Fitting Ideals

Filippo Alberto Edoardo Nuccio
Mathematisches Institut der Universität Heidelberg
Im Neuenheimer Feld 266, 69120 - Heidelberg
Germany

Guwahati, September $22^{\text{nd}} - 29^{\text{th}}$

This document is a summary of two talks given at the School on Arithmetic Geometry held in Guwahati, India, from September $22^{\text{nd}} - 29^{\text{th}}$ on Fitting ideals and their applications to Wiles' proof of Iwasawa Conjecture for totally real fields as in [Wil90]. The main references for the theory of Fitting ideals are [Nor76] and the appendix of [MW84]. Nothing in this notes is new, and every fact is taken - either directly or slightly adapted - from [Nor76] or [MW84]. Observe that a ring with only one maximal ideal is called semi-local in [Nor76] and it is called local if it is noetherian with only one maximal ideal.

1 General results on Fitting ideals

By "ring" we mean a commutative ring with 1. We fix such a ring and we call it R. If M is a finitely generated R-module and $\underline{x}$ is a set of generators of M (we will assume all such sets to be *ordered*), we indicate by $|\underline{x}|$ the number of elements it contains; an element $r = (r_1, \dots, r_{|\underline{x}|}) \in R^{|\underline{x}|}$ is called a relation among the generators in $\underline{x}$ if

$$\sum_{i=1}^{|\underline{x}|} r_i x_i = 0 \in M \ .$$

Definition 1. *Let M be a finitely generated R-module and let $\underline{x}$ be a set of generators of M. A matrix X is said to be a matrix of relations for $\underline{x}$ if*

1. $X \in \mathcal{M}_{q\times|\underline{x}|}(R)$ *with* $q \geq |\underline{x}|$*;*

2. $X \cdot \underline{x} = \underline{0}$, i. e. *every row is a relation among the* x_i*'s.*

We are now ready to define the main object of our study. If X is a $n \times m$-matrix (with $n \geq m$), we define its determinantal ideal $\mathrm{DetId}(X) \subseteq R$ to be the ideal of R generated by all $m \times m$-minors of X.

Definition 2. *Let M be a finitely generated R-module. We define the R-Fitting ideal of M to be*

$$\mathrm{Fitt}_R(M) = \sum_X \mathrm{DetId}(X)$$

where X runs through all matrices of relations for all sets of generators of M.

Remark. Observe that *a priori* the sum in the definition is extended to infinitely many ideals. Moreover, we want to stress that our convention that a matrix of relations has always more rows than columns (these being as many as the generators) is crucial for the definition of the determinantal ideal. Indeed, suppose that we allow every matrix whose rows are relations among a set of generators to be a *matrix of relations* and that we define its determinantal ideal to be the ideal generated by all minors of largest possible rank. Then if $\underline{x}$ is a set of generators, let $\underline{x}' = \{x_1, x_1, x_2, \ldots, x_{|\underline{x}|}\}$ be the old set of generators with one entry doubled - say the first. Then

$$(-1, 1, 0, \ldots, 0)$$

would be a matrix of relations, and $\mathrm{DetId}(X) = R$.

The definition of Fitting ideal given above is practically useless for any application: but it may be of some use in certain proofs. Thus, before passing to concrete examples, we want to show that in the definition it would have been enough to sum over all matrices of relations of *one fixed set of generators.* Indeed we have:

Proposition 1. *Let $\underline{x}$ be a fixed, finite set of generators of the finitely generated module M. Then*

$$\mathrm{Fitt}_R(M) = \sum_X \mathrm{DetId}(X)$$

where X runs through all matrices of relations for $\underline{x}$.

Proof. Only for the proof, for every set of generators $\underline{y}$ of M, set

$$A(\underline{y}) := \sum_{Y} \mathrm{DetId}(Y)$$

for Y running, as above, through all matrices of relations for $\underline{y}$. We need to show that for every set of generators $\underline{y}$, the equality $A(\underline{x}) = A(\underline{y})$ holds: indeed, by definition, $\mathrm{Fitt}_R(M) = \sum_{\underline{y}} A(\underline{y})$ and if they all coincide this sum reduces to $A(\underline{x})$.
Let then $\underline{y}$ be any set of generators and set $\underline{xy} := \{x_1, \dots, x_{|\underline{x}|}, y_1, \dots, y_{|\underline{y}|}\}$: clearly $|\underline{xy}| = |\underline{x}| + |\underline{y}|$. Since the x_i's generate M, we can find a relation

$$c_{k1}x_1 + c_{k2}x_2 + \cdots c_{k|\underline{x}|}x_{|\underline{x}|} + y_k = 0 \ ,$$

for suitable $c_{ki} \in R$, for every $1 \leq k \leq |\underline{y}|$. Let now $X = (a_{ij})$ be any $p \times |\underline{x}|$-matrix appearing in the sum $A(\underline{x})$ and define a new matrix, having $|\underline{x}| + |\underline{y}|$ columns,

$$\widetilde{X} = \begin{pmatrix} c_{11} & \dots & c_{1|\underline{x}|} & 1 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ c_{|\underline{y}|1} & \dots & c_{|\underline{y}||\underline{x}|} & 0 & \dots & 1 \\ a_{11} & \dots & a_{1|\underline{x}|} & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{p1} & \dots & a_{p|\underline{x}|} & 0 & \dots & 0 \end{pmatrix} .$$

It is clearly a matrix of relations for $\underline{xy}$ (it has $p + |\underline{y}| \geq |\underline{x}| + |\underline{y}|$ rows) and every $|\underline{x}| \times |\underline{x}|$-minor of X also appears as $|\underline{xy}| \times |\underline{xy}|$-minor of $\widetilde{X}$, showing the inclusion $A(\underline{x}) \subseteq A(\underline{xy})$.
Let now Y be a matrix of relations for $\underline{xy}$; define a new matrix

$$\widetilde{Y} = \left(\begin{array}{cccc|c} c_{11} & c_{12} & \dots & c_{1|\underline{x}|} & \\ \vdots & \vdots & \ddots & \vdots & \mathbb{I}_{|\underline{y}|} \\ c_{|\underline{y}|1} & c_{|\underline{y}|2} & \dots & c_{|\underline{y}||\underline{x}|} & \\ \hline \multicolumn{4}{c|}{Y} & \end{array}\right)$$

where $\mathbb{I}_{|\underline{y}|}$ is the $|\underline{y}| \times |\underline{y}|$ identity matrix. Then $\mathrm{DetId}(\widetilde{Y}) \supseteq \mathrm{DetId}(Y)$ (just observe that Y and $\widetilde{Y}$ have the same number of columns and every $|\underline{xy}| \times |\underline{xy}|$-

minor of Y is also a $|\underline{xy}| \times |\underline{xy}|$-minor of $\widetilde{Y}$) and $\widetilde{Y}$ is row equivalent to

$$\widetilde{Y'} = \left(\begin{array}{cccc|c} c_{11} & c_{12} & \dots & c_{1|\underline{x}|} & \\ \vdots & \vdots & \ddots & \vdots & \mathbb{I}_{|\underline{y}|} \\ c_{|\underline{y}|1} & c_{|\underline{y}|2} & \dots & c_{|\underline{y}||\underline{x}|} & \\ \hline & & X & & 0 \end{array}\right)$$

(for this, use the identity matrix in the upper right corner of Y to make every element of the lower right corner trivial by means of elementary row operations); since the determinantal ideals of similar matrices clearly coincide, we find that $\mathrm{DetId}(Y) \subseteq \mathrm{DetId}(\widetilde{Y}) = \mathrm{DetId}(\widetilde{Y'}) = \mathrm{DetId}(X)\mathrm{DetId}(\mathbb{I}_{|\underline{y}|}) = \mathrm{DetId}(X)$. Moreover, since the rows of $\widetilde{Y}$ are relations among the elements of $\underline{xy}$, the same holds for the rows of $\widetilde{Y'}$, so X is a matrix of relations for $\underline{x}$ (since Y was a matrix of relations, X has more rows than columns). This shows the inclusion $A(\underline{xy}) \subseteq A(\underline{x})$, and repeating the same argument with $\underline{y}$ at the place of $\underline{x}$ shows that $A(\underline{y}) = A(\underline{xy}) = A(\underline{x})$, as we needed. □

Remark. Observe that it is enough to restrict the computation to *square* $|\underline{x}| \times |\underline{x}|$-matrices. Indeed, substituting a matrix of relations X with all its $|\underline{x}| \times |\underline{x}|$-submatrices in the sum defining $\mathrm{DetId}(X)$ gives the same elements in the determinantal ideal.

Example. Let $M = R^a$ for some $a \geq 1$. A set of generators for M is $\underline{e}$, where e_i is the vector such that $(e_i)_j = \delta_{i,j}$. For every relation $(r_1, \dots, r_a) \in R^a$,

$$\sum_{i=1}^{a} r_i e_i = 0 \Longrightarrow r_i = 0 \quad \forall\, i\ .$$

Therefore there are no non-trivial relations and, in particular, the only matrix of relations for $\underline{e}$ is the 0 matrix. Accordingly, $\mathrm{Fitt}_R(R^a) = 0$.

Example. Let p be a prime number, $R = \mathbb{Z}$ and let $M = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2$. Then clearly $\mathrm{Ann}_{\mathbb{Z}}(M) = p^2\mathbb{Z}$. We want to compute $\mathrm{Fitt}_{\mathbb{Z}}(M)$. For this, let $\{(a,0),(0,b)\}$ be a set of generators of M, where $p \nmid ab$. Then a matrix of relations for this set is of the form

$$X = \begin{pmatrix} \alpha_1 & \beta_1 \\ \alpha_2 & \beta_2 \\ \vdots & \vdots \\ \alpha_q & \beta_q \end{pmatrix}$$

with $v_p(\alpha_i) \geq 1$ and $v_p(\beta_i) \geq 2$, for some $q \geq 2$. Therefore, any 2×2-minor of X looks like

$$\det(X_{ij}) = \begin{vmatrix} \alpha_i & \beta_i \\ \alpha_j & \beta_j \end{vmatrix}$$

and $v_p(\det(X_{ij}) = v_p(\alpha_i\beta_j - \alpha_i\beta_i) \geq 3$, showing via Proposition 1 that $\mathrm{Fitt}_{\mathbb{Z}}(M) = p^3\mathbb{Z}$. If we allowed "matrices of relations" having only one row, (p, p^2) would have been one such a matrix, generating the ideal $p^2\mathbb{Z}$. In this sense, this invariant is "finer" than the usual annihilator.

Remark. In his book [Nor76] Northcott defines the i-th Fitting ideal for every natural number $i \geq 0$. What we have defined is then the 0-th Fitting ideal, and is enough for the purposes of Wiles' proof.

We now gather the main elementary results on Fitting ideals.

Lemma 1. *Let $I \subseteq R$ be an ideal. Then* $\mathrm{Fitt}_R(R/I) = I$.

Proof. A generator for R/I is 1 and the general matrix of relations for it is

$$\begin{pmatrix} \alpha_1 \\ \dots \\ \alpha_q \end{pmatrix}$$

such that $\alpha_i \cdot 1 = 0 \in R/I$, *i. e.* such that $\alpha_i \in I$ for all i's. □

For the rest of this section M will denote a finitely generated R-module.

Lemma 2. *Let M' be a quotient of M and let $\pi : M \twoheadrightarrow M'$ be a surjection: then* $\mathrm{Fitt}_R(M) \subseteq \mathrm{Fitt}_R(M')$.

Proof. Let $\underline{x}$ be a set of generators for M; then $\underline{\pi(x)} = \{\pi(x)_1, \dots, \pi(x)_{|\underline{x}|}\}$ is a set of generators for M'. If $\{r_1, \dots, r_{|\underline{x}|}\}$ is a relation for $\underline{x}$, it is also one for $\underline{\pi(x)}$. Therefore any matrix of relations for $\underline{x}$ is also a matrix of relations for $\underline{\pi(x)}$, showing the desired inclusion. □

Lemma 3. *If $M \cong M_1 \times M_2$, then* $\mathrm{Fitt}_R(M) = \mathrm{Fitt}_R(M_1) \cdot \mathrm{Fitt}_R(M_2)$.

Proof. On one side, any two matrices X, Y of relations for M_1 and M_2, respectively, give a matrix of relations

$$\begin{pmatrix} X & 0 \\ 0 & Y \end{pmatrix}$$

for $M_1 \times M_2$. On the other side, choosing as set of generators for $M_1 \times M_2$ one of the form $\underline{xy} = \{x_1, \ldots, x_{|\underline{x}|}, y_1, \ldots, y_{|\underline{y}|}\}$ where $\underline{x}$ is a set of generators for M_1 and $\underline{y}$ is one for M_2, we can form from any matrix of relations for $\underline{xy}$ two matrices of relations for $\underline{x}$ and $\underline{y}$. These matrices verify clearly $\overline{\mathrm{DetId}}(X)\mathrm{DetId}(Y) = \mathrm{DetId}(XY)$, and our statement follows. □

Combining Lemma 3 and Lemma 1 we get

Corollary 1. *If $M = R/\mathfrak{a}_1 \times \cdots \times R/\mathfrak{a}_n$ for ideals $\mathfrak{a}_i \subseteq R$, then $\mathrm{Fitt}_R(M) = \mathfrak{a}_1 \cdots \mathfrak{a}_n$.*

□

Lemma 4. *If M can be generated by n elements, then*

$$\mathrm{Ann}_R(M)^n \subseteq \mathrm{Fitt}_R(M) \subseteq \mathrm{Ann}_R(M) \ .$$

Proof. First of all, let $\underline{x}$ be a set of generators with $|\underline{x}| = n$. Then, if $c_i \in \mathrm{Ann}_R(M)$ for $1 \leq i \leq n$, the matrix

$$C = \begin{pmatrix} c_1 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & c_n \end{pmatrix}$$

is a matrix of relations for $\underline{x}$ and $c_1 \cdots c_n = \det(C) \in \mathrm{Fitt}_R(M)$, so $\mathrm{Ann}_R(M)^n \subseteq \mathrm{Fitt}_R(M)$.
On the other hand, let X be a square $n \times n$-matrix of relations for $\underline{x}$: let X° be its *adjugate* matrix[1]. Then multiplying the equation

$$X \cdot \underline{x} = \underline{0}$$

by X° shows that $\det(X) \in \mathrm{Ann}_R(M)$. Since, as we observed, $\mathrm{Fitt}_R(M)$ is generated by these determinants, we find $\mathrm{Fitt}_R(M) \subseteq \mathrm{Ann}_R(M)$. □

Remark. This Lemma gives another proof that $\mathrm{Fitt}_R(R/I) = I$, since in that case $n = 1$ and $\mathrm{Ann}_R(M) = I$.

[1]The adjugate matrix X° of a square $n \times n$-matrix X with coefficients in a ring R is a matrix such that $XX^\circ = \det(X)\mathbb{I}_n$. It may be defined as the matrix whose (i, j)-entry is the (j, i)-cofactor of X.

During the school, Otmar Venjakob observed that since M admits n generators, there is a surjection

$$\Big(R/\mathrm{Ann}_R(M)\Big)^n \twoheadrightarrow M$$

and applying Lemma 2 gives the first inclusion.

Recall that a R-module M is said to be faithful if $\mathrm{Ann}_R(M) = 0$. Thus the above Lemma gives

Corollary 2. *If M is a faithful R-module, then* $\mathrm{Fitt}_R(M) = 0$.

□

Lemma 5. *If $I \subseteq R$ is any ideal of R, then*

$$\mathrm{Fitt}_{R/I}(M/IM) = \mathrm{Fitt}_R(M) + I \ \subseteq R/I$$

Proof. It is clear that if $\underline{x}$ is a set of generators for M, than its image under the canonical projection is a set of generators for M/I, and that any relation for the first set is also a relation for the second, giving $\mathrm{Fitt}_R(M) + I \subseteq \mathrm{Fitt}_{R/I}(M/IM)$.
If now $[X] = ([\xi_{ij}])$ is a matrix of relation for the set $[\underline{x}]$ of generators of M/IM (we denote by $[\cdot]$ the class $\cdot + I$), we can find elements $\alpha_{ij} \in I$ such that for all $1 \leq i \leq |\underline{x}|$ we have

$$\sum_{j=1}^{|\underline{x}|} \xi_{ij} x_j = \sum_{j=1}^{|\underline{x}|} \alpha_{ij} x_j$$

because every element of IM can be written as a finite sum of the generators of M with coefficients in I. The matrix $\widetilde{X}$ whose i-th row is

$$(\xi_{i1} - \alpha_{i1}, \ldots, \xi_{i|\underline{x}|} - \alpha_{i|\underline{x}|})$$

is a matrix of relations for M and $X \equiv \widetilde{X} \pmod{I}$. Therefore $\mathrm{DetId}([X]) = \mathrm{DetId}([\widetilde{X}]) = \mathrm{DetId}(\widetilde{X}) + I \subseteq \mathrm{Fitt}_R(M) + I$. This gives the other inclusion.
□

Lemma 6. *If $0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$ is an exact sequence of finitely generated R-modules, then*

$$\mathrm{Fitt}_R(M_1) \cdot \mathrm{Fitt}_R(M_3) \subseteq \mathrm{Fitt}_R(M_2)\ .$$

Proof. Without loss of generality, we may and will assume that $M_1 \subseteq M_2$ and that the first map above is the natural inclusion. Let now $[\underline{x}]$ be a set of generators for M_3 and let $\underline{x}$ be a lifting of it to M_2. Let $\underline{y}$ be a set of generators for $M_1 \subseteq M_2$. Then $\underline{xy}$ is a set of generators for M_2.
Let $X \in \mathcal{M}_{p\times|\underline{x}|}(R), Y \in \mathcal{M}_{q\times|\underline{y}|}(R)$ be matrices of relations for $[\underline{x}]$ and $\underline{y}$, respectively, and let $C = (-c_{ij}) \in \mathcal{M}_{p\times|\underline{y}|}(R)$, where

$$X \cdot \underline{x} = \begin{pmatrix} \sum_{i=1}^{|\underline{y}|} c_{1i}y_i \\ \sum_{i=1}^{|\underline{y}|} c_{2i}y_i \\ \vdots \\ \sum_{i=1}^{|\underline{y}|} c_{pi}y_i \end{pmatrix}.$$

Then the matrix

$$Z = \begin{pmatrix} X & C \\ 0 & Y \end{pmatrix}$$

is a $(p+q) \times |\underline{xy}|$-matrix of relations for M_2 and $\mathrm{DetId}(X) \cdot \mathrm{DetId}(Y) \subseteq \mathrm{DetId}(Z)$ since every minor of Z is of the form

$$\begin{vmatrix} M_X & M_C \\ 0 & M_Y \end{vmatrix} = \begin{vmatrix} M_X & 0 \\ 0 & M_Y \end{vmatrix}$$

where M_X is a submatrix of X and M_Y is a submatrix of Y. □

2 Applications to Wiles' proof

In this section we focus on the applications of the theory of Fitting ideals developed up to now to Wiles' proof. In a first part we will start by assuming that not only M is finitely generated, but that is in fact finitely presented; and we eventually specialize to the case $R = \mathcal{O}[[T]]$ where $\mathcal{O}$ is the ring of integers of a p-adic field.

2.1 Finite presentations

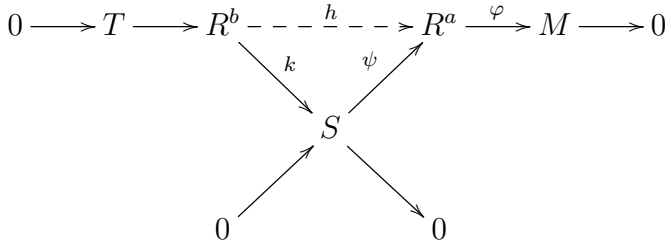
First of all, recall that an R-module M is said to be *finitely presented* if there is an exact sequence of R-modules

$$R^a \xrightarrow{h} R^b \xrightarrow{\varphi} M \to 0$$

for suitable $a, b \in \mathbb{N}$. Clearly, every finitely presented module is finitely generated, since it can be generated by $\varphi(e_i)$ for $1 \leq i \leq b$. If R is noetherian, the converse is also true: indeed, if M is finitely generated, it is a quotient of a finitely generated free module and there is an exact sequence

$$0 \to S \xrightarrow{\psi} R^b \xrightarrow{\varphi} M \to 0$$

for some S and for some $b \in \mathbb{N}$. Using that R is noetherian, S should also be finitely generated, say a quotient of R^a by a module T: we find



where $h := \psi \circ k$. We can therefore extract from the above diagram the sequence

$$R^a \xrightarrow{h} R^b \xrightarrow{\varphi} M \to 0$$

that is exact since $\mathrm{Ker}(\varphi) = \mathrm{Im}(\psi) = \mathrm{Im}(h)$.
Now we present some results that are true for general finitely presented R-modules. Thus, assuming noetherianity reduces this hypothesis to M being finitely generated.

From now on we we fix an R-module M and we assume it is finitely presented.

Proposition 2. *Let $R^a \xrightarrow{h} R^b \xrightarrow{\varphi} M \to 0$ be a finite presentation of M and let $H \in \mathcal{M}_{b\times a}(R)$ be a matrix attached to h. If $a \geq b$, then $\mathrm{Fitt}_R(M) = \mathrm{DetId}(H^{tr})$ and if $a < b$ then $\mathrm{Fitt}_R(M) = 0$.*

Proof. The finite presentation

$$R^a \xrightarrow{h} R^b \xrightarrow{\varphi} M \to 0$$

shows that a set of generators of M is $\{\varphi(e_1), \ldots, \varphi(e_b)\}$ and that the relations among these elements are precisely the kernel of φ, namely $\mathrm{Im}(h)$, that

is spanned by the columns of H. By Proposition 1, to compute $\mathrm{Fitt}_R(M)$ it suffices to consider matrices whose rows are relations among these generators.

If $a \geq b$, then H^{tr} is a matrix of relations; moreover, if X is any other matrix of relations, then all its sumbatrices are linear combinations of rows of H^{tr} and their determinant coincide with the determinant of those rows. Therefore $\mathrm{DetId}(X) \subseteq \mathrm{DetId}(H^{\mathrm{tr}})$, showing the desired equality.
If $a < b$, then every matrix of relations $X \in \mathcal{M}_{b\times b}(R)$ has at least two linearly dependent rows, since they belong to $\mathrm{Im}(h)$ and this module has R-rank $a < b$. Therefore $\mathrm{DetId}(X) = 0$ for all such matrices, showing $\mathrm{Fitt}_R(M) = 0$. $\square$

Lemma 7. *If I is a finitely generated ideal, then*

$$\mathrm{Fitt}_R(M) \subseteq \mathrm{Fitt}_R(M/IM) \subseteq (\mathrm{Fitt}_R(M), I) \subseteq R\ .$$

Proof. The first inclusion is Lemma 2. For the second, if

$$R^a \xrightarrow{h} R^b \to M \to 0$$

is a presentation of M and if $I = \langle \alpha_1, \ldots, \alpha_n \rangle$, then a presentation of M/IM is

$$R^{a+nb} \xrightarrow{h^*} R^b \to M/IM \to 0$$

where

$$\begin{aligned} h^*(w_1, \ldots, w_a, v_{1,1}, \ldots, v_{1,b}, \ldots, v_{n,1}, \ldots, v_{n,b}) =& h(w_1, \ldots, w_a) \\ &+ \sum_{j=1}^{n} (\alpha_j v_{j,1}, \ldots, \alpha_j v_{j,b})\ . \end{aligned}$$

A matrix associated to h^* is

$$H^* = \begin{pmatrix} H & 0 & \ldots & 0 \\ 0 & A & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & A \end{pmatrix}$$

where H is a matrix associated to h and A is the diagonal matrix

$$A = \begin{pmatrix} \alpha_1 & 0 & \ldots & 0 \\ 0 & \alpha_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \alpha_n \end{pmatrix}\ .$$

Any non-trivial $b \times b$ minor of H^* is either a $b \times b$ minor of H or a linear combination of suitable multiples of some α_j's, and hence we get the second inclusion. Observe that the above proof works both if $a \geq b$ and if $a < b$. $\square$

Combining this Lemma with Corollary 2 we get

Corollary 3. *If $I \subseteq R$ is a finitely generated ideal and M is a faithful R-module, then* $\mathrm{Fitt}_R(M/IM) \subseteq I$.

$\square$

2.2 Iwasawa Algebras

Next we focus on applications of the theory of Fitting ideal in Wiles' proof of the Iwasawa Conjecture. We assume for this that $\mathcal{O}$ is the ring of integers of a p-adic field and we let Λ denote the formal power series ring $\Lambda = \mathcal{O}[[T]]$: we refer the reader to chapters 7, 13 and 15 of [Was97] for basic facts about Λ-modules. This is a complete, local, noetherian ring: let $\mathfrak{m}$ denote its maximal ideal, that is generated (for instance) by π and T where π is a uniformizer of $\mathcal{O}$. Since it is noetherian, we can combine general results of Section 1 with those of § 2.1.
If $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ are prime ideals of height 1 in Λ and $r, e_1, \ldots, e_k$ are non-negative integers, define the finitely generated Λ-module $E(r, \mathfrak{p}_1^{e_1}, \ldots, \mathfrak{p}_k^{e_k})$ to be

$$E(r, \mathfrak{p}_1^{e_1}, \ldots, \mathfrak{p}_k^{e_k}) = \Lambda^r \oplus \bigoplus_{i=1}^{k} \Lambda/\mathfrak{p}_i^{e_i} \ :$$

These are called *elementary* Λ-modules: they are classified (up to isomorphism) by the above set of prime ideals and integers and every finitely generated Λ-module is pseudo-isomorphic to exactly one of these modules − a pseudo-isomorphism being a Λ-homomorphism with finite kernel and cokernel.
For a finitely generated *torsion* module M, $r = 0$ and a coarser (but often important) invariant than the entire set above is the so-called characteristic polynomial, that is the unique distinguished[2] polynomial $f_M(T)$ such that

$$f_M(T) \cdot \Lambda = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i} \ ;$$

[2] A power series is called a distinguished polynomial if it is either a constant in $\pi\mathcal{O}$ or it is a monic polynomial whose coefficients are all divisible by π but the leading one.

since this definition is easily seen to be multiplicative in exact sequences and since finite modules are pseudo-isomorphic to the trivial module, this is an invariant under pseudo-isomorphism. Observe that prime ideals of height 1 are all principal, generated either by a uniformizer of $\mathcal{O}$ or by irreducible distinguished polynomial. We start with the following

Lemma 8. *Let $N = E(0, \mathfrak{p}_1^{e_1}, \dots, \mathfrak{p}_k^{e_k})$ be an elementary torsion Λ-module. Then*

1. $f_N(T) \cdot \Lambda = \mathrm{Fitt}_\Lambda(N)$.
2. *If none of the $\mathfrak{p}_i$'s is $\pi \cdot \Lambda$, then*

$$\mathrm{Fitt}_\Lambda(N) = \mathrm{char}_\Lambda\big(\cdot T : N \to N\big) \cdot \Lambda \ .$$

where $\mathrm{char}_\Lambda\big(\cdot T : N \to N\big)$ is the characteristic polynomial (say, in the variable X) of the multiplication by T seen as $\mathcal{O}$-linear endomorphisms of the finite free $\mathcal{O}$-module N, evaluated at $X = T$.

Remark. Given a non-constant distinguished polynomial $g(T)$, the module $\Lambda/g(T)\Lambda$ is $\mathcal{O}$-torsion free; thus, if $\mathfrak{p}_i \neq \pi\Lambda$ for all i's, then N is finitely generated and torsion-free over the principal ideal domain $\mathcal{O}$, hence free of finite rank. Moreover, despite its name, we will always denote the characteristic polynomial of a Λ-module M by f_M, leaving the notation $\mathrm{char}_\Lambda(\cdot)$ for the usual meaning of the characteristic polynomial of a linear map (see Corollary 4 below for instances in which these two notions coincide).

Proof. The equality in 1. is clear after Corollary 1 and the definition of elementary module.
For 2. without loss of generality we can assume that $N = \Lambda/\mathfrak{p}^e$ with $\mathfrak{p} = g(T)\Lambda$ where $g(T)$ is a non-constant distinguished polynomial. Then $\mathfrak{p}^e = g(T)^e\Lambda$ and $g(T)^e$ is still distinguished, say of degree λ: let g_i be the coefficient of T^i in $g(T)^e$ for $0 \leq i \leq \lambda - 1$. Let $\{1, T, \dots, T^{\lambda-1}\}$ be a basis of N: the matrix attached to the multiplication by T in this basis is

$$\begin{pmatrix} 0 & 0 & 0 & 0 & -g_0 \\ 1 & 0 & 0 & 0 & -g_1 \\ \vdots & 1 & 0 & 0 & -g_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 1 & -g_{\lambda-1} \end{pmatrix}$$

and the characteristic polynomial is then

$$\begin{vmatrix} -X & 0 & 0 & 0 & -g_0 \\ 1 & -X & 0 & 0 & -g_1 \\ \vdots & 1 & -X & 0 & -g_2 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & 1 & -g_{\lambda-1} - X \end{vmatrix}$$

Developing the determinant along the first line shows, by induction on λ, that this characteristic polynomial is precisely

$$\sum_{i=0}^{\lambda-1} g_i X^i + X^\lambda = g(X)^e \ .$$

Using 1. and evaluating at $X = T$ yields 2., since $f_{\Lambda/g(T)^e\Lambda} = g(T)^2$. □

Corollary 4. *Let N be a finitely generated torsion Λ-module having no $\mathcal{O}$-torsion. Then N is a finite free $\mathcal{O}$-module and*

$$f_N(T) \cdot \Lambda = \mathrm{char}_\Lambda\big(\cdot\, T : N \to N\big) = \mathrm{Fitt}_\Lambda(E_N)$$

where E_N is the elementary module pseudo-isomorphic to N.

Proof. The freeness of N follows, as before, from $\mathcal{O}$ being a principal ideal domain; observe also that the elementary module attached to a module without $\mathcal{O}$-torsion does not have $\pi \cdot \Lambda$ in its set of invariants. Thanks to the above Lemma, the equality follows from $f_N(T) = f_{E_N}(T)$, which is clear since, by definition, the characteristic polynomial of a Λ-module depends only on its pseudo-isomorphism class; and from $\mathrm{char}_\Lambda\big(\cdot\, T : N \to N\big) = \mathrm{char}_\Lambda\big(\cdot\, T : E_N \to E_N\big)$. This last relation may be proven, for instance, by observing that both are monic polynomials with coefficients in $\mathcal{O}$ of the same degree that have the same image in $\Lambda \otimes \overline{\mathbb{Q}_p}$. □

Proposition 3. *Let N be a finitely generated torsion Λ-module having no $\mathcal{O}$-torsion. Then*

$$f_N(T) \cdot \Lambda = \mathrm{Fitt}_\Lambda(N) \ .$$

We start with the following Lemma:

Lemma 9 (Auslander-Buchsbaum resolution)**.** *Let N be finitely generated torsion Λ-module that is free of finite rank as $\mathcal{O}$-module. Then*

$$\Lambda \otimes_{\mathcal{O}} N \xrightarrow{\gamma} \Lambda \otimes_{\mathcal{O}} N \xrightarrow{\varepsilon} N \to 0$$

is a finite presentation of N as Λ-module, where

$$\gamma(\lambda \otimes n) = T\lambda \otimes n - \lambda \otimes Tn$$

and

$$\varepsilon(\lambda \otimes n) = \lambda n \ .$$

Proof. The fact that ε is surjective is clear, as well as the fact that both γ and ε are Λ-homomorphisms and that $\varepsilon \circ \gamma = 0$. Moreover, if we prove that the sequence is exact, it is a presentation of N since the freeness of N implies that of $\Lambda \otimes N$.
Thus we need only to show that $\mathrm{Im}(\gamma) \supseteq \mathrm{Ker}(\varepsilon)$ and this would follow from

$$x = \gamma(\xi) + 1 \otimes \varepsilon(x) \qquad \forall\, x \in \Lambda \otimes_{\mathcal{O}} N \tag{1}$$

for some ξ depending on x. Since (1) is $\mathcal{O}$-linear, we can check it only on elements of the form $x = T^k \otimes n$ (use also that $\mathcal{O}[T]$ is dense in Λ and both γ, ε are continuos) for suitable $k \geq 0$ and $n \in N$: this we do by induction on k. If $k = 1$, $x = T \otimes n = T \otimes n - 1 \otimes Tn + 1 \otimes Tn = \gamma(1 \otimes n) + 1 \otimes \varepsilon(T \otimes n)$, as we wanted. Asssuming (1) up to $k-1$, suppose $x = T^k \otimes n$: then

$$\begin{aligned} x &= TT^{k-1} \otimes n - T^{k-1} \otimes Tn + T^{k-1} \otimes Tn \overset{\text{induction}}{=} \\ &= T^{k-1}\big(T \otimes n - 1 \otimes Tn\big) + \gamma(\xi') + 1 \otimes \varepsilon\big(T^{k-1} \otimes Tn\big) = \\ &= T^{k-1}\gamma(1 \otimes n) + \gamma(\xi') + 1 \otimes T^k n = \\ &= \gamma\big(T^{k-1} \otimes n + \xi'\big) + 1 \otimes \varepsilon(x) \ . \end{aligned}$$

Setting $\xi = T^{k-1} \otimes n + \xi'$ we get (1). □

Remark. It is indeed easy to prove that γ is injective.

We can now prove Proposition 3:

Proof. If $\underline{x}$ is a $\mathcal{O}$-basis of N, the set $\{1 \otimes x_1, \ldots, 1 \otimes x_{|\underline{x}|}\}$ is a Λ-basis of $\Lambda \otimes N$: moreover, $\gamma = \vartheta - \tau$ where

$$\vartheta : \lambda \otimes n \mapsto T\lambda \otimes n \qquad \tau : \lambda \otimes n \mapsto \lambda \otimes Tn$$

and therefore $\det \mathrm{Mat}(\gamma) = \det\big(\mathrm{Mat}(\vartheta) - \mathrm{Mat}(\tau)\big)$, where we introduce - just along the proof - the notation $\mathrm{Mat}(\cdot)$ to denote the matrix attached to a linear map in the bases chosen above. Since ϑ maps every element of the Λ-basis $1 \otimes x_i$ to $T \otimes x_i$, and by definition of τ, we find

$$\mathrm{Mat}(\vartheta) = T \cdot \mathbb{I}_{|\underline{x}|} \quad \tau = \cdot T : N \to N \ .$$

This shows that the characteristic polynomial of multiplication by T (evaluated at $X = T$) is the determinant of $\mathrm{Mat}(\gamma)$ and, by Proposition 2 applied to the Auslander-Buschsbaum resolution, we see that this determinant generates the Λ-Fitting ideal of N. Corollary 4 then gives the stated equality. $\square$

Now that we have collected these results, let M be a finitely generated torsion Λ-module and assume that "$\mu = 0$", meaning[3] that π does not divide the characteristic polynomial $f_M(T)$ of M. Let $tor_{\mathcal{O}}(M) \subseteq M$ be the maximal $\mathcal{O}$-torsion submodule of M: it is a Λ-submodule of M and there is an exact sequence

$$0 \longrightarrow tor_{\mathcal{O}}(M) \longrightarrow M \longrightarrow N \longrightarrow 0 \tag{2}$$

where N satisfies the hypothesis of Corollary 4. Observe now that as an application of Lemma 6 we find

Corollary 5. *Suppose R is a local ring and $\mathfrak{m}$ is its maximal ideal. If M is an R-module of finite length, then*

$$\mathfrak{m}^{\mathrm{length}_R(M)} \subseteq \mathrm{Fitt}_R(M) \ .$$

Proof. We claim that over a local ring every module of length 1 is isomorphic to $k := R/\mathfrak{m}$. Granting the claim, the Corollary follows from Lemma 1 and from Lemma 6, by induction on $\mathrm{length}_R(M)$.
We now prove the claim: observe that if M is a k-vector space endowed with the natural R-action induced by $R \twoheadrightarrow k$, then the notion of k-vector subspace and of R-submodule of M coincide. Therefore $\mathrm{length}_R(M) = \mathrm{length}_k(M) = \dim_k(M)$. The module M has length 1, and therefore in the chain of inclusions

$$M \supseteq \mathfrak{m}M \supseteq 0$$

one is an equality. By Nakayama Lemma, $M = \mathfrak{m}M \Rightarrow M = 0$, and this is absurd since $\mathrm{length}_R(0) = 0$: therefore $\mathfrak{m}M = 0$, M is a k-vector space and our previous discussion shows that it has dimension 1 over k. $\square$

[3]Traditionally, μ is the exponent of $\pi \cdot \Lambda$ in the set of invariants of an elementary module.

Applying this to our situation, we get:

Proposition 4. *Let M be a finitely generated torsion Λ-module such that $\mu = 0$. Then*

$$f_M(T) \cdot (\pi, T)^{\mathrm{length}_\Lambda(tor_{\mathcal{O}}(M))} \subseteq \mathrm{Fitt}_\Lambda(M) \subseteq f_M(T) \cdot \Lambda \ .$$

Proof. Observe, first of all, that since $tor_{\mathcal{O}}(M)$ is finite, it has trivial characteristic polynomial and $f_M(T) = f_N(T)$. Now apply Lemma 6 to the above sequence (2). We find that

$$\mathrm{Fitt}_\Lambda(tor_{\mathcal{O}}(M)) \cdot \mathrm{Fitt}_\Lambda(N) \subseteq \mathrm{Fitt}_\Lambda(M) \ :$$

since $tor_{\mathcal{O}}(M)$ is of finite length and N has no $\mathcal{O}$-torsion, we can apply Corollary 5 and Corollary 4 (together with our first remark) to translate the above inclusion as $(\pi, T)^{\mathrm{lentgh}_\Lambda(tor_{\mathcal{O}}(M))} \cdot f_M(T) \subseteq \mathrm{Fitt}_\Lambda(M)$. The second inclusion just follows from Lemma 2 together with Corollary 4. □

References

[MW84] B. Mazur and A. Wiles, *Class fields of abelian extensions of* **Q**, Invent. Math. **76** (1984), no. 2, 179-330.

[Nor76] D. G. Northcott, *Finite free resolutions*, Cambridge University Press, Cambridge, 1976, Cambridge Tracts in Mathematics, No. 71.

[Was97] Lawrence C. Washington, *Introduction to Cyclotomic Fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, Berlin, 1997.

[Wil90] A. Wiles, *The Iwasawa conjecture for totally real fields*, Ann. of Math. (2) **131** (1990), no. 3, 493-540.