TATE SEQUENCES AND FITTING IDEALS OF IWASAWA MODULES

CORNELIUS GREITHER AND MASATO KURIHARA

ABSTRACT. We consider abelian CM extensions L/k of a totally real field k, and we essentially determine the Fitting ideal of the dualized Iwasawa module studied by the second author [Ku3] in the case that only places above p ramify. In doing so we recover and generalise results of loc. cit. Remarkably, our explicit description of the Fitting ideal, apart from the contribution of the usual Stickelberger element $\dot{\Theta}$ at infinity, only depends on the group structure of the Galois group $\mathrm{Gal}(L/k)$ and not on the specific extension L. From our computation it is then easy to deduce that $\dot{T}\dot{\Theta}$ is not in the Fitting ideal, as soon as the p-part of $\mathrm{Gal}(L/k)$ is not cyclic. We need a lot of technical preparations: resolutions of the trivial module $\mathbb{Z}$ over a group ring, discussion of the minors of certain big matrices that arise in this context, and auxiliary results about the behaviour of Fitting ideals in short exact sequences.

INTRODUCTION

0.1. As a refinement of the main conjecture in Iwasawa theory for ideal class groups, we can describe in certain cases the Fitting ideals of class groups as Galois modules (algebraic objects) by using the Stickelberger elements (analytic objects). But in general, the usual class group does not fit well with (étale) cohomology theory, and certain modified class groups are used in the theory of the leading terms of L-functions (for example, the (S,T)-modified class group can be used in the theory of Stark's conjecture where S contains the ramified places and T is used to get a torsion-free subgroup of the unit group). In order to treat the class group in the usual non-modified sense, we need several devices. In this paper, we study these non-modified class groups and determine the Fitting ideals of modules which are related to them, in several new cases.

We consider finite abelian extensions L/k where L is a CM-field and k is totally real. Let $G = \mathrm{Gal}(L/k)$, p be a fixed odd prime number, and let A_L be the minus part of the p-part of the classical ideal class group $cl(L)$. For example, if $k = \mathbb{Q}$, the second author showed with

2000 *Mathematics Subject Classification.* Primary 11R29.

Key words and phrases. Tate sequences, class groups, cohomology, totally real fields, CM fields.

T. Miura in [KM1] that the Fitting ideal of A_L over $\mathbb{Z}_p[G]$ equals the "Stickelberger ideal" (tensored with $\mathbb{Z}_p$). For general k, we know from earlier work (see [Gr2], [Ku2]) that the Pontrjagin dual of the class group (in the usual sense) works better than the class group itself, and the first author proved in [Gr2] that the Fitting ideal of the Pontrjagin dual $A_L^\vee$ over $\mathbb{Z}_p[G]$ equals the "Stickelberger ideal" (tensored with $\mathbb{Z}_p$), assuming the equivariant Tamagawa number conjecture and that the group $\mu_{p^\infty}(L)$ of the roots of unity in L with p-power order is cohomologically trivial. If the group μ_p of the p-th roots of unity in an algebraic closure of L is in L, the group $\mu_{p^\infty}(L)$ is rarely cohomologically trivial, so the problem lies in the case that L contains μ_p.

Let k_∞/k be the cyclotomic $\mathbb{Z}_p$-extension. In the following, we assume that $L \cap k_\infty = k$. If L contains a primitive p-th root of unity, then we encounter a totally different phenomenon on the Fitting ideal of $A_L^\vee$, namely the Fitting ideal of $A_L^\vee$ cannot equal the Stickelberger ideal, in general. In fact, if L contains μ_p and $G_{(p)} = G \otimes \mathbb{Z}_p$ is not cyclic, one knows, for example by Theorem 1.2 in [KM2], that

$$\mathrm{Ann}(\mu_{p^\infty}(L))\theta_{L/k} \not\subset \mathrm{Fit}(A_L^\vee),$$

at least when the primes that split in L/L^+ are unramified in L^+k_∞/k. Here, $\mathrm{Ann}(\mu_{p^\infty}(L))$ is the annihilator ideal of $\mu_{p^\infty}(L)$ over $\mathbb{Z}_p[G]$, $\theta_{L/k} = \sum_{\sigma\in\mathrm{Gal}(L/k)} \zeta_k(\sigma,0)\sigma^{-1} \in \mathbb{Q}[G]$ is the usual Stickelberger element, and $\mathrm{Fit}(A_L^\vee)$ is the Fitting ideal of $A_L^\vee$ over $\mathbb{Z}_p[G]$ with *cogredient action* of G as in [GK].

In this paper, we assume that L/k *is unramified outside* p, and that L contains μ_p. We decompose $G = \Delta \times G_{(p)}$ where $\#\Delta$ is prime to p and $G_{(p)}$ is a p-group. For any $\mathbb{Z}_p[G]$-module M and a character χ of Δ, we define the χ-component by $M_\chi = M \otimes_{\mathbb{Z}_p[\Delta]} \mathcal{O}_\chi$, where $\mathcal{O}_\chi = \mathbb{Z}_p[\mathrm{Im}(\chi)]$ is the $\mathbb{Z}_p[\Delta]$-module on which Δ acts via χ. Since $M = \bigoplus_\chi M_\chi$ where χ runs over $\mathbb{Q}_p$-equivalence classes of characters of Δ, knowing the structure of M as a $\mathbb{Z}_p[G]$-module is equivalent to knowing the structure of M_χ as an $\mathcal{O}_\chi[G_{(p)}]$-module for all χ. Let ω be the Teichmüller character of Δ, which corresponds to the action of Δ on μ_p. For any odd character χ with $\chi \neq \omega$, the Fitting ideal of $(A_L^\vee)_\chi$ can be computed by the method of the first author in [Gr2] if we assume the equivariant Tamagawa number conjecture. Therefore, our interest is in $(A_L^\vee)_\omega$, which is an $\mathcal{O}_\omega[G_{(p)}] = \mathbb{Z}_p[G_{(p)}]$-module.

Though our principal theorem is on a certain Iwasawa module, let us discuss some results for number fields (of finite degree over $\mathbb{Q}$) that follow from the main result, before we explain the main result itself. We put $s = \dim_{\mathbb{F}_p} G/G^p$ and $p^q = \#\mu_{p^\infty}(L)$. We define an ideal $\mathfrak{A}_G$ of $\mathbb{Z}_p[G][[T]]$ in §1, which plays a very important role in this paper (see also the next subsection §0.2). Let $(\mathfrak{A}_G^0)_L$ be the image of the ideal $T^{1-s}\mathfrak{A}_G \subset \mathbb{Z}_p[G][[T]]$ under the ring homomorphism $\mathbb{Z}_p[G][[T]] \longrightarrow$

$\mathbb{Z}_p[G]$ defined by $T \mapsto p^q$. This ideal $(\mathfrak{A}_G^0)_L$ of $\mathbb{Z}_p[G]$ is determined by the group structure of $G_{(p)}$ and q.

Theorem 0.1. *Suppose that L/k is unramified outside p, $\mu_p \subset L$, no prime above p splits completely in L/L^+, and the Iwasawa μ-invariant of the cyclotomic $\mathbb{Z}_p$-extension of L vanishes. Then we have*

$$\mathrm{Fit}_{\mathbb{Z}_p[G]}(A_L^\vee) = (\mathfrak{A}_G^0)_L \theta_{L/k} \ .$$

We give some corollaries which are obtained from Theorem 0.1 when G has a simple structure. In these corollaries, we assume the same conditions as in Theorem 0.1.

Corollary 0.2. *Suppose also that $G_{(p)}$ is cyclic, i.e. $s = 1$. Then we have*

$$\mathrm{Fit}_{\mathbb{Z}_p[G]}(A_L^\vee) = \mathrm{Ann}_{\mathbb{Z}_p[G]}(\mu_{p^\infty}(L))\theta_{L/k} \ .$$

In fact, $(\mathfrak{A}_G^0)_L = \mathrm{Ann}_{\mathbb{Z}_p[G]}(\mu_{p^\infty}(L))$ if $G_{(p)}$ is cyclic (see the computation before Corollary 3.4). But in general, $(\mathfrak{A}_G^0)_L$ is much smaller than $\mathrm{Ann}_{\mathbb{Z}_p[G]}(\mu_{p^\infty}(L))$.

Corollary 0.3. *Suppose that $G_{(p)}$ is elementary abelian and $s \leq 4$. We denote by $\mathfrak{M}_\omega$ the maximal ideal of $\mathbb{Z}_p[G]$ corresponding to the maximal ideal of $\mathcal{O}_\omega[G_{(p)}]$. Then we have*

$$\mathrm{Fit}_{\mathbb{Z}_p[G]}(A_L^\vee) = \mathrm{Ann}_{\mathbb{Z}_p[G]}(\mu_{p^\infty}(L))\mathfrak{M}_\omega^{s(s-1)/2}\theta_{L/k} \ .$$

More generally, we have

Corollary 0.4. *Assume that $G_{(p)} \simeq (\mathbb{Z}/p^a\mathbb{Z})^{\oplus s}$ for some positive integers a and $s \leq 4$.*
(i) *Suppose that $\mu_{p^a} \subset L$, that is, $q = \mathrm{ord}_p(\#\mu_{p^\infty}(L)) \geq a$. Then we have*

$$\mathrm{Fit}_{\mathbb{Z}_p[G]}(A_L^\vee) = \mathrm{Ann}_{\mathbb{Z}_p[G]}(\mu_{p^\infty}(L))(I_{\omega,a})^{s(s-1)/2}\theta_{L/k},$$

where $I_{\omega,a}$ is the ideal of $\mathbb{Z}_p[G]$ whose ω-component is the ideal generated by the augmentation ideal of $\mathcal{O}_\omega[G_{(p)}]$ and p^a, and whose other components are the ideals generated by 1.
(ii) *Suppose next that $q \leq a$. Then we have*

$$\mathrm{Fit}_{\mathbb{Z}_p[G]}(A_L^\vee) = \mathrm{Ann}_{\mathbb{Z}_p[G]}(\mu_{p^\infty}(L))^{(s^2-s+2)/2}\theta_{L/k} \ .$$

We note that the statements of Theorem 0.1 and of Corollaries 0.2, 0.3, 0.4 are all *equalities*, which give an exact relationship between the Fitting ideal and the Stickelberger element. These statements give more precise information than deciding whether $\mathrm{Ann}_{\mathbb{Z}_p[G]}(\mu_{p^\infty}(L))\theta_{L/k}$ is contained in $\mathrm{Fit}_{\mathbb{Z}_p[G]}(A_L^\vee)$ or not. We also note that under the conditions of Theorem 0.1 we can get $\mathrm{Ann}_{\mathbb{Z}_p[G]}(\mu_{p^\infty}(L))\theta_{L/k} \not\subset \mathrm{Fit}_{\mathbb{Z}_p[G]}(A_L^\vee)$ if $s \geq 2$ (in the setting of Corollaries 0.3 and 0.4, this fact can be clearly seen from the above formulae).

The numerical example in [KM2] §2 satisfies all the conditions of Corollary 0.3 with $s = 2$, and Corollary 0.4 with $s = 2$, $a = 1$, $q = 1$. In §4 we will discuss this numerical example in detail.

We assume in Theorem 0.1 that no so-called trivial zeros occur. In §4 we compute the Fitting ideal of a certain Galois group over L^+ without assuming the "no trivial zero" condition.

0.2. Our main theorem is on "the dualized Iwasawa module". Let L_∞/L be the cyclotomic $\mathbb{Z}_p$-extension, L_n the n-th layer, and $A_{L_\infty} = \text{ind.lim}\, A_{L_n}$ where A_{L_n} is the minus part of the p-part of the class group $cl(L_n)$. Our goal is to calculate the Fitting ideal of the Pontrjagin dual $A_{L_\infty}^\vee$, which is a module over the Iwasawa algebra $\mathbb{Z}_p[[\mathrm{Gal}(L_\infty/k)]]$, and is called the *dualized Iwasawa module.* We put $\Lambda = \mathbb{Z}_p[[\mathrm{Gal}(L_\infty/L)]]$, so $\mathbb{Z}_p[[\mathrm{Gal}(L_\infty/k)]] = \Lambda[G]$. As usual, we choose a generator γ of the Galois group $\mathrm{Gal}(L_\infty/L)$ and identify Λ with $\mathbb{Z}_p[[T]]$ where $T = \gamma - 1$.

The Fitting ideal of $A_{L_\infty}^\vee$ is determined in [Ku3] when $G_{(p)}$ is of order p. There exist at least two other Iwasawa modules, which are closely related but in general not isomorphic to $A_{L_\infty}^\vee$: the "standard Iwasawa module" $X_{std} = \text{proj.lim}\, A_n$, and another module X_{du} considered in [Gr1]; the latter module is actually isomorphic to the Iwasawa adjoint of $A_{L_\infty}^\vee$. The Fitting ideal of X_{std} was determined for $k = \mathbb{Q}$ by the second author in [Ku1], and the Fitting ideal of both X_{std} and X_{du} was calculated outside the Teichmüller component by the first author in [Gr1]. Neither X_{std} nor X_{du} will play a role in the present paper, which focusses on proving a generalisation of the results of [Ku3]. Basically, that paper did the case where the p-part of G is cyclic. Both [Ku3] and the present paper need to assume that $\mu = 0$ (which is conjecturally always the case) and that only places above p are ramified in L/k. The main novelty in our approach is the systematic use of the theory of Tate sequences. Our main result is Thm. 3.3. Let us state its second half here.

Theorem 0.5. *Suppose that L/k is unramified outside p, $\mu_p \subset L$, and the Iwasawa μ-invariant of L_∞/L vanishes. Then we have*

$$\mathrm{Fit}_{\Lambda[G]}(A_{L_\infty}^\vee) = \dot{T}^{1-s}\dot{\mathfrak{A}}_G\dot{\Theta}\ .$$

We explain the notation: s is the minimal number of generators of the p-part of G as in the previous subsection; $\dot{\Theta}$ is the equivariant Stickelberger element at infinity, namely the projective limit of $\theta_{L_n/k}$ for $n \gg 0$; the dot denotes taking the mirror image as customary in cyclotomic Iwasawa theory; and most importantly, the ideal $\mathfrak{A}_G \subset \Lambda[G]$ is a purely algebraic invariant that depends only on the group G, not on the particular fields L and k. The ideal $\dot{T}^{1-s}\dot{\mathfrak{A}}_G$ of $\Lambda[G]$ is of finite index in the ideal generated by $\dot{T}$ and the augmentation ideal of $\mathbb{Z}_p[G]$. The definition of $\mathfrak{A}_G$ in general is complicated, and we have to refer

the reader to the relevant sections of the paper, in particular §1. (For $s \leq 4$ we give a complete list of generators.) But in a sense all the complications are in the Teichmüller part. If χ is a character of Δ (the non-p-part of G) different from the Teichmüller character ω, then $(\dot{\mathfrak{A}}_G)_\chi = (\dot{T}^{s-1})$. This part of the theorem had been known, see (2.3.2) in [Ku3].

The main ingredients in determining the Fitting ideal of an Iwasawa module are usually twofold: firstly the Main Conjecture, and secondly techniques from algebra. These techniques often use, more or less explicitly, cohomologically trivial and projective modules. This is what happens in the present paper as well. The algebraic part of our arguments will be driven by the theory of Tate sequences. If we take the Iwasawa module X to be the mirror image of $A_{L_\infty}^\vee$, then there is a four-term sequence

$$0 \to X \to P \to B \to \mathbb{Z}_p \to 0$$

of $\Lambda[\mathrm{Gal}(L^+/k)]$-modules, where B and P have projective dimension at most 1. Our idea is now, very roughly, to take an *explicit* resolution of $\mathbb{Z}_p$ via modules of projective dimension ≤ 1, let Ω^2 be the second kernel in this resolution (so we get a similar 4-sequence with rightmost term $\mathbb{Z}_p$, this time with leftmost term Ω^2), calculate the Fitting ideal of Ω^2 by brute force, and finally establish a link between this Fitting ideal and the Fitting ideal of X, the object of our quest.

To implement this idea requires a fair amount of technical work. Before we give a short description of this, let us give two instances of the main result, which are relatively easy to state, so as not to overtax the reader's patience. Remember Δ is the non-p-part of G and $G_{(p)}$ denotes the p-part. Note that the Teichmüller character ω is $\mathbb{Z}_p$-valued, so that the ω-component of every $\Lambda[G]$-module is naturally a $\Lambda[G_{(p)}]$-module.

(I) *Assume $G_{(p)}$ is the direct product of two cyclic subgroups $\langle\sigma_1\rangle$ and $\langle\sigma_2\rangle$. Let $\nu_i = \sum_{t=0}^{o(\sigma_i)-1} \sigma_i^t$ be the corresponding norm elements, and let $\tau_i = \sigma_i - 1$ for $i = 1, 2$. Then*

$$\mathrm{Fit}_{\Lambda[G_{(p)}]}((A_{L_\infty}^\vee)_\omega) = \Big(\tau_1^2, \tau_1\tau_2, \tau_2^2, \tau_1\nu_2, \tau_2\nu_1, (\tau_1, \tau_2, \nu_1, \nu_2)\dot{T}, \dot{T}^2\Big)\dot{\Theta}.$$

This result will be shown just before Corollary 3.5.

(II) *Assume that the group $G_{(p)}$ is p-elementary of rank $s \leq 4$ with generators $\sigma_1, \ldots, \sigma_s$. Define τ_i and ν_i analogously as in* (I). *Let H be the augmentation ideal of $\mathbb{Z}_p[G_{(p)}]$, J the ideal in this group ring generated by H and all ν_i, and $\mathfrak{M}$ the maximal ideal of $\Lambda[G_{(p)}]$. (Note that $\mathfrak{M}$ is generated by p, H, and either one of T or $\dot{T}$.) Then*

$$\mathrm{Fit}_{\Lambda[G_{(p)}]}((A_{L_\infty}^\vee)_\omega) = \Big(H\, J^{s(s-1)/2} + \dot{T}\, \mathfrak{M}^{s(s-1)/2}\Big)\dot{\Theta}.$$

This result will be established at the end of the paper.

Let us now explain the technical parts of the paper. We write down an explicit resolution and describe Ω^2 by generators and relations. Then we have to deal with the minors of the relation matrix, in order to understand the Fitting ideal of Ω^2. All this is explained in §1, which in fact begins with some abstract calculations of matrix minors. The central issue in the main part §3 of the paper is the transition from Ω^2 to X. There does not seem to be a K-group suitable for our calculations, so we have to work from scratch. In doing so we need certain results on multiplicativity of Fitting ideals in short exact sequences, which cannot be extracted from the literature. We state and prove what we need in §2; the reader is advised to just have a quick glance at the results on a first reading. The main arithmetical arguments then follow in §3. As a corollary of our main result, we recover a negative result of the second author: If the p-part of G is not cyclic and I_{L_∞} denotes the annihilator of $\mathbb{Z}_p(1)$ over $\Lambda[G]$, then I_{L_∞} times the Stickelberger element is not contained in the Fitting ideal of $A_{L_\infty}^\vee$. We explain the consequences over number fields of finite degree in §4. As an appendix we give in §5 a simplified description of the ideal $\mathfrak{A}_G$ under some assumptions.

Further research might go in two directions. First, we would very much like to also deal with extensions L/k which have ramification at places not above p; the paper [Ku3] has some results in this direction already. Second, it would be interesting to have general results at finite level as well.

Acknowledgment: The first author would like to thank the second author for making possible a very enjoyable visit at Keio University in March 2013. The second author expresses his sincere gratitude to the first author for arranging his visit to Munich in September 2013, which led to further fruitful discussions on the subject of this paper. Both authors would like to thank Sören Kleine for his careful reading of our draft and for pointing out several errors.

1. Matrices, minors and resolutions

1.1. **The matrix M_s and its minors.** Fix a positive integer s and consider the set $I = \{1, \dots, s\}$. We are going to construct a very large sparse matrix M_s. Its entries are taken from the list $\nu_1, \dots, \nu_s$, where for the time being all ν_i are just variables. The column indices are "doubletons" in I, that is, two-element subsets of I. It is convenient to picture these indices as squarefree monomials of degree 2 in the formal variables $x_1, \dots, x_n$. The row indices are degree 3 monomials; but we only take those in which exactly two x_i occur, that is, which are of the form $x_i^2 x_j$. At the intersection of row $x_i^2 x_j$ with column $x_i x_j$ we put

the entry ν_i, for all $i \neq j$, $i, j \in I$. All other entries are zero. The relevance of this matrix and the origin of the row and column indices will be explained in the next subsection; for the moment we ask the reader to accept these data as they are. Example for $s = 3$: M_3 is the matrix

$$\begin{pmatrix} \nu_1 & 0 & 0 \\ \nu_2 & 0 & 0 \\ 0 & \nu_2 & 0 \\ 0 & \nu_3 & 0 \\ 0 & 0 & \nu_1 \\ 0 & 0 & \nu_3 \end{pmatrix},$$

where the row indices are $x_1^2x_2, x_1x_2^2, x_2^2x_3, \ldots$ and the column indices are x_1x_2, x_2x_3, x_1x_3 in this exact order.

For later use, we are interested in minors of M_s. To get the flavour of the question, let us look at the 3-minors of the above matrix. One has to pick exactly one of rows 1 and 2; similarly for the two following pairs of rows. Every 3-minor is a cubic monomial in ν_1, ν_2, ν_3 (let us neglect the sign right now). Since each ν_i occurs just twice in the matrix, it is plain that no minor can be ν_i^3. It is almost as easy as this to see that all other cubic monomials do occur. We want to see what happens for general s. The case $s = 1$ is trivial and the case $s = 2$ is clear: the maximal minors of the 2×1-matrix M_2 are just ν_1 and ν_2. For the generalization we need some notation and some combinatorial arguments.

Let $\mathcal{D}$ denote the set of all doubletons in I, so $\#\mathcal{D} = s(s-1)/2$. Picking a nonsingular square submatrix M of M_s of maximal size (which is $s(s-1)/2 \times s(s-1)/2$) amounts to the following: For each $D = \{i, j\} \in \mathcal{D}$, select either i or j. In other words, select either the row labeled $x_i^2x_j$ or the row labeled $x_ix_j^2$. This contributes a factor of either ν_i or ν_j towards the determinant of M (recall that we are ignoring all signs). The question is which monomials of degree $s(s-1)/2$ in $\nu_1, \ldots, \nu_s$ will arise in this way. Let us formalize this. A *selector* or *selection map* is a map $\varphi : \mathcal{D} \to I$ such that $\varphi(D)$ is an element of the doubleton D, for all $D \in \mathcal{D}$. Every selector corresponds to just one complete choice of $s(s-1)/2$ rows among all rows of M_s as just described. The monomial $\nu(\varphi)$ *attached to* φ is defined to be $\prod_{D \in \mathcal{D}} \nu_{\varphi(D)}$. This is up to sign the minor (determinant of the submatrix) arising from the selector φ. We can write $\nu(\varphi) = \prod_i \nu_i^{e_i(\varphi)}$; this defines an s-vector $e(\varphi) = (e_1(\varphi), \ldots, e_s(\varphi))$. We are now going to describe a condition on s-vectors of non-negative integers which will be easily seen to hold for all vectors $e(\varphi)$ coming from selectors; the point will be to show that this condition on a vector e conversely implies that e comes from a selector. We will assume for the moment that $e_1 + \ldots + e_s = s(s-1)/2$. This certainly holds for $e = e(\varphi)$.

Let $e = (e_1, \ldots, e_s) \in \mathbb{N}^s$. We define a reference vector $r = (s-1, s-2, \ldots, 1, 0)$. For each s-vector e let $\Sigma e = (e_1, e_1 + e_2, e_1 + e_2 + e_3, \ldots)$. Then $\Sigma r = (s-1, 2s-3, 3s-6, \ldots, s(s-1)/2, s(s-1)/2)$. A vector e will be called *admissible,* if $\Sigma e \leq \Sigma r$ (the relation $\leq$ being understood in every component).

Example $s = 3$: here $\Sigma r = (2, 3, 3)$. Then $\Sigma e \leq \Sigma r$ just means $e_1 \leq 2$, since we are assuming $e_1 + e_2 + e_3 = 3$. Can this now be the precise criterion for $\nu^e = \nu_1^{e_1}\nu_2^{e_2}\nu_3^{e_3}$ to occur as a 3-minor of M_3? Obviously not, since the condition is not symmetric in the indices. (Or differently put: $e = (0, 3, 0)$ satisfies the criterion but ν_2^3 is not a minor.) Something is missing, and this has to do with the ordering of the vector. We call e *ordered* if $e_1 \geq e_2 \geq \ldots \geq e_s$, and for every e we write $\tilde{e}$ for the ordered vector arising from e by suitably permuting the entries. (The ordered vector is unique, the permutation isn't always.) Obviously, e arises from a selection map if and only if $\tilde{e}$ does, so we may restrict our attention to ordered vectors. For $s = 3$, the ordered admissible vectors are: $(2, 1, 0)$ and $(1, 1, 1)$. These are exactly the ordered vectors e such that ν^e is a minor, see above.

Lemma 1.1. *For every selector φ, the vector $e(\varphi)$ is admissible.*

Proof: Take $1 \leq i \leq s$. Then $e_1(\varphi) + \ldots + e_i(\varphi)$ is the number of doubletons D such that $\varphi(D) \leq i$. Since $\varphi(D) \in D$, this number is at most the number of doubletons which contain some j between 1 and i (inclusive). It is easy to count these doubletons: there are $s-1$ which contain 1; then there are $s-2$ doubletons containing 2, not yet counted; $s-3$ containing 3 and not yet counted, and so on. Summing from 1 to i gives exactly the i-th entry of Σr. QED

We want to prove: If e is ordered and admissible, then there exists a selector φ with $e = e(\varphi)$. Let us rephrase this in graph-theoretical terms. A selector is simply a way of turning the complete non-oriented graph on s vertices into an oriented graph: if $\varphi(\{i, j\}) = i$, let the arrow point from j to i. The vector $e(\varphi)$ is just the vector of in-degrees of the s vertices in the resulting oriented graph. Thus, we have to show: any preselected in-degree vector which is ordered and admissible can be realized by "orienting" the complete non-oriented graph on the set I. More formally:

Proposition 1.2. *With notation s and I as above, every ordered admissible vector c is of the form $e(\varphi)$ for some selection map φ.*

Proof: This is done by induction on s; $s = 1$ and $s = 2$ being clear. So fix $s \geq 3$ and let c be an ordered and admissible s-vector of nonnegative integers. Write $\Sigma r = (q_1, \ldots, q_s)$, so $q_t = ts - (t+1)t/2$ for $t = 1, \ldots, s$. We call $t \leq s$ *critical* for c if $c_1 + \ldots + c_t = q_t$ but for all $i < t$ we have $c_1 + \ldots + c_i < q_i$. (Recall: admissibility just says $c_1 + \ldots + c_i \leq q_i$ for

all i). Since $c_1 + \ldots + c_s = q_s$, there is exactly one critical index t. We call the *vector* c *critical* if its critical index is different from s.

We first treat the case of a critical vector c. So $t < s$; we have $c_1 + \ldots + c_{t-1} < q_{t-1}$ and $c_1 + \ldots + c_t = q_t$, so $c_t > q_t - q_{t-1} = s - t$. Hence $c_i > s - t$ for all $i = 1, \ldots, t$. Now we can split I into $I' = \{1, \ldots, t\}$ and $I'' = I \setminus I'$. Let $c' = (c_1 - (s-t), \ldots, c_t - (s-t))$ and $c'' = (c_{t+1}, \ldots, c_s)$. Then both c' and c'' are ordered. An easy calculation shows that c' is admissible for I' (note the reference vector for I' is $(t-1, t-2, \ldots, 0)$ and that the entries of c' are positive). The fact that t is a critical index implies, by another direct calculation, that c'' is admissible for I''. (The indexing now goes from $t+1$ to s, but the notion of admissibility stays the same: $c_{t+1} \leq (s-t) - 1$, $c_{t+2} \leq (s-t) - 1 + (s-t) - 2$, and so on.) We now find a selector φ (an orientation of the complete graph on I) as follows: on I', draw arrows so as to obtain the in-degrees given by c'; on I'', draw arrows so as to obtain c''. Finally, draw an arrow from every vertex in I'' to every vertex in I'. This raises the in-degrees in I' by $s - t$, so it turns the vector c' back into the initial segment of c, and all is well.

Next suppose c is not critical, so $t = s$. Then c_s is positive, since $c_s = 0$ would imply $c_1 + \ldots + c_{s-1} = q_{t-1}$ (note $q_{t-1} = q_t = s(s-1)/2$), and c would be critical. We now do the following modification: raise c_1 by one and lower c_s by one. Call the resulting vector c'. By assumption all the inequalities $c_1 + \ldots + c_i \leq q_i$ with $i = 1, \ldots, s-1$ are sharp (we are not concerned with $i = s$ which always yields equality). This shows that c' is still admissible, and it is again ordered.

Case distinction: (1) The new vector c' is critical. Let $t' < s$ be its critical index. Then by the first part of the proof, there exists a selector φ producing the vector c' in which there is an arrow $s \to i$ for all $i \leq t'$. We just reverse the arrow $s \to 1$, to change c' back into c.

(2) The new vector c' is not critical. Then we do a second modification: lower $c'_s = c_s$ by 1 (again), raise $c'_2 (= c_2)$ by one. Call the resulting vector c''. It is again ordered. Its critical index t'' cannot be 1, since $c''_1 = c'_1$ does not equal q_1. We again distinguish: if $t'' < s$, we realize c'' as above; since $t'' \geq 2$, we can turn c'' back into c again, by reversing the two arrows $s \to 1$, $s \to 2$. If $t'' = s$, we modify a third time (this time moving one unit from c_s to c_3), and so forth.

Finally, since c_s cannot be more than $(s-1)/2$, the process must stop after at most that many steps, so we do not run out of possibilities to do the modifications. We repeat: if $c_s = 0$ then we are done. QED

We also will have to consider *partial* selectors ψ; this is, by definition, a map from a subset $\mathcal{D}_\psi \subset \mathcal{D}$ to I, again satisfying the condition $\psi(D) \in D$ whenever $\psi(D)$ is defined. One defines $\nu(\psi)$ and $e(\psi)$ just the same way as for total selectors. So one has in symbolic exponential

notation: $\nu(\psi) = \nu^{e(\psi)}$. The proof of the following result is easy and we omit it.

Lemma 1.3. *The following two statements are equivalent for a vector $c \in \mathbb{N}^I$:*

(i) There is a partial selector ψ with $c = e(\psi)$.

(ii) There is a selector φ such that $c \leq e(\varphi)$. (In fact φ can be chosen as an extension of ψ to the whole of $\mathcal{D}$.)

In other words: The monomials $\nu(\psi)$ with ψ a partial selector are precisely the divisors of the monomials $\nu(\varphi)$ with φ a (total) selector.

The preceding results allow us to describe all minors of M_s. As already explained in the case of maximal minors, specifying a minor amounts to the following: Among each pair of row indices $(x_i x_j^2, x_i^2 x_j)$ we must select *at most* one; this amounts to marking at most one element of the doubleton $\{i, j\}$. Hence we have to specify a partial selector function ψ, and the determinant of the square matrix that arises from this selection of rows is (up to sign) exactly the monomial $\nu^{e(\psi)}$. For any matrix A over a commutative ring R and any $j \geq 0$, let $\mathrm{Min}_j(A)$ be the R-ideal generated by the minors of size j of A. By convention $\mathrm{Min}_0(A)$ is the unit ideal. Now from the preceding lemma and proposition we obtain:

Proposition 1.4. *For any $j \geq 0$, the ideal $\mathrm{Min}_j(M_s)$ is generated by all monomials $\nu(\psi)$, where ψ ranges over all partial selectors whose domain of definition $\mathcal{D}_\psi$ has j elements. Equivalently, $\mathrm{Min}_j(M_s)$ is generated by all monomials of degree j which divide some $\nu(\varphi)$ where φ is a (total) selector.*

Lemma 1.1, Prop. 1.2 and Lemma 1.3 allow us to enumerate all the relevant monomials $\nu(\psi)$ of degree j: find all ordered admissible vectors c, take all degree j divisors of the monomials ν^c, and also take all ν-monomials obtained from what we already have by permuting the ν_i. For very small values of j it is faster to proceed directly. The special case $j = s(s-1)/2$ corresponds to maximal minors. There will be a worked example near the end of this section; we defer this since the matrix M_s is actually only a block in an even larger matrix $\tilde{M}_s$, and we also need to look at minors of $\tilde{M}_s$.

We now put aside our matrices for a moment; we will come back to them very soon.

1.2. **Complexes and resolutions, and the matrix $\tilde{M}_s$.** We will consider rings of the type $\mathbb{Z}[T]/(Tf)$ with f some monic polynomial, and tensor products of finitely many of these rings. The images of T and f in $\mathbb{Z}[T]/(Tf)$ will be written τ and ν respectively. For every cyclic group $\langle\sigma\rangle$, the group ring $\mathbb{Z}[\langle\sigma\rangle]$ is of this type: if σ has order

n, then $\mathbb{Z}[\langle\sigma\rangle] = \mathbb{Z}[s]/(s^n - 1) = \mathbb{Z}[T]/((T+1)^n - 1)$, and we put $f = ((T+1)^n - 1)/T$. Here we have $\tau = \sigma - 1$ and $\nu = \mathrm{N}_\sigma = 1 + \sigma + \ldots + \sigma^{n-1}$. In the sequel we will have to deal simultaneously with s such rings $R_i = \mathbb{Z}[T]/(Tf_i)$. In fact, all R_i will be group rings of *nontrivial cyclic* p-groups $\langle\sigma_i\rangle$. We write τ_i, ν_i for the image of σ_i (resp. N_{σ_i}) in R_i. Everything we do works also over $\mathbb{Z}_p$ instead of $\mathbb{Z}$; but let us stick with $\mathbb{Z}$ now and switch to $\mathbb{Z}_p$ later.

Let us look for a moment at one ring R_i and the trivial module $\mathbb{Z} = R_i/\tau_i R_i$ over it. We then have a very well-known periodic resolution:

$$\ldots \xrightarrow{\cdot\tau_i} R_i \xrightarrow{\cdot\nu_i} R_i \xrightarrow{\cdot\tau_i} R_i \longrightarrow \mathbb{Z} \longrightarrow 0.$$

Let $C^\bullet(R_i)$ denote the complex given by this infinite exact sequence, with the term $\mathbb{Z}$ deleted; so the rightmost R_i is in degree 0.

We now take rings $R_1, \ldots, R_s$ of this type and tensor together the resolutions $C^\bullet(R_i)$, the tensor product being taken over $\mathbb{Z}$. Let us point out that in our applications, all R_i will be cyclic group rings. It is known that the resulting complex

$$C^\bullet(R_1, \ldots, R_s) := C^\bullet(R_1) \otimes \ldots \otimes C^\bullet(R_s)$$

then defines a resolution of $\mathbb{Z} \otimes \ldots \otimes \mathbb{Z} = \mathbb{Z}$ over the tensor product of rings $R := R_1 \otimes \ldots \otimes R_s$. The main technical problem in working with this complex will be to manage the indices that occur when describing the terms of degree 1, 2 and 3. The degree 0 term of the complex is easy: this is just R. Note that R can be identified with the group ring $\mathbb{Z}[\Gamma]$ where Γ is defined to be $G_1 \times \ldots \times G_s$ and G_i is the cyclic p-group generated by σ_i. (Note: The letter Γ without subscript will never denote a Galois group isomorphic to $\mathbb{Z}_p$ in this paper.)

To continue, we need to set up more notation. Let M_i^q denote the degree q term of the complex $C^\bullet(R_i)$. For any multidegree $e = (e_1, \ldots, e_s)$ let $M^e = M_1^{e_1} \otimes \ldots \otimes M_s^{e_s}$. All these modules are free of rank one over R, with a canonical basis element that we call b_e. The weight $|e|$ of the multidegree e is just the sum $e_1 + \ldots + e_s$. Then we have

$$C^q(R_1, \ldots, R_s) = \bigoplus_{|e|=q} M^e.$$

The set of multidegrees e with weight q can also be identified with the set of degree q monomials in the variables $x_1, \ldots, x_s$.

We will mostly be concerned with Ω^2, which is defined as the cokernel of $C^3(R_1, \ldots, R_s) \to C^2(R_1, \ldots, R_s)$. So we have the four-term sequence

$$0 \to \Omega^2 \to C^1(R_1, \ldots, R_s) \to C^0(R_1, \ldots, R_s) \to \mathbb{Z} \to 0,$$

where the two modules in the middle are R-free of ranks s and 1 respectively. Quite generally, the R-rank of $C^q(R_1, \ldots, R_s)$ is $\binom{s+q-1}{q}$; for $q = 2$ this gives $s(s+1)/2$ and for $q = 3$ this gives $s(s+1)(s+2)/6$.

We repeat that the canonical basis for the degree q term is indexed by the degree q monomials in $x_1, \ldots, x_s$; however, these monomials are a mere bookkeeping device.

The main point is to calculate the differentials. Let ∂ for short be the differential in $C^\bullet(R_1, \ldots, R_s)$ from degree 3 to degree 2. Then ∂ is given by a matrix $\tilde{M}_s$ whose rows (columns) are indexed by the cubic (respectively quadratic) monomials in the x_i. If y is a cubic monomial and z a quadratic monomial, the (y, z)-entry is determined as follows:

— if z does not divide y, the entry is zero;

— if z divides y, then $y/z = x_i$ for exactly one i, and we declare the entry to be $\pm\tau_i$ if the degree of x_i in y is odd, and $\pm\nu_i$ if the degree of x_i in y is even. The sign is $(-1)^n$ where n is the sum of the degrees of the x_j in y with index $j < i$.

Let us describe some rows explicitly. First, take the row index x_i^3. Then plainly, the row has τ_i in position x_i^2, and zeros everywhere else. Second, take the row index $x_1x_2^2$. Then we get $-\nu_2$ in position x_1x_2 and τ_1 in position x_2^2. Third and last, take the row index $x_1x_2x_3$. Then we have τ_1 in position x_2x_3, $-\tau_2$ in position x_1x_3 and τ_3 in position x_1x_2.

In full generality the matrix $\tilde{M}_s$ can be written as a block matrix

$$\begin{pmatrix} A & 0 \\ B & M_s \\ 0 & C \end{pmatrix}$$

according to the following subdivision of indices: For the rows, first come the pure cubes x_i^3; then the cubic monomials involving exactly two of the x_i; and finally the products of three different x_i. For the columns, we first have the pure cubes x_i^2, and then the products x_ix_j with $i < j$. Please note at this point that the matrix written M_s here does coincide (up to some minus signs which were neglected previously) with the matrix given that name in the previous subsection.

The matrix A is diagonal of format $s \times s$ with entries τ_i. The matrix B is of format $s(s-1) \times s$; each of its rows has exactly one entry, and it is always of the form $\pm\tau_i$. The matrix C is less easily described. Let us just say that for $s = 3$ we already calculated it a few paragraphs ago: it is (with appropriate indexing) the row $(\tau_3\ \tau_1\ -\tau_2)$. Let us, for the sake of clarity, write down the entire matrix $\tilde{M}_s$ for $s = 3$, with

indices written out in the leftmost column and the top row:

	x_1^2	x_2^2	x_3^2	x_1x_2	x_2x_3	x_1x_3
x_1^3	τ_1					
x_2^3		τ_2				
x_3^3			τ_3			
$x_1^2x_2$	τ_2			ν_1		
$x_1x_2^2$		τ_1		$-\nu_2$		
$x_2^2x_3$		τ_3			ν_2	
$x_2x_3^2$			τ_2		$-\nu_3$	
$x_1^2x_3$	τ_3					ν_1
$x_1x_3^2$			τ_1			$-\nu_3$
$x_1x_2x_3$				τ_3	τ_1	$-\tau_2$

Let us now go back to the general case. In the compound matrix $\binom{A}{B}$, every column contains each τ_i (there happen to be no minus signs) exactly once, and the other entries are zero. This implies: Every monomial of degree s in $\tau_1, \dots, \tau_s$ arises as an s-minor of $\binom{A}{B}$.

Let us introduce a little ad-hoc terminology. A ν-monomial is a product of terms ν_i, and a τ-monomial is a product of terms τ_i. Every monomial is uniquely a product of a ν-monomial (its ν-part, we will say) and a τ-monomial.

In Prop. 1.4 we already computed the minors of M_s in terms of selector functions: Every minor is of the form (plus or minus) $\nu^{e(\psi)}$ for a partial selection function ψ. It is easy to see that the same holds for the ν-part of any monomial that occurs as a summand of a minor of the entire matrix $\tilde{M}_s$. A ν-monomial will be called *admissible* if it is of the form $\nu(\psi)$ with a partial selector ψ.

The R-Fitting ideal of Ω^2 is generated by the maximal minors of $\tilde{M}_s$. We can say a little about this ideal without calculating it exactly. Let $J \subset R$ be generated by all τ_i and all ν_i. We can then say at once that $\mathrm{Fit}_R(\Omega^2) \subset J^{s(s+1)/2}$.

Any minor of $\tilde{M}_s$ is a sum of (signed) monomials of the same degree. As seen above, the ν-part of any such monomial is admissible. Let H denote the ideal generated by $\tau_1, \dots, \tau_s$, let $\mathfrak{n}_j$ be the ideal generated by all admissible ν-monomials of degree j, and let $H^{(j)}$ be the ideal generated by all square-free monomials in the τ_i of degree j. (Note that $H^{(j)} = 0$ for $j > s$. Note also that the notation H^j will mean the usual j-th power of the ideal H.) We put $c = s(s+1)/2$ and look at the t-minors of $\tilde{M}_s$ for $t = c, c-1, \dots, 0$.

Proposition 1.5. *(a) For $c \geq t > s(s-1)/2 + 1$ the ideal $\mathrm{Min}_t(\tilde{M}_s)$ is zero.*

(b) For $s(s-1)/2+1 \geq t \geq 0$ we have inclusions

$$\sum_{d=0}^{t} H^{(t-d)}\mathfrak{n}_d \subset \mathrm{Min}_t(\tilde{M}_s) \subset \sum_{d=0}^{t} H^{t-d}\mathfrak{n}_d.$$

PROOF: (a) The ideal $\mathrm{Min}_t(\tilde{M}_s)$ is the $c-t$-th Fitting ideal of Ω^2. This latter module has locally everywhere rank at least $s-1$, as is clear from the four-term sequence defining it. Hence the Fitting ideals with indices $0, 1, \ldots, s-2$ are all zero, and $c-t \leq s-2$ is equivalent to $t > s(s-1)/2+1$.

(b) Let us look at a minor of $\tilde{M}_s$. As a determinant it is a sum of signed monomials x, each of degree t. We already mentioned that the ν-part x_ν of every such monomial x must be admissible. Let d be its degree; then $x = x_\tau x_\nu$ where x_τ is a τ-monomial of complementary degree $t-d$. This proves the second inclusion.

We now show the first inclusion. Given d so that $t-d \leq s$ and any square-free τ-monomial y of degree $t-d$, we can realise y as a $(t-d)$-minor of the square matrix A. Any $z \in \mathfrak{n}_d$ can be realised as a d-minor of M_s. Hence we can obtain yz as a t-minor of $\tilde{M}_s$. QED

Remark: We conjecture that the second inclusion in this proposition is actually an equality.

Starting from now, we replace the base ring $\mathbb{Z}$ by $\mathbb{Z}_p$ consistently. Also, we take $\Gamma = G_1 \times \ldots \times G_s$ which is a product of s cyclic nontrivial p-groups, R now means $\mathbb{Z}_p[\Gamma]$ instead of $\mathbb{Z}[\Gamma]$ and we make R and Ω^2 into modules over $\Lambda[\Gamma]$ with $\Lambda = \mathbb{Z}_p[[T]]$, just by letting T act trivially. We are interested in the ideal

$$\mathfrak{A} := \mathrm{Fit}_{\Lambda[\Gamma]}(\Omega^2).$$

We get a set of defining relations for Ω^2 over $\Lambda[\Gamma]$ by taking the defining relations over R, and adjoining a relation $Tb = 0$ for each generator b. From this we get the formula

$$\mathfrak{A} = \mathrm{Fit}^0_R(\Omega^2) + T \cdot \mathrm{Fit}^1_R(\Omega^2) + T^2 \cdot \mathrm{Fit}^2_R(\Omega^2) + \ldots$$

where $\mathrm{Fit}^i_R(\Omega^2)$ means the i-th higher Fitting ideal of Ω^2. Of course we have $\mathrm{Fit}^t_R(\Omega^2) = \mathrm{Min}_{c-t}(\tilde{M}_s)$ for all t, where we recall that $c = s(s+1)/2$. For simplicity let us abbreviate $\mathrm{Min}_t(\tilde{M}_s)$ by $\mathfrak{m}_t$. (Note that this hides the dependence on s!) We already have shown that $\mathfrak{m}_t = 0$ for $t > s(s-1)/2+1 = c-s+1$. Summing up, we have obtained:

Proposition 1.6.

$$\mathfrak{A} = \left\langle T^{s-1}\mathfrak{m}_{c-s+1}, T^s\mathfrak{m}_{c-s}, \ldots, T^{c-1}\mathfrak{m}_1, T^c\mathfrak{m}_0 \right\rangle_{\Lambda[\Gamma]}.$$

The terms $\mathfrak{m}_t = \mathrm{Min}_t(\tilde{M}_s)$ were to some extent determined in Proposition 1.5. Let us look at the case $s = 3$ in some detail. As said in loc.cit., $\mathfrak{m}_t = 0$ for $t = 6$ and $t = 5$. Before continuing we discuss what the admissible ν-monomials are. In degree 0, 1 and 2, all ν-monomials are admissible. In degree 3, a ν-monomial is admissible iff it is not a pure cube ν_i^3. (Reason: The ordered vectors $(2,1,0)$ and $(1,1,1)$ are admissible, but $(3,0,0)$ is not.) It can now be checked by hand that the right-hand inclusion in Prop. 1.5. *is an equality for* $s = 3$ (see comment below). This gives the following results: $\mathfrak{m}_0 = (1)$, $\mathfrak{m}_1 = J$, and:

- $\mathfrak{m}_2 = J^2$.
- $\mathfrak{m}_3$ is generated by all degree 3 monomials in $\tau_1, \tau_2, \tau_3, \nu_1, \nu_2, \nu_3$, *except* the pure cubic monomials ν_i^3, $i = 1, 2, 3$.
- $\mathfrak{m}_4$ is generated by all degree 4 monomials in $\tau_1, \tau_2, \tau_3, \nu_1, \nu_2, \nu_3$, except monomials consisting of ν-terms only, and monomials that are divisible by some ν_i^3.

Comment: (a) Take $s = 3$ (as before) and $t = 4$. Then the left-hand inclusion in Prop. 1.5 gives us $\tau_1\tau_2\nu_3^2 \in \mathfrak{m}_4$ but not $\tau_1^2\nu_3^2 \in \mathfrak{m}_4$; to see that this holds true too, one needs to have a direct look at the matrix. (Take rows 1,5,7,9 and columns 1,2,5,6.) It is not clear how to proceed for general s.

(b) For $s = 4$, a ν-monomial is admissible iff no variable ν_i has more than degree 3 in it, and the joint degree of any two variables never exceeds 5. We have verified that the right-hand inclusion of Prop. 1.5 *is an equality for* $s = 4$ *as well.* A more elegant argument that works *for all* s would be preferable, but is not in sight.

As the reader can see, our determination of $\mathfrak{A}$ is not quite complete, at least for $s \geq 5$. But the following information is very useful. Let $\varepsilon : \Lambda[\Gamma] \to \Lambda$ be the augmentation map. Then we obtain:

Proposition 1.7.

$$\varepsilon(\mathfrak{A}) \subset p^{s(s-1)/2}T^s\Lambda + p^{s(s-1)/2-1}T^{s+1}\Lambda + \ldots + T^{s(s+1)/2}\Lambda,$$

with equality if Γ *is of exponent* p *(in other words, elementary* p*-abelian).*

Proof: We apply ε to the right hand side in Prop. 1.6. Generally $\varepsilon(\mathfrak{m}_t)$ is contained in $p^t\Lambda$, since all τ-terms vanish under augmentation, and all ν-terms go to multiples of p. On the other hand it is an easy exercise to see that $\varepsilon(\mathfrak{n}_t) = p^t\Lambda$ if G has exponent p. Now every monomial generating $\mathfrak{m}_{c-s+1}$ has at least one τ-factor, so disappears under augmentation. Taking all this together, we obtain our result. QED

1.3. **More general groups.** We have explained the Fitting ideal of a certain module Ω^2 over the group ring $R = \mathbb{Z}_p[\Gamma]$ (where $\Gamma = G_1 \times \ldots \times G_s$ is a product of s cyclic nontrivial p-groups), and over $\Lambda[\Gamma]$, in terms of matrices and minors. Recall that Ω^2 occurs in a four-term sequence

$$0 \to \Omega^2 \to R^s \to R \to \mathbb{Z}_p \to 0. \tag{1}$$

This is in fact a minimal projective 2-step resolution of $\mathbb{Z}_p$: the map $R \to \mathbb{Z}_p$ is augmentation, and its kernel requires s generators. This information already determines Ω^2 up to R-isomorphism.

For later use, we need to allow somewhat more general groups. This will require more and partly different notation, which we are going to introduce now. In our arithmetical applications, Γ will always be the p-part $G_{(p)}$ of an abelian group G, which is a Galois group $\mathrm{Gal}(L/k)$. We will have $G = G_{(p)} \times \Delta$ with a group Δ whose order is prime to p, and if we put $G^+ = \mathrm{Gal}(L^+/k)$ we similarly get $G^+ = G_{(p)} \times \Delta^+$ (with the same group $G_{(p)}$). Since we need several versions of Ω^2, the Ω^2 in sequence (1) will be consistently written $\Omega^2_{G_{(p)}}$ from now on, and we will also write $\mathfrak{A}_{G_{(p)}}$ instead of $\mathfrak{A}$.

Since the kernel of augmentation $\mathbb{Z}_p[G^+] \to \mathbb{Z}_p$ is again minimally generated by s elements, there exists a projective 2-step resolution of quite similar shape, with $G_{(p)}$ replaced by G^+:

$$0 \to \Omega^2_{G^+} \to \mathbb{Z}_p[G^+]^s \to \mathbb{Z}_p[G^+] \to \mathbb{Z}_p \to 0. \tag{2}$$

If we take χ_0-parts of this, where χ_0 is the trivial character of Δ, then we get back the previous sequence (1). If we take χ-parts for any nontrivial character of Δ, then $(\mathbb{Z}_p)_\chi$ vanishes and we obtain that $(\Omega^2_{G^+})_\chi = \mathbb{Z}_p[G^+]^{s-1}_\chi$.

Now we again consider all modules in the 4-sequence (2) as Λ-modules, with $T \in \Lambda$ operating as zero. We define an ideal of $\Lambda[G^+]$ by

$$\mathfrak{A}_{G^+} := \mathrm{Fit}_{\Lambda[G^+]}(\Omega^2_{G^+}).$$

Then we have the following relations:

$$(\mathfrak{A}_{G^+})_{\chi_0} = \mathfrak{A}_{G_{(p)}};$$

$$(\mathfrak{A}_{G^+})_\chi = (T^{s-1}) \text{ for all nontrivial characters } \chi \text{ of } \Delta.$$

The reader already sees that the main difficulty and interest is in the χ_0-part; we include the other χ-parts only to get a more rounded-off result in the arithmetical setting.

2. Multiplicativity of Fitting ideals

In this section, which is again preparatory to the arithmetic matters proper, R is an arbitrary commutative ring. (So the use of the letter R in this section is not the same as in §1.) All modules will be finitely

generated; by an R-torsion module we will always understand an R-module annihilated by some nonzero-divisor in R.

The following is well known (for the local case see e.g. Lemma 3 of [CG]): if $0 \to A \to B \to C \to 0$ is a short exact sequence of modules over R and C is an R-torsion-module of projective dimension at most 1 (equivalently, C can be written as the quotient of a projective R-module by a projective submodule of the same rank), then $\mathrm{Fit}_R(B) = \mathrm{Fit}_R(A)\,\mathrm{Fit}_R(C)$. We will use this later; but this property will not suffice, since we will also encounter cases where it is A instead of C which has $pd = 1$. Over some rings R one can use duality (see [GK]) to show that multiplicativity of Fitting ideals holds in that situation as well, for instance $R = \Lambda[G]$ with G cyclic, and all modules finitely generated free over $\mathbb{Z}_p$. But again, this is not enough for us. In fact we will not be able to show multiplicativity of the Fitting ideal in s.e.s. with front term having $pd \leq 1$ in general, but only in a special situation which is fortunately sufficient for us.

Let P be a torsion module of $pd \leq 1$ over R, which we assume semilocal and connected, for simplicity. (The case $pd_R(P) = 0$ will only occur if $P = 0$ in later applications, so for the time being one should think of P as having $pd = 1$.) Then P can be written as the cokernel of an injective R-linear endomorphism of some free module R^n. We think of this endomorphism as given by a square matrix A whose determinant is a nonzero-divisor. Now let u be a variable. The *canonical u-extension* $P(u)$ of P is defined as the cokernel of the matrix uA on $R[u]^n$. There is a short exact sequence

$$0 \to R[u]^n/uR[u]^n \to P(u) \to R[u] \otimes_R P \to 0,$$

where the map $P(u) \to R[u] \otimes_R P$ is canonical (stemming from identity on $R[u]^n$), and the former map is induced by multiplication with the matrix A. Exactness of the sequence is easy to check, using the injectivity of multiplication by A. At least if we fix the number n, this extension (up to isomorphism) only depends on P, not on the choice of the matrix A. For instance if R is local, one can take n equal to the minimal number of generators of P, and then $P(u)$ is really unique in a strong sense. But these uniqueness questions are not important for us.

We now consider an R-submodule $X \subset P$ and we construct the pullback $X(u)$ as follows:

$$\begin{array}{ccccc} 0 & \longrightarrow & R[u]^n/uR[u]^n & \xrightarrow{=} & R[u]^n/uR[u]^n \\ & & \downarrow & & \downarrow \\ 0 & \longrightarrow & X(u) & \longrightarrow & P(u) \\ & & \downarrow & & \downarrow \\ 0 & \longrightarrow & R[u] \otimes_R X & \longrightarrow & R[u] \otimes_R P. \end{array}$$

All horizontal maps are injective, and all columns are short exact sequences. Note that in the rightmost column all modules have $pd \leq 1$ over $R[u]$, whereas in the middle column we only know this about the top module. Nevertheless we have:

Lemma 2.1. *With the above notation, we have*

$$\mathrm{Fit}_{R[u]}(X(u)) = \mathrm{Fit}_{R[u]}(R[u] \otimes_R X)\, \mathrm{Fit}_{R[u]}(R[u]^n/uR[u]^n).$$

Of course the first factor on the right is $\mathrm{Fit}_R(X)R[u]$*, and the second factor is* $u^n R[u]$*.*

Proof: We first remark that by a general property of Fitting ideals in short exact sequences, the right hand side is always contained in the left hand side. So we only have to show the inclusion from left to right.

Let M be a relation matrix for X over R, stemming from a set of generators $x_1, \ldots, x_r$ of X. Each row in M represents a relation, so M has r columns. Of course M is also a relation matrix for $R[u] \otimes_R X =: X[u]$ over $R[u]$. Let $e_1, \ldots, e_n$ be the obvious system of generators of $R[u]^n/uR[u]^n$ coming from the standard basis. Then the corresponding relation matrix for $R[u]^n/uR[u]^n$ over $R[u]$ is just u times I_n, the $n \times n$ unit matrix. The module $X(u)$ consists of all pairs $(x, q) \in X[u] \times P(u)$ having the same image in $R[u] \otimes_R P =: P[u]$. Let e_i' be the image of e_i in $P(u)$; then e_i' goes to zero in $P[u]$, so $(0, e_i') \in X(u)$. We also lift every generator $x_j \in X$ to some pair $(x_j, d_j) \in X(u)$. It is easy to see that $e_1', \ldots, e_n', x_1, \ldots, x_r$ is a system of generators of $X(u)$, and the corresponding relation matrix has the form

$$\begin{pmatrix} uI_n & 0 \\ B & M \end{pmatrix},$$

for some matrix B over $R[u]$. The Fitting ideal of $X(u)$ is generated by all $n + r$-minors of this matrix, and in calculating this, we may first apply elementary row operations to the matrix as we please. The entries u in the first n rows are very convenient: we can use them to reduce every entry of B to an element of R. (Write $B = (b_{ij})$ and $b_{ij} = c_{ij} + ud$ with $c_{ij} \in R$; subtract d times the j-th row of the total matrix from the $n + i$-th row of the total matrix. This eliminates the

term ud.) So we may suppose that B has all entries in R; we also recall that M has entries in R.

Now let $t \in R$ be a nonzero-divisor such that $tX = 0$. We base-change all our modules from R to $R[1/t]$. Then X becomes 0, and

$$\mathrm{Fit}_{R[1/t][u]}(X(u)[1/t]) = (u^n).$$

Hence the $R[u]$-ideal $\mathrm{Fit}_{R[u]}(X(u))$ is a subset of $u^n R[1/t][u]$. Recall that we have to show that the latter Fitting ideal lies in $u^n \mathrm{Fit}_R(X)R[u]$.

Let us discuss the minors that generate the Fitting ideal. They arise from picking a rows of the upper region $(uI_n \;\; 0)$ of the matrix, and $n+r-a$ rows of its lower region $(B \;\; M)$, and taking the determinant of the resulting matrix. If $a = n$, then the determinant that we get is simply u^n times some r-minor of M, and this is indeed in $u^n \mathrm{Fit}_R(X)$. So suppose $a < n$. Then the resulting determinant has the form $u^a\rho$, where ρ is an element of R. So by the previous paragraph this determinant is in the set

$$u^a R \cap u^n R[1/t][u].$$

By comparing coefficients of polynomials in the variable u and recalling that $R \to R[1/t]$ is injective, we see that this intersection only contains the zero element. So all minors with $a < n$ are zero. This shows the desired inclusion. QED

In the next step we eliminate the formal variable u. Let g be any nonzero-divisor of R. The base change from $R[u]$-modules to R-modules induced by $u \mapsto g$ will just be written with a superscript $(\dots)^{u=g}$ during the following argument. For any R-module N, the module $(R[u] \otimes_R N)^{u=g}$ identifies canonically with N itself.

It is clear from the construction that $P(u)^{u=g}$ has a description quite analogous to that of $P(u)$: $P(u)^{u=g}$ is the cokernel of the injective map $R^n \to R^n$ given by multiplication by gA. There is a similar s.e.s. $0 \to R^n/gR^n \to P(u)^{u=g} \to P \to 0$. Given this, we will write $P(g)$ for $P(u)^{u=g}$, hoping that the two constructions, the one involving the polynomial ring $R[u]$, the other performed over R, will not be confused; and we will call $P(g)$ a *canonical g-extension* of P.

We apply the downward basechange $()^{u=g}$ to the entire pullback diagram above; $X(g)$ will stand for $X(u)^{u=g}$. We obtain:

$$\begin{array}{ccccc}
0 & \longrightarrow & R^n/gR^n & \longrightarrow & R^n/gR^n \\
 & & \downarrow & & \downarrow \\
? & \longrightarrow & X(g) & \longrightarrow & P(g) \\
 & & \downarrow & & \downarrow \\
0 & \longrightarrow & X & \longrightarrow & P.
\end{array}$$

The upper righthand vertical map is monic; actually the right hand column is a s.e.s. that was mentioned a few lines ago. The top horizontal map is an equality. Therefore the upper lefthand map is monic as well. Hence the middle column is also a short exact sequence. This shows that the middle horizontal map is monic (we can replace the question mark by 0), and that the lower square is a pullback. Since Fitting ideals commute with base change, we know that $\mathrm{Fit}_R(X(g)) = g^n \mathrm{Fit}_R(X)$. We formulate what we have proved, recapitulating most hypotheses.

Proposition 2.2. *Let R be a semilocal commutative ring, P a torsion module of $pd \leq 1$ over R, $X \subset P$ a submodule, and $g \in R$ a nonzerodivisor. Let $P(g)$ be a canonical g-extension of P. (This involves the choice of a presentation of P.) Finally, let $X(g)$ be the pullback of X and $P(g)$ over P. Then*

$$\mathrm{Fit}_R(X(g)) = \mathrm{Fit}_R(R^n/gR^n) \cdot \mathrm{Fit}_R(X) = g^n \mathrm{Fit}_R(X).$$

We now show that this result continues to hold for a somewhat wider class of extensions.

Proposition 2.3. *Take any short exact sequence of torsion R-modules*

$$0 \to Q \to \tilde{P} \to P \to 0$$

in which $\tilde{P}$ and P have projective dimension at most one over R, and let X be any R-submodule of P. Define $\tilde{X}$ to be the pullback of X and $\tilde{P}$ over P, so there is another s.e.s.

$$0 \to Q \to \tilde{X} \to X \to 0.$$

Then

$$\mathrm{Fit}_R(\tilde{X}) = \mathrm{Fit}_R(Q) \mathrm{Fit}_R(X).$$

Proof: Since Fitting ideals commute with localization, we may and will assume that R is local. We may therefore suppose that there are free rank n submodules $\tilde{F} \subset F \subset R^n$ such that $P = R^n/F$ and $\tilde{P} = R^n/\tilde{F}$, the map $\tilde{P} \to P$ being the canonical one. Let A be a square matrix that expresses a basis of F in terms of the standard basis of R^n, and let B be a matrix that expresses a basis of $\tilde{F}$ in terms of a basis of F. Then P is the cokernel of A, and $\tilde{P}$ is the cokernel of AB. The determinants of A and B are nonzerodivisors; write $g = \det(B)$. Then $gI_n = BB'$ where B' is the adjoint matrix of B.

Let P' be the cokernel of $gA = ABB'$. Then there are surjections $P' \to \tilde{P} \to P$ of torsion modules having $pd \leq 1$. Moreover P' is a canonical g-extension of P. Recall $\tilde{X}$ is the pullback of X along $\tilde{P} \to P$ and let X' be the pullback of X along $P' \to P$. Then $X' \to \tilde{X}$ is onto with kernel isomorphic to $\ker(P' \to \tilde{P})$. The Fitting ideal of the latter module is principal and generated by $\det(B')$. Similarly, the surjection $\tilde{X} \to X$ has kernel $\ker(\tilde{P} \to P) = Q$, and the Fitting ideal

of this is principal generated by $\det(B)$. Finally, the kernel of $X' \to X$ is $\ker(P' \to P)$, whose Fitting ideal is generated by $\det(BB') = \det(gI_n) = g^n$. Thus:

$$\mathrm{Fit}_R(X') \supset \det(B')\,\mathrm{Fit}_R(\tilde{X}).$$

By the general inclusion formula for Fitting ideals in s.e.s., the right hand side contains $\det(B)\det(B')\,\mathrm{Fit}_R(X)$. By Prop. 2.2, the left hand side equals $\det(B)\det(B')\,\mathrm{Fit}_R(X)$. We thus obtain

$$\det(B)\det(B')\,\mathrm{Fit}_R(X) \supset \det(B')\,\mathrm{Fit}_R(\tilde{X}) \supset \det(B)\det(B')\,\mathrm{Fit}_R(X).$$

We see that both inclusions are equalities. Since $\det(B')$ is a nonzero-divisor, we can simplify by it in the first equality, and we obtain the desired result (recall $Q = \ker(\tilde{P} \to P)$). QED

These results will be applied for the ring $R = \Lambda[G_{(p)}]$, where $G_{(p)}$ is the p-part of a finite abelian group G.

3. Arithmetical modules

The field-theoretical setup will be as follows: $p > 2$, k is a totally real number field, L/k is an abelian CM extension, and $\zeta_p \in L$. Let $G = \mathrm{Gal}(L/k)$ and $G^+ = \mathrm{Gal}(L^+/k)$. Then of course $G^+ = G/\langle j\rangle$, where j means complex conjugation in G. We write $G = G_{(p)} \times \Delta$, with a p-group $G_{(p)}$ and a group Δ whose order is prime to p. Note that we then also have $G^+ = G_{(p)} \times \Delta^+$, where $\Delta^+ = \Delta/\langle j\rangle$. We also make the simplifying assumption that k_∞ and L are linearly disjoint over k. By Λ we denote the usual Iwasawa algebra $\mathbb{Z}_p[[\mathrm{Gal}(k_\infty/k)]] \cong \mathbb{Z}_p[[T]]$.

We assume that only places above p are ramified in L/k. (This is a serious restriction.) Finally, we assume $\mu = 0$ throughout.

We are interested in the "dual" Iwasawa module $A_{L_\infty}^\vee$, where $L_\infty = \bigcup_n L_n$ is the cyclotomic p-Iwasawa tower over L and $A_{L_\infty} = \varinjlim A_{L_n}$ with A_{L_n} the p-part of the minus part of the class group of L_n as usual. This module is by Kummer duality isomorphic to $X^\#(1)$, where $X = X_{S_p, L_\infty^+/k}$ is the standard Iwasawa module on the plus side, the exponent $\#$ means that the Galois group acts via inverses, and (1) is the Tate twist. More precisely, X is the Galois group of the maximal p-abelian p-ramified extension of L_∞^+. Note that the module X is identical to its plus part. So we may also consider it as a G^+-module.

Now S_p contains by assumption the set S of finite places that ramify in L^+/k, so as shown by Ritter and Weiss we can involve X in a four-term sequence of $\Lambda[G^+]$-modules with middle terms of projective dimension (pd) at most one, which is an analog of the Tate sequence at infinite level. Let us agree that all occurring modules are assumed to be finitely generated. Then the "Tate sequence at infinite level" looks as follows.

Proposition 3.1. *There is an exact sequence of $\Lambda[G^+]$-modules*

$$0 \to X \to P \to B \to \mathbb{Z}_p \to 0, \tag{1}$$

where both P and B are Λ-torsion and of projective dimension at most one over $\Lambda[G^+]$. (Note for further use that every module that has pd at most one over $\Lambda[G^+]$ automatically has pd at most one when considered as a $\Lambda[G]$-module, since the kernel of $G \to G^+$ is of order 2, hence has order prime to p.) One can actually assume that $B = \Lambda[G^+]/(T)$ and that the map $B \to \mathbb{Z}_p$ is induced by augmentation.

Proof: This is formula (3) on p.740 of [Gr1]. From that formula we also see that one may take $B = e^+\mathbb{Z}_p[G] = \Lambda[G^+]/(T)$ (the idempotent e^+ is defined as $(1+j)/2$ as usual), and the map $B = \Lambda[G^+]/(T) \to \mathbb{Z}_p$ to be the augmentation map. QED

As our next step we will modify this four-term sequence so as to make the two middle terms identical. We start with an easy technical result.

Lemma 3.2. *Let R be a commutative ring, and M be a torsion R-module of pd 1, with Fitting ideal generated by the nonzero-divisor $h \in R$. Let M be generated by n elements. Then for any nonzero-divisor $f \in R$ which is divisible by h, one can construct short exact sequences*

$$0 \to M \to (R/fR)^n \to M'' \to 0$$

and

$$0 \to M' \to (R/fR)^n \to M \to 0,$$

in which M' and M'' are again of pd ≤ 1.

Proof: This is very similar to a construction we saw in Section 2. We can write M as the cokernel of a matrix $A \in R^{n\times n}$ with determinant h. Then there is a matrix B such that $AB = fI_n$. Multiplication with B defines an injection $M \to (R/fR)^n$ with cokernel $M'' = R^n/im(B)$. Similarly, if we put $M' = R^n/im(B)$, then multiplication with A defines an injection $M' \to R^n/fR^n$ with cokernel M. (In checking injectivity one uses that the determinant of all occurring matrices is a nonzero-divisor.) QED

Now we take the exact sequence (1), assuming as we may that B has the special form $\Lambda[G^+]/(T)$. Choose an integer $n \geq 1$ such that P is n-generated, and a distinguished polynomial $f \in \Lambda$ which is a multiple of both $\mathrm{Fit}_{\Lambda[G]}(P)$ and $\mathrm{Fit}_{\Lambda[G]}(B)$. (These two Fitting ideals have generators that are nonzero-divisors in $\Lambda[G]$, with μ-invariant zero because B and X both have μ-invariant zero. Hence it is indeed possible, by taking the norm from $\Lambda[G]$ to Λ, to find a distinguished polynomial in Λ which is a common multiple of both generators.) Note that f

is divisible by T by our assumption on B. By the preceding lemma applied to $\Lambda[G^+]$, we get short exact sequences

$$0 \to B \to (\Lambda[G^+]/(f))^n \to B'' \to 0 \tag{2}$$

and

$$0 \to P' \to (\Lambda[G^+]/(f))^n \to P \to 0. \tag{3}$$

Now the s.e.s. (2) is used to modify the 4-sequence (1) on the right (pushout), and the s.e.s. (3) is used to modify the resulting 4-sequence on the left (pullback). These two processes commute with each other, and they simply reflect the functoriality of Ext^2 in both arguments. But in order to be quite clear, we visualise these modifications in a big diagram. The point is to obtain two equal terms in the middle of the bottom four-term sequence, and to know them explicitly.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & X & \longrightarrow & P & \longrightarrow & B & \longrightarrow & \mathbb{Z}_p & \longrightarrow & 0 \\
 & & \| & & \| & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & X & \longrightarrow & P & \longrightarrow & (\Lambda[G^+]/(f))^n & \longrightarrow & Z'' & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \| & & \| & & \\
0 & \longrightarrow & X' & \longrightarrow & (\Lambda[G^+]/(f))^n & \longrightarrow & (\Lambda[G^+]/(f))^n & \longrightarrow & Z'' & \longrightarrow & 0
\end{array}$$

In this diagram, the upper right-hand square is a pushout, and the lower left-hand square is a pullback. Moreover, the surjections $X' \to X$ and $(\Lambda[G^+]/(f))^n \to P$ both have kernel P', and the injections $B \to (\Lambda[G^+]/(f))^n$ and $\mathbb{Z}_p \to Z''$ both have cokernel B''.

We now go back to the general constructions of Section 1. Let s be the minimal number of generators of the p-part $G_{(p)}$ of G. We recall that there is a 4-term sequence

$$0 \to \Omega^2_{G^+} \to \mathbb{Z}_p[G^+]^s \to \mathbb{Z}_p[G^+] \to \mathbb{Z}_p \to 0. \tag{4}$$

This can also be viewed as a sequence of $\Lambda[G^+]$-modules, with T acting as zero. Note that the module $\mathbb{Z}_p[G^+]$ can be identified with B above, and also that the map $\mathbb{Z}_p[G^+] \to \mathbb{Z}_p$ is the same as above (augmentation). We now subject the four-term sequence (4) to the same modifications as the former four-term sequence (1). The outcome is (this time we only write the bottom row):

$$0 \to \tilde{\Omega} \to (\Lambda[G^+]/(f))^n \to (\Lambda[G^+]/(f))^n \to Z'' \to 0. \tag{5}$$

The module Z'' is indeed the same as before. We need to assume that n was chosen $\geq s$, which is no problem. We also need to use that T divides f. The surjection $\tilde{\Omega} \to \Omega^2_{G^+}$ has kernel Q which is of $pd \leq 1$ and whose Fitting ideal is generated by $f^n/T^s \in \Lambda[G^+]$.

The almost final step is now to invoke the theory of syzygies over the semilocal ring $\Lambda[G^+]/(f) = (\Lambda/(f))[G^+]$. We have found two second syzygies $\tilde{\Omega}$ and X' of the module Z'': the former syzygy in (5) and the latter in the bottom row of the big diagram above. Hence, by Schanuel's lemma, there are free $\Lambda[G^+]/(f)$-modules F_1, F_2 such that $\tilde{\Omega} \oplus F_1 \cong X' \oplus F_2$. In particular, the Fitting ideals of F_1 and F_2 over $\Lambda[G^+]$ are principal.

We now call two $\Lambda[G^+]$-torsion modules Y_1 and Y_2 *pf-equivalent* (in symbols $Y_1 \sim_{pf} Y_2$; pf stands for principal-Fitting) if there are nonzero-divisors $f_1, f_2 \in \Lambda[G^+]$ both having μ-invariant zero (i.e. invertible after localising at (p)) and such that $f_1 \operatorname{Fit}_{\Lambda[G^+]}(Y_1) = f_2 \operatorname{Fit}_{\Lambda[G^+]}(Y_2)$. This is indeed an equivalence relation. From the preceding paragraph we get $\tilde{\Omega} \sim_{pf} X'$.

Now from Prop. 2.3 we obtain that $\tilde{\Omega} \sim_{pf} \Omega^2_{G^+}$ and $X' \sim_{pf} X$. Taking all this together we get $X \sim_{pf} \Omega^2_{G^+}$.

Let $\Theta = \Theta_{L^+_\infty/k}$ be the Stickelberger element at infinity on the plus side. It lies in $T^{-1}\Lambda[G^+]$, and it is the mirror image of the more usual Stickelberger element on the minus side, written $\theta_{L_\infty/k}$ in [Ku3] (the projective limit of $\theta_{L_n/k}$). (We recall: Taking the mirror image means that we invert the Galois action and then take the first Tate twist. Taking the mirror image twice gives back the original object.) Now we need to use an argument (Lemma 2 in [Gr1]) that has gained some popularity. For all characters χ of G^+, let the subscript χ denote just for this proof: tensor with $\mathbb{Q}_p$ over $\mathbb{Z}_p$ and then take χ-parts. (Warning: Previously, χ denoted characters of Δ, not of G^+.) Then we know (loc.cit.): For any two principal ideals I and J of $\Lambda[G]$ with μ-invariant zero, the equality $I_\chi = J_\chi$ for all χ forces $I = J$.

Let $\mathfrak{A}_{G^+} = \operatorname{Fit}_{\Lambda[G^+]}(\Omega^2_{G^+})$. For every nontrivial character χ of G^+, the defining 4-sequence for $\Omega^2_{G^+}$ becomes

$$0 \to (\Omega^2_{G^+})_\chi \to \mathbb{Q}_p(\chi)^s \to \mathbb{Q}_p(\chi) \to 0,$$

with T acting trivially. Hence $(\mathfrak{A}_{G^+})_\chi = (T^{s-1})$. For the trivial character χ_0 of G^+, the $\mathbb{Z}_p$ term at the end does not vanish and we get

$$0 \to (\Omega^2_{G^+})_{\chi_0} \to \mathbb{Q}_p^s \to \mathbb{Q}_p \to \mathbb{Q}_p \to 0,$$

so $(\mathfrak{A}_{G^+})_{\chi_0} = (T^s)$. This particular behaviour of the trivial character is important to make all things fit together in the end.

For the final calculation, we recall that by the Main Conjecture (see [MW] for the absolutely abelian case, where by the way $\mu = 0$ is known to hold, and [Wi] for the general abelian CM case), the characteristic series of X_χ is $\chi(\Theta)$ for nontrivial χ, and $T\chi_0(\Theta)$ for $\chi = \chi_0$. Note that the characteristic series generates the Fitting ideal of X_χ over $\mathbb{Q}_p\Lambda(\chi)$.

From the pf-equivalence $X \sim_{pf} \Omega^2_{G^+}$ shown above, we know that there are two principal ideals I and J in $\Lambda[G^+]$ such that

$$I \cdot \mathfrak{A}_{G^+} = J \cdot \mathrm{Fit}_{\Lambda[G^+]}(X).$$

For nontrivial characters χ, this entails $I_\chi T^{s-1} = J_\chi \chi(\Theta)$. For the trivial character we get $I_{\chi_0} T^s = J_{\chi_0} T \chi_0(\Theta)$. Thus for *all* χ we have

$$(T^s \cdot I)_\chi = (T \cdot \Theta J)_\chi,$$

and $T\Theta$ is integral. Hence by the "popular argument" that was recalled just above, we have an equality of principal ideals

$$T^s I = T\Theta \cdot J,$$

rewritten in terms of fractional ideals: $I = T^{1-s}\Theta J$. Therefore

$$\mathrm{Fit}_{\Lambda[G^+]}(X) = IJ^{-1}\mathfrak{A}_{G^+} = T^{1-s}\mathfrak{A}_{G^+}\Theta.$$

This proves the first half of our main result. Before we state it, let us define $\mathfrak{A}_G$ to be the ideal which is $\mathfrak{A}_{G^+}$ in the plus part and the unit ideal in the minus part.

Theorem 3.3. *(a) Let L^+/k be a Galois extension of totally real number fields with Galois group G^+ which is a product of s cyclic groups of p-power order ($p > 2$ prime). Assume $\mu = 0$, L/k unramified outside p, and k_∞ linearly disjoint with L over k. Then the $\Lambda[G^+]$-Fitting ideal of the "p-ramified Iwasawa module" X (explained at the beginning of the section) is given by*

$$\mathrm{Fit}_{\Lambda[G^+]}(X) = T^{1-s}\mathfrak{A}_{G^+}\Theta,$$

where the ideal $\mathfrak{A}_{G^+}$ is defined, and in some cases determined, in Section 1.

(b) Let k be totally real and L/k be an abelian CM extension with group G such that L^+/k satisfies the hypotheses of (a), and in addition suppose that $L = L^+(\zeta_p)$. Then the $\Lambda[G]$- Fitting ideal of $A^\vee_{L_\infty}$ is given by the mirror of the ideal given in (a), which is

$$\dot{T}^{1-s}\dot{\mathfrak{A}}_{G^+}\dot{\Theta}$$

in the minus part, and the unit ideal in the plus part. The element $\dot{\Theta}$ is the usual Stickelberger element at infinity in the minus part.

Proof: There is nothing more to say about (a). Part (b) follows by noting that $A^\vee_{L_\infty}$ lives in the minus part, so the plus part of its Fitting ideal is the unit ideal and the minus part of its Fitting ideal is the mirror of the Fitting ideal of X, because of the mirror relation between X and $A^\vee_{L_\infty}$. QED

Note: In this note and the sequel, χ will again denote characters of Δ, the non-p-part of G. Taking χ-parts is again meant in the usual sense, without tensoring by $\mathbb{Q}_p$. From §1 we then know:

(i) For every nontrivial even character χ of Δ, $(\mathfrak{A}_G)_\chi = T^{s-1}$. Hence:

$$\mathrm{Fit}_{\Lambda(\chi)[G_{(p)}]}(X_\chi) = (\Theta).$$

This implies that for every odd character ψ of Δ distinct from the Teichmüller character ω, we have

$$\mathrm{Fit}_{\Lambda(\psi)[G_{(p)}]}(A_{L_\infty}^\vee)_\psi = (\dot{\Theta}).$$

(ii) For the trivial character χ_0 of Δ we have $(\mathfrak{A}_G)_{\chi_0} = \mathfrak{A}_{G_{(p)}}$ (recall $G_{(p)}$ is the p-part of G, and of G^+). Hence

$$\mathrm{Fit}_{\Lambda[G_{(p)}]}(X_{\chi_0}) = T^{1-s}\mathfrak{A}_{G_{(p)}}\Theta.$$

The ideal $\mathfrak{A}_{G_{(p)}}$ was discussed at length in §1. Its generators were described in terms of T and certain simple elements τ_i and ν_i of $\mathbb{Z}[G_{(p)}]$. As a consequence,

$$\mathrm{Fit}_{\Lambda[G_{(p)}]}(A_{L_\infty}^\vee)_\omega = \dot{T}^{1-s}\dot{\Theta}\dot{\mathfrak{A}}_{G_{(p)}}.$$

(iii) In the last formula, taking the mirror of the ideal $\mathfrak{A}_{G_{(p)}}$ only affects the terms T involved in the generators of $\mathfrak{A}$, not the terms τ_i and ν_i that come from the group $G_{(p)}$. More precisely, ν_i is its own mirror image, and τ_i is associated to its mirror image. Note in this context that $\dot{T}$ annihilates the projective limit of the roots of unity. (The Fitting ideal of that module is generated by $\dot{T}$ and all τ_i.)

Remark: If we do not make the assumption that L/K is unramified outside p, then a version of part (a) of the theorem holds, in which X is replaced by the Iwasawa module X_{S,L_∞^+}, where S is the set of finite places that ramify in L_∞^+/k. But the mirror of this is not the dualized Iwasawa module but something larger. We hope to be able to come back to this problem in the future.

To illustrate the theorem, let us repeat some information about the ideal $\mathfrak{A}$ (short for $\mathfrak{A}_{G_{(p)}}$). As shown in Prop. 1.6, we have

$$\mathfrak{A} = \mathfrak{m}_{\frac{s(s-1)}{2}+1}T^{s-1} + \mathfrak{m}_{\frac{s(s-1)}{2}}T^s + \ldots + \mathfrak{m}_1 T^{\frac{s(s+1)}{2}-1} + (T^{s(s+1)/2}),$$

where $\mathfrak{m}_t \subset \mathbb{Z}_p[G_{(p)}]$ is the ideal generated by the t-minors of a very large matrix $\tilde{M}_s$ that was given explicitly. The sequence of ideals $\mathfrak{m}_t$ is decreasing; $\mathfrak{m}_1$ is the ideal J generated by all τ_i and ν_i, and $\mathfrak{m}_0$ is the unit ideal. The ideal $\mathfrak{m}_{s(s-1)/2+1}$ is contained in the kernel of augmentation since every generating monomial has at least one τ-factor, and one can show that all other $\mathfrak{m}_i$ are of finite index in $\mathbb{Z}_p[G_{(p)}]$.

At the end of Section 1, we discussed the case $s = 3$ in detail. Let us do the cases $s = 1$ and $s = 2$ now.

Explicit description for $s = 1$:

Here $\tilde{M}_s = (\tau_1)$, a one-by-one matrix, and $\mathfrak{A} = \mathfrak{m}_1 + \mathfrak{m}_0 T$. Hence $\mathfrak{m}_1$ and $\mathfrak{m}_0$ are generated by τ_1 and 1 respectively, and we find $\mathfrak{A} = (\tau_1, T)$. Actually this shows that $\dot{\mathfrak{A}}$ is the annihilator of $\mathbb{Z}_p(1)$. From part (b) of the theorem we therefore obtain the following result:

Corollary 3.4. *If the p-part of G is cyclic, then*

$$\mathrm{Fit}_{\Lambda[G]}(A_{L_\infty}^\vee) = \mathrm{Ann}_{\Lambda[G]}(\mathbb{Z}_p(1)) \cdot \dot{\Theta}.$$

Note that this formula generalises a result of the second author: in Theorem 0.1 (2) of [Ku3], it was shown for the case that the p-part $G_{(p)}$ is (cyclic) of order p.

We now give the *explicit description for $s = 2$*; we will be more brief, just giving generators for the ideals $\mathfrak{m}_i$ and leaving the easy verifications to the reader.

- $\mathfrak{m}_2$ is generated by the monomials $\tau_1^2, \tau_1\tau_2, \tau_2^2, \tau_1\nu_2, \tau_2\nu_1$;
- $\mathfrak{m}_1$ is generated by $\tau_1, \tau_2, \nu_1, \nu_2$, in other words $\mathfrak{m}_1 = J$;
- $\mathfrak{m}_0$ is the unit ideal.

Taking into account the factor T^{1-s} in Thm. 3.3 and passing to mirror images, we get the result labeled (I) in the introduction.

We finish up by reproving another result of the second author (Theorem 0.3 in [Ku3]):

Corollary 3.5. *Assume the conditions of Thm. 3.3, and $s \geq 2$. Then $\dot{T}\dot{\Theta}$ is not in the Fitting ideal of the dualized Iwasawa module.*

Proof: It suffices of course to show that $T\Theta$ is not in the Fitting ideal $\mathrm{Fit}_{\Lambda[G^+]}(X)$. Let $\varepsilon^+ : \Lambda[G^+] \to \Lambda$ and $\varepsilon_p : \Lambda[G_{(p)}] \to \Lambda$ be the augmentation maps. Then

$$\varepsilon^+(T^{-s}\mathfrak{A}_{G^+}) = \varepsilon_p(T^{-s}\mathfrak{A}_{G_{(p)}}),$$

and we showed in Prop. 1.7 that this is a subset of

$$p^{s(s-1)/2}\Lambda + p^{s(s-1)/2-1}T\Lambda + \ldots + T^{s(s-1)/2}\Lambda.$$

Now if we had $T\Theta \in \mathrm{Fit}_{\Lambda[G^+]}(X)$, then via division by the nonzerodivisor $T\Theta$ we would obtain that 1 lies in the fractional ideal $T^{-s}\mathfrak{A}_{G^+}$. Hence 1 would also have to lie in the ideal $\varepsilon^+(T^{-s}\mathfrak{A}_{G^+}) = \varepsilon_p(T^{-s}\mathfrak{A}_{G_{(p)}})$; from the description of the latter ideal we just recalled, we see plainly that this fails to hold for $s > 1$. QED

Let us conclude by mentioning that we hope to obtain some results also in the case where some non-p-adic primes are ramified, in upcoming work. We already hinted at this in the last remark.

4. Consequences at finite level

In this section, we first prove Theorem 0.1 in the introduction. It is well-known that $H^i(L_n/L, E_{L_n})^- = H^i(L_n/L, \mu_{L_n}) = 0$ for all $i > 0$. This fact together with our assumption that there is no p-adic prime which splits in L/L^+ implies that the natural map $A_L \xrightarrow{\simeq} A_{L_n}^{\mathrm{Gal}(L_n/L)}$ is bijective. Therefore, we have an isomorphism

$$A_L \xrightarrow{\simeq} A_{L_\infty}^{\Gamma_\infty} \tag{6}$$

where $\Gamma_\infty = \mathrm{Gal}(L_\infty/L)$. By duality, the module of Γ_∞-coinvariants of $A_{L_\infty}^\vee$ is then isomorphic to $A_L^\vee$.

Let $\kappa : \Gamma_\infty \longrightarrow \mathbb{Z}_p^\times$ be the cyclotomic character. Since $\mu_{p^\infty}^{\Gamma_\infty} = \mu_{p^\infty}(L)$, we get $q = \mathrm{ord}_p(\#\mu_{p^\infty}(L)) = \mathrm{ord}_p(\kappa(\gamma) - 1)$ for a generator γ of Γ_∞. Therefore, the image of the ideal $\dot{T}^{1-s}\dot{\mathfrak{A}}_G$ under the natural homomorphism $\Lambda[G] \longrightarrow \mathbb{Z}_p[G]$ is the ideal $(\mathfrak{A}_G^0)_L$ described in the Introduction. Thus Theorem 3.3 (b) implies Theorem 0.1.

Next, in order to prove Corollaries 0.2, 0.3, 0.4, using the above isomorphism (6), we have only to compute the image of $\dot{T}^{1-s}\dot{\mathfrak{A}}_G$ under the canonical homomorphism $\pi : \Lambda[G] \longrightarrow \mathbb{Z}_p[G]$. In the case $s = 1$, by the computation before Corollary 3.4 we know that $\mathfrak{A}_{G_{(p)}} = (\tau_1, T)$. Therefore, the Teichmüller component of $\pi(\dot{\mathfrak{A}}_G)$ is $\pi(\dot{\mathfrak{A}}_{G_{(p)}}) = (\tau_1, p^q)$, and the other components are generated by 1. Therefore, $\pi(\dot{\mathfrak{A}}_G)$ is nothing but $\mathrm{Ann}_{\mathbb{Z}_p[G]}(\mu_{p^\infty}(L))$.

To prove Corollaries 0.3, 0.4, we need Theorem 5.4 below. Since Corollary 0.4 (i) is a generalization of Corollary 0.3, we have only to prove Corollary 0.4. In the following, we consider only the Teichmüller component, and work over $\Lambda[G_{(p)}]$ and $\mathbb{Z}_p[G_{(p)}]$. Let $\mathfrak{M}$, J, H be the ideals of $\Lambda[G_{(p)}]$ defined in the Appendix and used in Theorem 5.4.

Let H_T be the ideal generated by H and T. Then it is easy to check that $\pi(\dot{H}_T) = (\pi(H), p^q) = \mathrm{Ann}_{\mathbb{Z}_p[G]}(\mu_{p^\infty}(L))$. Suppose at first $q \geq a$. We have

$$\pi(\dot{\mathfrak{M}}) = (\pi(H), p^a, p^q) = (\pi(H), p^a) = \pi(\dot{J}) = I_{\omega,a}.$$

Therefore, we have $(\mathfrak{A}_G^0)_L = \pi(\dot{H}_T)\pi(\dot{J})^{s(s-1)/2} = \mathrm{Ann}_{\mathbb{Z}_p[G]}(\mu_{p^\infty}(L))I_{\omega,a}^{s(s-1)/2}$ by Theorem 5.4. If $q \leq a$, we have $\pi(\dot{\mathfrak{M}}) = (\pi(H), p^q) = \pi(\dot{H}_T) = \mathrm{Ann}_{\mathbb{Z}_p[G]}(\mu_{p^\infty}(L))$. Now Theorem 5.4 implies

$$\begin{aligned}
(\mathfrak{A}_G^0)_L &= \pi(H)(\pi(H), p^a)^{s(s-1)/2} + p^q(\pi(H), p^q)^{s(s-1)/2} \\
&= \pi(H)^{(s^2-s+2)/2} + p^q(\pi(H), p^q)^{s(s-1)/2} \\
&= (\pi(H), p^q)^{(s^2-s+2)/2} \\
&= \mathrm{Ann}_{\mathbb{Z}_p[G]}(\mu_{p^\infty}(L))^{(s^2-s+2)/2}.
\end{aligned}$$

Therefore, Theorem 0.1 implies Corollary 0.4.

Now we study the numerical example in [KM2] §2. Take $p = 3$, $k = \mathbb{Q}(\sqrt{1901})$ and $L = k(\sqrt{-3}, \alpha, \beta)$ where $\alpha^3 - 84\alpha - 191 = 0$ and $\beta^3 - 57\beta - 68 = 0$. Then $G_{(p)} = (\mathbb{Z}/p\mathbb{Z})^{\oplus 2}$, so $s = 2$. We note that A_L coincides with its ω-component since $p = 3$. We regard A_L as a $\mathbb{Z}_p[G]^- = \mathbb{Z}_p[G_{(p)}]$-module. We take generators σ_1, σ_2 of $G_{(p)} = \mathrm{Gal}(k(\alpha)/k) \times \mathrm{Gal}(k(\beta)/k) \simeq (\mathbb{Z}/p\mathbb{Z})^{\oplus 2}$ such that σ_1 is σ in [KM2] and σ_2 is τ in [KM2] (in particular, σ_1 is a generator of $\mathrm{Gal}(k(\alpha)/k)$ and σ_2 is a generator of $\mathrm{Gal}(k(\beta)/k)$). Put $\tau_i = \sigma_i - 1$ as before. Since L does not contain a primitive p^2-th root of unity, $\mathrm{Ann}_{\mathbb{Z}_p[G_{(p)}]}(\mu_{p^\infty}(L))$ coincides with the maximal ideal $\mathfrak{M} = (\tau_1, \tau_2, p)$ of $\mathbb{Z}_p[G_{(p)}]$. We regard $\theta_{L/k}$ as an element of $\mathbb{Z}_p[G_{(p)}]$. We can apply either of Corollary 0.3 or Corollary 0.4 to get

$$\mathrm{Fit}_{\mathbb{Z}_p[G_{(p)}]}(A_L^\vee) = \mathfrak{M}^2\theta_{L/k} \ .$$

On the other hand, the explicit long computation in [KM2] shows that

$$\mathrm{Fit}_{\mathbb{Z}_p[G_{(p)}]}(A_L^\vee) = (p^4, p^2\tau_1, p^2\tau_2, p\tau_1^2, p\tau_2^2, p\tau_1\tau_2)$$

(see the last line of page 425 of [KM2]). Let us check that these two descriptions agree. First of all, we use two equations on page 420, line 18 and 20, in [KM2]:

$$\begin{aligned} \tau_1\theta_{L/k} &= 8p\tau_1(1 + \tau_1\tau_2 + \tau_2^2 + \tau_1\tau_2^2); \\ \tau_2\theta_{L/k} &= 4p\tau_2(5 + p\tau_1^2 + 2\tau_1\tau_2 + 2\tau_1^2\tau_2). \end{aligned}$$

Since both $(1 + \tau_1\tau_2 + \tau_2^2 + \tau_1\tau_2^2)$ and $(5 + p\tau_1^2 + 2\tau_1\tau_2 + 2\tau_1^2\tau_2)$ are units, we have

$$\mathfrak{M}\theta_{L/k} = (\tau_1, \tau_2, p)\theta_{L/k} = (p\tau_1, p\tau_2, p\theta_{L/k}).$$

Therefore, we get

$$\begin{aligned} \mathfrak{M}^2\theta_{L/k} &= (\tau_1, \tau_2, p)(p\tau_1, p\tau_2, p\theta_{L/k}) \\ &= (p\tau_1^2, p\tau_1\tau_2, p\tau_2^2, p^2\tau_1, p^2\tau_2, p^2\theta_{L/k}). \end{aligned}$$

Thus, using the formula

$$\theta_{L/k} = 18 - 6\tau_1 - 2\tau_1^2 - 42\tau_2 - 18\tau_1\tau_2 - 14\tau_1^2\tau_2 - 14\tau_2^2 - 14\tau_1\tau_2^2 - \frac{38}{3}\tau_1^2\tau_2^2$$

on page 420 line 15 in [KM2], it is easy to check that

$$p^2\theta_{L/k} = 9\theta_{L/k} \equiv 162 = 2p^4 \mod (p^2\tau_1, p^2\tau_2, p\tau_1^2\tau_2^2).$$

This shows that

$$\mathfrak{M}^2\theta_{L/k} = (p^4, p^2\tau_1, p^2\tau_2, p\tau_1^2, p\tau_2^2, p\tau_1\tau_2),$$

and we have checked that the two descriptions do indeed agree.

Finally, we determine the Fitting ideal of a certain Galois group. Let M/L^+ be the maximal abelian pro-p extension which is unramified outside p. We note $L_\infty^+ \subset M$ and consider $\mathrm{Gal}(M/L_\infty^+)$, which is a $\mathbb{Z}_p[G^+]$-module.

Corollary 4.1. *Suppose that L^+/k is a finite abelian extension of totally real fields which is unramified outside p, and assume $\mu = 0$ for L^+. Then we have*

$$\mathrm{Fit}_{\mathbb{Z}_p[G^+]}(\mathrm{Gal}(M/L_\infty^+)) = (\mathfrak{m}_{s(s-1)/2+1} + T\mathfrak{m}_{s(s-1)/2})\Theta_{L^+},$$

where $(\mathfrak{m}_{s(s-1)/2+1} + T\mathfrak{m}_{s(s-1)/2})\Theta_{L^+}$ is the image of

$$(\mathfrak{m}_{s(s-1)/2+1} + T\mathfrak{m}_{s(s-1)/2})\Theta$$

under the canonical map $\Lambda[G^+] \longrightarrow \mathbb{Z}_p[G^+]$, and $\mathfrak{m}_{s(s-1)/2+1}$, $\mathfrak{m}_{s(s-1)/2+1}$ are the ideals of $\mathbb{Z}_p[G^+]$ defined just before Proposition 1.6 (note that the χ-components of $\mathfrak{m}_{s(s-1)/2+1}$ and $\mathfrak{m}_{s(s-1)/2+1}$ are both generated by 1 for every non-trivial character χ of Δ, and that Θ is not in $\Lambda[G^+]$, in general).

Proof: Consider the exact sequence

$$\begin{aligned} 0 \to H^1(L_\infty^+/L^+, \mathbb{Q}_p/\mathbb{Z}_p) &\to H^1(M_\infty/L^+, \mathbb{Q}_p/\mathbb{Z}_p) \\ &\to H^1(M_\infty/L_\infty^+, \mathbb{Q}_p/\mathbb{Z}_p)^{\mathrm{Gal}(L_\infty^+/L^+)} \to 0, \end{aligned}$$

where M_∞/L_∞^+ is the maximal abelian pro-p extension which is unramified outside p. We know $H^1(M_\infty/L^+, \mathbb{Q}_p/\mathbb{Z}_p) = H^1(M/L^+, \mathbb{Q}_p/\mathbb{Z}_p)$ and $H^1(M_\infty/L_\infty^+, \mathbb{Q}_p/\mathbb{Z}_p)$ is the Pontrjagin dual of X in Theorem 3.3. Taking the dual of the above exact sequence, we find that $\mathrm{Gal}(M/L_\infty^+)$ equals the module of $\mathrm{Gal}(L_\infty^+/L^+)$-coinvariants of X. Thus Theorem 3.3 implies this corollary. QED

5. Appendix: A calculation of the ideal $\mathfrak{A}$

Let us recall that $G_1, \ldots, G_s$ are nontrivial cyclic p-groups. In this appendix we make two extra assumptions:

(I) *The right-hand inclusion in Prop. 1.5 is an equality.* (True for $s \leq 4$.)

(II) *The group $\Gamma = G_1 \times \ldots \times G_s$ is homogeneous.*

(The latter is to say that the groups G_i all have the same order q. Note that all elementary abelian p-groups Γ are homogeneous.)

Under these assumptions we are able to derive a much simpler expression for $\mathfrak{A}$ (notation of §1.2). We review notation from §1: $\tau_i = \sigma_i - 1$ with $G_i = \langle \sigma_i \rangle$, and ν_i is the norm element of $\mathbb{Z}[G_i]$. All ideals are understood to be ideals of the ring $\Lambda[\Gamma]$. The ideals H and J are generated by $\tau_1, \ldots, \tau_s$ and by $\tau_1, \ldots, \tau_s, \nu_1, \ldots, \nu_s$ respectively. The ideal $\mathfrak{n}$ is spanned by all ν_i; $\mathfrak{n}_d$ is defined just prior to Prop. 1.5. Finally, $\mathfrak{m}_t$ is short for $\mathrm{Min}_t(\tilde{M}_s)$. We will need three fairly simple lemmas, building on each other.

Lemma 5.1. *Let y be a monomial of degree d in the ν_i and let y_1 be obtained from y by replacing one factor ν_i by ν_j, where $i, j \in \{1, \ldots, s\}$ are arbitrary indices. Then $y - y_1 \in H\mathfrak{n}^{d-1}$.*

PROOF: Write $y = \nu_i z$, $y_1 = \nu_j z$ with $z \in \mathfrak{n}^{d-1}$. Then $y - y_1 = (\nu_i - \nu_j)z$, and our homogeneity assumption (II) implies that $\nu_i - \nu_j$ has zero augmentation and hence is in H. QED

Lemma 5.2. *Fix some $t \leq s(s-1)/2$. Then for all $d \leq t$ we have $H^{t-d}\mathfrak{n}^d \subset \mathfrak{m}_t$.*

PROOF: Induction over d. The cases $d = 0$, $d = 1$ follow from our assumption (I) above; note that $\mathfrak{n}_1 = \mathfrak{n}^1$. Let us assume the statement holds for $d-1$ and pick a ν-monomial y of degree d. Since $t \leq s(s-1)/2$, there exists at least one degree d monomial y' in $\mathfrak{n}_d$. Then there is a chain $y_0 = y, y_1, \ldots, y_l = y'$ such that for all $h = 1, \ldots, l$, the monomial y_h is obtained from y_{h-1} by replacing one ν_i by some other ν_j, as in the statement of the previous lemma. Let $z \in H^{t-d}$ be arbitrary. Then we have the following congruences:

$$zy \equiv zy_1 \equiv \ldots \equiv zy' \mod H^{t-d+1}\mathfrak{n}^{d-1},$$

by the previous lemma. We have $zy' \in H^{t-d}\mathfrak{n}_d \subset \mathfrak{m}_t$ by Assumption (I), and $H^{t-d+1}\mathfrak{n}^{d-1} \subset \mathfrak{m}_t$ by inductive assumption. So we get $zy \in \mathfrak{m}_t$ and are done. QED

Lemma 5.3. *For $t \leq s(s-1)/2$ we have $\mathfrak{m}_t = J^t$, and $\mathfrak{m}_{s(s-1)/2+1} = HJ^{s(s-1)/2}$.*

PROOF: We begin by showing the first equality, so assume $t \leq s(s-1)/2$. The inclusion $\subset$ is obvious. On the other hand, $J^t = \sum_{d=0}^{t} H^{t-d}\mathfrak{n}^d$, and by the last lemma this right hand side is contained in $\mathfrak{m}_t$. Let us now look at the second equality. We have $\mathfrak{m}_{s(s-1)/2+1} = H \cdot \mathfrak{m}_{s(s-1)/2}$ (recall the reason: there are no admissible ν-monomials of degree $s(s-1)/2+1$). From this and the case $t = s(s-1)/2$, the second equality follows at once. QED

If we take all this together, including Assumption (I), we obtain, using again our shorthand c for $s(s+1)/2$ and $c-s$ for $s(s-1)/2$:

Theorem 5.4. *Under the assumptions (I) and (II) above, we have*

$$\begin{aligned} \mathfrak{A} &= HJ^{c-s}T^{s-1} + J^{c-s}T^s + J^{c-s-1}T^{s+1} + \ldots + JT^{c-1} + (T^c) \\ &= HJ^{c-s}T^{s-1} + T^s\mathfrak{M}^{c-s}, \end{aligned}$$

where $\mathfrak{M}$ is the ideal generated by J and T. (Note that this is the maximal ideal of $\Lambda[\Gamma]$ if all G_i are of order p.)

The result (II) given in the introduction follows from this: take Γ to be p-elementary, take the factor T^{1-s} in Thm. 3.3 into account and pass over to mirror images.

So we arrive at a much easier description of the ideal $\mathfrak{A}$ governing the algebraic structure of the Fitting ideal of the dualized Iwasawa module, if we are willing to sacrifice a little precision: at least in the elementary abelian case, $\mathfrak{A}$ *is fairly close to a high power of the maximal ideal.*

References

[CG] P. Cornacchia and C. Greither, Fitting ideals of class groups of real fields with prime power conductor, *J. Number Th.* **73** (1998), 459-471

[Gr1] C. Greither, Computing Fitting ideals of Iwasawa modules, Math. Zeitschrift **246** (2004), 733-767

[Gr2] C. Greither, Determining Fitting ideals of minus class groups via the equivariant Tamagawa number conjecture, Compositio Math. **143** (2007), 1399-1426.

[GK] C. Greither and M. Kurihara, Stickelberger elements, Fitting ideals of class groups of CM fields, and dualisation, *Math. Zeitschrift* **260** (2008), 905-930

[Ku1] M. Kurihara, Iwasawa theory and Fitting ideals, *J. reine angew. Math.* **561** (2003), 39-86

[Ku2] M. Kurihara, On the structure of ideal class groups of CM fields, *Documenta Math. Extra Vol. Kato* (2003), 539-563

[Ku3] M. Kurihara, On stronger versions of Brumer's conjecture, *Tokyo J. Math.* **34** (2011), 407-428.

[KM1] M. Kurihara and T. Miura, Stickelberger ideals and Fitting ideals of class groups for abelian number fields, Math. Annalen **350** (2011), 549-575.

[KM2] M. Kurihara and T. Miura, Ideal class groups of CM-fields with non-cyclic Galois action, *Tokyo J. Math.* **35** (2012), 411-439

[MW] B. Mazur and A. Wiles, Class fields of abelian extensions of $\mathbb{Q}$, *Invent. math.* **76** (1984), 179-330

[Wi] A. Wiles, The Iwasawa conjecture for totally real fields, *Ann. of Math.* **131** (1990), 493-540

Institut für Theoretische Informatik und Mathematik, Universität der Bundeswehr, München, 85577 Neubiberg, Germany

E-mail address: cornelius.greither@unibw.de

Department of Mathematics, Faculty of Science and Technology, Keio University, 3-14-1 Hiyoshi, Kohoku-ku, Yokohama, 223-8522, Japan

E-mail address: kurihara@math.keio.ac.jp