Mathematische Zeitschrift manuscript No.
(will be inserted by the editor)

Cornelius Greither · Masato Kurihara

Stickelberger elements, Fitting ideals of class groups of CM fields, and dualisation

Received: date / Revised: date

Abstract In this paper, we systematically construct abelian extensions of CM-fields over a totally real field whose Stickelberger elements are not in the Fitting ideals of the class groups. Our evidence indicates that Pontryagin duals of class groups behave better than the class groups themselves. We also explore the behaviour of Fitting ideals under projective limits and dualisation in a somewhat broader context.

0 Introduction

Let k be a totally real number field, and K be a CM-field such that K/k is a finite abelian extension.

Determining the structure of the ideal class group Cl_K as a $\mathrm{Gal}(K/k)$-module is a very important problem in algebraic number theory. In this paper, we are interested in the Fitting ideal of Cl_K as a $\mathbb{Z}[\mathrm{Gal}(K/k)]$-module and in related questions.

We denote by $\theta_{K/k}$ or simply by θ_K the Stickelberger element of the extension K/k, that is:

$$\theta_K = \sum_{\sigma \in \mathrm{Gal}(K/k)} \zeta_k(\sigma, 0)\sigma^{-1},$$

C. Greither
Fakultät Informatik, Universität der Bundeswehr München, 85577 Neubiberg, Germany
E-mail: cornelius.greither@unibw.de

M. Kurihara
Department of Mathematics, Keio University, 3-14-1 Hiyoshi, Kohoku-ku, Yokohama, 223-8522, Japan
E-mail: kurihara@math.keio.ac.jp

where $\zeta_k(\sigma, s)$ is the partial zeta function; this function is holomorphic on $\mathbb{C} \setminus \{1\}$, and if $\mathrm{Re}(s) > 1$, it has the expression $\zeta_k(\sigma, s) = \Sigma_{(\mathfrak{a}, K/k)=\sigma}(N\mathfrak{a})^{-s}$. Then, the conjecture of Brumer predicts that

$$\mathrm{Ann}_{\mathbb{Z}[\mathrm{Gal}(K/k)]}(\mu(K)) \cdot \theta_K \subset \mathrm{Ann}_{\mathbb{Z}[\mathrm{Gal}(K/k)]}(Cl_K),$$

where $\mu(K)$ denotes the group of roots of unity in K, and for a $\mathbb{Z}[\mathrm{Gal}(K/k)]$-module M, $\mathrm{Ann}_{\mathbb{Z}[\mathrm{Gal}(K/k)]}(M)$ denotes the annihilator of M. One may naturally ask whether the following strengthening might be true:

$$\mathrm{Ann}_{\mathbb{Z}[\mathrm{Gal}(K/k)]}(\mu(K)) \cdot \theta_K \subset \mathrm{Fitt}_{\mathbb{Z}[\mathrm{Gal}(K/k)]}(Cl_K). \tag{1}$$

We will show in this paper that (1) does not hold in general; we are able to systematically construct counterexamples.

First of all, we note that the problem (1) holds if and only if the restriction to p-primary components

$$\mathrm{Ann}_{\mathbb{Z}_p[\mathrm{Gal}(K/k)]}(\mu_{p^\infty}(K)) \cdot \theta_K \subset \mathrm{Fitt}_{\mathbb{Z}_p[\mathrm{Gal}(K/k)]}(Cl_K \otimes \mathbb{Z}_p) \tag{2}$$

hold for all primes p. Hence, in the following we fix p (we will assume $p > 2$ however), and consider this relation for the p-primary component of the class group.

The problem of giving a precise expression (in analytic terms) for the Fitting ideal of class groups or Iwasawa modules is not new. Such results already appeared in the milestone work [12] of Mazur and Wiles on the Main conjecture. Further results in this direction were obtained, among others, by the authors of this article independently (see [9], [10], [4], [5]). In [10] and [5] the authors were led to take Pontryagin duals: of the class group in [5], and of the inductive limit of class groups in [10]. In [9] and [4] the focus was on results concerning the original class groups (not dualised). Note however that in [4] an Iwasawa module X_{du} appeared which seemed to involve a dualising process. The connection of X_{du} to the module treated in [10] is clarified at the end of our paper.

The present paper in conjunction with [10] and [5] supports the hypothesis that in general one should look at the Fitting ideal of the dualised object (p-part of class group, or Iwasawa module) instead of the object itself; the Fitting ideal of the latter apparently has a tendency of being too small and even hard to predict. (Also from the viewpoint of ETNC, the Fitting ideal of the former appears more natural.) Of course one has to be extremely careful, since there are important exceptions: If the Galois group G of K/k has cyclic p-part, then dualising p-parts of class groups and Iwasawa modules does not change the Fitting ideals. (For class groups this is already contained in the appendix to [12], and for Iwasawa modules it is going to be proved in the appendix.) Moreover all instances for which we found the Fitting ideal of the non-dualised object to be misbehaved have base field larger than $\mathbb{Q}$. We also make an aside comment: since Tate-Shafarevich groups are self-dual under the standard assumption that they are finite, the problem of distinguishing between an object and its dual would not arise when we study analogous problems in the setting of elliptic curves.

We give a short outline of the paper. The first section sets the stage by proving a negative result for Iwasawa modules: under suitable hypotheses, the

standard Iwasawa module does not contain the relevant Stickelberger element at infinite level. The second section makes the point that this already implies the existence of similar counterexamples at finite level, since we are able to show that projective limits commute with Fitting ideals. This reasoning is however not constructive; this defect is remedied in Sections 3 and 4. There we present certain classes of cases (and we study one case in detail) for which the relevant Stickelberger element is not in the Fitting ideal of the class group but in the Fitting ideal of the dual. (Actually we work with the χ-part of the p-part for a fixed odd prime p and certain odd p-adic characters χ.) In the case study (§3), the top field K is of absolute degree 36. If one wants to deal with the statement (2) on the p-component with $p > 2$, this seems to be the minimal possible degree. The appendix proves a purely algebraic result: the Fitting ideal of a $\mathbb{Z}_p$-torsion free $\mathbb{Z}_p[[\Gamma \times G]]$-torsion module is unchanged under taking the $\mathbb{Z}_p$-dual, provided the finite p-group G is cyclic.

Errata for the paper [10]: The second-named author would like to take this opportunity for some corrections concerning his earlier paper [10].

1. Page 540, Theorem 0.1: The structure of A_K^χ is $A_K^\chi \simeq \bigoplus_{i\geq 1} \Theta_{i,K}^\chi/\Theta_{i-1,K}^\chi$ (note that $\Theta_{i,K}^\chi$ contains $\Theta_{i-1,K}^\chi$).

2. Page 551, Lemma 4.3: It is stated that there exists a unique cyclic extension $k_n(\lambda)/k$, but the word "unique" has to be deleted.

3. Page 560, definition of $\mathcal{H}$: The correct definition (which should be similar to that in [9] §3) is

$$\mathcal{H} = \{H_0 \times H_1 \times ... \times H_r \mid H_0 \text{ is a finite subgroup of } \mathrm{Gal}(F_\infty/k) \text{ with order prime to } p \text{ and } H_i \text{ is a subgroup of } P_{\lambda_i} \text{ for all } i\ (1 \leq i \leq r)\}.$$

Acknowledgments: The first-named author would like to thank Keio University for its generous hospitality during a visit in 2005, and he acknowledges support from the DFG. The second-named author would like to thank T. Komatsu for informing us of his computation of the class group of a certain number field (cf. Section 3). We also thank C. Popescu for asking whether (1) holds in the number field case, and D. Burns for his interest in this work.

1 Fitting ideals of Iwasawa modules

We fix an odd prime number p, and a totally real base field k. We consider a finite abelian extension K/k such that K is a CM-field. We decompose $\mathcal{G} = \mathrm{Gal}(K/k) = \Delta \times G$ where $\#\Delta$ is prime to p, and G is a p-group. The subfield of K fixed by G is denoted by F, hence $\mathrm{Gal}(F/k) = \Delta$ and $\mathrm{Gal}(K/F) = G$. For an odd character $\chi : \Delta \longrightarrow \overline{\mathbb{Q}_p}^\times$ and a $\mathbb{Z}_p[\mathrm{Gal}(K/k)]$-module M, we consider the χ-component M^χ which is defined by

$$M^\chi = M \otimes_{\mathbb{Z}_p[\mathrm{Gal}(F/k)]} O_\chi,$$

where $O_\chi = \mathbb{Z}_p[\mathrm{Image}(\chi)]$; this is a $\mathbb{Z}_p[\Delta]$-module on which Δ acts via χ. We regard M^χ to be an $O_\chi[G]$-module. When we study M^χ, we do not lose generality by assuming χ to be faithful. So we will make this assumption

throughout. In this paper, we also assume that $\chi \neq \omega$ where ω is the Teichmüller character.

For a general number field $\mathcal{K}$, we denote by $\mathcal{K}_\infty/\mathcal{K}$ the cyclotomic $\mathbb{Z}_p$-extension and by $\mathcal{K}_n$ the n-th layer, that is the intermediate field such that $[\mathcal{K}_n : \mathcal{K}] = p^n$. Let $A_{\mathcal{K}_n}$ denote the p-component of the ideal class group $Cl_{\mathcal{K}_n}$ of $\mathcal{K}_n$, i.e., $A_{\mathcal{K}_n} = Cl_{\mathcal{K}_n} \otimes_{\mathbb{Z}} \mathbb{Z}_p$. We define $X_{\mathcal{K}_\infty}$ by

$$X_{\mathcal{K}_\infty} := \varprojlim_n A_{\mathcal{K}_n}.$$

We take K and F as above, and consider the cyclotomic $\mathbb{Z}_p$-extensions K_∞/K, F_∞/F. The χ-component $X^\chi_{K_\infty}$ is an $O_\chi[[\mathrm{Gal}(K_\infty/F)]]$-module. Let θ_{K_n} be the Stickelberger element of the extension K_n/k. Since $\chi \neq \omega$, by Deligne and Ribet [3] we know that the χ-component $\theta^\chi_{K_n}$ is an element of $O_\chi[\mathrm{Gal}(K_n/F)]$, and $(\theta^\chi_{K_n})_{n\gg 0}$ becomes a projective system which defines an element $\theta^\chi_{K_\infty}$ in $O_\chi[[\mathrm{Gal}(K_\infty/F)]]$.

If the strong form (1) of the Brumer conjecture were true, $\theta^\chi_{K_n}$ would be in the Fitting ideal of $A^\chi_{K_n}$. Hence, it is natural to ask whether $\theta^\chi_{K_\infty}$ is in the Fitting ideal of $X^\chi_{K_\infty}$. The answer in general is no!

Theorem 1.1 *Suppose that there is a prime of k_∞ above p which splits completely in F_∞ and is ramified in K_∞ (so in particular it ramifies wildly in K_∞/k_∞). Then, $\theta^\chi_{K_\infty}$ is not in the Fitting ideal* $\mathrm{Fitt}_{O_\chi[[\mathrm{Gal}(K_\infty/F)]]}(X^\chi_{K_\infty})$.

Remark 1.2 (1) If K_∞/k is as above, and there exists at least one odd character $\chi \neq \omega$ of Δ (note this is a very mild restriction), then

$$\varprojlim_n (\mathrm{Ann}_{\mathbb{Z}_p[\mathrm{Gal}(K_n/k)]}(\mu_{p^\infty}(K_n))\theta_{K_n}) \not\subset \mathrm{Fitt}_{\mathbb{Z}_p[[\mathrm{Gal}(K_\infty/k)]]}(X_{K_\infty}),$$

because we do not have this inclusion for this χ-component.

(2) By the first named author [4] Theorem 7, if no prime of k_∞ above p is wildly ramified in K_∞/k_∞, we have

$$\theta^\chi_{K_\infty} \in \mathrm{Fitt}_{O_\chi[[\mathrm{Gal}(K_\infty/F)]]}(X^\chi_{K_\infty}),$$

at least assuming $\mu(X^\chi_{F_\infty}) = 0$.

(3) On the other hand, define

$$A^\chi_{K_\infty} = \varinjlim_n A_{K_n},$$

and consider the Pontryagin dual $\mathcal{A}_{K_\infty} = (A_{K_\infty})^\vee$ with cogredient action of $\mathrm{Gal}(K_\infty/k)$. By the second named author [10] Appendix, we have

$$\theta^\chi_{K_\infty} \in \mathrm{Fitt}_{O_\chi[[\mathrm{Gal}(K_\infty/F)]]}(\mathcal{A}^\chi_{K_\infty}),$$

if we assume $\mu(X^\chi_{F_\infty}) = 0$ and the Leopoldt conjecture for k. In this sense, the Pontryagin dual behaves better (this will happen again later on). Furthermore, by [4] Theorem 3, $\theta^\chi_{K_\infty}$ is always in the Fitting ideal of a certain module $X^\chi_{K_\infty,du}$ which is related to $\mathcal{A}^\chi_{K_\infty}$; see the appendix.

PROOF of Theorem 1.1: Put $G' = \mathrm{Gal}(K_\infty/F_\infty)$. By [9] Corollary 5.3, we have an exact sequence

$$0 \longrightarrow (\bigoplus_{v\in S} I_v(K_\infty/F_\infty))^\chi \longrightarrow (X_{K_\infty}^\chi)_{G'} \longrightarrow X_{F_\infty}^\chi \longrightarrow 0,$$

where $I_v(K_\infty/F_\infty)$ is the inertia subgroup of G' of a prime v of F_∞, and S is the set of primes of F_∞ which are ramified in K_∞. For $v \in S$, let w denote the prime of k below v. If w does not split completely in F, $(\bigoplus_{v|w} I_v(K_\infty/F_\infty))^\chi = 0$. Hence, it suffices to consider primes w which split completely in F.

We denote by $\mathcal{P}$ the set of primes of k which split completely in F. We divide $\mathcal{P} = \mathcal{P}_0 \cup \mathcal{P}_1$ where $\mathcal{P}_0$ is the subset of primes above p, and $\mathcal{P}_1$ is the subset of primes which are not above p. We define $\mathcal{Q} = \{v \in \mathcal{P} \mid v \text{ is ramified in } K_\infty\}$, $\mathcal{Q}_0 = \mathcal{Q} \cap \mathcal{P}_0$, and $\mathcal{Q}_1 = \mathcal{Q} \cap \mathcal{P}_1$. Let $\mathcal{P}_{F_\infty}$, $\mathcal{Q}_{F_\infty}$, $\mathcal{P}_{i,F_\infty}$, $\mathcal{Q}_{i,F_\infty}$ be the set of primes of F_∞ above $\mathcal{P}$, $\mathcal{Q}$, $\mathcal{P}_i$, $\mathcal{Q}_i$, respectively for $i = 0, 1$. We have

$$(\bigoplus_{v\in S} I_v(K_\infty/F_\infty))^\chi = (\bigoplus_{v\in Q_{F_\infty}} I_v(K_\infty/F_\infty))^\chi.$$

Since $X_{F_\infty}^\chi$ is of projective dimension ≤ 1, we have (see [2] Lemma 3)

$$\begin{aligned}&\mathrm{Fitt}_{O_\chi[[\mathrm{Gal}(F_\infty/F)]]}((X_{K_\infty}^\chi)_{G'})\\ &= \mathrm{Fitt}_{O_\chi[[\mathrm{Gal}(F_\infty/F)]]}((\textstyle\bigoplus_{v\in\mathcal{Q}_{F_\infty}} I_v(K_\infty/F_\infty))^\chi)\,\mathrm{Fitt}_{O_\chi[[\mathrm{Gal}(F_\infty/F)]]}(X_{F_\infty}^\chi).\end{aligned}$$

For $w \in \mathcal{Q}_1$, we find

$$(\bigoplus_{v|w} I_v(K_\infty/F_\infty))^\chi \simeq O_\chi[[\mathrm{Gal}(F_\infty/F)]]/(p^{e_w}, \varphi_w - 1),$$

where $p^{e_w} = \#I_v(K_\infty/F_\infty)$ (which is independent of the choice of v), and $\varphi_w \in \mathrm{Gal}(F_\infty/k)$ is the Frobenius of w. By the "Main Conjecture" (proved by Wiles [18]), we know $\mathrm{Fitt}_{O_\chi[[\mathrm{Gal}(F_\infty/F)]]}(X_{F_\infty}^\chi) = (\theta_{F_\infty}^\chi)$. Hence,

$$\mathrm{Fitt}_{O_\chi[[\mathrm{Gal}(F_\infty/F)]]}((X_{K_\infty}^\chi)_{G'}) = J(\prod_{w\in\mathcal{Q}_1}(p^{e_w}, \varphi_w - 1))\theta_{F_\infty}^\chi, \tag{3}$$

where $J = \mathrm{Fitt}_{O_\chi[[\mathrm{Gal}(F_\infty/F)]]}((\bigoplus_{v\in\mathcal{Q}_{0,F_\infty}} I_v(K_\infty/F_\infty))^\chi)$.

We denote by $\mathfrak{m}$ the maximal ideal of $O_\chi[[\mathrm{Gal}(F_\infty/F)]]$ (so $\mathfrak{m} = (p, \gamma - 1)$ where γ is a generator of $\mathrm{Gal}(F_\infty/F)$). Since we assumed $\mathcal{Q}_0 \neq \emptyset$, we get $J \subset \mathfrak{m} = (p, \gamma - 1)$. Hence,

$$\mathrm{Fitt}_{O_\chi[[\mathrm{Gal}(F_\infty/F)]]}((X_{K_\infty}^\chi)_{G'}) \subset \mathfrak{m}(\prod_{w\in\mathcal{Q}_1}(p^{e_w}, \varphi_w - 1))\theta_{F_\infty}^\chi. \tag{4}$$

Let $\overline{\theta}_{K_\infty}^\chi$ be the image of $\theta_{K_\infty}^\chi$ in $O_\chi[[\mathrm{Gal}(F_\infty/F)]]$. Then we know by Tate [16] (Proposition 1.6 on p. 86) that

$$\overline{\theta}_{K_\infty}^\chi = \prod_w (1 - \varphi_w^{-1})\theta_{F_\infty}^\chi,$$

where w runs over the primes of k which are unramified in F_∞ and which are ramified in K_∞. Therefore,

$$\overline{\theta}^{\chi}_{K_\infty} = \prod_{w \in \mathcal{Q}_1} (1 - \varphi_w^{-1}) \theta^{\chi}_{F_\infty} \qquad \text{modulo units.}$$

Comparing this with (4), we obtain $\overline{\theta}^{\chi}_{K_\infty} \notin \mathrm{Fitt}_{O_\chi[[\mathrm{Gal}(F_\infty/F)]]}((X^{\chi}_{K_\infty})_{G'})$. Indeed: assuming the contrary would lead to

$$\prod_{w \in \mathcal{Q}_1} (1 - \varphi_w^{-1}) \in \mathfrak{m} \prod_{w \in \mathcal{Q}_1} (p^{e_w}, \varphi_w - 1)),$$

since $\theta^{\chi}_{F_\infty}$ is a nonzerodivisor, and the preceding equation leads to a contradiction modulo p because p does not divide $1 - \varphi_w^{-1}$. This shows that $\theta^{\chi}_{K_\infty}$ is not an element of the ideal $\mathrm{Fitt}_{O_\chi[[\mathrm{Gal}(K_\infty/F)]]}(X^{\chi}_{K_\infty})$. □

In order to obtain similar results at finite level, it seems reasonable to first examine the behaviour of Fitting ideals under projective limits. This is the subject of the next section.

2 Projective limits and Fitting ideals

We state and prove the result below not in maximal generality but in a way we consider most appropriate for immediate applications in Iwasawa theory. Let us fix some notation.

The letter Λ has its standard meaning $O[[T]]$, where O is the ring of integers of a finite extension of $\mathbf{Q}_p$, and T corresponds to $\gamma - 1$, with γ a chosen generator of the free pro-cyclic p-group Γ; ω_n is $(1+T)^{p^n} - 1$. By G we denote a finite abelian group, $R = \Lambda[G]$, and $R_n = R/\omega_n R \cong (\Lambda/\omega_n\Lambda)[G]$. Then $(R_n)_n$ is a projective system with limit R. We will only consider projective systems $(A_n)_n$ of modules A_n over R_n such that the transition maps $A_m \to A_n$ $(m \geq n)$ are R_m-linear in the obvious sense. The limit $X := \varprojlim_n A_n$ will then be an R-module. Note the intentional change of letter for the limit. Also, all limits in this section will be projective limits.

We say that the system $(A_n)_n$ is *surjective from n_0 onwards,* if $A_m \to A_n$ is onto for all $m \geq n \geq n_0$. With this notation in place, we can state:

Theorem 2.1 *Assume that the projective system $(A_n)_n$ satisfies the following two properties:*

(i) *$(A_n)_n$ is surjective from some $n_0 \in \mathbb{N}$ onwards.*

(ii) *The limit X is a finitely generated torsion module over Λ.*

If ι denotes the natural identification $R \cong \varprojlim_n R_n$, then

$$\iota(\mathrm{Fitt}_R(X)) = \varprojlim_n \mathrm{Fitt}_{R_n}(X_n).$$

In other words, there is a natural isomorphism $\mathrm{Fitt}_R(X) \cong \varprojlim_n \mathrm{Fitt}_{R_n}(X_n)$.

We prove the theorem in several steps.

(1) Since $X \to A_n$ is surjective for large n, the minimal number m_n of generators of the R_n-module A_n is bounded independently of n, by hypothesis (ii). On the other hand, the map $n \to m_n$ is nondecreasing for $n \geq n_0$ by condition (i), hence eventually constant. By an obvious shift in the indices, we may assume that *all* maps in the projective system $(A_n)_n$ are surjective, and that A_n requires *exactly* m generators over R_n, for some constant m and all n.

(2) As a consequence we obtain that the canonical epimorphism

$$A_{n+1}/rad(R_{n+1})A_{n+1} \to A_n/rad(R_n)A_n$$

is an isomorphism, because both sides are $O/rad(O)$-vectorspaces of dimension m.

(3) Next we construct, for every n, an m-vector $(x_n^{(1)}, \ldots, x_n^{(m)})$ with entries in A_n, which form a (minimal) system of R_n-generators of A_n, and such that each sequence $(x_n^{(i)})_n$ $(i = 1, \ldots, m)$ is coherent. This is done by induction: for $n = 0$ we can take any system of m generators of A_0. If the case n is already done, we take $x_{n+1}^{(i)}$ to be an arbitrary preimage of $x_n^{(i)}$ in A_{n+1}, for $i = 1, \ldots, m$. By (2) and by Nakayama's Lemma we see that the resulting vector is a system of generators of A_{n+1}.

(4) Let $g_n : R_n^m \to A_n$ be the R_n-linear epimorphism which sends the i-th standard basis vector to $x_n^{(i)}$, and let $B_n = \ker(g_n)$. We obtain a commutative ladder:

$$\begin{array}{ccccccccc}
 & & \vdots & & \vdots & & \vdots & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & B_{n+1} & \longrightarrow & R_{n+1}^m & \longrightarrow & A_{n+1} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & B_n & \longrightarrow & R_n^m & \longrightarrow & A_n & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \vdots & & \vdots & & \vdots & &
\end{array}$$

(5) We claim that there exists some r such that every B_n can be generated by r elements over R_n.

To prove this, we use the torsion hypothesis in (ii) and take a nonzerodivisor $f \in \Lambda$ which annihilates the limit X. Then $fR_n^m \subset B_n \subset R_n^m$ for all n, so if we find some r_0 such that all $B_n' := B_n/fR_n^m$ are r_0-generated we will be done, with $r := r_0 + m$. Now every B_n' is a module over $S := R/fR = (\Lambda/f\Lambda)[G]$, and B_n' is a submodule of $(S/\omega_n)^m$. Let B_n'' be the preimage of B_n' in S^m. It suffices to show that all B_n'' are r-generated over S for an appropriate r. But S is local noetherian of Krull dimension 1. This implies (see for instance [15]) the existence of a constant d_S such that all ideals of S can

be generated by d_S elements. By an easy argument then, all submodules of S^m can be generated by $r_0 := md_S$ elements.

(6) We set $B_\infty = \varprojlim_n B_n$ and pass to the projective limit in the above diagram. Since every B_n is compact, we again have a short exact sequence in the limit (that is, the limit of the surjections $R_n^m \to A_n$ is again a surjective map). This follows directly from Theorem 7.1 in [8]. But we will actually reprove this in the final part (8) below, because we need it there in somewhat greater generality, to wit: there will be no exact sequences but only continuous surjective morphisms with compact fibers between inverse systems of topological spaces.

Using the canonical isomorphism $\iota : R^m \to \varprojlim_n R_n^m$ we can write the obtained sequence like this:

$$0 \to \iota^{-1}B_\infty \to R^m \to X \to 0.$$

We need some shorthand notation. The symbol Y_n will stand for $m \times m$-matrices over R_n. Then $\mathrm{Fitt}_{R_n}(A_n)$ is generated by all $\det(Y_n)$, where Y_n runs through all $m \times m$-matrices whose rows are arbitrarily chosen from B_n. Similarly, $\mathrm{Fitt}_R(X)$ is generated by all $\det(Y)$, where Y runs through all $m \times m$-matrices whose rows are arbitrarly chosen from $\iota^{-1}B_\infty$.

From this we may already observe that the canonical map $R \to R_n$ takes $\mathrm{Fitt}_R(X)$ into $\mathrm{Fitt}_{R_n}(A_n)$. This implies at once that $\iota(\mathrm{Fitt}_R(X)) \subset \varprojlim_n \mathrm{Fitt}_{R_n}(A_n)$. The non-obvious point is to show that this inclusion is an *equality.*

Assume that we are given a coherent sequence $(z_n)_n$, $z_n \in \mathrm{Fitt}_{R_n}(A_n)$. The general form of an element of $\mathrm{Fitt}_{R_n}(A_n)$ is not just one determinant $\det(Y_n)$ but an R_n-linear combination of such determinants. But since B_n is r-generated, any element of $\mathrm{Fitt}_{R_n}(A_n)$ can surely be written as an R_n-linear combination of at most $s := r^m$ such determinants. Moreover we can replace "R_n-linear combination" simply by "sum", since scalar factors may obviously be moved inside the determinants. We can therefore write each z_n in the form

$$z_n = \sum_{i=1}^{s} \det(Y_n^{(i)}),$$

with $Y_n^{(i)} \in B_n^m$, which we consider as a subspace of $R_n^{m,m}$ (an m-tuple of elements of B_n is packed into a matrix, row by row).

(7) Now suppose for a moment that for all $i = 1, \dots, s$, the sequence of matrices $(Y_n^{(i)})_n$ is *coherent.* Then we may pass to the limits, which we indicate by putting ∞ instead of the index n. The limit matrices $Y_\infty^{(i)}$ are in B_∞^m, and since taking determinants commutes with the limit, we find:

$$\iota^{-1}z_\infty = \sum_{i=1}^{s} \det(\iota^{-1}Y_\infty^{(i)}) \in \mathrm{Fitt}_R(X).$$

This shows the claimed equality, under the coherence assumption.

(8) The rest of the proof eliminates the problem that the above matrix sequences need not be coherent to start with. Theorem 7.1 in [8] is not applicable here, because we have to deal with non-linear maps. So even though

there is certainly no surprise for experts, we give the full argument for the reader's convenience.

Let $W_n = (B_n^m)^s$, and let $\phi_n : W_n \to R_n$ be the map

$$\phi_n(Y_n^{(1)}, \dots, Y_n^{(s)}) = \sum_{i=1}^{s} \det(Y_n^{(i)}).$$

We must show: if the sequence $(z_n)_n$ (with $z_n \in \mathrm{Im}(\phi_n)$) is coherent, then it is possible to find a coherent sequence $(w_n)_n$ so that $\phi_n(w_n) = z_n$ for all n.

Let $C_n \subset W_n$ be the preimage of z_n under ϕ_n. All sets W_n carry the topology inherited from the topology of R^n, and all ϕ_n are continuous in this topology. Moreover all C_n are nonempty and closed in W_n, and hence compact, since W_n is. We let $\nu_{i,n}$ denote the transition maps $W_i \to W_n$ for $i > n$, and we let C'_n be the subset of stable "norms":

$$C'_n = \bigcap_{i>n} \nu_{i,n} C_i.$$

Since the maps $\nu_{i,n}$ are also continuous, all $\nu_{i,n}C_i$ are compact and closed in C_n, and nonempty. Hence their intersection C'_n is not empty. We claim that the transition maps $\nu_{n+1,n}$ induce a surjection $C'_{n+1} \to C'_n$. To see this we proceed as follows.

Let n_0 be fixed, $c \in C'_{n_0}$. By definition we find $c_n \in C_n$ mapping to c for all $n \geq n_0$. The usual Bolzano-Weierstraß type argument shows: There are infinite subsets $I_0 \supset I_1 \supset I_2 \dots$ of $\mathbb{N}$ such that $\min(I_k) \geq n_0 + k$ for all k, and the sequence $(\nu_{i,n_0+k}(c_i))_{i \in I_k}$ converges to some element c'_{n_0+k}, for all $k \in \mathbb{N}$. If we now take a diagonal sequence of indices $n(k) \in I_k$ for all $k \geq 0$, then the images of $c_{n(k)}$ in C_{n_0+k} converge to c'_{n_0+k} for all k. Therefore $(c'_{n_0+k})_k$ is coherent. This shows: c'_{n_0+1} is in C'_{n_0+1} since it starts a coherent series. Also, c'_{n_0+1} is a preimage of c_{n_0} under ν_{n_0+1,n_0}.

Thus all transition maps in the system $(C'_n)_n$ are onto, and hence its projective limit is not empty. Any element of this projective limit is a coherent sequence $(w_n)_n$ such that $\phi_n(w_n) = z_n$ for all n. By the argument given in (7), we are done with the proof of the theorem. □

Remark 2.2 (1) Both hypotheses of the theorem are of course satisfied for $A_n = Cl_{K_n} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ in the usual situation: K/F G-Galois, K_n the n-th level in any $\mathbb{Z}_p$-extension of the form KF_∞. (Condition (i) follows from the fact that for n large, all p-adic primes ramify in K_{n+1}/K_n. Condition (ii) is clear from Iwasawa theory.)

(2) In the case where K has only one prime above p, we have $A_n = X/\omega_n X$ (see [17] Proposition 13.22), and hence $\mathrm{Fitt}_{R_n}(A_n)$ is just the image of $\mathrm{Fitt}_R(X)$ in R_n. In this case the statement of the theorem is easy to see.

(3) It should be easy to generalize the theorem; but as said before, we prefer to focus on applications in Iwasawa theory.

3 Number fields of finite degree: a first result and an example

From Sections 1 and 2 we already know that there must be examples K/k and $n \geq 0$ such that $\theta_{K_n}^{\chi} \notin \mathrm{Fitt}_{O_\chi[\mathrm{Gal}(K_n/F)]}(A_{K_n}^{\chi})$. Our first goal is to establish a result which allows us to find an explicit value for the level n where this happens. Before we start, let us note that Popescu [14] has similar examples for function fields; his methods are different, and so is his setting: he is working in a "higher rank" situation, where one considers Fitting ideals of exterior powers of arithmetic objects.

3.1. We use the same notation as in Section 1. Instead of pursuing full generality, we study the following simple case for now. We assume that $[K : F] = p$, $K \cap F_\infty = F$, and $\mu(X_{F_\infty}^{\chi}) = 0$. Put $G = \mathrm{Gal}(K/F)$ and $\Gamma = \mathrm{Gal}(F_\infty/F)$. Hence, $\mathrm{Gal}(K_\infty/F) = G \times \Gamma$. Suppose that $\mathfrak{p}_1, ..., \mathfrak{p}_s$ are the primes of k above p which split completely in F. We assume that $s \geq 1$ and every prime of F above $\mathfrak{p}_1, ..., \mathfrak{p}_s$ is totally ramified in K_∞. Then, $\mathrm{rank}_{O_\chi}((X_{F_\infty}^{\chi})_\Gamma) = s$, hence $\lambda_{O_\chi}(X_{F_\infty}^{\chi}) \geq s$. We further assume that $\lambda_{O_\chi}(X_{F_\infty}^{\chi}) = s$, and $A_F^{\chi} = 0$. Under these assumptions, we can show the following result.

Theorem 3.1 *Suppose that $s < p^n$. Then we have*

$$\theta_{K_n}^{\chi} \notin \mathrm{Fitt}_{O_\chi[\mathrm{Gal}(K_n/F)]}(A_{K_n}^{\chi}).$$

Remark 3.2 By the same reason as in §1, the above result implies

$$\mathrm{Ann}_{\mathbb{Z}[\mathrm{Gal}(K_n/k)]}(\mu(K_n))\theta_{K_n} \not\subset \mathrm{Fitt}_{\mathbb{Z}[\mathrm{Gal}(K_n/k)]}(Cl_{K_n}).$$

On the other hand, consider the Pontryagin dual $\mathcal{A}_K = (A_K)^\vee$ with cogredient action. Then, by [5], the equivariant Tamagawa number conjecture implies

$$\theta_K^{\chi} \in \mathrm{Fitt}_{O_\chi[\mathrm{Gal}(K/F)]}(\mathcal{A}_K^{\chi})$$

for *any* K (assuming $\chi \neq \omega$). We can obtain the same conclusion by the result [10] we mentioned in Remark 1.2 (3), assuming the Leopoldt conjecture for k. In this respect, $\mathcal{A}_K^{\chi}$ behaves better than A_K^{χ}. We will see this happens again in Section 4.

Proof of Theorem 3.1: Suppose that O_χ is the $O_\chi[G]$-module on which G acts trivially, and R_χ is the $O_\chi[G]$-module $O_\chi[G]/(N_G) \simeq O_\chi[\zeta_p]$, where $N_G = \Sigma_{\sigma \in G}\sigma$ and ζ_p is a primitive p-th root of unity. Suppose that $\ell_1, ..., \ell_m$ are the primes of k not above p which split completely in F, and which are ramified in K/F. By Kida's formula, we have $\mathrm{rank}_{O_\chi}(X_{K_\infty}^{\chi}) = ps + (p-1)m$. We can compute $H^1(G, X_{K_\infty}^{\chi}) = (O_\chi/pO_\chi)^{\oplus(s+m)}$ and $H^2(G, X_{K_\infty}^{\chi}) = (O_\chi/pO_\chi)^{\oplus s}$ (cf. [9] §5). Hence, as an $O_\chi[G]$-module, $X_{K_\infty}^{\chi}$ is isomorphic to $O_\chi^{\oplus s} \oplus R_\chi^{\oplus(s+m)}$, because we know that $X_{K_\infty}^{-}$ has no $\mathbb{Z}_p$-torsion. We write $X_{K_\infty}^{\chi} = M_1 \oplus M_2$ where $M_1 \simeq O_\chi^{\oplus s}$ and $M_2 \simeq R_\chi^{\oplus(s+m)}$. Then, both M_1 and M_2 have intrinsic descriptions: M_1 as the maximal G-fixed submodule and M_2 as the kernel of N_G. (Here, we used again that $X_{K_\infty}^{-}$ has no $\mathbb{Z}_p$-torsion.) For this reason, the decomposition $X_{K_\infty}^{\chi} = M_1 \oplus M_2$ respects the action of Γ, and consequently M_1 and M_2 even are $O_\chi[[\mathrm{Gal}(K_\infty/F)]]$-modules.

Since the norm map $X^{\chi}_{K_\infty} \longrightarrow X^{\chi}_{F_\infty}$ factors through M_1 and is surjective, it induces an isomorphism between M_1 and $X^{\chi}_{F_\infty}$. Since Γ acts trivially on $X^{\chi}_{F_\infty}$, we see that it has to act trivially on M_1, too. By [9] Proposition 5.2, we have an exact sequence

$$0 \longrightarrow (\bigoplus_v I_v(K_\infty/K))^{\chi} \xrightarrow{i} (X^{\chi}_{K_\infty})_{\Gamma} \longrightarrow A^{\chi}_K \longrightarrow 0, \tag{5}$$

where v runs over the primes of K above $\mathfrak{p}_1$,...,$\mathfrak{p}_s$.

(As an aside, we claim that $\mathrm{pr}_1 \circ i : (\bigoplus_v I_v(K_\infty/K))^{\chi} \xrightarrow{i} (X^{\chi}_{K_\infty})_{\Gamma} = M_1 \oplus (M_2)_{\Gamma} \xrightarrow{\mathrm{pr}_1} M_1$ is bijective. In fact, using the same exact sequence for $X^{\chi}_{F_\infty}$ and our assumption $A^{\chi}_F = 0$, we know that the norm map induces a surjective homomorphism $(\bigoplus_v I_v(K_\infty/K))^{\chi} \longrightarrow (X^{\chi}_{F_\infty})_{\Gamma} = X^{\chi}_{F_\infty}$. Hence, comparing the ranks of both modules, we know that $\mathrm{pr}_1 \circ i$ is bijective. This fact is not needed in this proof, but will be useful for the example afterwards.)

Next, we use Proposition 5.2 in [9] for K_∞/K_n, and obtain an exact sequence

$$0 \longrightarrow (\bigoplus_{v_n} I_{v_n}(K_\infty/K_n))^{\chi} \longrightarrow (X^{\chi}_{K_\infty})_{\mathrm{Gal}(K_\infty/K_n)} \longrightarrow A^{\chi}_{K_n} \longrightarrow 0. \tag{6}$$

Here v_n runs over the primes of K_n above $\mathfrak{p}_1$,...,$\mathfrak{p}_s$. Since $(\bigoplus_{v_n} I_{v_n}(K_\infty/K_n))^{\chi} = p^n(\bigoplus_v I_v(K_\infty/K))^{\chi}$, comparing (5) and (6), we obtain

$$A^{\chi}_{K_n} \simeq \frac{M_1 \oplus (M_2)_{\mathrm{Gal}(K_\infty/K_n)}}{\mathrm{Image}(p^n i)}. \tag{7}$$

In particular,

$$A^{\chi}_{K_n} \otimes_{O_\chi} (O_\chi/p^n O_\chi) \simeq M_1/p^n M_1 \oplus (M_2/p^n M_2)_{\mathrm{Gal}(K_\infty/K_n)}.$$

Therefore,

$$A^{\chi}_{K_n} \otimes_{O_\chi[G]} (R_\chi/p^n R_\chi) \simeq (R_\chi/(\zeta_p - 1))^{\oplus s} \oplus (M_2/p^n M_2)_{\mathrm{Gal}(K_\infty/K_n)}.$$

Suppose that $\psi : G \longrightarrow \overline{\mathbb{Q}_p}^{\times}$ is a faithful character. Consider a character $\chi\psi$, and the main conjecture for $\chi\psi$ proved by Wiles [18], namely the equality $\mathrm{char}\, X^{\chi\psi}_{K_\infty} = (\theta^{\chi\psi}_{K_\infty/k})$. (Note that $\theta^{\chi\psi}_{K_\infty/k}$ is the image of $\theta^{\chi}_{K_\infty/k}$ in $R_\chi[[\Gamma]]$.) This implies that $\mathrm{Fitt}_{R_\chi[[\Gamma]]}(M_2) = (\theta^{\chi\psi}_{K_\infty/k})$. Hence,

$$\mathrm{Fitt}_{R_\chi[\mathrm{Gal}(K_n/K)]}((M_2)_{\mathrm{Gal}(K_\infty/K_n)}) = (\theta^{\chi\psi}_{K_n/k})$$

for $n \geq 1$. Therefore,

$$\mathrm{Fitt}_{(R_\chi/p^n R_\chi)[\mathrm{Gal}(K_n/K)]}(A^{\chi}_{K_n} \otimes R_\chi/p^n) = \mathfrak{m}^s \theta^{\chi\psi}_{K_n/k}$$

where $\mathfrak{m} = (\zeta_p - 1, \gamma - 1)$. Now if $\theta^{\chi}_{K_n/k}$ were an element of the ideal $\mathrm{Fitt}_{O_\chi[\mathrm{Gal}(K_n/F)]}(A^{\chi}_{K_n})$, then the image of $\theta^{\chi\psi}_{K_n/k}$ would be in

$$\mathrm{Fitt}_{(R_\chi/p^n R_\chi)[\mathrm{Gal}(K_n/K)]}(A^{\chi}_{K_n} \otimes R_\chi/p^n) \subset (R_\chi/p^n R_\chi)[\mathrm{Gal}(K_n/K)].$$

But this contradicts the preceding formula for the following reason: if $p^n > s = \lambda(\theta^{\chi\psi}_{K_\infty/k})$, then the image of $\theta^{\chi\psi}_{K_\infty/k}$ in $(R_\chi/pR_\chi)[\mathrm{Gal}(K_n/K)]$ (this ring is the same as $R_\chi[\Gamma]/(p, T^{p^n})$) is nonzero, since it is associated to a unitary polynomial of degree s. Note that we also used $s \geq 1$. □

3.2. We illustrate this theorem by means of an explicit example, for which we are able to check the statement of 3.1 directly, and even more, we can calculate the Fitting ideal completely.

We take $p = 3$, $k = \mathbb{Q}(\sqrt{29})$, and $F = k(\sqrt{-2})$. The ideal $\mathfrak{p} = (3)$ is a prime ideal of k, and it splits in F. Suppose that k' is the minimal splitting field of $x^3 - 12x - 13 = 0$ over $\mathbb{Q}$. Then, k' contains k. The extension k'/k is a cubic extension which is unramified outside $\mathfrak{p}$, and totally ramified at $\mathfrak{p}$. We take $K = Fk'$. The two prime ideals of F above $\mathfrak{p}$ are both totally ramified in K_∞/F. Take χ to be the unique non-trivial character of $\mathrm{Gal}(F/k)$. Then, $A^\chi_F = A^-_F = A_F = 0$, so we get $X^\chi_{F_\infty} = X^-_{F_\infty} = X_{F_\infty} = X_{\mathbb{Q}(\sqrt{-2})}$. Since $A_{\mathbb{Q}(\sqrt{-2})} = 0$ and $A_{\mathbb{Q}(\sqrt{-2})_1} = A_{\mathbb{Q}(\sqrt{-2},\cos(2\pi/9))} = \mathbb{Z}/3\mathbb{Z}$, we can easily check $\lambda(X_{\mathbb{Q}(\sqrt{-2})}) = 1$ and $X_{\mathbb{Q}(\sqrt{-2})} \simeq \mathbb{Z}_p$. Hence, $X^\chi_{F_\infty} \simeq \mathbb{Z}_p$. Thus, this example satisfies all assumptions of Theorem 3.1 with $s = 1$ and $m = 0$. We now try to verify the conclusion of that theorem, by independent means.

We calculated by Pari-GP that $Cl_K \simeq \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, hence $A^\chi_K = A_K \simeq \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. Let σ be a generator of $G = \mathrm{Gal}(K/F)$, and γ be a generator of $\Gamma = \mathrm{Gal}(F_\infty/F)$. Put $\Lambda[G] = \mathbb{Z}_p[[G \times \Gamma]]$, and $S = \sigma - 1$, $T = \gamma - 1 \in \Lambda$. We use the same notation as in the proof of Theorem 3.1. In our case, $M_1 = \mathbb{Z}_p$ and $M_2 = R_\chi$. The isomorphism (7) with $n = 0$ in the proof of Theorem 3.1, with the aside claim established within the proof, yields a bijection $(M_2)_\Gamma \simeq A^\chi_K \simeq \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. Hence, $(M_2)_\Gamma$ is isomorphic to $R_\chi/((\zeta_p - 1)^2)$, and $\mathrm{char}_{R_\chi[[\Gamma]]}(M_2) = (T - \overline{u}(\zeta_p - 1)^2)$ for some $\overline{u} \in R_\chi[[\Gamma]]^\times$. Hence, by the expression (7) with $n = 1$ for $A^\chi_{K_n}$ given in the proof, we know that $A^\chi_{K_1} \simeq \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}$. This was also checked by T. Komatsu using Pari-GP. He computed the class groups of suitable subfields of K_1 of degree 18, and obtained the above isomorphism. We thank him very much for informing us of his computation.

Now, we consider $\mathcal{A}_{K_\infty}$ (cf. Remark 1.2 (3)). Since $H^i(G, \mathcal{A}_{K_\infty}) = 0$ for $i = 1$ and 2 (cf. [10] Lemma A2), we get $\mathcal{A}_{K_\infty} \simeq \mathbb{Z}_p[G]$ as a $\mathbb{Z}_p[G]$-module. Hence, $\mathcal{A}_{K_1} = (A_{K_1})^\vee$ is also cyclic as a $\mathbb{Z}_p[G]$-module. Since we know that $\mathcal{A}_{K_1}$ is annihilated by 9 as an abelian group, there must be an exact sequence $0 \longrightarrow \mathbb{Z}/3\mathbb{Z} \longrightarrow \mathbb{Z}/9\mathbb{Z}[G] \longrightarrow \mathcal{A}_{K_1} \longrightarrow 0$. Taking the dual, we get an isomorphism

$$A_{K_1} \simeq \mathrm{Ker}(\mathbb{Z}/9\mathbb{Z}[G] \longrightarrow \mathbb{Z}/3\mathbb{Z}).$$

In other words: A_{K_1} is isomorphic to the maximal ideal $\mathfrak{m}$ of $\mathbb{Z}/9\mathbb{Z}[G]$ as a $\mathbb{Z}_p[G]$-module.

Since $X^\chi_{K_\infty} = M_1 \oplus M_2$, we can check that T acts on $\mathcal{A}_{K_\infty}$ by uS^2 for some $u \in \Lambda[G]^\times$. By the Weierstrass preparation theorem with the λ-invariant $= 1$ and the μ-invariant $= 0$ in this case, $\theta^\chi_{K_\infty}$ can be written as $v(T - \alpha)$ for some $\alpha \in \Lambda[G]$, and $v \in \Lambda[G]^\times$. Since we know the Leopoldt conjecture holds for k and $\mu(X_{F_\infty}) = 0$, we can apply [10] Appendix to get that $\theta^\chi_{K_\infty}$ is in

the Fitting ideal of $\mathcal{A}_{K_\infty}$. In particular, we know that $\theta^\chi_{K_\infty}$ annihilates $\mathcal{A}_{K_\infty}$. Hence, we must have $\alpha = uS^2$, and therefore

$$\theta^\chi_{K_\infty} = v(T - uS^2).$$

Using the isomorphism $A^\chi_{K_1} \simeq \mathfrak{m}$, we take two generators e_1, e_2 of $A^\chi_{K_1}$ which correspond to p and S respectively. Then, the $\mathbb{Z}_p[G]$-module $\mathfrak{m}$ is described by these two generators and the three relations $Se_1 = pe_2$, $pe_1 = 0$, and $N_G e_2 = 0$. Note that $p^2 e_2 = 0$ as a consequence. To take care of the action of T, one needs two more relations $\theta^\chi_{K_1} e_1 = 0$, and $\theta^\chi_{K_1} e_2 = 0$ (note that $\theta^\chi_{K_1}$ is the image of $\theta^\chi_{K_\infty}$). ¿From this it is straightforward to calculate

$$\mathrm{Fitt}_{\mathbb{Z}_p[\mathrm{Gal}(K_1/F)]}(A^\chi_{K_1}) = (p^2, pS^2, p\theta^\chi_{K_1}, S\theta^\chi_{K_1}, (\theta^\chi_{K_1})^2).$$

We can show that

$$(p^2, pS^2, p\theta^\chi_{K_1}, S\theta^\chi_{K_1}, (\theta^\chi_{K_1})^2) = (N_{\mathrm{Gal}(K_1/F)}, p\theta^\chi_{K_1}, S\theta^\chi_{K_1}, T\theta^\chi_{K_1})$$

as ideals of $\mathbb{Z}_p[\mathrm{Gal}(K_1/F)]$ where $N_{\mathrm{Gal}(K_1/F)} = \Sigma_{s\in\mathrm{Gal}(K_1/F)} s$. Hence, we certainly have $\theta^\chi_{K_1} \notin \mathrm{Fitt}_{\mathbb{Z}_p[\mathrm{Gal}(K_1/F)]}(A^\chi_{K_1})$. (This can already be seen from the first description by calculating modulo p.)

On the other hand, we have $\mathcal{A}^\chi_{K_1} \simeq (\mathbb{Z}_p/p^2\mathbb{Z}_p)[\mathrm{Gal}(K_1/F)]/(pS^2, \theta^\chi_{K_1})$. As ideals of $\mathbb{Z}_p[\mathrm{Gal}(K_1/F)]$, we have $(p^2, pS^2, \theta^\chi_{K_1}) = (N_{\mathrm{Gal}(K_1/F)}, \theta^\chi_{K_1})$. Hence,

$$\mathrm{Fitt}_{\mathbb{Z}_p[\mathrm{Gal}(K_1/F)]}(\mathcal{A}^\chi_{K_1}) = (N_{\mathrm{Gal}(K_1/F)}, \theta^\chi_{K_1}).$$

This shows clearly that the Fitting ideal of the dual of the class group is better behaved than the Fitting ideal of the class group itself in this case.

We finally mention that we were able to calculate $\theta = \theta^\chi_{K_1}$. In this way, everything becomes explicit, including the two units u and v. We give a brief sketch how the calculation was done. Of course $\theta^\chi_{K_1} \in \mathbb{C}[\mathrm{Gal}(K_1/F)] = \mathbb{C}[\langle\sigma,\gamma\rangle]$ is uniquely determined by the nine values $\psi(\theta) = L(0, \psi^{-1}\chi)$. Here χ is the nontrivial character of $\mathrm{Gal}(F/k)$, now identified with the nontrivial character of $\mathrm{Gal}(K_1/K_1^+)$; ψ runs through the characters of $\mathrm{Gal}(K_1/F)$, and all involved L-functions are meant to omit all Euler factors at places that ramify in K_1/k. We obtained these L-values by finding the corresponding values at $s = 1$ and using the functional equation. The values at $s = 1$ were rather naively calculated by evaluating the relevant Euler product up to factors attached to primes over rational primes < 8000. We have confidence in the result (see below) for two reasons: firstly, the calculated coefficients of θ were close enough to integers (which we then took as the actual value of course), and secondly, some checks involving the class numbers of subfields $F \subset K' \subset K$ with $[K : K'] = 3$ confirmed our numbers. We now write down the result (note that we do not specify our choice of σ and γ, but it could be done):

$$\frac{1}{4}\theta^\chi_{K_1} = (3 - 6\sigma - 6\sigma^2) + 5\gamma + 2\gamma^2(\sigma + \sigma^2).$$

For a consistency check, we rewrite this in terms of S and T:

$$\begin{aligned}\frac{1}{4}\theta_{K_1}^{\chi} &= 8S^2 + 4S^3 + 13T - 8S^2T - 4S^3T + 4T^2 - 4S^2T^2 - 2S^3T^2 \\ &= v(T - uS^2),\end{aligned}$$

where $v = (1 + (4/13 - 132/2197S^2 - 66/2197S^3 + ...)T)(13 - 136/13S^2 - 68/13S^3 + 1056/2197S^4 + ...)^{-1}$ and $u = -8/13 - 4/13S - 1088/2197S^2 - 1088/2197S^3 + ...$ are units. Since $\theta_{K_1}^{\chi}$ is in $\mathrm{Fitt}_{\mathbb{Z}_p[\mathrm{Gal}(K_1/F)]}(\mathcal{A}_{K_1}^{\chi})$, T acts on A_{K_1} by uS^2. This agrees with what was said earlier concerning the action of T on A_{K_1}.

4 The case of finite level: complements

In this section we present another two systematic methods for producing examples of the kind that we just saw. They are similar in spirit but perhaps each has its own advantages. The first of them does not encompass the explicit example of the last section; the second method however does.

4.1. We study a class of examples for which we can show by the consideration of λ-invariants that the Stickelberger element is not in the Fitting ideal. Suppose that F, K, χ ... are as in §1. We also use the notation $\mathcal{P}$, $\mathcal{Q}$, $\mathcal{P}_i$, $\mathcal{Q}_i$, $\mathcal{P}_{i,F_\infty}$, $\mathcal{Q}_{i,F_\infty}$ with $i = 0$, 1, etc. from the proof of Theorem 1.1. We define

$$s = \#\mathcal{P}_{0,F_\infty} \quad \text{and} \quad m = \#\mathcal{Q}_{1,F_\infty}.$$

For every $v \in \mathcal{Q}_{F_\infty}$, we denote by $I_v(K_\infty/F_\infty)$ the inertia subgroup of v inside $\mathrm{Gal}(K_\infty/F_\infty)$. We define

$$t = \dim_{O_\chi/pO_\chi}\Big(\bigoplus_{v\in\mathcal{Q}_{0,F_\infty}} I_v(K_\infty/F_\infty)\otimes\mathbb{Z}_p/p\mathbb{Z}_p\Big)^{\chi}.$$

We assume $\mu(X_{F_\infty}^{\chi}) = 0$, and $K \cap F_\infty = F$. We define $\lambda = \lambda_{O_\chi}(X_{F_\infty}^{\chi})$, that is: $X_{F_\infty}^{\chi} \simeq O_\chi^{\lambda}$ as O_χ-modules.

Proposition 4.1 *Assume that $s < t$, and n is large enough so that every prime above $\mathcal{P}_0$ is totally ramified in K_∞/K_{n-1} and that $\lambda + s + m < p^n$. Then we have*

$$\theta_{K_n}^{\chi} \notin \mathrm{Fitt}_{O_\chi[\mathrm{Gal}(K_n/F)]}(A_{K_n}^{\chi}).$$

The condition $s < t$ in Proposition 4.1 is satisfied, for example, if $G = \mathrm{Gal}(K/F)$ is not cyclic, $\mathcal{P}_0$ is non-empty, and every prime above $\mathcal{P}_0$ is totally ramified in K_∞/F. Note here that the explicit example in §3 involved a cyclic group G.

Proof of Proposition 4.1: We put $T = \gamma - 1$, where γ is a generator of $\mathrm{Gal}(F_\infty/F)$. By (3) in the proof of Theorem 1.1, we have

$$\mathrm{Fitt}_{O_\chi/pO_\chi[[\mathrm{Gal}(F_\infty/F)]]}((X_{K_\infty}^{\chi})_G \otimes_{O_\chi} O_\chi/pO_\chi) = (T^{\lambda+m+t}). \qquad (8)$$

Assume that $\theta^{\chi}_{K_n} \in \mathrm{Fitt}_{O_\chi[\mathrm{Gal}(K_n/F)]}(A^{\chi}_{K_n})$. By [16] page 86 Proposition 1.6, the image $\overline{\theta}^{\chi}_{K_n}$ of $\theta^{\chi}_{K_n}$ in $O_\chi[\mathrm{Gal}(F_n/F)]$ may be written as $\overline{\theta}^{\chi}_{K_n} = \prod_w (1-\varphi_w^{-1})\theta^{\chi}_{F_n}$ where w runs over those primes of k which are unramified in F_n but are ramified in K_n. Hence, $\overline{\theta}^{\chi}_{K_n} \equiv \overline{u}T^{\lambda+m} \bmod (p)$ for some $\overline{u} \in O_\chi[\mathrm{Gal}(F_n/F)]^\times$ because $(\theta^{\chi}_{F_\infty}) = (T^\lambda)$ as ideals of $O_\chi[[\mathrm{Gal}(F_\infty/F)]]$. (Note that by our assumption $m < p^n$, every prime of F_n above $\mathcal{Q}_1$ is inert in F_∞/F_n, and that every prime above $\mathcal{P}_0$ is ramified in F_n.)

Again by Proposition 5.2 in [9], the sequence

$$0 \longrightarrow (\bigoplus_{\mathfrak{p}\in\mathcal{P}_{0,K_n}} \mathbb{Z}_p)^\chi \longrightarrow (X^{\chi}_{K_\infty})_{\mathrm{Gal}(K_\infty/K_n)} \longrightarrow A^{\chi}_{K_n} \longrightarrow 0$$

is exact, where $\mathfrak{p}$ ranges over all primes of K_n above $\mathcal{P}_0$. For $w \in \mathcal{P}_0$, $((\bigoplus_{\mathfrak{p}|w}\mathbb{Z}_p)^\chi)_G$ is cyclic as an $O_\chi[\mathrm{Gal}(F_n/F)]$-module, and $(1+T)^{s_w}-1$ kills it where s_w is the number of primes of F_n above w. Hence, it follows from $s = \Sigma_{w\in\mathcal{P}_0} s_w$ that there is an element

$$x \in \mathrm{Fitt}_{O_\chi[\mathrm{Gal}(K_n/F)]}((\bigoplus_{\mathfrak{p}\in\mathcal{P}_{0,K_n}} \mathbb{Z}_p)^\chi)$$

such that $x \equiv T^s$ modulo (p, I_G) where I_G is the augmentation ideal of $G = \mathrm{Gal}(K_n/F_n) = \mathrm{Gal}(K/F)$.

¿From the above exact sequence we see that

$$x\theta^{\chi}_{K_n} \in \mathrm{Fitt}_{O_\chi[\mathrm{Gal}(K_n/F)]}((X^{\chi}_{K_\infty})_{\mathrm{Gal}(K_\infty/K_n)}).$$

Since $\theta^{\chi}_{K_n} \equiv uT^{\lambda+m}$ modulo (p, I_G) for some $u \in O_\chi[\mathrm{Gal}(K_n/F)]^\times$, there is an element $\alpha \in \mathrm{Fitt}_{O_\chi[[\mathrm{Gal}(K_\infty/F)]]}(X^{\chi}_{K_\infty})$ such that $\alpha \equiv T^{\lambda+m+s}$ modulo (p, I_G, T^{p^n}). Hence, by (8) and our assumption $\lambda+m+s < p^n$, we obtain $\lambda+m+s \geq \lambda+m+t$. But this contradicts our assumption $s < t$. □

4.2. We finally present another approach which does not use cyclotomic extensions. Therefore the top field will now be written K (not K_n); to obtain the example in §3.2, one has to change the notation back from K to K_1. We retain the notation F for the maximal extension of k with prime-to-p degree inside K, and we write $\mathrm{Gal}(K/k) = G \times \Delta$ with $K^G = F$. (Note that this group G corresponds to $G \times \langle\gamma\rangle$ in §3.2.)

We describe an algebraic situation where the relevant Stickelberger element is not in the Fitting ideal of the undualised module; afterwards we will exhibit arithmetic criteria which imply that this situation arises in certain cases.

Proposition 4.2 *Suppose χ is an odd character of Δ and:*

(i) *G is not cyclic (we call this condition (NC));*
(ii) *A^{χ}_K is annihilated by the norm element N_G, and*

$$\mathrm{Fitt}_{R_\chi}((A^{\chi}_K)^\vee) = (\theta^{\chi}_K),$$

where we have put $R_\chi = O_\chi[G]/(N_G)$.

(iii) *θ_K^χ is not a unit of R_χ.*

Then $\theta_K^\chi \notin \mathrm{Fitt}_{R_\chi}(A_K^\chi)$.

Proof: Let $M = (A_K^\chi)^\vee$. It follows from Prop. 4 in [2] that as a consequence of hypothesis (ii), M has projective dimension at most 1 over R_χ, so there is a presentation $R_\chi^n \to R_\chi^n \to M \to 0$, where the leftmost map is right multiplication with an $n \times n$-matrix V over R_χ with $\det(V) = \theta_K^\chi$. Moreover we can assume that the number n is minimal. (The vectors in R_χ^n are considered to be rows.) From this we can calculate the Fitting ideal of $M^\vee = A_K^\chi$; the result will be that it does not contain θ_K^χ. The details go as follows:

We apply the functor $\mathrm{Hom}_{O_\chi}(-, O_\chi)$ to the short exact sequence $0 \to R_\chi^n \to R_\chi^n \to M \to 0$. Since $M^\vee$ can be identified with $\mathrm{Ext}^1_{O_\chi}(M, O_\chi)$, we get

$$0 \to \mathrm{Hom}(R_\chi^n, O_\chi) \to \mathrm{Hom}(R_\chi^n, O_\chi) \to M^\vee \to 0,$$

where the second arrow is induced from $R_\chi^n \xrightarrow{V} R_\chi^n$. On the other hand, $\mathrm{Hom}(R_\chi, O_\chi)$ can be identified with the augmentation ideal $I_G \subset O_\chi[G]$. If we do this, we obtain a short exact sequence of $O_\chi[G]$-modules

$$0 \to I_G^n \to I_G^n \to M^\vee \to 0,$$

in which the second map is right multiplication with the transposed matrix ${}^tV$.

Write G as the direct product of cyclic nontrivial subgroups $\langle \sigma_i \rangle$, for $i = 1, \dots, t$. Then one can check that I_G is presented by t generators x_i (mapping to $s_i := \sigma_i - 1$) and $t + t(t-1)/2$ relations: $N_{\sigma_i} x_i = 0$ and $s_j x_i = s_i x_j$ for $i \neq j$, $1 \leq i, j \leq t$. Hence, I_G^n is presented by nt generators $x_i^{(h)}$ (with $h = 1, \dots, n$; $x_i^{(h)}$ is in the h-th copy of I_G inside I_G^n), and $nt(t+1)/2$ relations. A presentation of $M^\vee$ now arises by taking the cokernel of right multiplication with $B := {}^tV$. If we reorder the generators as follows: $x_1^{(1)}, x_1^{(2)}, \dots, x_1^{(n)}, x_2^{(1)}, \dots$, we obtain the following relation matrix (every

block is of shape $n \times n$, and I is the identity matrix):

$$A = \begin{pmatrix} B & & & & \\ & B & & & \\ & & \ddots & & \\ & & & & B \\ N_{\sigma_1} & & & & \\ & N_{\sigma_2} & & & \\ & & \ddots & & \\ & & & & N_{\sigma_t} \\ s_2 I & -s_1 I & & & \\ s_3 I & & -s_1 I & & \\ \vdots & & & \ddots & \\ s_t I & & & & -s_1 I \\ & s_3 I & -s_2 I & & \\ & & \ddots & & \\ & & & s_t I & -s_{t-1} I \end{pmatrix}$$

The Fitting ideal J of $M^\vee$ is generated by all tn-minors of this matrix, and unpleasant to determine exactly. Therefore we will work over the ring $R' := O_\chi[G]/(N_{\sigma_1}, s_2, \dots, s_t)$. Since θ_K^χ is a nonzerodivisor and non-unit in R_χ (by hypotheses (ii) and (iii)), the same holds for the image θ' of θ_K^χ in this quotient ring R'. We will show that the ideal J' generated by all tn-minors of the image A' of A over R' is contained in $rad(R')\theta'$. Then J' does not contain θ', and it will follow that J cannot contain θ_K^χ.

Now all blocks of A' in the leftmost column have become zero, with the exception of the topmost one which is (the image of) B. ¿From this it is clear that any nonzero tn-minor of A' has to "pass through" this block, that is, it has the value $\det(B)$ times a $(t-1)n$ minor of the matrix A' with the first n rows and columns deleted. Any such minor is certainly in the radical of R' (actually to a high power), since all entries of B are in the radical to begin with (n was minimal). Hence indeed every minor is in $Rad(R')\theta'$, and we are done. □

As promised we now explain how one can apply this proposition to actually obtain examples. Consider, in addition to (NC) (see 4.2) the following conditions:

— (R1) If a prime $\mathfrak{p}$ of k above p splits in F/F^+, every prime of F above $\mathfrak{p}$ is totally ramified in K/F.
— (R2) The decomposition group of every non-p-adic prime $\mathfrak{q}$ of k that ramifies in K but not in F contains complex conjugation. In other words: if a non-p-adic prime $\mathfrak{q}$ splits in F/F^+, it is unramified in K.

Theorem 4.3 *Assume $\zeta_p \notin K$, Hypotheses (NC), (R1), (R2), $A_F^- = 0$ and $A_K^\chi \neq 0$. Assume further that (at least) one of the following two assumptions is true:*

(a) *The p-adic μ-invariant of F vanishes, and the Leopoldt conjecture holds for k and p; or*

(b) *The equivariant Tamagawa Number Conjecture (which we call ETNC) holds for p and K/k (for details on ETNC see [5]).*
Then the conditions of Proposition 4.2 hold.

PROOF: Condition (i) is just (NC). If we have condition (ii) and A_K^χ is nonzero, then θ_K^χ cannot be a unit, so (iii) follows as well. It therefore suffices to establish the validity of (ii). Let us first do this under the assumption (a).

The fact that $N_G A_K^\chi = 0$ is an immediate consequence of $A_F^\chi = 0$. We must show that

$$\mathrm{Fitt}_R((A_K^\chi)^\vee) = (\theta_K^\chi),$$

where we put $R = O_\chi[G]/(N_G)$.

Let $\mathcal{A}$ be the Pontryagin dual of the direct limit $\varinjlim_n A_{K_n}$. The p-adic μ-invariant is zero for K as well, since this property propagates upwards in p-extensions. So Theorem A.5 of [10] is applicable and tells us:

$$\mathrm{Fitt}_{\mathbf{Z}_p[[\Gamma\times\Delta\times G]]^-}(\mathcal{A}^-) = I_{K_\infty/k}.$$

A few comments concerning notations and conventions are necessary. In loc.cit., the ideal $I_{K_\infty/k}$ is written $\iota(\Theta^\sim_{K_\infty/k})$. The involution ι is not present in our setting since we take cogredient actions on duals. Also, the exponent $\sim$ can be omitted because there is no ω-part in our setting. The ideal $I_{K_\infty/k}$ is defined by using an auxiliary field $F'_\infty \supset K_\infty$ as in [10]. What we have to consider is the element $\theta^\chi_{L'_\infty}$ for subfields L'_∞ of F'_∞. But taking the image in $\mathbf{Z}_p[[\mathrm{Gal}(K_\infty/k)]]$, what we finally get is an element of the form

$$a(L_\infty) cor_{K_\infty/L_\infty}\theta_{L_\infty}$$

for some $L_\infty \subset K_\infty$ where $a(L_\infty) \in \mathbf{Z}_p[[\mathrm{Gal}(K_\infty/k)]]$. In particular, $a(K_\infty) = 1$. We consider a character ξ which will run over all odd characters of Δ (note that χ is a fixed character of Δ). We denote by $F_\xi = F^{Ker(\xi)}$ the field cut out by ξ, and $K_\xi = K^{Ker(\xi)}$, hence $\mathrm{Gal}(K_\xi/F_\xi) = G$. We consider the ξ-component. Since $a(K_{\xi,\infty}) = 1$ and $(cor_{K_\infty/K_{\xi,\infty}})^\xi$ is a unit, we have $\theta^\xi_{K_{\xi,\infty}} \in I^\xi_{K_\infty/k}$. For L_∞ such that $K_{\xi,\infty} \supset L_\infty \supset F_{\xi,\infty}$, by our assumption (R2) and [16] Proposition 1.6 on p. 86, the image of $\theta^\xi_{K_{\xi,\infty}}$ in $\mathbf{Z}_p[[\mathrm{Gal}(L_\infty/k)]]^\xi$ is $\theta^\xi_{L_\infty}$ times some unit. (For a non-p-adic prime $\mathfrak{q}$ of k which ramifies in K/F, by the condition (R2) we have $\xi(\mathfrak{q}) \neq 1$ and $\xi(\mathfrak{q}) - 1$ is a unit for all odd characters ξ. Hence, $\mathfrak{q}$ has no influence modulo units. Any prime above p is ramified in L_∞, so has no influence.) Hence, $(a(L_\infty) cor_{K_\infty/L_\infty}\theta_{L_\infty})^\xi$ is a multiple of $\theta^\xi_{K_\infty}$.

This shows that

$$\mathrm{Fitt}_{\mathbf{Z}_p[[\mathrm{Gal}(K_\infty/k)]]^\xi}(\mathcal{A}^\xi) = (\theta^\xi_{K_{\xi,\infty}}).$$

Similarly as before, the condition (R1) implies that the image of $\theta_{K_{\xi,\infty}}$ in $O_\xi[G]$ is a unit times θ_{K_ξ}. Since $\mathcal{A}^\xi \longrightarrow (A^\xi_{K_\xi})^\vee$ is surjective, it follows that $\theta^\xi_{K_\xi}$ is in $\mathrm{Fitt}_{O_\xi[G]}(A^\xi_{K_\xi}) = \mathrm{Fitt}_{O_\xi[G]}(A^\xi_K)$.

We recall that $R = O_\chi[G]/(N_G)$, and we are assuming $K_\chi = K$ in this paper. Define $A' = (\mathcal{A}^\chi/(N_G))_{\mathrm{Gal}(K_\infty/K)}$, that is, A' is the Γ-coinvariants of $\mathcal{A}^\chi/(N_G)$. Since $A_F^\chi = 0$, we have a natural map

$$A' \to (A_K^\chi)^\vee$$

which is surjective. We have $\mathrm{Fitt}_R(A') = (\theta_K^\chi)$ because as we saw above, the image of θ_{K_∞} in R is a unit times θ_K. Hence, if we can show that the above surjection is an isomorphism, then we will be done. To achieve this, we use the analytic class number formula.

Let $\mathcal{X}(G)$ denote the group of characters of G. By the usual arguments one proves:

$$\mathrm{ord}_p(\#A') = \mathrm{ord}_p(\prod_{\psi\in\mathcal{X}(G),\psi\neq 1} \theta_K^{\chi\psi}). \tag{9}$$

For any odd character ξ of Δ, we have $\theta_{K_\xi}^\xi \in \mathrm{Fitt}_{O_\xi[G]}(A_K^\xi)$, as seen above. Further, by our assumption $A_F^- = 0$, we know that A_F^ξ is trivial and $\theta_{F_\xi}^\xi$ is a unit. Hence,

$$\mathrm{ord}_p(\#A_K^\xi) \le \mathrm{ord}_p(\prod_{\xi\in\mathcal{X}(G),\psi\neq 1} \theta_{K_\xi}^{\xi\psi}). \tag{10}$$

On the other hand, by the analytic class number formula we have

$$\mathrm{ord}_p(\#(A_K^-)) = \mathrm{ord}_p(\prod_{\xi}\prod_{\psi\in\mathcal{X}(G)} \theta_{K_{\xi\psi}}^{\xi\psi}), \tag{11}$$

where $K_{\xi\psi}$ is the field cut out by $\xi\psi$. First of all, we note that $\mathrm{ord}_p(\theta_{K_{\xi\psi}}^{\xi\psi}) = \mathrm{ord}_p((\theta_{K_\xi}^\xi)^\psi)$ for $\psi \neq 1$. This can be proved by essentially the same argument as used before on the ideal $I_{K_\infty/k}$: if ψ is non-trivial, then (R1) and (R2) insure that the Euler factors by which $\theta_{K_{\xi\psi}}^{\xi\psi}$ differs from $\theta_{K_\xi}^\xi$ are p-adic units.

Hence, (11), $A_F^- = 0$ and $\mathrm{ord}_p \#A_K^- = \Sigma_\xi \mathrm{ord}_p \#A_K^\xi$ imply that (10) becomes an equality. Hence, by (9) and the equality (10) for $\xi = \chi$, we get

$$\mathrm{ord}_p(\#A_K^\chi) = \mathrm{ord}_p(\#A') = \mathrm{ord}_p(\prod_{\psi\in\mathcal{X}(G),\psi\neq 1} \theta_K^{\chi\psi})$$

(recall again that $K_\chi = K$). This completes the proof of Theorem 4.3 under assumption (a).

The proof of property (ii) under assumption (b) instead of (a) is rather similar. One begins with the main result of [5] which gives an expression for the R-Fitting ideal of $(A_K^-)^\vee$. The resulting ideal $\mathrm{SKu}_{K/k}$ is a very close analog of the ideal $I_{K_\infty/k}$ discussed before, but it already is defined at finite level. For details we refer to [5]. The discussion of the generators of this ideal is quite analogous to what was said on $I_{K_\infty/k}$, and we will omit the details. The result is exactly as desired: modulo N_G we obtain a cyclic Fitting ideal generated by θ_K^χ, and no descent argument is required, contrary to

the preceding proof. (Avoiding the descent seems to be the only essential difference between the approaches coming from [10] and [5]; the descent is implicitly hidden in ETNC.)

□

Remark 4.4 Our explicit example (we repeat that K_1 plays the role of K) fits the conditions of the above theorem, with hypothesis (a). In fact, we could take $K = K_n$ for any $n > 0$. So the example is covered twice, by 4.3 and 2.1. Even though the list of hypotheses used in 4.3 looks a little clumsy, it requires no knowledge of λ-invariants. In fact, the condition $A_K^\chi \neq 0$ may be replaced by a simpler one, since one can show that in the presence of all the other hypotheses it is implied (for some χ) by the existence of a prime above p which splits from F^+ to F. The condition on A_F^- is easy to control since F has much lower absolute degree than K.

A Appendix: Fitting ideals of $\mathbb{Z}_p$-duals

The main result of this section is Theorem 5.8, which says that the Fitting ideal of a $\mathbb{Z}_p[[H]]$-module M does not change under taking the $\mathbb{Z}_p$-dual, when M is finitely generated free over $\mathbb{Z}_p$ and H is an abelian pro-p-group requiring at most two generators. We will explain the connection with Iwasawa adjoints at the end. Theorem 5.8 requires, at present, a very technical result (Theorem 5.3) in its proof.

We begin with two combinatorial lemmas.

Let us fix a positive integer n throughout this section. Let $K \subset \{1, \dots, n\}$ be any subset and let $K' = \{1, \dots, n\} \setminus K$ denote the complement. For the following definition and lemmas, one should think of 1, 2, ... , n as counters having one green side and one red side, placed in a row on the table; the indices in K stand for counters showing their green side and indices in K' stand for counters with the red side up.

We define the "disorder index" $\varepsilon(K)$ to be the parity of the number of instances where a green counter is to the right of a red one:

$$\varepsilon(K) = (-1)^{\#Dis(K)}, \quad Dis(K) = \{(i,j) \in K \times K' : i > j\}.$$

Note that the "disorder set" $Dis(K)$ is empty iff K is an initial segment of $\{1, \dots, n\}$.

Lemma A.1 *(a) If k, l are distinct and not in K, then*

$$\varepsilon(K \cup \{k,l\}) = (-1)^{l-k-1}\varepsilon(K).$$

(b) If I, J, U are disjoint subsets of $\{1, \dots, n\}$ and $\#I = \#J$, then

$$\varepsilon(I \cup U)\varepsilon(J \cup U) = \varepsilon(I)\varepsilon(J).$$

Proof: (a) We may assume $k < l$. Let c (resp. d) denote the number of green (resp. red) counters strictly between counter k and l (the two latter are red, at present). Let e (resp. f) denote the number of green counters strictly to the right of counter l (resp. red counters strictly to the left of counter k). We flip counter l to make it green. This removes e pairs from $Dis(K)$ (look to the right of counter l) and introduces $d + f + 1$ new pairs; the $+1$ comes from counter k which is still red. We now flip counter k to make it green too. This removes $c + e + 1$ pairs, the $+1$

coming from counter l which is already green, and introduces f new pairs, coming from the left. So the cardinal of $Dis((K \cup \{k,l\})$ is that of $Dis(K)$ plus

$$-e + (d+f+1) - (c+e+1) + f,$$

which is congruent to $c+d = l-k-1$ modulo 2.

(b) If $\#U$ is even, this can be proved by repeatedly taking pairs of elements out of U; according to part (a) the left hand side will not change under this process. If U is odd, we let $U' = U \cup \{n+1\}$ (so we work with subsets of $\{1,\dots,n,n+1\}$ for a moment), and we observe that $\varepsilon(I \cup U') = (-1)^{n-\#I-\#U}\varepsilon(I \cup U)$. From this, and the analog with J replacing I, we deduce $\varepsilon(I \cup U)\varepsilon(J \cup U) = \varepsilon(I \cup U')\varepsilon(J \cup U')$. Now $\#U'$ is even, so we obtain equality of the last product with $\varepsilon(I)\varepsilon(J)$. Now we are done, because it makes no difference for $\varepsilon(I)$ and $\varepsilon(J)$ whether I and J are taken as subsets of $\{1,\dots,n\}$ or of $\{1,\dots,n,n+1\}$. □

For later use we need another definition: If I and J are disjoint subsets of $\{1,\dots,n\}$ satisfying $\#I = \#J$, then we set

$$\delta(I,J) = (-1)^{\#I}\varepsilon(I \cup J).$$

Lemma A.2 *Assume $I, J \subset \{1,\dots,n\}$ are disjoint, with $\#I = \#J$.*

(a) If k, l are distinct and not in $I \cup J$, then

$$\delta(I \cup \{k\}, J \cup \{l\}) = (-1)^{l-k}\delta(I,J).$$

(b) If $k \in I$ and $k' \notin I \cup J$, then

$$\delta((I \setminus \{k\}) \cup \{k'\}, J) = (-1)^{k'-k}\delta(I,J).$$

(c) We have

$$\varepsilon(I)\varepsilon(J) = \delta(I,J).$$

Proof: Part (a) is a direct consequence of Lemma 5.1 and the definition of δ.

For part (b) we note (again) that $\delta(I,J)$ will not change if n is replaced by any $n' > n$. (Only red counters are added, all on the right.) Hence we may pick some l not in $I \cup J$, and distinct from k'. With this auxiliary l we get, using Lemma 5.1 (a) twice:

$$\varepsilon((I \setminus \{k\}) \cup \{k'\} \cup J) = (-1)^{k-l}\varepsilon((I \cup \{k'\}) \cup (J \cup \{l\})) = (-1)^{k-l}(-1)^{l-k'}\varepsilon(I,J).$$

This implies the desired formula.

(c) If $\#I$ is even, then this follows by repeatedly shifting pairs of elements from I over to J; by Lemma 5.1 (a) the product $\varepsilon(I)\varepsilon(J)$ is unchanged by this process, and $\varepsilon(\emptyset) = 1$. We can reduce the case $\#I$ odd to the even case as follows: let $I' = I \cup \{n+1\}$ and $J' = J \cup \{n+2\}$. Then $\varepsilon(I') = (-1)^{n-\#I}\varepsilon(I)$ and $\varepsilon(J') = (-1)^{n+1-\#I}\varepsilon(J)$. Therefore $\varepsilon(I)\varepsilon(J) = -\varepsilon(I')\varepsilon(J')$. By the even case, the latter is equal to $-\varepsilon(I' \cup J') = -\varepsilon(I \cup J \cup \{n+1, n+2\})$. By Lemma 5.1 (a) this is $-\varepsilon(I \cup J)$, and this finally equals $\delta(I,J)$ by definition. □

Our next goal is the statement and proof of a very technical result concerning matrix minors (Theorem 5.3).

We consider two $n \times n$-matrices A and B over an arbitrary commutative ring and the n-minors of the two-block matrix $\left[\begin{smallmatrix} A \\ B \end{smallmatrix}\right] \in R^{2n,n}$. We need a precise method of labeling such minors and proceed as follows.

A *label* is, by definition, a triple (I, J, α) where I and J are disjoint subsets of $\{1,\dots,n\}$ with $\#I = \#J$, and α is a map from $\{1,\dots,n\} \setminus (I \cup J)$ to the two-element set $\{up, down\}$.

To each label we attach an $n \times n$-matrix $M(I, J, \alpha; A, B)$ by choosing n rows among the rows of A and B as follows: For $k \in I$, the k-th row of A and of B are both chosen. For $k \in J$ we choose neither the k-th row of A nor the k-th row of B. For $k \in \{1, \dots, n\} \setminus (I \cup J)$ we choose exactly one k-th row: that of A if $\alpha(k) = up$ and that of B if $\alpha(k) = down$. These chosen rows are packed into a square matrix using the natural ordering, that is, the same order in which they appear in the block matrix $\left[\begin{smallmatrix} A \\ B \end{smallmatrix}\right]$.

This exhausts all possibilities of forming $n \times n$-matrices from the rows of the block matrix $\left[\begin{smallmatrix} A \\ B \end{smallmatrix}\right]$ by deletion of n rows. We let

$$m(I, J, \alpha; A, B) = \det(M(I, J, \alpha; A, B)).$$

Then $m(I, J, \alpha; A, B)$ runs over all n-minors of the block matrix when (I, J, α) runs over all labels. We now formulate our main technical result; it may look surprising at first sight.

Theorem A.3 *Assume R is reduced and the two matrices $A, B \in R^{n,n}$ commute with each other. Then for every label (I, J, α) we have*

$$m(I, J, \alpha; A, B) = \delta(I, J) \cdot m(J, I, \alpha; {}^tA, {}^tB).$$

Note that I and J get exchanged but the indicator map α remains the same.

We begin by some reductions.

Proposition A.4 *In proving Theorem 5.3 we may assume that R is an algebraically closed field and that at least one of A and B is diagonalisable (even without multiple eigenvalues if we like).*

Proof: The first statement holds since every reduced ring injects into a product of algebraically closed fields.

The second reduction is less trivial. We work over $R = k$ an algebraically closed field and look at the variety V of all pairs of commuting matrices A and B over k. Theorem 5.3 states that two morphisms (left and right hand side expression) from V to k are equal. By the Motzkin-Taussky theorem (see [1] or [6], cf. [11]), V is irreducible. The discriminant of the characteristic polynomial of A defines a morphism δ from V to k, and the preimage $W := \delta^{-1}(k \setminus 0)$ consists exactly of the commuting pairs (A, B) for which A has no multiple eigenvalues. (Such A are all diagonalisable of course.) Since k is infinite, there certainly exist diagonal matrices A without multiple eigenvalues, and hence W is not empty (because $(A, E_n) \in W$ for any such A). Thus, W is an open nonempty subset of V and therefore dense in V. Hence it suffices to prove the equality of the two morphisms on the subset W, which is exactly the reduction we claimed. □

Proposition A.5 *(Compatibility with block decomposition) If $n = n_1 + n_2$, A and B are commuting block matrices of the shape*

$$A = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}, \quad B = \begin{pmatrix} B_1 & 0 \\ 0 & B_2 \end{pmatrix}$$

with $A_1, B_1 \in R^{n_1,n_1}$ and $A_2, B_2 \in R^{n_2,n_2}$, and Theorem 5.3 holds true for (A_1, B_1) and (A_2, B_2), then it holds true for (A, B).

Proof: We take sets I and J and a map α as in the statement of Theorem 5.3. Then $I = I_1 \cup I_2$ with $I_1 \subset \{1, \dots, n_1\}$ and $I_2 \subset \{n_1 + 1, \dots, n\}$; similarly for J. We claim that the involved minors are zero unless the equality $\#I_1 = \#J_1$ (and

then also $\#I_2 = \#J_2$) holds. Indeed, if the equalities are violated, we are either taking less than n_1 rows among rows $1, \dots, n_1, n+1, \dots, n+n_1$ of the block matrix

$$\begin{pmatrix} A_1 & 0 \\ 0 & A_2 \\ B_1 & 0 \\ 0 & B_2 \end{pmatrix},$$

or we are taking less than n_2 rows among the remaining rows $n_1+1, \dots, n$, $n+n_1+1, \dots, 2n$. In either case the determinant will be zero, and the same holds for the block matrix in which A_1, A_2, B_1, B_2 are replaced by their transposes. Hence we may assume $\#I_1 = \#J_1$ and $\#I_2 = \#J_2$. In this case the minors split up nicely as products: $m(I, J, \alpha; A, B) = \pm m(I_1, J_1, \alpha_1; A_1, B_1) \cdot m(I_2, J_2, \alpha_2; A_2, B_2)$ and similarly in the transposed case, where α_1 (resp. α_2) denotes the restriction of α to $\{1, \dots, n_1\}$ and $\{n_1+1, \dots, n\}$ respectively. Our proposition will be proved as soon as we can show that the sign (which occurs since the rows that come from A_2 have to be moved past the rows that come from B_1) is the same in the untransposed and the transposed case. This is easy to check: the sign in either case is $(-1)^{a_2 b_1}$, where a_i is the number of A_i-rows that are chosen ($i = 1, 2$), and similarly for b_i. Explicitly, a_i equals $\#I_i$ plus the number of indices j with $\alpha_i(j) = up$. In the transposed situation we get the same numbers since α_i is unchanged and $\#I_i = \#J_i$. □

Proposition A.6 *Theorem 5.3 is true if $A = \lambda E_n$ is a scalar multiple of the identity matrix.*

Proof: Let I, J, α be as in the statement of the theorem, and let U (resp. D) denote the set of k with $\alpha(k) = up$ (resp. *down*). Thus, the index set $\{1, \dots, n\}$ is the disjoint union of I, J, U, D. For index subsets $K, L \subset \{1, \dots, n\}$ let A_{KL} denote the matrix obtained from A by retaining (not: deleting) rows indexed in K and columns indexed in L. If we neglect signs, we have

$$m(I, J, \alpha; A, B) = \pm \lambda^{\#I + \#U} \det(B_{I \cup D, J \cup D}),$$

and

$$m(J, I, \alpha; {}^tA, {}^tB) = \pm \lambda^{\#J + \#U} \det(({}^tB)_{J \cup D, I \cup D}),$$

which is the same. So it remains to check that the sign is predicted correctly by the theorem. When calculating $m(I, J, \alpha; A, B)$ exactly, we get $\lambda^{\#I+\#U}$ times the determinant of the appropriate submatrix of B, times the sign factor $\varepsilon(I \cup U)$. (This corresponds to the positions of the λ's which arise from the A-rows which are taken.) Similarly, we get the sign factor $\varepsilon(J \cup U)$ in the transposed case. We thus need to know that

$$\varepsilon(I \cup U)\varepsilon(J \cup U) = \delta(I, J).$$

But this is an easy consequence of Lemma 5.1 (b) and Lemma 5.2 (c). □

The hardest (and most unexpected) part of the proof is to establish the following result:

Proposition A.7 *In case $R = k$ is a field, the validity of Theorem 5.3 is "stable under conjugation", that is: If the theorem is true for A, B, and if C is any invertible matrix in $k^{n,n}$, then it is also true for CAC^{-1}, CBC^{-1}.*

We postpone the proof and explain how Theorem 5.3 is proved from the preceding lemmas and propositions:

We may assume $R = k$ is a field. By Proposition 5.4 we may assume A is conjugate to a diagonal matrix; so by Proposition 5.7 we may assume A is itself diagonal. By conjugating again if necessary, we sort the diagonal entries of A (i.e. the eigenvalues) into consecutive strings of equal values. Then it is easy to see that any B commuting with A has diagonal block structure, corresponding to the

decomposition of A into diagonal blocks induced by grouping the eigenvalues as above. By Proposition 5.5 we are reduced to the case where A itself is a multiple of the identity matrix, and so we are done by Proposition 5.6. □

Now we turn to the proof of Proposition 5.7. First we may assume that C has determinant one. We now observe that the involved minors do not change if $A, B, {}^tA, {}^tB$ are multiplied *on the right* by arbitrary matrices in $SL_n(k)$. So we can forget about multiplying A, B on the right by C^{-1}, and we can forget about multiplying ${}^tA, {}^tB$ on the right by ${}^tC$. We certainly have to worry about the multiplications on the left hand side. To simplify terminology, let us say the quadruple of matrices (A, B, A', B') behaves well, if the statement of Theorem 5.3 holds, with ${}^tA, {}^tB$ replaced by A', B'. We have to prove the following statement:

if (A, B, A', B') *behaves well, then so does* $(CA, CB, {}^tC^{-1}A', {}^tC^{-1}B')$ (*)

for every $C \in SL(n, k)$. We now use that any $C \in SL(n, k)$ is the product of so-called basic elementary matrices, that is matrices $C = E_{kl}(c)$ which have all diagonal entries equal to 1, and only one off-diagonal entry nonzero, namely the entry in the k-th row and l-th column, and that entry is c. It is then enough to prove the implication (*) for C of this particular shape. The transpose-inverse of C is then $E_{lk}(-c)$. The proof now proceeds by direct calculation, using a longish distinction of cases. Fairly often the indicator map α will be irrelevant, and we will drop it from notation whenever possible. Recall in particular that the sign in Theorem 5.3 (which appears to be the critical issue) does not depend on α.

CA arises from A by adding c times the l-th row (which we shall call the "modifying row") to the k-th row (the "modified row"); the same goes for CB arising from B. From this we draw two remarks:

(1) *If* $l \in I$, *then* $m(I, J; A, B) = m(I, J; CA, CB)$. Reason: The right hand side is the determinant of a submatrix which contains the l-th row of both A and B (note the l-th rows do not change). So whether any k-th row is present or not, we can undo the row operation that led from A, B to CA, CB before computing the determinant.

(2) *If* $k \in J$, *then again* $m(I, J; A, B) = m(I, J; CA, CB)$. The reason is even simpler: only the two rows numbered k were changed, and they are not used in the minors we are considering.

Quite analogously we have:

(1') *If* $k \in J$, *then* $m(J, I; A', B') = m(J, I; {}^tC^{-1}A', {}^tC^{-1}B')$.

(2') *If* $l \in I$, *then* $m(J, I; A', B') = m(J, I; {}^tC^{-1}A', {}^tC^{-1}B')$.

This means in particular that our main claim (*) is already proved for $l \in I$ or $k \in J$, for the simple reason that nothing changes.

After having gotten these easy cases out of the way, we assume $l \notin I$ and $k \notin J$ and continue. Let us call the indices k which are outside $I \cup J$ "ordinary".

(3) *The case that both* k *and* l *are ordinary.*

If $\alpha(k) = \alpha(l)$, then a similar argument as in (1) above tells us that the relevant minors do not change. Thus we will assume, without serious loss of generality: $\alpha(k) = up$ and $\alpha(l) = down$. Then we get

$$\begin{aligned} m(I, J, \alpha; CA, CB) &= \det M(I, J, \alpha; CA, CB) \\ &= \det M(I, J, \alpha; A, B) + c \det(D), \end{aligned}$$

where D is obtained from the matrix $M(I, J, \alpha; A, B)$ via replacing the "upper" k-th row by the "upper" l-th row. ("Upper" means "coming from A" of course). Now D is again obtained from $\left[\begin{smallmatrix} A \\ B \end{smallmatrix}\right]$, except for the fact that the rows are not in the correct order: the l-th row is misplaced. To put it into place, one needs exactly r row exchanges, where r is the number of A-rows going into D with row numbers strictly between k and l. On performing these row changes, D turns into the matrix $M(I \cup \{l\}, J \cup \{k\}, \alpha; A, B)$, so we may continue the above equalities by

$$\ldots = m(I, J, \alpha; A, B) + (-1)^r c\, m(I \cup \{l\}, J \cup \{k\}, \alpha; A, B).$$

Exactly in the same way we obtain

$$\begin{aligned} &m(J,I,\alpha;{}^tC^{-1}A',{}^tC^{-1}B') \\ &\quad = m(J,I,\alpha;A',B') - (-1)^{r'}c\,m(J\cup\{k\},I\cup\{l\},\alpha;A',B'), \end{aligned}$$

where now r' denotes the number of B'-rows with indices strictly between k and l that are selected in $M(J,I,\alpha;A',B')$. The minus sign preceding $(-1)^{r'}$ comes from the minus sign at c in the transpose-inverse of C. We claim that $r+r'=l-k-1$. Indeed every index j properly between k and l contributes exactly the amount 1 either toward r or toward r': if $j\in I$ or $\alpha(j)=up$, it is towards r; if $j\in J$ or $\alpha(j)=down$, it is towards r'.

Therefore, we can replace $-(-1)^{r'}$ by $(-1)^r(-1)^{l-k}$ in the last formula. If we now use the hypothesis that (A,B,A',B') behaves well, and the formula $\delta(I\cup\{l\},J\cup\{k\})=(-1)^{l-k}\delta(I,J)$ from Lemma 5.2 (a), we can deduce that $(CA,CB,{}^tC^{-1}A',{}^tC^{-1}B')$ behaves well, the desired conclusion.

(4) *The case $k\in I$ and l ordinary.* We assume, without loss, that $\alpha(l)=up$. This means we may disregard the change in the upper k-th row, but not in the lower k-th row. We get

$$m(I,J;CA,CB)=m(I,J;A,B)+c\det(D),$$

where D is obtained from $M(I,J,\alpha;A,B)$ via replacing the lower k-th row by the lower l-th row. Let r denote the number of lower rows with indices strictly between k and l that go into $M(I,J,\alpha;A,B)$. We get that

$$m(I,J;A,B)+c\det(D)=m(I,J;A,B)+(-1)^r cm((I\setminus\{k\})\cup\{l\},J;A,B).$$

Similarly, if D' denotes $M(J,I,\alpha;A',B')$ with "upper l-th row" replaced by "upper k-th row" and r' the number of selected upper rows indexed strictly between k and l, we find

$$\begin{aligned} m(J,I;{}^tC^{-1}A',{}^tC^{-1}B') &= m(J,I;A',B')-c\det(D') \\ &= m(J,I;A',B')-(-1)^{r'}c\,m(J,(I\setminus\{k\})\cup\{l\};A',B'). \end{aligned}$$

Again $r+r'=l-k-1$, and the argument finishes as in (3), this time using Lemma 5.2 (b).

(5) *The case k ordinary and $l\in J$* is quite similar to case (4).

(6) *The last case: $k\in I$, $l\in J$.* Let D be the matrix $M(I,J,\alpha;A,B)$. Let D_1 arise from D via replacing the upper k-th row by the upper l-th row; let D_2 arise similarly from D reading "lower" instead of "upper"; and finally let D_3 arise from D by doing both replacements. Then we get:

$$\begin{aligned} m(I,J;CA,CB) &= m(I,J;A,B)+c\det(D_1)+c\det(D_2)+c^2\det(D_3) \\ &= m(I,J;A,B) \\ &\quad +(-1)^r cm(I\setminus\{k\},J\setminus\{l\},k\downarrow,l\uparrow;A,B) \\ &\quad +(-1)^{r'}cm(I\setminus\{k\},J\setminus\{l\},k\uparrow,l\downarrow;A,B) \\ &\quad +(-1)^{r+r'}c^2m((I\setminus\{k\})\cup\{l\},(J\setminus\{l\})\cup\{k\};A,B). \end{aligned}$$

Here the notation $k\downarrow$ means that α is extended by sending k to *down*, etc.; the letters r and r' have the same meaning as in case (3).

In the same way we obtain the equation

$$\begin{aligned} &m(J,I;{}^tC^{-1}A',{}^tC^{-1}B') \\ &\quad = m(J,I;A',B') \\ &\quad -(-1)^r cm(J\setminus\{l\},I\setminus\{k\},l\downarrow,k\uparrow;A',B') \\ &\quad -(-1)^{r'}cm(J\setminus\{l\},I\setminus\{k\},l\uparrow,k\downarrow;A',B') \\ &\quad +(-1)^{r+r'}c^2m((J\setminus\{l\})\cup\{k\},(I\setminus\{k\})\cup\{l\};A',B'). \end{aligned}$$

Denote the four summands in the expression for $m(I,J;CA,CB)$ by T_1, T_2, T_3, T_4 and the four summands in the expression for $m(J,I;{}^tC^{-1}A',{}^tC^{-1}B')$ by $T_1',\dots,T_4'$. We check to see by what sign they differ; there is a twist, that is, T_2 is compared to T_3' (not T_2') and vice versa. If the four signs all agree with $\delta(I,J)$, then we are done.

By hypothesis we have $T_1' = \delta(I,J)T_1$; that's the easy part.

We compare T_2 and T_3'. Here the factor is $(-1)^{r+r'+1}\delta(J\setminus\{l\}, I\setminus\{k\})$; the power of (-1) here is $(-1)^{l-k}$ as before, and we are done by Lemma 5.2 (a).

The argument for T_3 and T_2' is exactly the same.

Finally, for T_4 and T_4', the explicit powers of (-1) agree anyway, so the sign factor is $\delta((J\setminus\{l\})\cup\{k\}, (I\setminus\{k\})\cup\{l\})$. But this agrees with $\delta(J,I)=\delta(I,J)$, again for the trivial reason that δ only depends on the union of its two arguments and on $\#I(=\#J)$.

This finishes the proof of the Proposition 5.7, and hence Theorem 5.3 is proved as well. □

We are finally ready for the application which motivated the preceding work in this section.

Theorem A.8 *Let p be any fixed prime, H an abelian pro-p-group which is pro-generated by two elements γ and σ. Let * denote cogredient $\mathbb{Z}_p$-dual, as a contravariant functor on the category of $\mathbb{Z}_p[[H]]$-modules. Then for every $\mathbb{Z}_p[[H]]$-module M which is finitely generated and free over $\mathbb{Z}_p$, we have*

$$\mathrm{Fitt}_{\mathbb{Z}_p[[H]]}(M) = \mathrm{Fitt}_{\mathbb{Z}_p[[H]]}(M^*).$$

Proof: Choose a basis $m_1,\dots,m_n$ of M over $\mathbb{Z}_p$. Let A_0 (resp. B_0) denote the $\mathbb{Z}_p$-matrices which give the action of γ (resp. σ), via right multiplication if M is identified (using the chosen basis) with the space of n-rows $(\mathbb{Z}_p)_n$. This gives a presentation of M as a $\mathbb{Z}_p[[H]]$-module, with generators $m_1,\dots,m_n$ and relation matrix

$$\begin{bmatrix} A_0-\gamma E_n \\ B_0-\sigma E_n \end{bmatrix}.$$

(Every row corresponds to a relation.) If M^* is identified with $(\mathbb{Z}_p)_n$ using the dual basis $m_1^*,\dots,m_n^*$, then the γ-action on M^* is given by the matrix ${}^tA$ and the σ-action by ${}^tB$. Thus M^* has a presentation with again n generators and relation matrix

$$\begin{bmatrix} {}^tA_0-\gamma E_n \\ {}^tB_0-\sigma E_n \end{bmatrix}.$$

Hence if A denotes $A_0-\gamma E_n$ and B denotes $B_0-\sigma E_n$, the Fitting ideal of M over $\mathbb{Z}_p[[H]]$ is generated by all n-minors of the block matrix $\left[\begin{smallmatrix} A \\ B \end{smallmatrix}\right]$, and the Fitting ideal of M^* over $\mathbb{Z}_p[[H]]$ is generated by all n-minors of $\left[\begin{smallmatrix} {}^tA \\ {}^tB \end{smallmatrix}\right]$. Since A_0 and B_0 must commute (H is abelian), the matrices A and B commute as well. By Theorem 5.3, we may conclude that the ideal generated by the n-minors of $\left[\begin{smallmatrix} A \\ B \end{smallmatrix}\right]$ is equal to the ideal generated by the n-minors of $\left[\begin{smallmatrix} {}^tA \\ {}^tB \end{smallmatrix}\right]$, and this proves the equality stated in the Theorem. (Note that all group rings covered by the theorem are indeed reduced, as required in Theorem 5.3.) □

Comment: The equality of ideals which we just used to prove our theorem looks much weaker than the statement of Theorem 5.3. We did not succeed however to make the argument work with a less explicit version of Theorem 5.3.

Obvious examples for H include the free abelian pro-p-group $\Gamma\times\Gamma$ on two generators, and groups of the form $\Gamma\times G$ where G is finite and cyclic, and Γ has its usual meaning in Iwasawa theory; in the latter case we can write $\mathbb{Z}_p[[H]] = \Lambda[G]$. Note that Theorem 5.8 for $\Gamma\times\Gamma$ implies the same for quotient groups of $\Gamma\times\Gamma$ by an easy argument. However it is not clear whether Theorem 5.8 for all finite quotients of $\Gamma\times\Gamma$ would imply Theorem 5.8 for $\Gamma\times\Gamma$.

Remark A.9 It is not difficult to give a counterexample which shows that the analog of Theorem 5.8 for three generators is not true. One can take $H = \Gamma^3$ (so $\mathbb{Z}_p[[H]] \cong \mathbb{Z}_p[[X,Y,Z]]$ is a power series ring in three variables) and $M = \mathbb{Z}_p[[X,Y,Z]]/\langle X,Y,Z\rangle^2$. We leave the details to the reader. Counterexamples involving a finite group exist as well, as shown by the next remark.

Remark A.10 Take $p = 2$ and $H = \langle \sigma, \tau, \rho\rangle$ the elementary abelian group of order 8. Let $\bar{H}$ denote the quotient of H modulo $\langle \sigma\tau\rho\rangle$. Let $M = \mathbb{Z}_2[\bar{H}]/(N_{\bar{H}})$ considered as an $R = \mathbb{Z}_2[H]$-module. Then M is free over $\mathbb{Z}_2$, and it is cyclic over R. One checks by direct calculation that $\mathrm{Fitt}_R(M)$ contains $1 - \sigma\tau\rho$ but $\mathrm{Fitt}_R(M)^*$ does not.

We discuss the relation with adjoints. For Λ-modules and more generally for $\Lambda[G]$-modules M (with G finite abelian), one can also consider the Iwasawa adjoint $\alpha'(M)$. (See [13] p.269ff. or Iwasawa's classical paper [7].) On Λ-torsion modules without $\mathbb{Z}_p$-torsion this is a duality, and it seems more appropriate than the $\mathbb{Z}_p$-dual in case M is annihilated by a power of p. The obvious question concerning the relationship of these two duality functors is easily answered:

Proposition A.11 *Let G be finite abelian and α' the cogredient Iwasawa adjoint as explained before. Then there is a functorial isomorphism*

$$\alpha'(M) = \mathrm{Hom}_{\mathbb{Z}_p}(M, \mathbb{Z}_p)$$

of contravariant functors on the category of $\Lambda[G]$ modules that are finitely generated free over $\mathbb{Z}_p$.

Proof: It is not hard to prove this directly, but we may also quote Cor. 5.5.7 of [13]. □

We make a final observation concerning a certain Iwasawa module treated in previous work [4] of the first author. We review notation: As usual, K/F is G-Galois, $\mathcal{A}_{K_\infty} = \mathcal{A}$ is the inductive limit of the $A_n = Cl_{K_n} \otimes_{\mathbb{Z}} \mathbb{Z}_p$. The module X_{du} is defined in [4], see also below. The module X_p is the Galois group of the maximal abelian p-ramified pro-p-extension of K_∞ (this is only needed in the proof). The result is, then:

Proposition A.12 $(\mathcal{A}^-)^\vee \cong \alpha'(X_{du}^-)$.

Proof: By Kummer duality, $X_p^+(1)$ is the Pontryagin dual of $\mathcal{A}^-$. So by definition $X_{du}^- = \alpha'(X_p^+(1)) = \alpha'((\mathcal{A}^-)^\vee)$. From this, the assertion follows, since $\alpha'\alpha'$ is naturally isomorphic to the identity functor. □

This leads to the following corollary, which explains why the results in [10] and [4] must agree, at least in certain situations:

Corollary A.13 *If K/k, F and χ are as in §1 and if G (the p-part of $\mathrm{Gal}(K/k)$) is cyclic, then the $O_\chi[[\mathrm{Gal}(K_\infty/F)]]$-modules $X_{K_\infty,du}^\chi$ and $\mathcal{A}_{K_\infty}^{\chi\vee}$ have the same Fitting ideal.*

References

1. R. Basili, On the irreducibility of varieties of commuting matrices. *J. Pure Appl. Algebra* **149** (2000), 107-120
2. P. Cornacchia and C. Greither, Fitting ideals of class groups of real fields with prime power conductor, *J. Number Th.* **73** (1998), 459-471

3. P. Deligne and K. Ribet, Values of abelian L-functions at negative integers over totally real fields, *Invent. Math.* **59** (1980), 227–286
4. C. Greither, Computing Fitting ideals of Iwasawa modules, *Math. Zeit.* **246** (2004), 733-767
5. C. Greither, Determining Fitting ideals of minus class groups via the equivariant Tamagawa number conjecture, *Compositio Math.* **143** (2007), 1399-1426.
6. R. Guralnick, A note on commuting pairs of matrices, *Linear Multilinear Algebra* **31** (1992), 71-75
7. K. Iwasawa, On $\mathbb{Z}_l$-extensions of algebraic number fields, *Ann. of Math. (2)* **98** (1973), 246-326
8. C. U. Jensen, *Les foncteurs dérivés de* $\varprojlim$ *et leurs applications en théorie des modules,* Lecture Notes in Mathematics 254, Springer-Verlag 1972
9. M. Kurihara, Iwasawa theory and Fitting ideals, *J. reine angew. Math.* **561** (2003), 39-86
10. M. Kurihara, On the structure of ideal class groups of CM fields, *Documenta Math. Extra Vol. Kato* (2003), 539-563
11. T. S. Motzkin and O. Taussky, Pairs of matrices with property L, II. *Trans. Am. Math. Soc.* **80** (1955), 387-401
12. B. Mazur and A. Wiles, Class fields of abelian extensions of $\mathbb{Q}$, *Invent. Math.* **76** (1984), 179-330
13. J. Neukirch, A. Schmidt, K. Wingberg, *Cohomology of number fields,* Grundlehren 323, Springer 2000
14. C. Popescu, Stark's question and a refinement of Brumer's conjecture extrapolated to the function field case, *Compos. Math.* **140** (2004), 631-646
15. A. Shalev, On the number of generators of ideals in local rings, *Advances Math.* **59** (1986), 82-94
16. J. Tate, *Les conjectures de Stark sur les fonctions L d'Artin en* $s = 0$, Progress in Math. 47, Birkhäuser 1984
17. L. Washington, *Introduction to cyclotomic fields,* Springer GTM 83, Springer 1982 (2nd ed. 1997)
18. A. Wiles, The Iwasawa conjecture for totally real fields, *Ann. of Math. (2)* **131** (1990), 493–540