I \;\longrightarrow\!\!\!\!\!\rightarrow\; \mathbb{Z}_p[\underline{\zeta}] \; , \qquad f \;\longmapsto\; f(\zeta_{p^{l_1}} - 1, \ldots, \zeta_{p^{l_d}} - 1) \; ,$$

where $\underline{\zeta} = (\zeta_{p^{l_1}}, \ldots, \zeta_{p^{l_d}}) \in W$ (this is well-defined since $g(\underline{\zeta}) = 0$ for every $g \in I$).

Lemma 5.85. *Suppose that $m_d > \max(n_1, \ldots, n_{d-1})$. Then the cokernel of the map φ is annihilated by $p^{n_1+\ldots+n_{d-1}+(n_d-m_d)}$.*

Proof. This is an adaption of Lemma 2.1 in [CM 81]. In course of the proof of that lemma, the authors observe that the polynomials defined by

$$G_0^n(T) := \sum_{j=1}^{p^n} T^j \in \mathbb{Z}_p[T]$$

and $G_s^n(T) := G_0^n(T^{p^s}) - G_0^n(T^{p^{s-1}})$ for $0 < s \leq n$ have the property that $G_s^n(\zeta) = p^n$ whenever ζ is a primitive p^s-th root of unity, and $G_s^n(\zeta) = 0$ if $\zeta^{p^n} = 1$, but ζ is no primitive p^s-th root of unity.

Letting $H_0^{(n,m)}(T) := G_0^{n-m}(T^{p^m})$, we may conclude that $H_0^{(n,m)}(\zeta) = p^{n-m}$ whenever ζ is a p^m-th root of unity, and $H_0^{(n,m)}(\zeta) = 0$ if $\zeta^{p^n} = 1$, $\zeta^{p^m} \neq 1$.

More generally, for $m \geq 0$ and $n - m \geq s > 0$, we define

$$H_s^{(n,m)}(T) := H_0^{(n,m)}(T^{p^s}) - H_0^{(n,m)}(T^{p^{s-1}}) .$$

Then $H_s^{(n,m)}(\zeta) = 0$ if $\zeta^{p^n} = 1$, but ζ is no primitive p^{m+s}-th root of unity, and $H_s^{(n,m)}(\zeta) = p^{n-m}$ otherwise.

Finally, let $\underline{\zeta} = (\zeta_{p^{l_1}}, \ldots, \zeta_{p^{l_d}}) \in W$, i.e., $m_i < l_i \leq n_i$ for each $i \in \{1, \ldots, d\}$. Since $m_d > \max(n_1, \ldots, n_{d-1})$ by assumption, we have $l_d = \max(l_1, \ldots, l_d)$. We therefore may choose integers $a_1, \ldots, a_{d-1}$ such that $\zeta_{p^{l_d}}^{a_j} = \zeta_{p^{l_j}}$, respectively.

We let

$$H_{\underline{\zeta}}(T_1, \ldots, T_d) := H_{l_d - m_d}^{(n_d, m_d)}(T_d) \cdot \prod_{j=1}^{d-1} G_0^{n_j}(T_d^{a_j} \cdot T_j) .$$

Then $H_{\underline{\zeta}}(\underline{\zeta}') = 0$ for every $\underline{\zeta}' = (\zeta'_{p^{l'_1}}, \ldots, \zeta'_{p^{l'_d}}) \in W$, unless $l'_d = l_d$ and $(\zeta'_{p^{l'_d}})^{a_j} \cdot \zeta'_{p^{l'_j}} = 1$ for every $1 \leq j \leq d-1$, i.e., unless $\underline{\zeta}'$ is conjugate to $\underline{\zeta}$. Note that $H_{\underline{\zeta}}(\underline{\zeta}') = p^{n_1 + \ldots + n_{d-1} + n_d - m_d}$ for every $\underline{\zeta}'$ conjugate to $\underline{\zeta}$.

If $\underline{\zeta}'$ denotes an element conjugate to $\underline{\zeta}$, and if $z \in p^{n_1 + \ldots + n_{d-1} + n_d - m_d} \cdot \mathbb{Z}_p[\underline{\zeta}']$ denotes an arbitrary given element, then we can find a polynomial

$$g \in \mathbb{Z}_p[T_1, \ldots, T_d] \subseteq \Lambda$$

such that $(g \cdot H_{\underline{\zeta}})(\underline{\zeta}') = z$. Moreover, $g \cdot H_{\underline{\zeta}}$ vanishes at all $\underline{\zeta}'' \in W$ that are not conjugate to $\underline{\zeta}$. This proves the lemma. □

Corollary 5.86. *Under the above assumptions,*

$$\varphi : \Lambda_d / I \longrightarrow Z = \bigoplus \mathbb{Z}_p[\underline{\zeta}]$$

is injective with finite cokernel annihilated by $p^{n_1 + \ldots + n_{d-1} + n_d - m_d}$.

Proof. Choose $k \in \{0, \ldots, d\}$ such that $m_1 = \ldots = m_k = -1$ and $m_i \geq 0$ for every $i > k$. Then both Λ_d / I and Z are free $\mathbb{Z}_p$-modules of rank

$$p^{n_1} \cdot \ldots \cdot p^{n_k} \cdot (p^{n_{k+1}} - p^{m_{k+1}}) \cdot \ldots \cdot (p^{n_d} - p^{m_d})$$

(compare the proof of Lemma 5.46). Since the cokernel of φ is annihilated by $p^{n_1 + \ldots + n_{d-1} + n_d - m_d}$, by the previous lemma, we may conclude that the image of φ has full rank. Therefore φ has to be injective. □

Remark 5.87. In the proof of the above corollary, there is no need to use Lemma 5.46, since Lemma 5.85 actually reproves the fact that Λ_d/I is a free $\mathbb{Z}_p$-module of rank $p^{n_1} \cdot \ldots \cdot p^{n_k} \cdot (p^{n_{k+1}} - p^{m_{k+1}}) \cdot \ldots \cdot (p^{n_d} - p^{m_d})$: Obviously this quotient is generated as a $\mathbb{Z}_p$-module by the elements $T_1^{s_1} \cdot \ldots \cdot T_d^{s_d}$ with $0 \leq s_i < \deg(\nu_{(n_i,m_i)}(T_i))$, respectively. Since the number of these elements is equal to the $\mathbb{Z}_p$-rank of Z, and since the cokernel of φ is finite by the above lemma, it follows that Λ_d/I in fact is $\mathbb{Z}_p$-free.

We will now use the map φ for the study of finitely generated Λ_d-modules. Let N denote such a module. For every $\underline{\zeta} = (\zeta_{p^{l_1}}, \ldots, \zeta_{p^{l_d}}) \in W$, we define a finitely generated $\mathbb{Z}_p[\underline{\zeta}]$-module

$$N_{\underline{\zeta}} \;:=\; N \,/\, (I_{\underline{\zeta}} \cdot N) \;,$$

where $I_{\underline{\zeta}} \subseteq \Lambda_d$ denotes the kernel of the map

$$\pi_{\underline{\zeta}} : \Lambda_d \;\longrightarrow\; \mathbb{Z}_p[\underline{\zeta}] \;, \quad f \;\longmapsto\; f(\zeta_{p^{l_1}} - 1, \ldots, \zeta_{p^{l_d}} - 1) \;.$$

$N_{\underline{\zeta}}$ is a $\mathbb{Z}_p[\underline{\zeta}]$-module via $z \cdot \overline{n} := \overline{yn}$, where $y \in \Lambda_d$ denotes any element such that $\pi_{\underline{\zeta}}(y) = z$.

Lemma 5.88. *There exists a fixed integer $c = c(N)$ such that p^c annihilates the $\mathbb{Z}_p$-torsion submodule of the finitely generated $\mathbb{Z}_p[\underline{\zeta}]$-module $N_{\underline{\zeta}}$ for every $\underline{\zeta} \in W$.*

Proof. This is Lemma 2.6 in [CM 81] (in fact this result does not only hold for the $\underline{\zeta} \in W$, but for *every* tuple of p-power roots of unity). □

The projections $N \longrightarrow N_{\underline{\zeta}}$ canonically induce a map $\varphi : N \longrightarrow \bigoplus N_{\underline{\zeta}}$, where the sum is taken over a set of representatives of the conjugacy classes of the $\underline{\zeta} \in W$.

Lemma 5.89. *Suppose that $m_d > \max(n_1, \ldots, n_{d-1})$. Then both the kernel and the cokernel of the induced map*

$$\Phi : N/(I \cdot N) \;\longrightarrow\; \bigoplus N_{\underline{\zeta}}$$

are annihilated by $p^{n_1 + \ldots + n_{d-1} + (n_d - m_d)}$.

Proof. First note that the map Φ is well-defined, since for each $\underline{\zeta} \in W$, the ideal I is contained in the kernel $I_{\underline{\zeta}}$ of $\pi_{\underline{\zeta}}$, respectively.

If $g_1, \ldots, g_r$ are generators of the Λ_d/I-module $N/(I \cdot N)$, then the images $\Phi(g_1), \ldots, \Phi(g_r)$ generate $\bigoplus N_{\underline{\zeta}}$ over $Z = \bigoplus \mathbb{Z}_p[\underline{\zeta}]$ (acting component-wise). Since the image of Φ contains every linear combination of $\Phi(g_1), \ldots, \Phi(g_r)$ with coefficients in Λ_d/I (instead of Z), the statement for the cokernel follows from Lemma 5.85.

The result for the kernel may be proved analogously to Lemma 2.7 in [CM 81]: Since N is finitely generated over Λ_d, there exist a finitely generated free Λ_d/I-module F and a surjective homomorphism $F \twoheadrightarrow N/(I \cdot N)$. Choose generators $u_1, \ldots, u_k \in F$ of the kernel of this homomorphism.

Let $\overline{x} \in \ker(\Phi)$. Choose some $x \in F$ that is mapped to $\overline{x}$. We consider the map $F \longrightarrow F_{\underline{\zeta}}$ for some fixed $\underline{\zeta} \in W$. Note that the kernel of the map

$$F \longrightarrow F_{\underline{\zeta}} = F/(I_{\underline{\zeta}} \cdot F) \longrightarrow N/(I_{\underline{\zeta}} \cdot N)$$

is equal to $I_{\underline{\zeta}} \cdot F + <u_1, \ldots, u_k>$. We may conclude that

$$x = \sum_{i=1}^{k} a_{i,\underline{\zeta}} \cdot u_i \mod (I_{\underline{\zeta}} \cdot F)$$

for suitable $a_{i,\underline{\zeta}} \in \mathbb{Z}_p[\underline{\zeta}]$, since the image of x in $N_{\underline{\zeta}}$ is trivial.

Lemma 5.85 implies that for every $i \in \{1, \ldots, k\}$, there exists an element $a_i \in \Lambda_d$ such that $\varphi(a_i) \in Z$ has component $p^{n_1+\ldots+n_{d-1}+n_d-m_d} \cdot a_{i,\underline{\zeta}}$ in every $\mathbb{Z}_p[\underline{\zeta}]$, respectively. Therefore

$$\varphi(p^{n_1+\ldots+n_{d-1}+n_d-m_d} \cdot x - \sum_{i=1}^{k} a_i u_i) = 0$$

vanishes in every $F_{\underline{\zeta}}$, and thus $p^{n_1+\ldots+n_{d-1}+n_d-m_d} \cdot x = \sum a_i u_i$, since F is free over Λ_d/I and

$$\varphi : \Lambda_d/I \longrightarrow Z = \bigoplus \mathbb{Z}_p[\underline{\zeta}]$$

is injective by Corollary 5.86. But this means that $\overline{x} \in \ker(\Phi)$ satisfies

$$p^{n_1+\ldots+n_{d-1}+n_d-m_d} \cdot \overline{x} = \overline{0}\,.$$

□

Now we are ready for the *proof of Lemma 5.80*:

Proof. We consider the map $\Phi : N/(I \cdot N) \longrightarrow \bigoplus N_{\underline{\zeta}}$ of the previous lemma. If $\overline{x}$ is contained in the $\mathbb{Z}_p$-torsion subgroup of $N/(I \cdot N)$, then $\Phi(\overline{x})$ represents a $\mathbb{Z}_p$-torsion element in each of the $N_{\underline{\zeta}}$.

Therefore $p^{c(N)} \cdot \overline{x} \in \ker(\Phi)$, where $c(N)$ denotes the constant defined in Lemma 5.88. But then

$$p^{n_1+\ldots+n_{d-1}+(n_d-m_d)+c(N)} \cdot \overline{x} = \overline{0}\,,$$

by Lemma 5.89. □

5.9 The rank inequality

In this section, we will prove the Rank Inequality Conjecture 5.65 in some special cases. This yields weak unconditional versions of Theorem 5.77. We will state basically three main results.

Theorem 5.90. *Write $E = \Lambda_d/(\mathfrak{p})$ for some $\mathfrak{p} \in \Lambda_d$.*

(i) Suppose that $\operatorname{rank}_{(T_1,\dots,T_d)}(E) < \infty$ for a choice of variables of Λ_d. Then $\operatorname{rank}_{(\tilde{T}_1,\dots,\tilde{T}_d)}(E) < \infty$ for every set of variables arising from $\{T_1,\dots,T_d\}$ by an admissible change of variables in the sense of Definition 4.6.

(ii) If $T_1,\dots,T_d$ can be chosen such that moreover, there exists some index $i \in \{1,\dots,d\}$ such that the residue class of $\mathfrak{p}$ in

$$\Lambda_d/(T_1,\dots,T_{i-1},T_{i+1},\dots,T_d) \;\cong\; \mathbb{Z}_p[[T_i]]$$

is coprime to every polynomial $\nu_{(n,0)}(T_i) \in \mathbb{Z}_p[T_i]$, $n \in \mathbb{N}$, then the Rank Inequality Conjecture 5.65 holds for every tuple $\{\tilde{T}_1,\dots,\tilde{T}_d\}$.

Proof. (i) We first note that whenever $\tilde{T}_1,\dots,\tilde{T}_d$ are obtained from $T_1,\dots,T_d$ by an admissible change of variables, then we have an equality of ideals

$$(T_1,\dots,T_d) \;=\; (\tilde{T}_1,\dots,\tilde{T}_d)\,.$$

Indeed,

$$\tilde{T}_i \;=\; \prod_{j=1}^{d}(T_j+1)^{a_{ij}} - 1$$

for each $1 \le i \le d$, where $a_{ij} \in \mathbb{Z}_p$ denote suitable elements, respectively. Therefore $\tilde{T}_i \in (T_1,\dots,T_d)$ for every i.
Conversely, the set $\{T_1,\dots,T_d\}$ arises as an admissible change of variables of $\{\tilde{T}_1,\dots,\tilde{T}_d\}$, and therefore also $T_i \in (\tilde{T}_1,\dots,\tilde{T}_d)$ for every i.
This means that

$$\operatorname{rank}_{(T_1,\dots,T_d)}(N) \;=\; \operatorname{rank}_{(\tilde{T}_1,\dots,\tilde{T}_d)}(N)$$

for every Λ_d-module N, proving the first statement of the theorem. Note that $\operatorname{rank}_{(T_1,\dots,T_d)}(\Lambda_d/(\mathfrak{p})) < \infty$ if and only if $\mathfrak{p} \notin (T_1,\dots,T_d)$, which means that $\mathfrak{p}$ has a 'non-trivial constant coefficient'.
We will now turn to the proof of (ii). We write $\Lambda_d = \mathbb{Z}_p[[\Gamma^d]]$, where $\Gamma^d \cong \mathbb{Z}_p^d$ is generated topologically by the elements

$$\gamma_1 \;:=\; T_1+1,\;\dots,\;\gamma_d \;:=\; T_d+1\,.$$

By the above, we are free to choose a different set of generators of Γ^d and prove the conjecture for the corresponding variables.

(ii) After renumbering the variables $T_1,\dots,T_d$, we may assume that the residue class of $\mathfrak{p}$ in $\mathbb{Z}_p[[T_1,\dots,T_{d-2},T_d]] \cong \mathbb{Z}_p[[T_{d-1}]]$ is coprime to the polynomials $\nu_{(n,0)}(T_{d-1})$, $n \in \mathbb{N}$. This condition is equivalent to saying that

$$\operatorname{rank}_{(T_1,\dots,T_{d-2},\nu_{(n,0)}(T_{d-1}),T_d)}(E) \;<\; \infty$$

for every $n \in \mathbb{N}$ (compare Lemma 1.17).
Let $\tilde{E} \subseteq E$ denote a submodule such that $M := E/\tilde{E}$ is a pseudo-null Λ_d-module. Let $\tilde{h} \in \Lambda_d$ be an annihilator of M which is coprime to $\mathfrak{p}$ (compare Remarks 2.20, (3)). We write $\mathfrak{p} = p^{m_0}\cdot g$ and $\tilde{h} = p^{n_0}\cdot h$ with $p \nmid g\cdot h$ in Λ_d (so that $m_0 = 0$ or $n_0 = 0$).

After an admissible change of variables, we may assume that g and h are regular with respect to T_d in the sense of Definition 4.9 (compare Lemma 4.7). Note that such a change of variables does not destroy the property that $\mathrm{rank}_{(T_1,\ldots,T_{d-2},\nu_{(n,0)}(T_{d-1}),T_d)}(E) < \infty$ for every $n \in \mathbb{N}$. Indeed, the new variables $X_1, \ldots, X_d$ are obtained from $T_1, \ldots, T_d$ by the rule

$$\begin{aligned} X_1 &= (T_1+1)(T_d+1)^{a_1} - 1 \,, \\ &\vdots \\ X_{d-1} &= (T_{d-1}+1)(T_d+1)^{a_{d-1}} - 1 \,, \\ X_d &= T_d \,, \end{aligned}$$

where $a_1, \ldots, a_{d-1} \in \mathbb{Z}_p$ are suitable powers of p. But then

$$X_i \equiv T_i \mod T_d$$

for every $1 \leq i \leq d-1$, and therefore

$$\mathrm{rank}_{(X_1,\ldots,X_{d-2},\nu_{(n,0)}(X_{d-1}),X_d)}(E) = \mathrm{rank}_{(T_1,\ldots,T_{d-2},\nu_{(n,0)}(T_{d-1}),T_d)}(E)$$

for every $n \in \mathbb{N}$.
We now apply the following result of J. Minardi.

Lemma 5.91 (Minardi)**.** *Suppose that $d \geq 3$, and let $g, h \in \mathbb{Z}_p[[T_1, \ldots, T_d]]$ be relatively prime and both regular with respect to T_d. Then for all but finitely many subgroups $<\sigma> \subseteq H := <\gamma_1, \ldots, \gamma_{d-1}>$ satisfying $H/<\sigma> \cong \mathbb{Z}_p^{d-2}$, the residue classes of g and h in $\Lambda_d/<\sigma - 1>$ are relatively prime.*

Proof. See Proposition 4.C in [Min 86]. □

Inductively, we see that the generators $\gamma_1, \ldots, \gamma_d$ of Γ^d may be chosen such that the images of g and h in

$$\Lambda_2 := \mathbb{Z}_p[[T_{d-1}, T_d]] \cong \Lambda_d/(T_1, \ldots, T_{d-2})$$

still are relatively prime.
After multiplication of g by a unit in Λ_d, we may assume that g equals a monic polynomial in $(\mathbb{Z}_p[[T_1, \ldots, T_{d-1}]])[T_d]$. We therefore may choose a representative of the residue class of g in Λ_2 of the form

$$f_0(T_{d-1}) + f_1(T_{d-1}) \cdot T_d + \ldots + f_{k-1}(T_{d-1}) \cdot T_d^{k-1} + T_d^k \,,$$

$k \in \mathbb{N}$, where $f_0, \ldots, f_{k-1} \in \mathbb{Z}_p[[T_{d-1}]]$. Then $f_0(0) \neq 0$, since we assume that $\mathrm{rank}_{(T_1,\ldots,T_d)}(E)$ is finite and therefore $\mathfrak{p} = p^{m_0} \cdot g \notin (T_1, \ldots, T_d)$.
Now we apply another result of Minardi.

Lemma 5.92 (Minardi)**.** *Suppose that $g, h \in \Lambda_2$ are relatively prime, and that we can write*

$$g = f_0(T_{d-1}) + f_1(T_{d-1}) \cdot T_d + \ldots + f_{k-1}(T_{d-1}) \cdot T_d^{k-1} + T_d^k \,.$$

We assume that $f_0(T_{d-1})$ is relatively prime to p and to each of the polynomials $\nu_{(n,0)}(T_{d-1}) \cdot T_{d-1} = (T_{d-1}+1)^{p^n} - 1$, $n \in \mathbb{N}$. Then the following holds.
For every $l \in \mathbb{N}$, there exists an element $\alpha \in p^l \cdot \mathbb{Z}_p$ such that the residue classes of g and h in $\Lambda_2/(T_\alpha)$ are relatively prime, where

$$T_\alpha := (T_d+1)(T_{d-1}+1)^{-\alpha} - 1 \, .$$

Proof. See Lemma 4.2 in [Min 86]; we will give a sketch of the proof in course of the proof of the next lemma. □

We may actually modify this result, obtaining the following lemma.

Lemma 5.93. *Suppose that $\mathfrak{p}, \tilde{h} \in \Lambda_2$ are relatively prime, and that we can write*

$$\mathfrak{p} = p^{m_0} \cdot (f_0(T_{d-1}) + f_1(T_{d-1}) \cdot T_d + \ldots + f_{k-1}(T_{d-1}) \cdot T_d^{k-1} + T_d^k)$$

for some $m_0 \in \mathbb{N}_0$. We assume that $f_0(T_{d-1})$ is coprime to each of the polynomials $\nu_{(n,0)}(T_{d-1}) \cdot T_{d-1}$, $n \in \mathbb{N}$.
Then $l_0 \in \mathbb{N}$ can be chosen large enough such that for every $l > l_0$, there exists an element $\alpha \in p^l \cdot \mathbb{Z}_p$ such that the residue classes of $\mathfrak{p}$ and $\tilde{h}$ in $\Lambda_2/(T_\alpha)$ are relatively prime.

Proof. We will first describe the strategy behind Minardi's proof of Lemma 5.92. Let thus $g, h \in \Lambda_2$ be as in the statement of that lemma. For $\alpha \in \mathbb{Z}_p$, we define

$$g_\alpha(T_{d-1}) := f_0(T_{d-1}) + f_1(T_{d-1})((T_{d-1}+1)^\alpha - 1) + \ldots + ((T_{d-1}+1)^\alpha - 1)^k \, .$$

Then $g \equiv g_\alpha \mod T_\alpha$. Note that $T_\alpha \nmid g_\alpha$, since $f_0(T_{d-1})$ is coprime to T_{d-1} and therefore $g \notin (T_1, \ldots, T_{d-1}, T_d) = (T_1, \ldots, T_{d-1}, T_\alpha)$. Moreover, if α is divisible by a sufficiently large power of p, then $p \nmid g_\alpha$, since $f_0(T_{d-1})$ is coprime to p. Indeed, $f_0(T_{d-1})$ is associated to a distinguished polynomial $\tilde{f}_0 \in \mathbb{Z}_p[T_{d-1}]$. Let $\tilde{l} := \deg(\tilde{f}_0)$, and choose $l \in \mathbb{N}$ large enough to ensure that $p^{l-1} > \tilde{l}$. Let $\alpha \in p^l \cdot \mathbb{Z}_p$, and let ζ denote a primitive p^l-th root of unity contained in a suitable algebraic extension K of $\mathbb{Q}_p$. If $p \mid g_\alpha$, then $g_\alpha(\zeta - 1) \equiv 0 \mod p$ in the ring of integral elements of K. But $((\zeta - 1) + 1)^\alpha - 1 = 0$, because $\alpha \in p^l \cdot \mathbb{Z}_p$. Therefore $g_\alpha(\zeta - 1) = f_0(\zeta - 1)$ is associated to $\tilde{f}_0(\zeta - 1)$. Since

$$\deg(\tilde{f}_0) = \tilde{l} < p^{(l-1)}(p-1) \, ,$$

we may conclude that $v_p(\tilde{f}_0(\zeta - 1)) < 1$, proving that $p \nmid g_\alpha(\zeta - 1)$.
For every α, Minardi chose an irreducible distinguished polynomial factor $P_\alpha(T_{d-1})$ of $g_\alpha(T_{d-1}) \in \mathbb{Z}_p[[T_{d-1}]]$, respectively, and he proved that the set of prime ideals

$$\{\mathfrak{A}_\alpha = (T_\alpha, P_\alpha(T_{d-1})) \mid \alpha \in p^l \cdot \mathbb{Z}_p\}$$

of Λ_2 is infinite for every $l \in \mathbb{N}$. This step of the proof needs the assumption that $f_0(T_{d-1})$ is coprime to every polynomial $\nu_{(n,0)}(T_{d-1}) \cdot T_{d-1}$ in $\mathbb{Z}_p[[T_{d-1}]]$.
Minardi then explained that

$$\bigcap_{\alpha \in p^l \cdot \mathbb{Z}_p} \mathfrak{A}_\alpha$$

is contained in a prime ideal $(R) \subseteq \Lambda_2$ of height one.
Now suppose that the images of g and h in $\Lambda_2/(T_\alpha)$ are not relatively prime. Then we can choose some $P_\alpha(T_{d-1})$ dividing both g and h modulo T_α, and therefore

$$g, h \in \mathfrak{A}_\alpha = (T_\alpha, P_\alpha(T_{d-1}))$$

for this choice of P_α. If the statement of the lemma was wrong, we could therefore conclude that

$$g, h \in \bigcap_{\alpha \in p^l \cdot \mathbb{Z}_p} \mathfrak{A}_\alpha \subseteq (R) ,$$

in contradiction to the assumption that $g, h \in \Lambda_2$ are relatively prime.

Now we start with the proof of Lemma 5.93. Suppose first that $m_0 = 0$, but that p divides $f_0(T_{d-1})$. We have to exclude the possibility that the residue classes of $\mathfrak{p} = g$ and $\tilde{h}$ in $\Lambda_2/(T_\alpha)$ both are divisible by p. Then each irreducible common factor will be associated to some distinguished polynomial $P_\alpha(T_{d-1})$, and Minardi's proof will go through.
Since $l_0(\mathfrak{p}) < \infty$, there exists an integer $l \in \mathbb{N}$ such that $\overline{\gamma_\alpha - 1}$ does not divide $\overline{\mathfrak{p}} \in \Lambda_2/(p)$ for every $0 \neq \alpha \in p^l \cdot \mathbb{Z}_p$, where

$$\gamma_\alpha := \gamma_d \cdot \gamma_{d-1}^{-\alpha} = T_\alpha + 1 .$$

Here we use the fact that the irreducible elements $\overline{\gamma_\alpha - 1} \in \Lambda_2/(p)$, $\alpha \in \mathbb{Z}_p$, are pairwise coprime since the elements $\gamma_\alpha \in \Gamma^d \setminus (\Gamma^d)^p$ generate different subgroups of Γ^d, respectively.
But this means that $\mathfrak{p} \notin (p, T_\alpha) \in \Lambda_2$ for every $0 \neq \alpha \in p^l \cdot \mathbb{Z}_p$, and thus the image of $\mathfrak{p}$ in $\Lambda_2/(T_\alpha)$ is coprime to the residue class of p for these α.
Finally, suppose that $m_0 > 0$. Then p divides the image of $\mathfrak{p}$ in $\Lambda_2/(T_\alpha)$ for each $\alpha \in \mathbb{Z}_p$. However, $p \nmid \tilde{h}$, since $\mathfrak{p}$ and $\tilde{h}$ are coprime in Λ_2. If $l \in \mathbb{N}$ is large enough to ensure that $\overline{\gamma_\alpha - 1}$ does not divide the residue class of $\tilde{h}$ in $\Lambda_2/(p)$ for every $0 \neq \alpha \in p^l \cdot \mathbb{Z}_p$, then the residue class of $\tilde{h}$ in $\Lambda_2/(T_\alpha)$ is coprime to p. Therefore, for these α, each possible common factor of the classes of $\mathfrak{p}$ and $\tilde{h}$ in $\Lambda_2/(T_\alpha)$ is divisible by some distinguished polynomial $P_\alpha(T_{d-1})$. □

For every $\alpha \in \mathbb{Z}_p$, the set $\{\gamma_1, \ldots, \gamma_{d-2}, \gamma_{d-1}, \gamma_\alpha = \gamma_d \cdot \gamma_{d-1}^{-\alpha}\}$ topologically generates the group Γ^d. We have therefore proved the following fact.

Proposition 5.94. *Under the assumptions of Theorem 5.90, (ii), we may choose variables $T_1, \ldots, T_d$ of Λ_d such that*

$$M/((T_1, \ldots, T_{d-2}, T_d) \cdot M)$$

is finite.

Proof. This follows from Lemmas 5.91 and 5.93. Indeed, Lemma 5.91 implies that we may choose variables $T_1, \ldots, T_d$ such that the images of g and h in Λ_2 are coprime. Since both g and h are regular with respect to T_d, the corresponding residue classes both are also coprime to p. Therefore at most one of the images of the elements $\mathfrak{p}$ and $\tilde{h}$ in the unique factorisation domain Λ_2 is divisible by p.
In order to be able to apply Lemma 5.93, it therefore remains to prove that $f_0(T_{d-1})$ in the representation of g is coprime to $\nu_{(n,0)}(T_{d-1}) \cdot T_{d-1}$ for every $n \in \mathbb{N}$. First, $f_0(T_{d-1})$ is coprime to T_{d-1}, since $g \notin (T_1, \ldots, T_{d-2}, T_{d-1}, T_d)$ by assumption.
Moreover, we also assume that the residue class of $\mathfrak{p} = p^{m_0} \cdot g$ in the quotient $\Lambda_d/(T_1, \ldots, T_{d-2}, T_d)$ is coprime to each $\nu_{(n,0)}(T_{d-1})$. Since the element $p^{m_0} \cdot f_0(T_{d-1})$ is contained in this residue class, the conditions of Lemma 5.82 are fulfilled.
Lemma 5.93 implies that the images of $\mathfrak{p}$ and $\tilde{h}$ in

$$\Lambda_d/(T_1, \ldots, T_{d-2}, T_d) \;\cong\; \mathbb{Z}_p[[T_{d-1}]]$$

are coprime for a suitable choice of T_d (let $T_d := T_\alpha$ in the notation from Lemma 5.93). Therefore $\Lambda_d/(T_1, \ldots, T_{d-2}, T_d, \mathfrak{p}, \tilde{h})$ is finite. But this means that also $M/((T_1, \ldots, T_{d-2}, T_d) \cdot M)$ is finite.

□

The next step of the proof may be formulated in a more general setting.

Proposition 5.95. *Let $f_1, \ldots, f_d \in \Lambda_d$ be such that $\operatorname{rank}_{(f_1,\ldots,f_d)}(E)$ is finite, and suppose that there exists some index $i \in \{1, \ldots, d\}$ such that $\Lambda_d/(f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_d)$ is a unique factorisation domain. Then multiplication by f_i on $E/((f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_d) \cdot E)$ is injective.*

Proof. The local ring

$$Q \;:=\; \Lambda_d/(f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_d)$$

has Krull dimension at least two by Proposition 2.17, (ii) and Corollary 10.9 in [Ei 95].
Suppose that multiplication by f_i on

$$E/((f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_d) \cdot E) \;=\; Q/(\mathfrak{p} \cdot Q)$$

is not injective. Since Q is a unique factorisation domain, this means that the residue classes of f_i and $\mathfrak{p}$ in Q are not coprime. If d denotes an irreducible common divisor, then the classes of both f_i and $\mathfrak{p}$ are contained in the principal ideal of Q generated by d. In particular,

$$|E/((f_1, \ldots, f_d) \cdot E)| \;=\; |Q/((f_i, \mathfrak{p}) \cdot Q)| \;\geq\; |Q/(d)| \,.$$

This contradicts the assumption that $\operatorname{rank}_{(f_1,\ldots,f_d)}(E) < \infty$, because $Q/(d)$ is a local domain having Krull dimension at least equal to

$$\dim(Q) - 1 \;\geq\; 1$$

by Corollary 10.9 in [Ei 95], and therefore $Q/(d)$ is infinite, using Corollary 10.7 of [Ei 95]. □

Lemma 5.96. *Let E, $\tilde{E}$ and $M = E/\tilde{E}$ be defined as above, let further $f_1, \ldots, f_d \in \Lambda_d$ be elements as in Proposition 5.95. Suppose that additionally,*

$$M/((f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_d) \cdot M)$$

is finite for the index $i \in \{1, \ldots, d\}$ from Proposition 5.95.
Then $\operatorname{rank}_{(f_1,\ldots,f_d)}(\tilde{E}) \geq \operatorname{rank}_{(f_1,\ldots,f_d)}(E)$.

Proof. Let $I \subseteq \Lambda_d$ be the ideal generated by $f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_d$. The exact sequence

$$0 \longrightarrow \tilde{E} \longrightarrow E \longrightarrow M \longrightarrow 0$$

induces an exact sequence

$$0 \longrightarrow \underbrace{\tilde{E}/\tilde{N}}_{=:\, N_1} \longrightarrow \underbrace{E/(I \cdot E)}_{=:\, N_2} \longrightarrow \underbrace{M/(I \cdot M)}_{=:\, N_3} \longrightarrow 0\,,$$

where $\tilde{N} := I \cdot E \cap \tilde{E}$.
We let $N_j[f_i] := \{x \in N_j \mid f_i \cdot x = 0\}$, $j \in \{1, 2, 3\}$. As in the proof of Proposition 3.43, (ii), we can apply the Snake Lemma to the commutative diagram

$$\begin{array}{ccccccccc}
 & & N_1[f_i] & & N_2[f_i] & & N_3[f_i] & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & N_1 & \longrightarrow & N_2 & \longrightarrow & N_3 & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \cdot f_i} & & \downarrow{\scriptstyle \cdot f_i} & & \downarrow{\scriptstyle \cdot f_i} & & \\
0 & \longrightarrow & N_1 & \longrightarrow & N_2 & \longrightarrow & N_3 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & N_1/(f_i \cdot N_1) & & N_2/(f_i \cdot N_2) & & N_3/(f_i \cdot N_3) & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

and obtain a long exact sequence

$$\begin{array}{l}
0 \longrightarrow N_1[f_i] \longrightarrow N_2[f_i] \longrightarrow N_3[f_i] \\
\qquad \longrightarrow N_1/(f_i \cdot N_1) \longrightarrow N_2/(f_i \cdot N_2) \longrightarrow N_3/(f_i \cdot N_3) \longrightarrow 0\,.
\end{array}$$

Since Proposition 5.95 implies that

$$N_2[f_i] \;=\; (E/(I \cdot E))[f_i] \;=\; \{\overline{0}\}\,,$$

we obtain an exact sequence

$$0 \longrightarrow (M/(I\cdot M))[f_i] \longrightarrow \tilde{E}/(\tilde{N}+(f_1,\ldots,f_d)\cdot\tilde{E}) \longrightarrow E/((f_1,\ldots,f_d)\cdot E) \longrightarrow M/((f_1,\ldots,f_d)\cdot M) \longrightarrow 0\ .$$

Since $E/((f_1,\ldots,f_d)\cdot E)$ is finite and therefore also $\tilde{E}/((f_1,\ldots,f_d)\cdot\tilde{E})$ is finite by Lemma 5.59, in fact all the four quotients occurring in this exact sequence are finite.
Moreover,

$$\frac{|(M/(I\cdot M))[f_i]|}{|\tilde{E}/(\tilde{N}+(f_1,\ldots,f_d)\cdot\tilde{E})|}\cdot\frac{|E/((f_1,\ldots,f_d)\cdot E)|}{|M/((f_1,\ldots,f_d)\cdot M)|} \;=\; 1\ ,$$

i.e.,

$$\begin{aligned} v_p(|(M/(I\cdot M))[f_i]|)+\mathrm{rank}(E) &= v_p(|\tilde{E}/(\tilde{N}+(f_1,\ldots,f_d)\cdot\tilde{E})|) \\ &\quad +\ \mathrm{rank}(M) \\ &\leq \mathrm{rank}(\tilde{E})\ +\ \mathrm{rank}(M)\ , \end{aligned}$$

where rank always denotes $\mathrm{rank}_{(f_1,\ldots,f_d)}$. Therefore

$$\mathrm{rank}_{(f_1,\ldots,f_d)}(\tilde{E}) \;\geq\; \mathrm{rank}_{(f_1,\ldots,f_d)}(E)+C\ ,$$

where $C := v_p(|(M/(I\cdot M))[f_i]|)-\mathrm{rank}_{(f_1,\ldots,f_d)}(M)$. Since the quotient $M/(I\cdot M)$ is finite by assumption, it is easy to see that

$$v_p(|(M/(I\cdot M))[f_i]|) \;=\; \mathrm{rank}_{(f_1,\ldots,f_d)}(M)\ ,$$

and therefore $C=0$ (compare the proof of Proposition 3.43, (i)). □

Theorem 5.90 now immediately follows from Proposition 5.94, Proposition 5.95 and Lemma 5.96 (apply Proposition 5.95 to the elements $f_j = T_j$, $1\leq j\leq d$, and let $i=d-1$).

□

Remarks 5.97.
(1) The assumption in Theorem 5.90, (ii) that the residue class of $\mathfrak{p}$ in

$$\Lambda_d/(T_1,\ldots,T_{d-2},T_d)$$

is coprime to the polynomials $\nu_{(n,0)}(T_{d-1})$, $n\in\mathbb{N}$, is not as restrictive as it might seem at first glance. In fact, each $\nu_{(n+1,n)}(T_{d-1})$, $n\in\mathbb{N}$, is irreducible of degree $p^n(p-1)$. If $g\in\mathbb{Z}_p[[T_{d-1}]]$ denotes a representative of the residue class of $\mathfrak{p}$, and if

$$g \;=\; p^r\cdot u\cdot\tilde{g}$$

for some unit $u\in(\mathbb{Z}_p[[T_{d-1}]])^*$ and a suitable distinguished polynomial $\tilde{g}\in\mathbb{Z}_p[T_{d-1}]$ of degree t, then the above conditions are fulfilled if $\tilde{g}$ is coprime to the finitely many $\nu_{(n+1,n)}$ of the $n\in\mathbb{N}$ satisfying $p^n(p-1)\leq t$.

(2) MINARDI proved that the conditions are satisfied in the following example: If $\mathbb{K}$ denotes the $\mathbb{Z}_p^2$-extension of $K := \mathbb{Q}(\sqrt{-31})$, K_∞/K denotes the cyclotomic $\mathbb{Z}_p$-extension, and if the restriction of $\gamma_1 \in \mathrm{Gal}(\mathbb{K}/K)$ to K_∞ topologically generates $\mathrm{Gal}(K_\infty/K)$, then the residue class of the characteristic power series $\mathfrak{p} \in \Lambda_2$ of $\mathbb{K}/K$ in $\mathbb{Z}_p[[\mathrm{Gal}(K_\infty/K)]] \cong \mathbb{Z}_p[[T_1]]$, $T_1 := \gamma_1 - 1$, is coprime to the polynomials $\nu_{(n,0)}(T_1)$ for every $n \in \mathbb{N}$ (compare p. 27 in [Min 86]).
We will formalise and generalise this example by using the following result.

Let $\mathbb{K}/K$ be a $\mathbb{Z}_p^d$-extension of a number field K, $d \in \mathbb{N}$, and let L be a $\mathbb{Z}_p^{d-1}$-extension of K which is contained in $\mathbb{K}$. Let $H(\mathbb{K})$, respectively, $H(L)$, denote the maximal p-abelian unramified extensions of $\mathbb{K}$, respectively, of L. Let further $X := \mathrm{Gal}(H(\mathbb{K})/\mathbb{K})$.

If γ denotes a topological generator of $\mathrm{Gal}(\mathbb{K}/L) \cong \mathbb{Z}_p$, and if $T := \gamma - 1$, then the completed group ring $\mathbb{Z}_p[[T]] \cong \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{K}/L)]]$ acts on X via conjugation, as in Section 1.3.

Lemma 5.98. *Let $\mathbb{K}$ and L be as above. We assume that exactly one prime ramifies in $\mathbb{K}/L$. Then there exists a $\mathbb{Z}_p[[\mathrm{Gal}(L/K)]]$-module homomorphism*

$$X/(T \cdot X) \longrightarrow \mathrm{Gal}(H(L)/L)$$

whose kernel and cokernel are annihilated by $p^{e(\mathbb{K}/L)}$. Here $e(\mathbb{K}/L)$ is defined as in Proposition 1.3.
More generally, if $\mathbb{K}/L$ is a $\mathbb{Z}_p^i$-extension, $i \in \mathbb{N}$, such that exactly one prime is ramified in $\mathbb{K}/L$, if this prime is totally ramified, and if $\mathrm{Gal}(\mathbb{K}/L)$ is generated topologically by $\gamma_1, \ldots, \gamma_i$, then there exists a bijective $\mathbb{Z}_p[[\mathrm{Gal}(L/K)]]$-module homomorphism

$$X/((T_1, \ldots, T_i) \cdot X) \longrightarrow \mathrm{Gal}(H(L)/L)\ ,$$

where $T_1 = \gamma_1 - 1, \ldots, T_i = \gamma_i - 1$.

Proof. We will first assume that the prime of L ramifying in $\mathbb{K}$ is totally ramified. Then $\mathbb{K} \cap H(L) = L$.

Moreover, Proposition 1.34 implies that $H(L) \subseteq H(\mathbb{K})$. As in the proof of Lemma 4.3, (ii), we may conclude that there exists a canonical $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{K}/K)]]$-module homomorphism

$$X = \mathrm{Gal}(H(\mathbb{K})/\mathbb{K}) \twoheadrightarrow \mathrm{Gal}((\mathbb{K} \cdot H(L))/\mathbb{K}) \cong \mathrm{Gal}(H(L)/L)$$

with kernel $Y_0 := \mathrm{Gal}(H(\mathbb{K})/(\mathbb{K} \cdot H(L)))$. We will show that our assumptions imply that $Y_0 = (T_1, \ldots, T_i) \cdot X$; this in particular proves the lemma in the case where $\mathbb{K}/L$ is a $\mathbb{Z}_p$-extension satisfying $e(\mathbb{K}/L) = 0$.

First note that the topological commutator subgroup of $G := \mathrm{Gal}(H(\mathbb{K})/L)$ is equal to $(T_1, \ldots, T_i) \cdot X$, by Lemma 5.19.

Moreover, since $H(\mathbb{K})/L$ is a pro-p-extension, $H(L) \subseteq H(\mathbb{K})$ is the maximal subextension which is unramified and abelian over L. This means that

$\mathrm{Gal}(H(\mathbb{K})/H(L))$ is the closed subgroup of $G = \mathrm{Gal}(H(\mathbb{K})/L)$ which is generated by the topological commutator subgroup of G and by the inertia subgroup I of some prime $\mathfrak{P}$ of $H(\mathbb{K})$ dividing the prime $\mathfrak{p}$ of L that ramifies in $H(\mathbb{K})$.

Recall that $\mathfrak{p}$ is totally ramified in $\mathbb{K}/L$. Since $H(\mathbb{K})/\mathbb{K}$ is unramified, we may conclude that $I \cap X = \{1\}$ and $I \cong G/X$, i.e., $G \cong X \rtimes I$, as in Section 1.3. This implies that

$$\begin{aligned} \mathrm{Gal}((\mathbb{K} \cdot H(L))/\mathbb{K}) &\cong \mathrm{Gal}(H(L)/L) \\ &\cong G \,/\, \mathrm{Gal}(H(\mathbb{K})/H(L)) \\ &\cong (X \rtimes I) \,/\, <(T_1, \ldots, T_i) \cdot X, I> \\ &\cong X/((T_1, \ldots, T_i) \cdot X) \end{aligned}$$

(compare the proofs of Lemma 1.37 and Lemma 5.23).

But then

$$Y_0 \;=\; \mathrm{Gal}(H(\mathbb{K})/(\mathbb{K} \cdot H(L))) \;\cong\; (T_1, \ldots, T_i) \cdot X \;,$$

proving that we have in fact equality because $(T_1, \ldots, T_i) \cdot X \subseteq Y_0$, since

$$G/Y_0 \;\cong\; \mathrm{Gal}((\mathbb{K} \cdot H(L))/L)$$

is abelian.

Now suppose that $\mathbb{K}/L$ is a $\mathbb{Z}_p$-extension such that $e := e(\mathbb{K}/L) > 0$. We denote by $\mathbb{K}_e \subseteq \mathbb{K}$ the unique subfield which is cyclic of degree p^e over L. Then $H(L) \cap \mathbb{K} = \mathbb{K}_e$. As in the first case, we consider the surjective $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{K}/K)]]$-module homomorphism

$$X \;\longrightarrow\!\!\!\!\!\rightarrow\; \mathrm{Gal}((\mathbb{K} \cdot H(L))/\mathbb{K}) \;\cong\; \mathrm{Gal}(H(L)/\mathbb{K}_e)$$

with kernel $Y_0 := \mathrm{Gal}(H(\mathbb{K})/(\mathbb{K} \cdot H(L)))$. If $\sigma \in \mathrm{Gal}(H(L)/L)$, then the order of $\sigma|_{\mathbb{K}_e}$ is bounded by p^e. This means that $\sigma^{p^e} \in \mathrm{Gal}(H(L)/\mathbb{K}_e)$, proving that the cokernel of the induced homomorphism

$$X \;\longrightarrow\!\!\!\!\!\rightarrow\; \mathrm{Gal}(H(L)/\mathbb{K}_e) \hookrightarrow \mathrm{Gal}(H(L)/L)$$

is annihilated by p^e.

Let $\mathfrak{p}$ be the unique prime of L which ramifies in $\mathbb{K}$, and let

$$I \;\subseteq\; G \;=\; \mathrm{Gal}(H(\mathbb{K})/L)$$

denote the inertia subgroup of some prime of $H(\mathbb{K})$ dividing $\mathfrak{p}$.

We note that the closure of the commutator subgroup of G is equal to $T \cdot X$. This has been proved by Greenberg (compare the proof of Proposition 2 in [Gr 73]).

Since $H(L) \subseteq H(\mathbb{K})$ is the maximal subextension which is unramified and abelian over L, it follows that $\mathrm{Gal}(H(\mathbb{K})/H(L))$ is generated by $T \cdot X$ and I, as in the first case.

The exact sequence

$$1 \longrightarrow X \longrightarrow G \longrightarrow G/X \longrightarrow 1$$

and the fact that $G/X \cong \mathrm{Gal}(\mathbb{K}/L)$ is $\mathbb{Z}_p$-free imply that G is isomorphic to the semidirect product $X \rtimes G/X$. If $e(\mathbb{K}/L) > 0$, then the injection $I \hookrightarrow G/X$ will not be surjective, and in fact $p^e \cdot (G/X) \cong I$. If

$$g \;=\; x \cdot \gamma \;\in\; X \rtimes G/X \;,$$

then

$$p^e \cdot g \;=\; (\nu_{(e,0)} \cdot x) \cdot \gamma^{p^e}$$

(compare p. 280 in [Wa 97]). Therefore

$$p^e \cdot G \;\cong\; (\nu_{(e,0)} \cdot X) \rtimes I \;.$$

This implies that we have isomorphisms

$$\begin{aligned} p^e \cdot \mathrm{Gal}(H(L)/L) &\cong p^e \cdot (G \,/\, \mathrm{Gal}(H(\mathbb{K})/H(L))) \\ &\cong p^e \cdot (G \,/ <T \cdot X, I>) \\ &\cong \nu_{(e,0)} \cdot (X/(T \cdot X)) \;. \end{aligned}$$

We have already mentioned above that

$$p^e \cdot \mathrm{Gal}(H(L)/L) \;\subseteq\; \mathrm{Gal}(H(L)/\mathbb{K}_e) \;.$$

The above isomorphisms therefore induce an injection

$$\nu_{(e,0)} \cdot (X/(T \cdot X)) \;\lhook\joinrel\longrightarrow\; \mathrm{Gal}(H(L)/\mathbb{K}_e) \;.$$

But $\mathrm{Gal}(H(L)/\mathbb{K}_e) \cong X/Y_0$ by definition of Y_0, and therefore we obtain an injective map

$$\nu_{(e,0)} \cdot (X/(T \cdot X)) \;\lhook\joinrel\longrightarrow\; X/Y_0 \;.$$

This means that $\nu_{(e,0)} \cdot Y_0 \subseteq T \cdot X$. Since $Y_0 \subseteq X$ and therefore $T \cdot Y_0 \subseteq T \cdot X$, it follows that

$$p^e \cdot Y_0 \;\subseteq\; T \cdot X \;,$$

proving Lemma 5.98. □

Corollary 5.99. *Let $\mathbb{K}/K$ be a $\mathbb{Z}_p^d$-extension of a number field K such that exactly one prime of K ramifies in $\mathbb{K}/K$, and such that this prime is totally ramified.*

(i) Then $T \nmid F_{A^{(M)}}(T)$ for every $\mathbb{Z}_p$-extension $M \subseteq \mathbb{K}$ of K.

(ii) If $M \subseteq \mathbb{K}$ is an arbitrary $\mathbb{Z}_p$-extension of K, and if $T_1, \ldots, T_d$ are variables of $\Lambda_d = \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{K}/K)]]$ such that $\gamma_{d-1} = T_{d-1} + 1$ topologically generates $\mathrm{Gal}(M/K)$, then

$$\mathrm{rank}_{(T_1,\ldots,T_d)}(A^{(\mathbb{K})}) < \infty \quad \textit{and} \quad \mathrm{rank}_{(T_1,\ldots,T_{d-2},\nu_{(n,0)}(T_{d-1}),T_d)}(A^{(\mathbb{K})}) < \infty$$

for every $n \in \mathbb{N}$. In particular, this means that the image of the characteristic power series $F_{A^{(\mathbb{K})}}$ of $A^{(\mathbb{K})}$ in $\Lambda_d/(T_1, \ldots, T_{d-2}, T_d)$ is coprime to T_{d-1} and to each $\nu_{(n,0)}(T_{d-1})$, $n \in \mathbb{N}$.

Proof. (i) We apply Lemma 5.98 with $L = K$. For every $M \in \mathcal{E}(K)$, this yields a $\mathbb{Z}_p$-module homomorphism

$$\varphi^{(M)} : A^{(M)}/(T^{(M)} \cdot A^{(M)}) \longrightarrow \mathrm{Gal}(H(K)/K) ,$$

where $T^{(M)} = \gamma^{(M)} - 1$ for some topological generator $\gamma^{(M)}$ of the group $\mathrm{Gal}(M/K) \cong \mathbb{Z}_p$, respectively. Moreover, if $M \subseteq \mathbb{K}$, then this map actually is a bijection, because $e(M/K) = 0$ for every $M \subseteq \mathbb{K}$.

(ii) Let $M \subseteq \mathbb{K}$ be fixed, let $X := \mathrm{Gal}(H(\mathbb{K})/\mathbb{K})$. Lemma 5.98 implies that we have a bijective $\mathbb{Z}_p[[T_{d-1}]]$-module homomorphism

$$X/((T_1, \ldots, T_{d-2}, T_d) \cdot X) \longrightarrow \mathrm{Gal}(H(M)/M) \cong A^{(M)} .$$

Since $T_{d-1} \nmid F_{A^{(M)}}(T_{d-1})$, by (i), it follows that

$$|X/((T_1, \ldots, T_{d-2}, T_{d-1}, T_d) \cdot X)| = |A^{(M)}/(T_{d-1} \cdot A^{(M)})|$$

is finite.
Analogously,

$$X/((T_1, \ldots, T_{d-2}, \nu_{(n,0)}(T_{d-1}), T_d) \cdot X)$$

is finite because the characteristic polynomial of $A^{(M)}$ is coprime to every $\nu_{(n,0)}(T_{d-1})$, $n \in \mathbb{N}$, since $e(M/K) = 0$ (compare Proposition 1.44).
Corollary 5.62 implies that

$$\mathrm{rank}_{(T_1,\ldots,T_{d-2},T_{d-1},T_d)}(E_{A^{(\mathbb{K})}}) < \infty$$

and

$$\mathrm{rank}_{(T_1,\ldots,T_{d-2},\nu_{(n,0)}(T_{d-1}),T_d)}(E_{A^{(\mathbb{K})}}) < \infty$$

for every $n \in \mathbb{N}$, where $E_{A^{(\mathbb{K})}} = \Lambda_d/(F_{A^{(\mathbb{K})}})$.
If the residue class of $F_{A^{(\mathbb{K})}}$ in $\Lambda_d/(T_1, \ldots, T_{d-2}, T_d)$ was not coprime to T_{d-1}, then the Krull dimension of

$$E_{A^{(\mathbb{K})}}/((T_1, \ldots, T_{d-2}, T_{d-1}, T_d) \cdot E_{A^{(\mathbb{K})}}) = \Lambda_d/(F_{A^{(\mathbb{K})}}, T_1, \ldots, T_d)$$

was greater or equal to 1, in contradiction to the fact that

$$\mathrm{rank}_{(T_1,\ldots,T_d)}(E_{A^{(\mathbb{K})}}) < \infty$$

(compare the proof of Proposition 5.95).
Analogously, we see that $F_{A^{(\mathbb{K})}}$ is coprime to each $\nu_{(n,0)}(T_{d-1})$, respectively. □

Remark 5.100. Corollary 5.99, (i) may be generalised as follows: If M/K denotes any $\mathbb{Z}_p$-extension of a number field K such that exactly one prime ramifies in M/K, then $T \nmid F_{A^{(M)}}(T)$ (compare also Remarks 3.47, (3)).
Indeed, Lemma 5.98 implies that there exists a $\mathbb{Z}_p$-module homomorphism

$$\varphi^{(M)} : A^{(M)}/(T \cdot A^{(M)}) \longrightarrow \mathrm{Gal}(H(K)/K)$$

such that the kernel of $\varphi^{(M)}$ is annihilated by $p^{e(M/K)}$. But

$$\ker(\varphi^{(M)}) \subseteq A^{(M)}/(T \cdot A^{(M)})$$

is finitely generated over $\mathbb{Z}_p$ and therefore finite, proving that $A^{(M)}/(T \cdot A^{(M)})$ is finite.

As an application, we obtain the following result.

Theorem 5.101. *Suppose that $\mathbb{K}/K$ denotes a $\mathbb{Z}_p^d$-extension. We assume that there exists a unique prime $\mathfrak{p}$ of K ramifying in $\mathbb{K}$, and that $\mathfrak{p}$ is totally ramified in $\mathbb{K}/K$.*
Then m_0 is locally bounded near $\mathbb{K}$, i.e., there exist a neighbourhood $U = \mathcal{U}(\mathbb{K}, r)$ of $\mathbb{K}$ and an integer $k \in \mathbb{N}$ such that

$$m_0(\mathbb{L}/K) \leq k$$

for every $\mathbb{L} \in U$.

Proof. Indeed, let $n \geq e(\mathbb{K}/K) + 1$ be an integer. Then every $\mathbb{L} \in \mathcal{U}(\mathbb{K}, n)$ is totally ramified at the prime $\mathfrak{p}$, and unramified outside $\mathfrak{p}$ by Proposition 5.39. Moreover, Corollary 5.99, (ii) implies that the conditions from Theorem 5.90, (ii) are satisfied for each $\mathbb{L} \in \mathcal{U}(\mathbb{K}, n)$ and every choice of variables $T_1, \ldots, T_d$, respectively.

Therefore inequality (5.1) from the proof of Theorem 5.77 holds for the tuple $(T_1, \ldots, T_d)$ and for each $\mathbb{L} \in \mathcal{U}(\mathbb{K}, r)$, provided that $r \geq n$ is large enough. In other words,

$$\operatorname{rank}_{(T_1,\ldots,T_d)}(E_{A^{(\mathbb{L})}}) \leq \operatorname{rank}_{(T_1,\ldots,T_d)}(A^{(\mathbb{K})}) =: C$$

for every such $\mathbb{L}$. But

$$\operatorname{rank}_{(T_1,\ldots,T_d)}(E_{A^{(\mathbb{L})}}) = m_0(\mathbb{L}/K) + v_p(|F_{A^{(\mathbb{L})}}(0, \ldots, 0)|) .$$

□

We now come to the second one of the three results announced at the beginning of the current section. Let $E = \Lambda_d/(\mathfrak{p})$ and $M = E/\tilde{E}$ be as above.

Theorem 5.102. *Under the assumptions of Theorem 5.90, (ii), suppose that additionally, $\mathfrak{p} \in \Lambda_d$ is regular with respect to the variable T_i in the sense of Definition 4.9. Then the Rank Inequality Conjecture also holds for the tuple*

$$(T_1, \ldots, T_{i-1}, T_{i+1}, \ldots, T_d, p)$$

and for every tuple

$$(T_1, \ldots, T_{i-1}, \nu_{(n,m)}(T_i), T_{i+1}, \ldots, T_d) ,$$

$n, m \in \mathbb{N}$ with $n > m$, for a suitable choice of $T_1, \ldots, T_{i-1}, T_{i+1}, \ldots, T_d$.

Proof. As in the proof of Theorem 5.90, we may assume that $i = d-1$. We first note that the additional assumption on $\mathfrak{p}$ ensures that

$$\operatorname{rank}_{(T_1,\dots,T_{d-2},T_d,p)}(E)$$

is finite. Indeed, $\mathfrak{p}$ is (up to multiplication by a unit) associated to a distinguished polynomial in

$$(\mathbb{Z}_p[[T_1,\dots,T_{d-2},T_d]])[T_{d-1}]\,,$$

and therefore

$$Q \;:=\; \Lambda_d/(T_1,\dots,T_{d-2},T_d,\mathfrak{p})$$

is isomorphic to a finitely generated free $\mathbb{Z}_p$-module (compare Remarks 5.47, (1)). But then $E/((T_1,\dots,T_{d-2},T_d,p)\cdot E) = Q/(p\cdot Q)$ is finite.

Moreover, if $n,m \in \mathbb{N}$, then the residue classes of $\mathfrak{p}$ and $\nu_{(n,m)}(T_{d-1})$ in $\Lambda_d/(T_1,\dots,T_{d-2},T_d) \cong \mathbb{Z}_p[[T_{d-1}]]$ are coprime by assumption, and therefore the ideal of $\mathbb{Z}_p[[T_{d-1}]]$ generated by these two residue classes contains the class of some power of p, by Lemma 1.17, (i). This proves that also

$$E/((T_1,\dots,T_{d-2},\nu_{(n,m)}(T_{d-1}),T_d)\cdot E)$$

is finite for every $n > m$.

The proof of Theorem 5.90 implies that we may choose variables $T_1,\dots,T_d$ such that $M/((T_1,\dots,T_{d-2},T_d)\cdot M)$ is finite (compare Proposition 5.94). Moreover, the admissible changes of variables which are used in course of this proof do not destroy the property that $\mathfrak{p}$ is regular with respect to the variable T_{d-1}.

Now we apply Proposition 5.95 with $i = d-1$, $f_i = p$, respectively, with $f_i = \nu_{(n,m)}(T_{d-1})$, and with $f_j = T_j$, $j \neq i$. This implies that multiplication by p, respectively, $\nu_{(n,m)}(T_{d-1})$, is injective on $E/((T_1,\dots,T_{d-2},T_d)\cdot E)$. The claim now follows from Lemma 5.96. □

The above theorem may be used for a proof of the following variant of Theorem 5.77 which does not presume the validity of Conjecture 5.65.

Theorem 5.103. *Let $\mathbb{K}/K$ be a $\mathbb{Z}_p^d$-extension. Suppose that there exists a prime of K that is totally ramified in $\mathbb{K}/K$, and that this is the only prime ramifying in $\mathbb{K}/K$. We assume that $m_0(\mathbb{K}/K) = 0$.*
Then there exist a neighbourhood $U = \mathcal{U}(\mathbb{K},r)$ of $\mathbb{K}$ and an integer $k \in \mathbb{N}$ such that

$$l_0(\mathbb{L}/K) \;\leq\; k$$

for every $\mathbb{L} \in U$.

Proof. Let $A = A^{(\mathbb{K})}$, and let $N := A/\tilde{A}$ be defined as in Section 5.7. Since $m_0(\mathbb{K}/K) = 0$, we may choose variables $T_1,\dots,T_d$ of Λ_d such that there exists an annihilator $g \in \Lambda_d$ of N such that g is divisible by the characteristic power series F_A of A, and regular with respect to T_{d-1} (compare the proof of Lemma 5.72).

This means that

$$E_A/((T_1,\dots,T_{d-2},T_d,p)\cdot E_A) \;=\; \Lambda_d/(F_A,T_1,\dots,T_{d-2},T_d,p)$$

and $N/((T_1,\dots,T_{d-2},T_d,p)\cdot N)$ are finite (compare the proof of Theorem 5.102). Proposition 5.52, (i) implies that

$$\operatorname{rank}_{(T_1,\dots,T_{d-2},T_d,p)}(A) \;\leq\; \operatorname{rank}_{(T_1,\dots,T_{d-2},T_d,p)}(E_A) \;+\; \operatorname{rank}_{(T_1,\dots,T_{d-2},T_d,p)}(N)$$

is also finite. We therefore may choose an integer $r_0 \in \mathbb{N}$, $r_0 \geq e(\mathbb{K}/K)+1$, such that

$$\operatorname{rank}_{(T_1,\dots,T_{d-2},T_d,p)}(A^{(\mathbb{L})}) \;=\; \operatorname{rank}_{(T_1,\dots,T_{d-2},T_d,p)}(A) \;<\; \infty$$

for every $\mathbb{L} \in \mathcal{U}(\mathbb{K},r_0)$.

In particular, Corollary 5.62 implies that $\operatorname{rank}_{(T_1,\dots,T_{d-2},T_d,p)}(E_{A^{(\mathbb{L})}}) < \infty$ for each $\mathbb{L} \in \mathcal{U}(\mathbb{K},r_0)$, proving that for these $\mathbb{L}$, the characteristic power series $F_{A^{(\mathbb{L})}}$ is regular with respect to T_{d-1}, respectively. Indeed, otherwise we have $F_{A^{(\mathbb{L})}} \in (p,T_1,\dots,T_{d-2},T_d)$ for some $\mathbb{L}$. But then

$$E_{A^{(\mathbb{L})}}/((T_1,\dots,T_{d-2},T_d,p)\cdot E_{A^{(\mathbb{L})}}) \;=\; \Lambda_d/(T_1,\dots,T_{d-2},T_d,p)$$

was infinite, yielding a contradiction.

If $\mathbb{L} \in \mathcal{U}(\mathbb{K},r_0)$, then $\mathcal{P}(\mathbb{L}) = \mathcal{P}(\mathbb{K})$ by Lemma 5.34, (i), and therefore the conditions from Corollary 5.99 are satisfied for every $\mathbb{L} \in \mathcal{U}(\mathbb{K},r_0)$, proving that we may apply Theorem 5.102 to every $\mathbb{L} \in \mathcal{U}(\mathbb{K},r_0)$.

For every $n,m \in \mathbb{N}$, $n > m$, we may find a neighbourhood $\mathcal{U}_{n,m} \subseteq \mathcal{U}(\mathbb{K},r_0)$ of $\mathbb{K}$ such that

$$\operatorname{rank}_{(T_1,\dots,T_{d-2},\nu_{(n,m)}(T_{d-1}),T_d)}(A^{(\mathbb{L})}) \;=\; \operatorname{rank}_{(T_1,\dots,T_{d-2},\nu_{(n,m)}(T_{d-1}),T_d)}(A)$$

for every $\mathbb{L} \in \mathcal{U}_{n,m}$. Moreover, the analogon of inequality (5.1) holds for $(T_1,\dots,T_{d-2},\nu_{(n,m)}(T_{d-1}),T_d)$ and every $\mathbb{L} \in \mathcal{U}_{n,m}$, by Theorem 5.102.

The proof of Lemma 5.78 shows that there exists a constant $C \in \mathbb{N}$ such that

$$\operatorname{rank}_{(T_1,\dots,T_{d-2},\nu_{(n,m)}(T_{d-1}),T_d)}(A/\tilde{A}) \;\leq\; C\cdot(n-m)$$

for every $n > m \geq e(\mathbb{K}/K)$. In fact, the p-rank of

$$(A/\tilde{A})/((T_1,\dots,T_{d-2},\nu_{(n,m)}(T_{d-1}),T_d)\cdot(A/\tilde{A}))$$

is bounded, and the main term comes from Lemma 5.80; compare Section 5.8.

As in the proof of Theorem 5.77, n and m may be taken large enough to ensure that

$$l_0(\mathbb{L}/K) \;\leq\; l_0(\mathbb{K}/K)+C$$

for each $\mathbb{L} \in \mathcal{U}_{n,m}$ (note that $m_0(\mathbb{L}/K)=0$ for every $\mathbb{L}$, since $F_{A^{(\mathbb{L})}}$ is regular with respect to T_{d-1}, respectively). □

The last result to be discussed in this section provides some evidence for our conjecture that the Rank Inequality not only holds in the special cases stated above, but in fact is valid for more general elements $f_1,\dots,f_d \in \Lambda_d$. We will make use of the following fact from commutative algebra.

Lemma 5.104 (Artin-Rees)**.** *Let R be a Noetherian ring, let $I \subseteq R$ be an ideal. Suppose that M is a finitely generated R-module, and let $N \subseteq M$ be a submodule. Then there exists an integer $k \geq 1$ such that*

$$I^n \cdot M \cap N \;=\; I^{n-k} \cdot ((I^k \cdot M) \cap N) \;\subseteq\; I^{n-k} \cdot N$$

for every $n \geq k$.

Proof. This follows from Lemma 5.1 in [Ei 95]. □

Corollary 5.105. *Let $E = \Lambda_d/(\mathfrak{p})$ be a cyclic Λ_d-module, let $\tilde{E} \subseteq E$ be a submodule such that $M := E/\tilde{E}$ is pseudo-null. Moreover, let $f_1, \ldots, f_d \in \Lambda_d$ be elements such that $\mathrm{rank}_{(f_1,\ldots,f_d)}(E) < \infty$. We write $I := (f_1, \ldots, f_d)$.*
Then there exists an integer $k \geq 1$ such that

$$\mathrm{rank}_{I^n}(\tilde{E}) \;\geq\; \mathrm{rank}_{I^{n-k}}(E) \quad \textit{and} \quad \mathrm{rank}_{I^n}(E) \;\geq\; \mathrm{rank}_{I^{n-k}}(\tilde{E})$$

for every $n > k$, where we let $\mathrm{rank}_{I^m}(N) := v_p(|N/(I^m \cdot N)|)$ for every $m \in \mathbb{N}$ and every Λ_d-module N, respectively, whenever this is finite.

Proof. We apply the Artin-Rees Lemma to $M = \tilde{E}$ and $N = E$. Let $k \in \mathbb{N}$ be the integer attached to I, and fix some $n > k$.

Since $M = E/\tilde{E}$ is pseudo-null, inclusion of $\tilde{E}$ in E yields a pseudo-isomorphism $\varphi : \tilde{E} \longrightarrow E$. Since both E and $\tilde{E}$ are finitely generated and Λ_d-torsion, there exists also a pseudo-isomorphism $\psi : E \longrightarrow \tilde{E}$ (compare Remarks 2.22, (1)). ψ actually is an injection, because the cyclic Λ_d-module $E = \Lambda_d/(\mathfrak{p})$ does not contain any non-trivial pseudo-null submodules. We therefore obtain an exact sequence

$$0 \longrightarrow E \xrightarrow{\psi} \tilde{E} \longrightarrow \underbrace{\tilde{E}/E}_{=:\,\tilde{M}} \longrightarrow 0\,.$$

As in the proof of Lemma 5.96, this induces an exact sequence

$$0 \longrightarrow E/D \longrightarrow \tilde{E}/(I^n \cdot \tilde{E}) \longrightarrow \tilde{M}/(I^n \cdot \tilde{M}) \longrightarrow 0\,,$$

where $D := I^n \cdot \tilde{E} \cap E$.

The Artin-Rees Lemma now implies that

$$D \;\subseteq\; I^{n-k} \cdot E\,.$$

Therefore

$$\begin{aligned} \mathrm{rank}_{I^n}(\tilde{E}) &= \mathrm{rank}_{I^n}(\tilde{M}) \;+\; v_p(|E/D|) \\ &\geq \mathrm{rank}_{I^n}(\tilde{M}) \;+\; \mathrm{rank}_{I^{n-k}}(E) \\ &\geq \mathrm{rank}_{I^{n-k}}(E)\,. \end{aligned}$$

Interchanging the roles of E and $\tilde{E}$, and using the pseudo-isomorphism $\varphi : \tilde{E} \longrightarrow E$ (which is an injection since $\tilde{E} \subseteq E$ does not contain any non-trivial pseudo-null submodules), we obtain the second inequality. □

Remarks 5.106.

(1) The Artin-Rees number k from Lemma 5.104 depends on the ideal I and on the modules M and N. There exist ***uniform*** versions of this lemma, providing an integer that works for every ideal I of R (compare [Hu 92]). However, the corresponding integer still depends on the modules M and N.

(2) Since Λ_d is a regular local ring, it seems reasonable to believe that the uniform Artin-Rees numbers occurring in (1) can be bounded in terms of the Krull dimension of Λ_d (compare Remark 4.14 in [Hu 92]). In fact, the connections to the so-called *Briançon-Skoda Theorem* (compare [LS 81]) suggest that $\dim(\Lambda_d)–1 = d$ may serve as such a bound.
Using this estimate, we could conclude that

$$\operatorname{rank}_I(E) \;\leq\; \operatorname{rank}_{I^d}(\tilde{E}) \quad \text{and} \quad \operatorname{rank}_I(\tilde{E}) \;\leq\; \operatorname{rank}_{I^d}(E)\,,$$

whenever these ranks are finite. In particular, if $d = 1$, then we recover the statement $\operatorname{rank}_I(E) = \operatorname{rank}_I(\tilde{E})$ of Proposition 3.41, (i).
Suppose that $\mathbb{K}/K$ is a $\mathbb{Z}_p^d$-extension such that some prime of K is totally ramified in $\mathbb{K}$. If we replace inequality (5.1) in the proof of Theorem 5.77 by the inequality

$$\operatorname{rank}_I(E_{A^{(\mathbb{L})}}) \;\leq\; \operatorname{rank}_{I^d}(E_{A^{(\mathbb{K})}}) + \operatorname{rank}_{I^d}(A/\tilde{A})\,,$$

$I := (\nu_{(n_1,m_1)}(T_1), \ldots, \nu_{(n_d,m_d)}(T_d))$, then we obtain new proofs of the local boundedness of m_0- and l_0-invariants.

5.10 Pseudo-null Λ_2-modules

In this section, let K be a number field such that exactly one prime of K divides p, and let $\mathbb{K}/K$ be a $\mathbb{Z}_p^2$-extension. We will develop a method that bounds the l_0-invariant of $\mathbb{K}$ in terms of the λ-invariants of $\mathbb{Z}_p$-extensions of K contained in $\mathbb{K}$. In some situations, this approach may be used in order to show that the Greenberg module of $\mathbb{K}/K$ is pseudo-null.

Lemma 5.107. *Let K be a number field containing exactly one prime dividing p. Let $\mathcal{A}(K) \subseteq \mathcal{E}(K)$ denote the subset of $\mathbb{Z}_p$-extensions L/K satisfying $e(L/K) = 0$. Then $\mathcal{A}(K)$ is open in $\mathcal{E}(K)$ with respect to Greenberg's topology. Moreover, if $\mathbb{K}$ denotes a $\mathbb{Z}_p^2$-extension of K, $m_0 := m_0(\mathbb{K}/K)$ and*

$$\mathcal{A}^{m_0}(K) \;:=\; \{L \in \mathcal{A}(K) \mid \mu(L/K) \,=\, m_0\}\,,$$

then $L \in \mathcal{A}^{m_0}(K)$ for all but finitely many $L \in \mathcal{A}(K) \cap \mathcal{E}^{\subseteq \mathbb{K}}(K)$, and

$$l_0(\mathbb{K}/K) \;\leq\; \min(\{\lambda(L/K) \mid L \in \mathcal{A}^{m_0}(K) \cap \mathcal{E}^{\subseteq \mathbb{K}}(K)\})\,.$$

Proof. If $L \in \mathcal{A}(K)$ and $n \in \mathbb{N}$, then $e(M/K) = 0$ for every $M \in \mathcal{E}(L,n)$, proving that $\mathcal{A}(K) \subseteq \mathcal{E}(K)$ is open.

If $\mathbb{K}/K$ denotes any $\mathbb{Z}_p^2$-extension, then Lemma 5.10 implies that there exist only finitely many $\mathbb{Z}_p$-extensions $L \subseteq \mathbb{K}$ of K such that $\mu(L/K) \neq m_0$.

Let now $L \in \mathcal{A}^{m_0}(K) \cap \mathcal{E}^{\subseteq \mathbb{K}}(K)$ be arbitrary, but fixed. Let furthermore $\Gamma := \mathrm{Gal}(\mathbb{K}/K) \cong \mathbb{Z}_p^2$. We choose topological generators γ_1, γ_2 of Γ such that γ_1 generates $\mathrm{Gal}(\mathbb{K}/L)$ and such that $\gamma_2|_L$ is a topological generator of $\mathrm{Gal}(L/K)$. Let $T_1 = \gamma_1 - 1$, $T_2 = \gamma_2 - 1$ denote the corresponding variables.

Then the homomorphism

$$\pi_L : \Lambda_2 = \mathbb{Z}_p[[T_1, T_2]] \quad \longrightarrow\!\!\!\!\!\rightarrow \quad \Lambda = \mathbb{Z}_p[[T]]$$

induced by the restriction map

$$\mathrm{Gal}(\mathbb{K}/K) \quad \longrightarrow\!\!\!\!\!\rightarrow \quad \mathrm{Gal}(L/K)$$

satisfies $\pi_L(T_1) = 0$ and $\pi_L(T_2) = T$.

Now consider the characteristic power series $F_{A^{(\mathbb{K})}} \in \Lambda_2$ of $\mathbb{K}/K$. We write $F_{A^{(\mathbb{K})}} = p^{m_0} \cdot g$, with $p \nmid g$. Let $X = \mathrm{Gal}(H(\mathbb{K})/\mathbb{K})$. Since Lemma 4.3, (i) implies that $\mu(L/K) = \mu(X_{\pi_L})$, the condition $\mu(L/K) = m_0$ is equivalent to saying that $p \nmid \pi_L(g)$.

Replacing γ_1 by $\tilde{\gamma}_1 := \gamma_1 \cdot \gamma_2^{p^n}$ for a suitable $n \in \mathbb{N}$, we may assume that g is regular with respect to T_2 (compare Definition 4.9 and Lemma 4.7). Moreover, we may assume that n has been chosen large enough to ensure that

$$\mu(M/K) = \mu(L/K) \quad \text{and} \quad \lambda(M/K) \leq \lambda(L/K)$$

for every $M \in \mathcal{E}(L, n)$. Indeed, this is possible because of Theorem 3.57, since

$$\mu(M/K) \geq m_0 = \mu(L/K)$$

for every $M \in \mathcal{E}^{\subseteq \mathbb{K}}(K)$ (note that $\mathcal{E}(L, n) = U(L, n)$ for every $n \in \mathbb{N}$, because K contains only one prime dividing p).

We write

$$g = T_2^k + T_2^{k-1} \cdot h_{k-1} + \ldots + h_0 \,,$$

with $k \in \mathbb{N}$ and $h_0, \ldots, h_{k-1} \in (p, \tilde{T}_1)$, where

$$\tilde{T}_1 = \tilde{\gamma}_1 - 1 = (T_1 + 1)(T_2 + 1)^{p^n} - 1 \,.$$

Let $M \in \mathcal{E}^{\subseteq \mathbb{K}}(K)$ be the subfield of $\mathbb{K}$ that is fixed by $\tilde{\gamma}_1$. Then $M \in \mathcal{E}(L, n)$ by Lemma 3.19, (i). Moreover, the corresponding homomorphism

$$\pi_M : \Lambda_2 \longrightarrow\!\!\!\!\!\rightarrow \Lambda$$

satisfies $\pi_M(\tilde{T}_1) = 0$ and $\pi_M(T_2) = T$.

This means that the reduced degree of $\pi_M(g) \in \mathbb{Z}_p[[T]]$ is equal to k. We want to show that $k \leq \lambda(M/K)$. In view of Lemma 5.70, this will yield a chain of inequalities

$$l_0(\mathbb{K}/K) = l_0(f) \leq k \leq \lambda(M/K) \leq \lambda(L/K) \,,$$

concluding the proof of the lemma.

Lemma 5.98 implies that there exists a $\mathbb{Z}_p[[\mathrm{Gal}(M/K)]]$-module homomorphism

$$X_{\pi_M} \;=\; X/(\tilde{T}_1 \cdot X) \;\longrightarrow\; A^{(M)}$$

whose kernel and cokernel are annihilated by a power of p. In particular, modulo possible powers of p, the characteristic polynomial $f_{X_{\pi_M}}$ of X_{π_M} divides $F_{A^{(M)}}(T)$. But $f_{X_{\pi_M}}$ is divisible by $\pi_M(F_{A^{(\mathbb{K})}})$ and therefore by $\pi_M(g)$, proving that $k \le \lambda(M/K)$. □

Lemma 5.108. *Let K be a number field containing exactly one prime dividing p. Let $\mathbb{K}/K$ denote a $\mathbb{Z}_p^2$-extension.*
If there exists a $\mathbb{Z}_p$-extension $L \subseteq \mathbb{K}$ of K such that

$$\mu(L/K) \;=\; m_0(\mathbb{K}/K) =: m_0 \quad \textit{and} \quad e(L/K) \;=\; \lambda(L/K) \;=\; 0\,,$$

then the characteristic power series $F_{A^{(\mathbb{K})}}$ of $\mathbb{K}/K$ is associated to a power of p.

Proof. We will use the notation from the preceding lemma. Since our assumptions ensure that $L \in \mathcal{A}^{m_0}(K)$, this lemma implies that $l_0(\mathbb{K}/K) = 0$. Actually the proof of Lemma 5.107 shows more:

If $F_{A^{(\mathbb{K})}} \;=\; p^{m_0} \cdot g$ for some non-unit $g \in \Lambda_2$ coprime to p, then

$$\pi_L(g) \in \mathbb{Z}_p[[T]]$$

is coprime to p and therefore is associated to a distinguished polynomial. Since $e(L/K) = 0$, Lemma 5.98 implies that, modulo possible powers of p, $\pi_L(g)$ divides $F_{A^{(L)}}(T)$. But $F_{A^{(L)}}(T) = 1$, because $\lambda(L/K) = 0$, yielding a contradiction. □

Corollary 5.109. *Let K be a number field containing exactly one prime dividing p. Let $\mathbb{K}/K$ denote a $\mathbb{Z}_p^2$-extension.*
If there exists a $\mathbb{Z}_p$-extension $L \subseteq \mathbb{K}$ of K such that

$$\mu(L/K) \;=\; \lambda(L/K) \;=\; e(L/K) \;=\; 0\,,$$

then the Λ_2-module $X = \mathrm{Gal}(H(\mathbb{K})/\mathbb{K})$ is pseudo-null.

Proof. Lemma 4.3, (i) and Proposition 4.34, (i) imply that

$$m_0(\mathbb{K}/K) \;\le\; \mu(L/K) \;=\; 0\,.$$

Moreover, Lemma 5.108 implies that the characteristic power series of $\mathbb{K}/K$ is not divisible by any irreducible element coprime to p. □

Corollary 5.110. *Let K be an imaginary quadratic number field. Suppose that the rational prime p is inert or ramified in K. Let $\mathbb{K}$ denote the composite of all $\mathbb{Z}_p$-extensions of K.*
If p does not divide the class number $h_K := |\mathrm{Cl}(K)|$ of K, then $\mathrm{Gal}(H(\mathbb{K})/\mathbb{K})$ is pseudo-null.

Proof. Since $K/\mathbb{Q}$ is abelian, Leopoldt's Conjecture is valid for K, i.e., the field $\mathbb{K}$ is a $\mathbb{Z}_p^2$-extension of K by Theorem 1.7. Moreover, the assumption that $p \nmid h_K$ implies that each $\mathbb{Z}_p$-extension of K is totally ramified at the unique prime of K dividing p. Finally, this assumption also implies that $\mu(L/K) = \lambda(L/K) = 0$ for every $L \in \mathcal{E}(K)$ (compare Proposition 13.22 of [Wa 97]). Now apply Corollary 5.109. □

Remarks 5.111.

(1) *Greenberg's Generalised Conjecture* predicts that for every number field K, the Greenberg module attached to the composite $\mathbb{K}$ of all $\mathbb{Z}_p$-extensions of K is pseudo-null as a Λ_d-module, where $d = \mathrm{rank}_{\mathbb{Z}_p}(\mathrm{Gal}(\mathbb{K}/K))$, respectively. The above corollary proves a special case of this conjecture.

(2) In his Ph.D. thesis, J. Minardi studied pseudo-null Λ_d-modules in great detail. Minardi observed that the Greenberg module X of a $\mathbb{Z}_p^d$-extension is pseudo-null if there exists a choice of variables of Λ_d such that, for example, $X/(T_1 \cdot X)$ is pseudo-null as a module over $\Lambda_{d-1} = \mathbb{Z}_p[[T_2, \ldots, T_d]]$ (see, for example, Section 4.B of [Min 86]). In particular, the Corollaries 5.109 and 5.110 were known to Minardi (compare Proposition 3.A of [Min 86]).
We believe that Lemmas 5.107 and 5.108 are slight, but nevertheless important generalisations of Minardi's results, fitting into the pattern of one of the main innovations of this thesis, namely, the possibility to obtain results concerning λ- (or, more generally, l_0-) invariants even in the case of non-vanishing μ- (respectively, m_0-) invariants.

(3) There is not known any concrete example of a $\mathbb{Z}_p^d$-extension, $d > 1$, whose characteristic power series is *not* associated to a power p^n, $n \in \mathbb{N}_0$, of p (while there do exist examples constructing $\mathbb{Z}_p^d$-extensions having a non-trivial m_0-invariant).

(4) Let $\mathbb{K}/K$ be as in Lemma 5.108. The results of Chapter 3 provide a tool to explicitly test whether a given $\mathbb{Z}_p$-extension L/K contained $\mathbb{K}$ satisfies the conditions from Lemma 5.108. Namely, suppose that $L \subseteq \mathbb{K}$ satisfies $e(L/K) = 0$, and assume that $m_0 := m_0(\mathbb{K}/K)$ is known. Then $\mu(L/K) = m_0$ and $\lambda(L/K) = 0$ if there exist integers $n, m \in \mathbb{N}_0$, $n > m$, such that

$$\mathrm{rank}_{\nu_{(n,m)}}(A^{(L)}) \;<\; m_0 \cdot (p^n - p^m) + D \;, \qquad (\star)$$

where $D := \min(n - m, p^m(p-1))$. Moreover, in this case, we have $\nu(L/K) < n - m$.
Indeed, if $E_{A^{(L)}}$ denotes the elementary Λ-module attached to $A^{(L)}$, then the proof of Theorem 3.57 shows that

$$\mathrm{rank}_{\nu_{(n,m)}}(E_{A^{(L)}}) \;\geq\; \mu(L/K) \cdot (p^n - p^m) \;+\; \lambda(L/K) \cdot (n - m)$$

if $m \in \mathbb{N}$ is large enough to ensure that $\lambda(L/K) < p^{m-1}(p-1)$. Otherwise,

$$\mathrm{rank}_{\nu_{(n,m)}}(E_{A^{(L)}}) \;\geq\; \mu(L/K) \cdot (p^n - p^m) \;+\; p^m(p-1)$$

(corresponding to the case $r \geq 1$ in equation (3.4)).
Since Lemma 4.3, (i) and Proposition 4.34, (i) imply that $\mu(L/K) \geq m_0$, $(\star)$ implies that $\mu(L/K) = m_0$ and $\lambda(L/K) = 0$.

Note that $\operatorname{rank}_{\nu_{(n,m)}}(A^{(L)})$ can be determined with the help of Theorem 3.6 by computing the ranks of the first layers $A_n^{(L)}$, until the first stabilisation occurs.

Bibliography

[AM 69] Atiyah, M. F.; MacDonald, I.G.: *Introduction to Commutative Algebra*, Westview Press, 1969

[Ba 76] Babaĭcev, V. A.: *On some questions in the theory of* Γ*-extensions of algebraic number fields. II*, Math. USSR Izvestiya, vol. 10, no. 4, 675-685, 1976

[Ba 81] Babaĭcev, V. A.: *On the boundedness of the Iwasawa invariant* μ, Math. USSR Izvestiya, vol. 16, no. 1, 1-19, 1981

[Ba 82] Babaĭcev, V. A.: *On the linear nature of the behaviour of Iwasawa's* μ*-invariant*, Math. USSR Izvestiya, vol. 19, no. 1, 1-12, 1982

[Be 12] Bembom, T.: *The Capitulation Problem in Class Field Theory*, Ph.D. Thesis, University of Göttingen, 2012

[Bo 03] Bosch, S.: *Algebra*, 5th edition, Springer, Berlin-Heidelberg-New York, 2003

[Bou 89] Bourbaki, N.: *Commutative algebra, Chapters 1-7*, Springer, 1989

[Bou 90] Bourbaki, N.: *Algebra, Chapters 4-7*, Springer Berlin-Heidelberg-New York, 1990

[Br 67] Brumer, A.: *On the units of algebraic number fields*, Mathematika 14, 121-124, 1967

[CK 81] Carroll, J. E.; Kisilevsky, H.H.: *On Iwasawa's* λ*-invariant for certain* $\mathbb{Z}_l$*-extensions*, Acta Arithmetica XL, 1-8, 1981

[CM 81] Cuoco, A. A.; Monsky, P.: *Class numbers of* $\mathbb{Z}_p^d$*-extensions*, Math. Ann. 255, 235-258, 1981

[Ei 95] Eisenbud, D.: *Commutative Algebra with a View toward Algebraic Geometry*, Springer New York, 1995

[Fe 86] Federer, L. J.: *Noetherian* $\mathbb{Z}_p[[T]]$*-Modules, Adjoints, and Iwasawa Theory*, Illinois Journal of Mathematics, vol. 30, no. 4, 636-652, 1986

[FJ 08] Fried, M. D.; Jarden, M.: *Field Arithmetic*, 3rd edition, Springer Berlin-Heidelberg, 2008

[FW 79] Ferrero, B.; Washington, L. C.: *The Iwasawa invariant μ_p vanishes for abelian number fields*, Ann. of Math. (2) 109, no. 2, 377-395, 1979

[Fu 94] Fukuda, T.: *Remarks on $\mathbb{Z}_p$-extensions of Number Fields*, Proc. Japan Acad. 70, Ser. A, 264-266, 1994

[GJ 85] Grandet, M.; Jaulent,J.-F.: *Sur la capitulation dans une $\mathbb{Z}_l$-extension*, J. für Reine u. Angew. Math. 362, 213-217, 1985

[Gou 97] Gouvêa, Fernando Q.: *p-adic Numbers*, 2nd edition, Springer Berlin-Heidelberg, 1997

[Gr 73] Greenberg, R.: *The Iwasawa Invariants of Γ-Extensions of a Fixed Number Field*, American Journal of Math. 95, 204-214, 1973

[Gr 73(2)] Greenberg, R.: *On a certain l-adic Representation*, Inventiones math. 21, 117-124, 1973

[Gr 76] Greenberg, R.: *On the Iwasawa invariants of totally real number fields*, American Journal of Math. 98, no. 1, 263–284, 1976

[Hi 97] Hilbert, D.: *Die Theorie der algebraischen Zahlkörper („Zahlbericht“)*, Jahresbericht der Deutschen Mathematiker-Vereinigung 4, 175-535, Berlin 1897

[Hu 92] Huneke, C.: *Uniform bounds in Noetherian rings*, Invent. math. 107, no. 1, 203-223, 1992

[Iw 73] Iwasawa, Kenkichi: *On $\mathbb{Z}_l$-extensions of algebraic number fields*, Annals of Mathematics, vol. 98, no. 2, 246-326, 1973

[Ja 73] Janusz, G.J.: *Algebraic Number Fields*, Academic Press, 1973

[JS 06] Jantzen, J.C.; Schwermer, J.: *Algebra*, Springer Berlin-Heidelberg, 2006

[La 90] Lang, S.: *Cyclotomic Fields I and II*, Combined Second Edition, Springer New York-Berlin-Heidelberg, 1990

[La 93] Lang, S.: *Algebra*, 3rd edition, Addison-Wesley Publishing Company, Inc., 1993

[LS 81] Lipman, J.; Sathaye, A.: *Jacobian ideals and a theorem of Briançon-Skoda*, Mich. Math. J. 28, 199-222, 1981

[Mat 86] Matsumura, H.: *Commutative ring theory*, Cambridge University Press, 1986

[Min 86] Minardi, J.: *Iwasawa modules for $\mathbb{Z}_p^d$-extensions of algebraic number fields*, Ph.D. Thesis, University of Washington, 1986

[Miz 10] Mizusawa, Y.: *On unramified Galois 2-Groups over $\mathbb{Z}_2$-Extensions of Real Quadratic Fields*, Proceedings of the American Math. Society, vol. 138, no. 9, 3095-3103, 2010

[Mo 81] Monsky, P.: *Some Invariants of $\mathbb{Z}_p^d$-Extensions*, Math. Ann. 255, 229-233, 1981

[Neu 92] Neukirch, J.: *Algebraische Zahlentheorie*, Springer Berlin-Heidelberg, 1992

[NSW 08] Neukirch, J.; Schmidt, A.; Wingberg, K.: *Cohomology of Number Fields*, 2nd edition, Springer Berlin-Heidelberg, 2008

[Os 92] Ossa, E.: *Topologie*, Vieweg Braunschweig-Wiesbaden, 1992

[Rib 01] Ribenboim, P.: *Classical Theory of Algebraic Numbers*, Springer New York, 2001

[Sa 91] Sands, J. W.: *On small Iwasawa invariants and imaginary quadratic fields*, Proceedings of the Amer. Math. Soc., vol. 112, no. 3, 671-684, 1991

[Sc 85] Schmithals, B.: *Kapitulation der Idealklassen und Einheitenstruktur in Zahlkörpern*, J. Reine Angew. Math. 358, 43-60, 1985

[Wa 97] Washington, L. C.: *Introduction to Cyclotomic Fields*, 2nd edition, Springer New York, 1997