Invariant Factors of an Endomorphism and Finite Free Resolutions

Jose A. Hermida-Alonso
Departamento de Algebra
Facultad de Ciencias
Universidad de Valladolid
47005-Valladolid, Spain

and

Miriam Pisonero
Departamento de Matemática Aplicada Fundamental
E.T.S. Arquitectura
Universidad de Valladolid
47014-Valladolid, Spain

Submitted by Robert M. Guralnick

ABSTRACT

Polynomial invariants are associated to an endomorphism u of a module M that has a finite free resolution. The first invariant $\chi(u, X)$ (characteristic polynomial of u) is a monic polynomial of degree the Euler characteristic of M. Its construction is based on the MacRae invariant. When M is a finite free module, $\chi(u, X)$ is the classical characteristic polynomial of u. With additional assumptions there is constructed a finite sequence of monic polynomials $\{d_i(u, X)\}_{i \geq 0}$ such that their product is $\chi(u, X)$ and $d_i(u, X)$ divides $d_{i+1}(u, X)$. When R is a field, these polynomials are the invariant factors of u. A generalized Cayley-Hamilton theorem is given. The generic behavior of the polynomials $\chi(u, X)$ and $\{d_i(u, X)\}_{i \geq 0}$ in Spec R is proved. Finally it is shown, under certain assumptions that there exists a free submodule F of M, invariant with respect to u, such that the restriction of u to F is similar to the endomorphism of F defined by the diagonal block matrix where the ith block is the companion matrix of $d_i(u, X)$.

LINEAR ALGEBRA AND ITS APPLICATIONS 187: 201–226 (1993) 201

655 Avenue of the Americas, New York, NY 10010 0024-3795/93/$6.00

INTRODUCTION

Let R be a commutative ring with unit, and M a finitely generated R-module. In this paper we attack the classical problem of classification of M-endomorphisms when M has a finite free resolution. We shall assign to each endomorphism u of M a finite set of monic polynomials $\{d_i(u, X)\}_{1 \leqslant i \leqslant t}$ such that when $R = K$ is a field and $M = V$ is a finite dimensional vector space these polynomials are the classical invariant factors associated to u.

Let M be an R-module and $u : M \to M$ an R-homomorphism. The endomorphism u converts M into an $R[X]$-module by

$$X \cdot m = u(m).$$

We denote M as $R[X]$-module via u by M_u. If $\tilde{u}$ denotes the $R[X]$-endomorphism of $M[X]$ obtained from u by extension of scalars, then one has the *characteristic exact sequence*

$$0 \to M[X] \xrightarrow{\psi} M[X] \xrightarrow{\varphi} M_u \to 0,$$

with $\psi = t_X - \tilde{u}$ and t_X denoting multiplication by X.

Let's consider the classical case first, i.e. when $R = K$ is a field and $M = V$ is a finite dimensional vector space. It is well known that the invariant factors $\{d_i(u, X)\}_{1 \leqslant i \leqslant t}$ of u, where $d_i(u, X)$ divides $d_{i+1}(u, X)$ for $i = 1, \dots, t-1$, can be obtained as the monic generators of the ideals $\{(\mathcal{F}_{t-i}(V_u) : \mathcal{F}_{t-i+1}(V_u))\}_{0 \leqslant i \leqslant t-1}$, where $\mathcal{F}_i(V_u)$ is the ith Fitting invariant of V_u. Two endomorphisms u and v are similar if and only if $d_i(u, X) = d_i(v, X)$ for each i, or equivalently, if and only if $\mathcal{F}_i(V_u) = \mathcal{F}_i(V_v)$ for each i. The initial Fitting invariant $\mathcal{F}_0(V_u)$ is the principal ideal of $K[X]$ generated by the characteristic polynomial $\chi(u, X)$ of u.

Let's consider the free case, i.e. when R is a commutative ring with unit and $M = R^n$ is a free R-module of rank n. In this situation the ideal $\mathcal{F}_0((R^n)_u)$ is principal and generated by the characteristic polynomial $\chi(u, X)$ of u, while the ideals $\mathcal{F}_i((R^n)_u)$ for $i \geqslant 1$ are not principal in general. In consequence, in this case one can talk about a characteristic polynomial but not about invariant factors.

In the general case, i.e. when R is a commutative ring with unit and M a finitely generated R-module, the ideals $\mathcal{F}_i(M_u)$ are not principal and neither is $\mathcal{F}_0(M_u)$. When $M = P$ is a finitely generated projective R-module, O. Goldman [4] constructs a characteristic polynomial of u, defining first the determinant of an endomorphism of a finitely generated projective module and then the characteristic polynomial of u as $\det(t_X - \tilde{u})$, following the free case. G. Almkvist [1] also talks about a characteristic polynomial of u when $M = P$ is a finitely generated projective module. He constructs it by defining its coefficients as the traces of the exterior powers of u up to a sign, also following the free case. The two polynomials, in general, are different. They are only equal when P is a finitely generated projective module of constant rank.

This paper is organized in the following way. Let M be an R-module that has a finite free resolution. In Section 2 we shall associate to an endomorphism $u : M \to M$ a monic polynomial $\chi(u, X)$ that generates the smallest principal ideal of $R[X]$ containing $\mathscr{F}_0(M_u)$. We shall call $\chi(u, X)$ the characteristic polynomial of u.

The classical Cayley-Hamilton theorem, i.e. that u annihilates its characteristic polynomial, does not hold for the polynomial $\chi(u, X)$. In Section 3 we give a generalized version of the Cayley-Hamilton theorem. Namely, for every $\Delta \in \mathscr{F}_n(M)$ we have $\Delta\chi(u, u) = 0$, where n is the Euler characteristic of M.

In Section 4, under certain assumptions, we shall associate to u a sequence of monic polynomials $\{d_i(u, X)\}_{1 \leqslant i \leqslant t}$ verifying:

(i) $d_1(u, X)d_2(u, X) \cdots d_t(u, X) = \chi(u, X)$.

(ii) $d_i(u, X)$ divides $d_{i+1}(u, X)$ for $1 \leqslant i \leqslant t - 1$.

(iii) $(\prod_{i=1}^{t-r} d_i(u, X))$ is the smallest principal ideal of $R[X]$ generated by a monic polynomial that contains $\mathscr{F}_r(M_u)$, $1 \leqslant r \leqslant t - 1$.

(iv) There exists a dense Zariski open set $C(M, u)$ of Spec R such that if $\mathfrak{p} \in C(M, u)$ then the invariant factors of the $k(\mathfrak{p})$-endomorphism of vector spaces

$$u \otimes 1 : M \otimes k(\mathfrak{p}) \to M \otimes k(\mathfrak{p})$$

are the images of $\{d_i(u, X)\}_{1 \leqslant i \leqslant t}$ in $k(\mathfrak{p})[X]$, where $k(\mathfrak{p})$ denotes the residue field at $\mathfrak{p}$, i.e. $k(\mathfrak{p}) = R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$.

(v) There exists a free submodule F of M, invariant with respect to u and with rank equal to the Euler characteristic of M, such that the restriction of u to F is similar to the endomorphism of F defined by the diagonal block matrix

$$\begin{pmatrix} D_1 & & & \\ & D_2 & & \\ & & \ddots & \\ & & & D_t \end{pmatrix},$$

where D_i is the companion matrix of $d_i(u, X)$.

When $M = R^n$, the previous polynomial $\chi(u, X)$ is the classical characteristic polynomial of u, and when $R = K$ is a field, the previous sequence of polynomials $\{d_i(u, X)\}_{1 \leqslant i \leqslant t}$ is the sequence of the classical invariant factors of u.

We start this paper with a short exposition of the techniques that we shall use through this work.

1. PRELIMINARIES AND NOTATION

Fitting Ideals

Let R be a commutative ring with unit, and let M be a finitely presented R-module. We denote by $\mathscr{F}_i(M)$ [3] the ith Fitting ideal of M, i.e., if

$$R^r \xrightarrow{f} R^s \to M \to 0$$

is a presentation of M, and A is the matrix of f relative to bases of R^r and R^s, then

$$\mathscr{F}_i(M) = \begin{cases} \mathscr{U}_{s-i}(A) & \text{if } 0 \leqslant i \leqslant s-1, \\ R & \text{if } i \geqslant s, \end{cases}$$

where $\mathscr{U}_{s-i}(A)$ is the ideal generated by all the $(s-i) \times (s-i)$ minors of A.

Fitting ideals satisfy the following properties [8, Chapters 3, 4]:

(i) $\mathscr{F}_0(M) \subseteq \mathscr{F}_1(M) \subseteq \cdots \subseteq \mathscr{F}_i(M) \subseteq \cdots$.
(ii) $\mathscr{F}_i(M \oplus M') = \sum_{p+q=i} \mathscr{F}_p(M)\mathscr{F}_q(M')$ for $i \geqslant 0$.
(iii) Let $\mathfrak{A}$ be an ideal of R. Then

$$\mathscr{F}_i(R/\mathfrak{A}) = \begin{cases} \mathfrak{A} & \text{for } i = 0, \\ R & \text{for } i \neq 0. \end{cases}$$

By properties (ii) and (iii) the Fitting ideals characterize finitely generated modules over a principal ideal domain.

(iv) If M is generated by s elements, then

$$(\mathrm{Ann}_R M)^s \subseteq \mathscr{F}_0(M) \subseteq \mathrm{Ann}_R M,$$

where $\text{Ann}_R\, M$ denotes the annihilator ideal of M.

(v) Suppose that

$$0 \to F_m \xrightarrow{f_m} F_{m-1} \to \cdots \to F_1 \xrightarrow{f_1} F_0 \xrightarrow{f_0} M \to 0$$

is a finite free resolution of M. Let n be the Euler characteristic of M, i.e. $n = \sum_{i=0}^{n}(-1)^i \operatorname{rank}_R F_i$. Then $\mathscr{F}_n(M)$ is the first Fitting invariant nonzero and

$$\left(0 \underset{R}{:} \mathscr{F}_n(M)\right) = (0).$$

(vi) *Change of base.* Let $f: R \to R'$ be a homomorphism of commutative rings with unit. Then

$$\mathscr{F}_i\left(M_{(R')}\right) = \mathscr{F}_i(M)R' \qquad \text{for} \quad i \geqslant 0,$$

where $M_{(R')}$ is the R'-module obtained from M by extension of scalars.

MacRae's Invariant

We say that an R-module K is elementary if there exists an exact sequence of the form

$$0 \to R^n \to R^n \to K \to 0.$$

If K is an elementary R-module, then $\mathscr{F}_0(K)$ is a principal ideal generated by a non-zero-divisor of R.

Let M be an R-module. An exact sequence

$$0 \to K_m \to K_{m-1} \to \cdots \to K_1 \to K_0 \to M \to 0$$

where each K_i is elementary will be called a finite elementary resolution of M of length m. In this situation MacRae [6] proves:

(i) The function

$$G(M) = \mathscr{F}_0(K_0)\mathscr{F}_0(K_1)^{-1}\mathscr{F}_0(K_2) \cdots \mathscr{F}_0(K_m)^{(-1)^m} = \frac{\alpha}{\beta}R,$$

where $\alpha, \beta \in R$ are non-zero-divisors, is an invariant associated to M, i.e., it is independent of the finite elementary resolution of M chosen.

(ii) $G(M)$ is the smallest principal ideal of R containing $\mathscr{F}_0(M)$. It is necessarily generated by a non-zero-divisor.

We shall refer to $G(M)$ as the MacRae invariant of M.

PROPOSITION 1.1.

(i) Additivity. *If* $0 \to M' \to M \to M'' \to 0$ *is an exact sequence of R-modules that have finite elementary resolutions, then*

$$G(M) = G(M')G(M'').$$

(ii) Change of base. *Let* $f: R \to R'$ *be a homomorphism of commutative rings with unit. If M is an R-module that has a finite elementary resolution and if* $M_{(R')}$ *(the module obtained from M by extension of scalars) also has a finite elementary resolution over* R', *then*

$$G(M_{(R')}) \subseteq G(M)R'.$$

Proof. (i): See [6].
(ii): As we have just noticed, we know that $\mathscr{F}_0(M) \subseteq G(M)$, so

$$\mathscr{F}_0(M_{(R')}) = \mathscr{F}_0(M)R' \subseteq G(M)R',$$

where the equality is due to the behavior of Fitting invariants under change of rings. Hence $G(M)R'$ is a principal ideal containing $\mathscr{F}_0(M_{(R')})$, but $G(M_{(R')})$ is the smallest ideal in this situation. The desired conclusion then follows. ■

The R[X]-Module Associated to an Endomorphism of an R-Module

Let M be an R-module, and let $u: M \to M$ be an R-homomorphism. The endomorphism u converts M into an $R[X]$-module by $Xm = u(m)$. We denote M as $R[X]$-module via u by M_u. Let $\tilde{u}$ denote the $R[X]$-endomorphism of $M[X]$ obtained from u by extension of scalars.

In this context, there is a *characteristic sequence* [2, p. 106]

$$0 \to M[X] \xrightarrow{\psi} M[X] \xrightarrow{\varphi} M_u \to 0,$$

which is an exact sequence of $R[X]$-modules, where $\varphi(\sum m_i X^i) = \sum u^i(m_i)$ and $\psi = t_X - \tilde{u}$, where t_X denotes multiplication by X. In particular, when

$M = R^n$ the characteristic sequence proves that $(R^n)_u$ is an elementary $R[X]$-module and moreover

$$(\chi(u, X)) = \mathscr{F}_0((R^n)_u) = G((R^n)_u).$$

Let N be an $R[X]$-module. We denote by $\overline{N}$ the R-module obtained from N by restriction of scalars. If t_X is the multiplication by X over $\overline{N}$, then $(\overline{N})_{t_X} = N$. Conversely, if M and u are as above, then $\overline{M_u} = M$ and so $(\overline{M_u})_{t_X} = M_u$.

Proposition 1.2. *Let $f: R \to R'$ be a ring homomorphism.*

(i) *If M is an R-module and u is an endomorphism of M, then the $R'[X]$-modules $(M_{(R')})_{u_{(R')}}$ and $(M_u)_{(R'[X])}$ are isomorphic, where $u_{(R')}$ is the R'-endomorphism of $M_{(R')}$ obtained from u by extension of scalars. Consequently the R'-modules $\overline{(M_{(R')})_{u_{(R')}}}$ and $\overline{(M_u)_{(R'[X])}}$ are isomorphic.*

(ii) *If N is an $R[X]$-module, then the R'-modules $\overline{N}_{(R')}$ and $\overline{N_{(R'[X])}}$ are isomorphic.*

Proof. (i): From the characteristic sequence of u by extension of scalars we obtain the exact sequence of $R'[X]$-modules

$$M[X]_{(R'[X])} \xrightarrow{(t_X - \tilde{u})_{(R'[X])}} M[X]_{(R'[X])} \to (M_u)_{(R'[X])} \to 0,$$

or equivalently, we have the exact sequence of $R'[X]$-modules

$$M_{(R')}[X] \xrightarrow{\psi = t_X - u_{(R')}} M_{(R')}[X] \to (M_u)_{(R'[X])} \to 0.$$

By comparison with the characteristic sequence of $u_{(R')}$ it follows that the $R'[X]$-modules $(M_{(R')})_{u_{(R')}}$ and $(M_u)_{(R'[X])}$ are isomorphic.

(ii): Since $(\overline{N})_{t_X} = N$, it follows that $((\overline{N})_{t_X})_{(R'[X])} = N_{(R'[X])}$. Now by (i) we have that $(\overline{N}_{(R')})_{t_X} \cong ((\overline{N})_{t_X})_{(R'[X])}$. Therefore $N_{(R'[X])} \cong (\overline{N}_{(R')})_{t_X}$ and hence

$$\overline{N_{(R'[X])}} \cong \overline{(\overline{N}_{(R')})_{t_X}} = \overline{N}_{(R')}. \qquad \blacksquare$$

Proposition 1.3. *Let M and M' be two R-modules, and u and u' endomorphisms of M and M' respectively. If $g: M \to M'$ is an R-homomorphism, then the following conditions are equivalent:*

(i) $gu = u'g$.
(ii) $g : M_u \to M'_{u'}$ *is a homomorphism of* $R[X]$*-modules.*

Furthermore, in this situation the diagram (whose rows are characteristic exact sequences)

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & M[X] & \xrightarrow{\psi} & M[X] & \xrightarrow{\varphi} & M_u & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \tilde{g}} & & \downarrow{\scriptstyle \tilde{g}} & & \downarrow{\scriptstyle g} & & \\
0 & \longrightarrow & M'[X] & \xrightarrow{\psi'} & M'[X] & \xrightarrow{\varphi'} & M'_{u'} & \longrightarrow & 0
\end{array}
$$

is commutative.

Proof. See [2, p. 106]. ∎

The above behavior of the characteristic sequence can be generalized to an exact sequence of R-modules. We describe a particular situation that we shall use throughout this paper. If we have a diagram of R-modules

$$
\begin{array}{ccccccccccccccc}
0 & \longrightarrow & F_m & \xrightarrow{f_m} & F_{m-1} & \longrightarrow & \cdots & \longrightarrow & F_1 & \xrightarrow{f_1} & F_0 & \xrightarrow{f_0} & M & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle u_m} & & \downarrow{\scriptstyle u_{m-1}} & & & & \downarrow{\scriptstyle u_1} & & \downarrow{\scriptstyle u_0} & & \downarrow{\scriptstyle u} & & \\
0 & \longrightarrow & F_m & \xrightarrow{f_m} & F_{m-1} & \longrightarrow & \cdots & \longrightarrow & F_1 & \xrightarrow{f_1} & F_0 & \xrightarrow{f_0} & M & \longrightarrow & 0
\end{array}
$$

commutative and exact where F_i is a finitely generated free module, then the diagram of $R[X]$-modules

$$
\begin{array}{ccccccccccccccc}
 & & 0 & & 0 & & & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & F_m[X] & \xrightarrow{\tilde{f}_m} & F_{m-1}[X] & \longrightarrow & \cdots & \longrightarrow & F_1[X] & \xrightarrow{\tilde{f}_1} & F_0[X] & \xrightarrow{\tilde{f}_0} & M[X] & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \psi_m} & & \downarrow{\scriptstyle \psi_{m-1}} & & & & \downarrow{\scriptstyle \psi_1} & & \downarrow{\scriptstyle \psi_0} & & \downarrow{\scriptstyle \psi} & & \\
0 & \longrightarrow & F_m[X] & \xrightarrow{\tilde{f}_m} & F_{m-1}[X] & \longrightarrow & \cdots & \longrightarrow & F_1[X] & \xrightarrow{\tilde{f}_1} & F_0[X] & \xrightarrow{\tilde{f}_0} & M[X] & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \varphi_m} & & \downarrow{\scriptstyle \varphi_{m-1}} & & & & \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_0} & & \downarrow{\scriptstyle \varphi} & & \\
0 & \longrightarrow & (F_m)_{u_m} & \xrightarrow{f_m} & (F_{m-1})_{u_{m-1}} & \longrightarrow & \cdots & \longrightarrow & (F_1)_{u_1} & \xrightarrow{f_1} & (F_0)_{u_0} & \xrightarrow{f_0} & M_u & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & & & 0 & & 0 & & 0 & &
\end{array}
$$

is commutative with exact rows and columns. So if M has a finite free resolution over R, then M_u has an elementary resolution of finite length over $R[X]$, because, as we noticed before, $(F_i)_{u_i}$ is elementary for $0 \leqslant i \leqslant m$.

2. CHARACTERISTIC POLYNOMIAL

For short, in the sequel, we shall denote by $\mathbb{F}_R$ the class of R-modules that have a finite free resolution. If $M \in \mathbb{F}_R$, we denote by $\mathrm{Char}_R\, M$ the Euler characteristic of M.

THEOREM 2.1. *Let $M \in \mathbb{F}_R$, and let u be an endomorphism of M. Then the MacRae invariant $G(M_u)$ of the $R[X]$-module M_u is generated by a monic polynomial of degree* $\mathrm{Char}_R\, M$.

Proof. Let

$$0 \to F_m \xrightarrow{f_m} F_{m-1} \to \cdots \to F_1 \xrightarrow{f_1} F_0 \xrightarrow{f_0} M \to 0$$

be a finite free resolution of M. Then for $u : M \to M$ we have a commutative diagram

$$\begin{array}{ccccccccccccc}
0 & \longrightarrow & F_m & \xrightarrow{f_m} & F_{m-1} & \longrightarrow & \cdots & \longrightarrow & F_1 & \xrightarrow{f_1} & F_0 & \xrightarrow{f_0} & M & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle u_m} & & \downarrow{\scriptstyle u_{m-1}} & & & & \downarrow{\scriptstyle u_1} & & \downarrow{\scriptstyle u_0} & & \downarrow{\scriptstyle u} & & \\
0 & \longrightarrow & F_m & \xrightarrow{f_m} & F_{m-1} & \longrightarrow & \cdots & \longrightarrow & F_1 & \xrightarrow{f_1} & F_0 & \xrightarrow{f_0} & M & \longrightarrow & 0
\end{array}$$

with exact rows, where the u_i are liftings of u. Therefore we obtain the elementary resolution of the $R[X]$-module M_u

$$0 \to (F_m)_{u_m} \to (F_{m-1})_{u_{m-1}} \to \cdots \to (F_1)_{u_1} \to (F_0)_{u_0} \to M_u \to 0.$$

By the definition of MacRae invariant,

$$G(M_u) = \prod_{i=0}^{m} \left(\mathscr{F}_0((F_i)_{u_i})\right)^{(-1)^i} = \prod_{i=0}^{m} (\chi(u_i, X))^{(-1)^i}.$$

Since $G(M_u)$ is a principal ideal of $R[X]$, it follows that the polynomial

$$\prod_{\substack{0 \leqslant i \leqslant m \\ i \text{ odd}}} \chi(u_i, X)$$

divides the polynomial

$$\prod_{\substack{0 \leqslant i \leqslant m \\ i \text{ even}}} \chi(u_i, X).$$

The quotient polynomial

$$\frac{\prod_{\substack{0 \leqslant i \leqslant m \\ i \text{ even}}} \chi(u_i, X)}{\prod_{\substack{0 \leqslant i \leqslant m \\ i \text{ odd}}} \chi(u_i, X)}$$

has degree

$$\sum_{\substack{0 \leqslant i \leqslant m \\ i \text{ even}}} \operatorname{rank} F_i - \sum_{\substack{0 \leqslant i \leqslant m \\ i \text{ odd}}} \operatorname{rank} F_i = \operatorname{Char}_R M,$$

and it is monic, being a quotient of monic polynomials. ■

DEFINITION 2.2. Let $M \in \mathbb{F}_R$, and let u be an endomorphism of M. We define the characteristic polynomial of u, as the only monic generator of $G(M_u)$, and denote it as $\chi(u, X)$.

REMARK 2.3.

(i) $\chi(u, X)$ is an invariant associated to u and M, that is, it does not depend on the finite free resolution or the morphism u_i chosen for its construction.

(ii) If M is a finite free R-module, this definition gives the classic characteristic polynomial.

(iii) If $\operatorname{Char}_R M = 0$, then $\chi(u, X) = 1$ for every endomorphism u of M.

(iv) O. Goldman [4] and G. Almkvist [1] gave two different extensions to the concept of characteristic polynomial of an endomorphism of a finitely generated projective module, as we noticed before. When these two definitions and the previous one apply (i.e., M is supplementable projective), then all of them give the same polynomial.

PROPOSITION 2.4. *Let $M \in \mathbb{F}_R$ and let u be an endomorphism of M.*

(i) *If M' and M'' are R-modules that have finite free resolutions and*

$$\begin{array}{ccccccccc}
0 & \longrightarrow & M'' & \longrightarrow & M & \longrightarrow & M' & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle u''} & & \downarrow{\scriptstyle u} & & \downarrow{\scriptstyle u'} & & \\
0 & \longrightarrow & M'' & \longrightarrow & M & \longrightarrow & M' & \longrightarrow & 0
\end{array}$$

is a commutative diagram of R-modules with exact rows, then

$$\chi(u, X) = \chi(u'', X)\chi(u', X).$$

(ii) *If v is another endomorphism of M, then $\chi(uv, X) = \chi(vu, X)$, and if v is an isomorphism then $\chi(v^{-1}uv, X) = \chi(u, X)$.*

Proof. (i): It follows from Proposition 1.1.
(ii): Let

$$0 \to F_m \xrightarrow{f_m} F_{m-1} \to \cdots \to F_1 \xrightarrow{f_1} F_0 \xrightarrow{f_0} M \to 0$$

be a finite free resolution of M, and let $\{u_i\}_{0 \leqslant i \leqslant m}$ and $\{v_i\}_{0 \leqslant i \leqslant m}$ be families of liftings of u and v respectively. Then $\{u_i v_i\}_{0 \leqslant i \leqslant m}$ and $\{v_i u_i\}_{0 \leqslant i \leqslant m}$ are families of liftings of uv and vu respectively.

Now the result follows from the construction that we have established for the characteristic polynomial and to the fact that the property is true for finite free R-modules. ■

Let $f : R \to R'$ be a homomorphism of rings with unit. If $p(X) = a_r X^r + \cdots + a_0 \in R[X]$, we denote by $f(p(X))$ the polynomial of $R'[X]$ given by $f(p(X)) = f(a_r)X^r + \cdots + f(a_0)$.

PROPOSITION 2.5. *Let $M \in \mathbb{F}_R$, let u be an endomorphism of M, and let $f : R \to R'$ be a homomorphism of rings with unit.*

(i) *If $M_{(R')} \in \mathbb{F}_{R'}$, then the polynomial $f(\chi(u, X))$ divides $\chi(u_{(R')}, X)$.*
(ii) $\mathrm{Char}_R\, M = \mathrm{Char}_{R'}\, M_{(R')}$ *if and only if the two polynomials are equal.*

Proof. (i): Using the isomorphism (see Proposition 1.2)

$$(M_{(R')})_{u_{(R')}} \cong (M_u)_{(R'[X])}$$

and the behavior of MacRae invariant under ring extensions, Proposition 1.1, we have the desired result. ■

REMARK 2.6. Let R be an integral domain, K its quotient field, $M \in \mathbb{F}_R$, and u be an endomorphism of M. Then $\chi(u, X)$ is the classical characteristic polynomial of $u_{(K)}$.

In the same situation, if M is a finitely generated R-module but $M \notin \mathbb{F}_R$, the characteristic polynomial of $u_{(K)}$ can have its coefficients in $K - R$, as the next example will show: Let $R = \mathbb{C}[[Z, T]]/(T^2 - Z^3)$, $M = (Z, T)/(T^2 - Z^3)$, and

$$M \xrightarrow{u} M,$$

$$\bar{Z} \to -\bar{T},$$

$$\bar{T} \to -\bar{Z}^2,$$

where $\bar{Z}$ is the canonical image of Z in M. Then M has no finite free resolution over R (because R is not a regular local ring), and

$$\chi(u_{(K)}, X) = X + \frac{\bar{T}}{\bar{Z}}.$$

We denote by Spec R the set of prime ideals of R with the Zariski topology and by Min R the set of minimal prime ideals of R. Under the assumptions of Theorem 2.1, the next result will allow us to look at the characteristic polynomial $\chi(u, X)$ as a generic polynomial in Spec R with respect to the endomorphisms induced by u passing to the residue fields.

Let $M \in \mathbb{F}_R$, and let u be an endomorphism of M. If $\mathfrak{p}$ is a prime ideal of R, we denote by $k(\mathfrak{p})$ the residue field of $\mathfrak{p}$, i.e. $k(\mathfrak{p}) = R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$; by $M(\mathfrak{p})$ the finite dimensional $k(\mathfrak{p})$-vector space $M_{(k(\mathfrak{p}))}$; by $u(\mathfrak{p})$ the endomorphism induced by u in $M(\mathfrak{p})$; and by $\pi_{\mathfrak{p}}$ the canonical homomorphism from R to $k(\mathfrak{p})$. Finally we denote by $C_r(M)$ the set

$$C_r(M) = \{\mathfrak{p} \in \operatorname{Spec} R \mid \dim_{k(\mathfrak{p})} M(\mathfrak{p}) = r\},$$

where $r \geqslant 0$ is an integer.

Observe that

$$C_r(M) = D(\mathscr{F}_r(M)) \cap V(\mathscr{F}_{r-1}(M)) \qquad \text{for} \quad r > 0$$

and

$$C_0(M) = D(\mathscr{F}_0(M)),$$

where

$$D(\mathcal{F}_r(M)) = \{\mathfrak{p} \in \operatorname{Spec} R \mid \mathcal{F}_r(M) \not\subset \mathfrak{p}\},$$

$$V(\mathcal{F}_{r-1}(M)) = \{\mathfrak{p} \in \operatorname{Spec} R \mid \mathcal{F}_{r-1}(M) \subseteq \mathfrak{p}\}.$$

THEOREM 2.7. *Let $M \in \mathbb{F}_R$ with $\operatorname{Char}_R M = n$, and let u be an endomorphism of M.*

(i) *$\pi_{\mathfrak{p}}(\chi(u, X))$ divides $\chi(u(\mathfrak{p}), X)$ for each prime ideal $\mathfrak{p}$ of R, and $\pi_{\mathfrak{p}}(\chi(u, X)) = \chi(u(\mathfrak{p}), X)$ if and only if $\mathfrak{p} \in C_n(M) = D(\mathcal{F}_n(M))$.*

(ii) *$\operatorname{Min} R \subseteq C_n(M)$, and in consequence $C_n(M)$ is a dense open set of* Spec *R.*

(iii) *$C_n(M) = \operatorname{Spec} R$ if and only if M is supplementable projective.*

Proof. (i): If $n > 0$, by property (v) of the Fitting ideals we have $\mathcal{F}_{n-1}(M) = 0$. Therefore

$$C_n(M) = D(\mathcal{F}_n(M)) \cap V(\mathcal{F}_{n-1}(M)) = D(\mathcal{F}_n(M)).$$

Since

$$C_n(M) = \left\{\mathfrak{p} \in \operatorname{Spec} R \,\middle|\, \operatorname{Char}_R M = \operatorname{Char}_{k(\mathfrak{p})} M(\mathfrak{p}) = \dim_{k(\mathfrak{p})} M(\mathfrak{p})\right\},$$

the result follows from Proposition 2.5.

(ii): Let $\mathfrak{p}$ be a minimal prime ideal of R. Suppose that $\mathfrak{p}$ is not in $C_n(M)$, i.e. $\mathcal{F}_n(M) \subseteq \mathfrak{p}$. Then by property (vi) of the Fitting ideals we have

$$\mathcal{F}_n(M_{\mathfrak{p}}) = \mathcal{F}_n(M) R_{\mathfrak{p}} \subseteq \mathfrak{p} R_{\mathfrak{p}} = \mathcal{N}(R_{\mathfrak{p}}),$$

where $\mathcal{N}(R_{\mathfrak{p}})$ is the set of nilpotents of $R_{\mathfrak{p}}$.

If $\mathcal{F}_n(M)$ is generated by $a_0, \dots, a_t$, then because $a_i/1$ is nilpotent in $R_{\mathfrak{p}}$, it follows that the polynomial

$$g(X) = \frac{a_0}{1} + \frac{a_1}{1} X + \cdots + \frac{a_t}{1} X^t$$

is nilpotent in $R_{\mathfrak{p}}[X]$. However, since the Euler characteristic of $M_{\mathfrak{p}}$ is n, by property (v) of the Fitting ideals we have

$$\left(0 \underset{R_{\mathfrak{p}}}{:} \mathcal{F}_n(M_{\mathfrak{p}})\right) = 0,$$

or equivalently, that $g(X)$ is a non-zero-divisor on $R_{\mathfrak{p}}[X]$. This concludes the proof by contradiction.

(iii): Since $\mathscr{F}_{n-1}(M) = 0$ (see [8, p. 123]), we have $\mathscr{F}_n(M) = R$ if and only if M is projective of constant rank. But under the assumption of M having a finite free resolution, M is projective if and only if M is supplementable projective (see [8, Theorem 14, p. 70]). ∎

3. CAYLEY-HAMILTON THEOREM

Our next aim is to give a reasonable extension of the Cayley-Hamilton theorem, i.e., $\chi(u, u) = 0$, where $u : R^n \to R^n$ is a homomorphism. The proof of this result is an immediate consequence of the invariants that we are using. Precisely, we have

$$(\chi(u, X)) = G((R^n)_u) = \mathscr{F}_0((R^n)_u) \subseteq \operatorname{Ann}_{R[X]}(R^n)_u,$$

so $\chi(u, X)$ belongs to $\operatorname{Ann}_{R[X]}(R^n)_u$, or equivalently, $\chi(u, u) = 0$.

However, in general, even if the module has a finite free resolution, this Cayley-Hamilton result does not hold. To notice this, it is enough to consider a nonzero module with Euler characteristic zero. Even more, there can be found endomorphisms of modules with positive Euler characteristic for which the result fails: Let $R = \mathbb{Z}$, $M = \mathbb{Z} \oplus \mathbb{Z}/(2)$, and $u(n, \overline{m}) = (0, \overline{m})$. Then, considering the commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & R & \xrightarrow{(0\ 2)} & R^2 & \longrightarrow & M & \longrightarrow & 0 \\
 & & \Big\downarrow{\scriptstyle \mathrm{Id}} & & \Big\downarrow{\scriptstyle 0 \oplus \mathrm{Id}} & & \Big\downarrow{\scriptstyle u} & & \\
0 & \longrightarrow & R & \xrightarrow{(0\ 2)} & R^2 & \longrightarrow & M & \longrightarrow & 0
\end{array}$$

with exact rows, we have $\chi(u, X) = X$, so $\chi(u, u) = u \neq 0$.

THEOREM 3.1 (Cayley-Hamilton generalized). *Let $M \in \mathbb{F}_R$ with $\operatorname{Char}_R M = n$, and let u be an endomorphism of M. Then for every $\Delta \in \mathscr{F}_n(M)$ we have*

$$\Delta \chi(u, u) = 0.$$

Proof. Firstly we shall see the inclusion

$$\mathscr{F}_n(M)(\chi(u, X)) \subseteq \mathscr{F}_0(M_u).$$

Let

$$0 \to F_m \xrightarrow{f_m} F_{m-1} \xrightarrow{f_{m-1}} \cdots \xrightarrow{f_2} F_1 \xrightarrow{f_1} F_0 \xrightarrow{f_0} M \to 0$$

be a finite free resolution of M. Following the notation of Section 1, the diagram of $R[X]$-modules

$$\begin{array}{ccccccc}
F_1[X] & \xrightarrow{\tilde{f}_1} & F_0[X] & \xrightarrow{\tilde{f}_0} & M[X] & \longrightarrow & 0 \\
\downarrow{\scriptstyle \psi_1} & & \downarrow{\scriptstyle \psi_0} & & \downarrow{\scriptstyle \psi} & & \\
F_1[X] & \xrightarrow{\tilde{f}_1} & F_0[X] & \xrightarrow{\tilde{f}_0} & M[X] & \longrightarrow & 0 \\
\downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_0} & & \downarrow{\scriptstyle \varphi} & & \\
(F_1)_{u_1} & \xrightarrow{\tilde{f}_1} & (F_0)_{u_0} & \xrightarrow{\tilde{f}_0} & M_u & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \\
0 & & 0 & & 0 & &
\end{array}$$

is commutative with exact rows and columns. Then, by a diagram chase, we obtain the exact sequence of $R[X]$-modules

$$F_1[X] \oplus F_0[X] \xrightarrow{f_1 + \psi_0} F_0[X] \xrightarrow{f_0 \varphi_0} M_u \to 0.$$

Let $\mathscr{B}_1$ and $\mathscr{B}_0$ be bases of F_1 and F_0 respectively; we obtain in a natural way bases $\mathscr{B}$ and $\mathscr{B}'$ of $F_1[X] \oplus F_0[X]$ and $F_0[X]$ respectively. If f_1 and u_0 are represented by the matrices

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1s} \\ a_{21} & a_{22} & \cdots & a_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ a_{r1} & a_{r2} & \cdots & a_{rs} \end{pmatrix}, \qquad B = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1s} \\ b_{21} & b_{22} & \cdots & b_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ b_{s1} & b_{s2} & \cdots & b_{ss} \end{pmatrix}$$

in the bases $\mathscr{B}_1$ and $\mathscr{B}_0$ respectively, then $\tilde{f}_1 + \psi_0$ is represented by the matrix

$$C = \begin{pmatrix} A \\ XI - B \end{pmatrix}$$

in the bases $\mathscr{B}$ and $\mathscr{B}'$.

By definition of Fitting invariants we have that $\mathscr{F}_n(M)$ is the ideal of R generated by all the $(s-n)\times(s-n)$ minors of A, and $\mathscr{F}_0(M_u)$ is the ideal of $R[X]$ generated by all the $s\times s$ minors of C.

Let $\Delta\in\mathscr{F}_n(M)$ be the $(s-n)\times(s-n)$ minor of A defined by the rows $\{i_1,\dots,i_{s-n}\}$ and the columns $\{j_1,\dots,j_{s-n}\}$ with $1\leqslant i_1<\cdots<i_{s-n}\leqslant r$ and $1\leqslant j_1<\cdots<j_{s-n}\leqslant s$. If A' is the $(s-n)\times s$ submatrix of A defined by the rows $\{i_1,\dots,i_{s-n}\}$, and B' the $n\times s$ submatrix of $XI-B$ whose rows are obtained by striking out $\{j_1,\dots,j_{s-n}\}$ from $\{1,\dots,s\}$, then

$$C'=\begin{pmatrix}A'\\B'\end{pmatrix}$$

is an $s\times s$ submatrix of C, and therefore we have

$$\det C'\in\mathscr{F}_0(M_u)\subseteq(\chi(u,X)).$$

By the construction of C',

$$\det C'=\pm\Delta X^n+\text{terms of less degree in } X,$$

and since $\chi(u,X)$ is a monic polynomial of degree n which divides $\det C'$, it follows that

$$\det C'=\pm\Delta\chi(u,X).$$

In consequence, we have

$$\Delta\chi(u,X)\in\mathscr{F}_0(M_u).$$

Because the $(s-n)\times(s-n)$ minors of A generate $\mathscr{F}_n(M)$, we obtain the desired inclusion

$$\mathscr{F}_n(M)(\chi(u,X))\subseteq\mathscr{F}_0(M_u).$$

Finally, since the first Fitting invariant of a module is always included in the annihilator of the module [property (iv) of the Fitting ideals], we have

$$\begin{aligned}\mathscr{F}_n(M)(\chi(u,X))&\subseteq\mathscr{F}_0(M_u)\\&\subseteq\operatorname{Ann}_{R[X]}M_u=\{p(X)\in R[X]\,|\,p(u)\equiv 0\}.\end{aligned}$$

Hence for each $\Delta\in\mathscr{F}_n(M)$ we obtain $\Delta\chi(u,X)\in\operatorname{Ann}_{R[X]}M_u$, or equivalently, $\Delta\chi(u,u)=0$. ■

COROLLARY 3.2. *If*

$$\left(0 \underset{M}{:} \mathscr{F}_n(M)\right) = 0,$$

then the classical Cayley-Hamilton theorem holds, i.e. $\chi(u, u) = 0$.

REMARK 3.3. The above situation is what happens when M is a supplementable projective module, in particular when M is free, because $\mathscr{F}_n(M) = R$.

PROPOSITION 3.4. *Let* $M \in \mathbb{F}_R$, *let* u *be an endomorphism of* M, *and let* $\mathfrak{p}$ *be a prime ideal of* R. *If* $\chi(u, u) = 0$, *then the principal* $k(\mathfrak{p})[X]$*-ideals* $(\chi(u(\mathfrak{p}), X))$ *and* $\left(\pi_{\mathfrak{p}}(\chi(u, X))\right)$ *have the same radical ideal. Hence, the roots of* $\chi(u(\mathfrak{p}), X)$ *and* $\pi_{\mathfrak{p}}(\chi(u, X))$ *in the algebraic closure of* $k(\mathfrak{p})$ *are the same except for multiplicities.*

Proof. For an ideal $\mathfrak{A}$ we denote by $\sqrt{\mathfrak{A}}$ the radical ideal of $\mathfrak{A}$. Since $\pi_{\mathfrak{p}}(\chi(u, X))$ divides $\chi(u(\mathfrak{p}), X)$, we have

$$\sqrt{(\chi(u(\mathfrak{p}), X))} \subseteq \sqrt{\left(\pi_{\mathfrak{p}}(\chi(u, X))\right)}.$$

Reciprocally, our assumption $\chi(u, u) = 0$ ensures that

$$\chi(u, X) \in \operatorname{Ann}_{R[X]} M_u$$

and therefore

$$\pi_{\mathfrak{p}}(\chi(u, X)) \in \operatorname{Ann}_{k(\mathfrak{p})[X]} M(\mathfrak{p})_{u(\mathfrak{p})}.$$

By property (iv) of the Fitting ideals we know

$$\sqrt{\mathscr{F}_0\left(M(\mathfrak{p})_{u(\mathfrak{p})}\right)} = \sqrt{\operatorname{Ann}_{k(\mathfrak{p})[X]} M(\mathfrak{p})_{u(\mathfrak{p})}},$$

and since

$$\mathscr{F}_0\left(M(\mathfrak{p})_{u(\mathfrak{p})}\right) = (\chi(u(\mathfrak{p}), X)),$$

we obtain

$$\begin{aligned}\pi_{\mathfrak{p}}(\chi(u,X)) &\in \operatorname{Ann}_{k(\mathfrak{p})[X]} M(\mathfrak{p})_{u(\mathfrak{p})}\\ &\subseteq \sqrt{\mathscr{F}_0(M(\mathfrak{p})_{u(\mathfrak{p})})} = \sqrt{(\chi(u(\mathfrak{p}),X))}. \qquad \blacksquare\end{aligned}$$

4. INVARIANT FACTORS

Let M be an R-module with $M \in \mathbb{F}_R$, and u an endomorphism of M. Let $\wedge^r M_u$ be the rth exterior power of M_u, and suppose that $\overline{\wedge^r M_u} \in \mathbb{F}_R$ for each $r \geqslant 0$. We denote by $\chi_r(u, X)$ the characteristic polynomial of

$$t_X\colon \overline{\wedge^r M_u} \to \overline{\wedge^r M_u}.$$

With this notation $\chi(u, X)$ becomes $\chi_1(u, X)$.

Since

$$\wedge^r M_u = \left(\overline{\wedge^r M_u}\right)_{t_X},$$

by property (ii) of MacRae's invariant it follows that $(\chi_r(u, X))$ is the smallest principal ideal of $R[X]$ containing $\mathscr{F}_0(\wedge^r M_u)$.

REMARK 4.1. Note that for a finite dimensional vector space V and an endomorphism u of V the following are equivalent:

(i) The knowledge of the invariant factors of u.
(ii) The knowledge of the ideals $\mathscr{F}_r(V_u)$ for $r \geqslant 0$.
(iii) The knowledge of the ideals $\mathscr{F}_0(\wedge^r V_u)$ for $r \geqslant 0$.
(iv) The knowledge of the polynomials $\chi_r(u, X)$ for $r \geqslant 0$.

Let us state the relations between the invariant factors $\{d_i(u, X)\}_{1 \leqslant i \leqslant t}$ and the invariants $\{\chi_r(u, X)\}_{r \geqslant 1}$: Given the invariant factors $\{d_i(u, X)\}_{1 \leqslant i \leqslant t}$ with $d_i(u, X)$ dividing $d_{i+1}(u, X)$, we have

$$\chi_r(u, X) = \begin{cases} \displaystyle\prod_{i=1}^{t-(r-1)} (d_i(u, X))^{\binom{t-i}{r-1}} & \text{if } 0 < r \leqslant t, \\ 1 & \text{if } r > t \end{cases}$$

Conversely, given the invariants $\{\chi_r(u, X)\}_{r \geqslant 1}$, we have:

(a) The number of proper invariant factors of u is

$$t = \max\{r \in \mathbb{N} \mid \wedge^r V_u \neq 0\} = \max\{r \in \mathbb{N} \mid \chi_r(u, X) \neq 1\}.$$

(b) The first invariant factor of u is

$$d_1(u, X) = \chi_t(u, X),$$

and

$$d_r(u, X) = \frac{\chi_{t-(r-1)}(u, X)}{\prod_{i=1}^{r-1}(d_i(u, X))^{\binom{t-i}{t-r}}}.$$

Proposition 4.2. *For every prime ideal $\mathfrak{p}$ of R, $\pi_{\mathfrak{p}}(\chi_r(u, X))$ divides $\chi_r(u(\mathfrak{p}), X)$. Furthermore there exists a dense open set $C_r(M, u)$ of* Spec R *such that $\pi_{\mathfrak{p}}(\chi_r(u, X)) = \chi_r(u(\mathfrak{p}), X)$ for $\mathfrak{p} \in C_r(M, u)$.*

Proof. Let $\mathfrak{p}$ be a prime ideal of R. Since $\chi_r(u, X)$ is the characteristic polynomial of

$$t_X : \overline{\wedge^r M_u} \to \overline{\wedge^r M_u},$$

by Theorem 2.7 it follows that $\pi_{\mathfrak{p}}(\chi_r(u, X)$ divides the characteristic polynomial of

$$t_X(\mathfrak{p}) : (\overline{\wedge^r M_u})(\mathfrak{p}) \to (\overline{\wedge^r M_u})(\mathfrak{p}).$$

By (ii) of Proposition 1.2 we have

$$(\overline{\wedge^r M_u})(\mathfrak{p}) \cong \overline{(\wedge^r M_u)_{(k(\mathfrak{p})[X])}},$$

and using the good behavior of the exterior product with the tensor product combined with (i) of Proposition 1.2, we obtain

$$\overline{(\wedge^r M_u)_{(k(\mathfrak{p})[X])}} \cong \overline{\wedge^r((M_u)_{(k(\mathfrak{p})[X])})} \cong \overline{\wedge^r M(\mathfrak{p})_{u(\mathfrak{p})}}.$$

Hence the $k(\mathfrak{p})$-vector spaces $(\overline{\wedge^r M_u})(\mathfrak{p})$ and $\overline{\wedge^r M(\mathfrak{p})_{u(\mathfrak{p})}}$ are isomorphic, and the homomorphisms

$$t_X(\mathfrak{p}) : (\overline{\wedge^r M_u})(\mathfrak{p}) \to (\overline{\wedge^r M_u})(\mathfrak{p}),$$

$$t_X : \overline{\wedge^r M(\mathfrak{p})_{u(\mathfrak{p})}} \to \overline{\wedge^r M(\mathfrak{p})_{u(\mathfrak{p})}}$$

are equivalent. Consequently the characteristic polynomial of $t_X(\mathfrak{p})$ is $\chi_r(u(\mathfrak{p}), X)$.

Let n_r be the Euler characteristic of the R-module $\overline{\wedge^r M_u}$. By Theorem 2.7, $\pi_{\mathfrak{p}}(\chi_r(u, X)) = \chi_r(u(\mathfrak{p}), X)$ if and only if $\mathfrak{p} \in C_{n_r}(\overline{\wedge^r M_u})$, where

$$C_{n_r}(\overline{\wedge^r M_u}) = \left\{\mathfrak{p} \in \operatorname{Spec} R \,\middle|\, \dim_{k(\mathfrak{p})}(\overline{\wedge^r M_u})(\mathfrak{p}) = n_r\right\}.$$

Taking $C_r(M, u) = C_{n_r}(\overline{\wedge^r M_u})$ the last statement in the proposition follows at once. ■

We denote by $C(M, u)$ the set

$$C(M,u) = \bigcap_{r \geqslant 1} C_r(M,u) = \bigcap_{r=1}^{s} C_r(M,u),$$

which is a dense open set of Spec R; here s is the number of elements that generates M.

The following result gives the construction of the invariant factors associated to an endomorphism of a module that has a finite free resolution.

THEOREM 4.3. *Let R be a reduced ring (without nonzero nilpotent elements), $M \in \mathbb{F}_R$ with a nonzero Euler characteristic, and u be an endomorphism of M. Suppose that for each positive integer r the R-module $\overline{\wedge^r M_u}$ has a finite free resolution. Then there exist a positive integer t and t monic polynomials $d_1(u, X), d_2(u, X), \dots, d_t(u, X)$ of positive degree which are unique verifying*:

(i) $\chi(u, X) = d_1(u, X) d_2(u, X) \cdots d_t(u, X)$.

(ii) *$d_i(u, X)$ divides $d_{i+1}(u, X)$ for $1 \leqslant i \leqslant t-1$.*

(iii) *If $\mathfrak{p} \in C(M, u)$, then the invariant factors of the $k(\mathfrak{p})$-endomorphism $u(\mathfrak{p})$ are the images of $\{d_i(u, X)\}_{1 \leqslant i \leqslant t}$ in $k(\mathfrak{p})[X]$.*

Proof. Let $t = \max\{r \in \mathbb{N} \mid \chi_r(u, X) \neq 1\}$. Since for a prime ideal $\mathfrak{p}$ of R the number of proper invariant factors of $u(\mathfrak{p})$ is

$$\max\left\{r \in \mathbb{N} \middle| \wedge^r M(\mathfrak{p})_{u(\mathfrak{p})} \neq 0\right\} = \max\left\{r \in \mathbb{N} \middle| \chi_r(u(\mathfrak{p}), X) \neq 1\right\},$$

by the above proposition it follows that for every $\mathfrak{p} \in C(M, u)$ the number of invariant factors of $u(\mathfrak{p})$ is t. We denote by $d_1(u(\mathfrak{p}), X)$, $d_2(u(\mathfrak{p}), X), \ldots, d_t(u(\mathfrak{p}), X)$, with $d_i(u(\mathfrak{p}), X)$ dividing $d_{i+1}(u(\mathfrak{p}), X)$, the invariant factors of $u(\mathfrak{p})$ for $\mathfrak{p} \in C(M, u)$.

Since $d_1(u(\mathfrak{p}), X) = \chi_t(u(\mathfrak{p}), X)$, we define $d_1(u, X)$ as the monic polynomial of $R[X]$

$$d_1(u, X) = \chi_t(u, X).$$

with positive degree. By construction the image of $d_1(u, X)$ in $k(\mathfrak{p})[X]$ is $d_1(u(\mathfrak{p}), X)$ for $\mathfrak{p} \in C(M, u)$.

In order to define $d_2(u, X)$, note that $d_1(u(\mathfrak{p}), X)^{\binom{t-1}{t-2}}$ divides $\chi_{t-1}(u(\mathfrak{p}), X)$ for $\mathfrak{p} \in C(M, u)$. We shall see that in $R[X]$ one has that $d_1(u, X)^{\binom{t-1}{t-2}}$ divides $\chi_{t-1}(u, X)$.

Since the two polynomials are monic, there exist polynomials $c(X)$ and $r(X)$ in $R[X]$ such that

$$\chi_{t-1}(u, X) = c(X) d_1(u, X)^{\binom{t-1}{t-2}} + r(X),$$

where the degree of $r(X)$ is smaller than the degree of $d_1(u, X)^{\binom{t-1}{t-2}}$. Considering the above equality in $k(\mathfrak{p})[X]$ for $\mathfrak{p} \in C(M, u)$, we have

$$\pi_{\mathfrak{p}}(\chi_{t-1}(u, X)) = \pi_{\mathfrak{p}}(c(X)) \pi_{\mathfrak{p}}\left(d_1(u, X)^{\binom{t-1}{t-2}}\right) + \pi_{\mathfrak{p}}(r(X)),$$

or equivalently, by Theorem 2.7,

$$\chi_{t-1}(u(\mathfrak{p}), X) = \pi_{\mathfrak{p}}(c(X)) d_1(u(\mathfrak{p}), X)^{\binom{t-1}{t-2}} + \pi_{\mathfrak{p}}(r(X)).$$

Therefore $\pi_{\mathfrak{p}}(r(X)) = 0$ for every $\mathfrak{p} \in C(M, u)$. Since R is a reduced ring and $C(M, u)$ contains Min R, it follows that $r(X) = 0$. We define $d_2(u, X)$ as the monic polynomial of positive degree

$$d_2(u, X) = \frac{\chi_{t-1}(u, X)}{d_1(u, X)^{\binom{t-1}{t-2}}}.$$

By construction the image of $d_2(u, X)$ in $k(\mathfrak{p})[X]$ is $d_2(u(\mathfrak{p}), X)$ for $\mathfrak{p} \in C(M, u)$.

In the same way we can define $d_3(u, X), \dots, d_t(u, X)$; namely, if we have defined $d_1(u, X), d_2(u, X), \dots, d_{r-1}(u, X)$, then

$$d_r(u, X) = \frac{\chi_{t-(r-1)}(u, X)}{\prod_{i=1}^{r-1} d_i(u, X)^{\binom{t-i}{t-r}}}.$$

As we have noticed, at each step $\pi_{\mathfrak{p}}(d_1(u, X)), \pi_{\mathfrak{p}}(d_2(u, X)), \dots, \pi_{\mathfrak{p}}(d_t(u, X))$ are the invariant factors of $u(\mathfrak{p})$ for $\mathfrak{p}$ in $C(M, u)$. Conditions (i) and (ii) and the uniqueness in the theorem can be proved by the same techniques used above. ∎

DEFINITION 4.4. Let the assumptions and notation be as in Theorem 4.3. We define the invariant factors of u as the polynomials $\{d_i(u, X)\}_{1 \leqslant i \leqslant t}$.

REMARK 4.5. Let R be an integral domain, K its quotient field, $M \in \mathbb{F}_R$, and u be an endomorphism of M. Then $\{d_i(u, X)\}_{1 \leqslant i \leqslant t}$ are the classical invariant factors of $u_{(K)}$.

The explicit obtaining of the invariant factors, following the construction that we have made, is difficult because it needs the knowledge of finite free resolutions of the R-modules $\overline{\wedge^r M_u}$. The next result allows us to compute the invariant factors in an easier way.

THEOREM 4.6. *Let R be a reduced ring, $M \in \mathbb{F}_R$ with a nonzero Euler characteristic, and u be an endomorphism of M. Suppose that for each positive integer r the R-module $\overline{\wedge^r M_u}$ has a finite free resolution. If $d_1(u, X), d_2(u, X), \dots, d_t(u, X)$ with $d_i(u, X)$ dividing $d_{i+1}(u, X)$ are the invariant factors of u, then*:

(i) *For each integer r with $0 \leqslant r \leqslant t - 1$ the ideal $(\prod_{i=1}^{t-r} d_i(u, X))$ is the smallest principal ideal of $R[X]$ generated by a monic polynomial that contains $\mathcal{F}_r(M_u)$.*

(ii) *For each integer r with $r \geqslant t$ the smallest principal ideal of $R[X]$ generated by a monic polynomial that contains $\mathcal{F}_r(M_u)$ is $R[X]$.*

Proof. Firstly we prove

$$\mathcal{F}_r(M_u) \subseteq \left(\prod_{i=1}^{t-r} d_i(u, X)\right)$$

for $0 \leqslant r \leqslant t-1$.

If $\mathfrak{p}$ is a minimal prime ideal of R, then

$$\mathscr{F}_r(M(\mathfrak{p})_{u(\mathfrak{p})}) = \left(\prod_{i=1}^{t-r} d_i(u(\mathfrak{p}), X)\right),$$

by Theorem 2.7 we have

$$\left(\prod_{i=1}^{t-r} d_i(u(\mathfrak{p}), X)\right) = \left(\prod_{i=1}^{t-r} d_i(u, X)\right) k(\mathfrak{p})[X],$$

and by the property of a change of base of Fitting ideals and Proposition 1.2 we obtain

$$\mathscr{F}_r(M(\mathfrak{p})_{u(\mathfrak{p})}) = \mathscr{F}_r(M_u)k(\mathfrak{p})[X].$$

Hence

$$\mathscr{F}_r(M_u)k(\mathfrak{p})[X] = \left(\prod_{i=1}^{t-r} d_i(u, X)\right) k(\mathfrak{p})[X]$$

for each minimal prime ideal $\mathfrak{p}$ of R. Now if $p(X) \in \mathscr{F}_r(M_u)$ with $0 \leqslant r \leqslant t-1$, then $\prod_{i=1}^{t-r} \pi_{\mathfrak{p}}(d_i(u, X))$ divides $\pi_{\mathfrak{p}}(p(X))$ for each minimal prime ideal $\mathfrak{p}$ of R. In consequence the desired inclusion holds, since R is a reduced ring.

Let suppose that there exists another principal ideal $(q_r(X))$ that contains $\mathscr{F}_r(M_u)$ with $q_r(X)$ monic. For $\mathfrak{p} \in \operatorname{Min} R$ we have that

$$\mathscr{F}_r(M_u)k(\mathfrak{p})[X] = \begin{cases} \left(\prod_{i=1}^{t-r} d_i(u, X)\right) k(\mathfrak{p})[X] & \text{if} \quad 0 \leqslant r \leqslant t-1, \\ k(\mathfrak{p})[X] & \text{if} \quad r \geqslant t \end{cases}$$

is contained in $(q_r(X))k(\mathfrak{p})[X]$. Equivalently, $\pi_{\mathfrak{p}}(q_r(X))$ divides $\pi_{\mathfrak{p}}(\prod_{i=1}^{t-r} d_i(u, X))$ if $0 \leqslant r \leqslant t-1$ and $(\pi_{\mathfrak{p}}(q_r(X))) = k(\mathfrak{p})[X]$ if $r \geqslant t$. Again because R is a reduced ring and $q_r(X)$ monic, it follows that $q_r(X)$ divides $\prod_{i=1}^{t-r} d_i(u, X)$ if $0 \leqslant r \leqslant t-1$ and $(q_r(X)) = R$ if $r \geqslant t$. ■

We next apply the study of the invariant factors of u to obtaining submodules of M invariants by u.

For a polynomial $q(X) = X^r + a_{r-1}X^{r-1} + \cdots + a_0 \in R[X]$ we shall define the companion matrix of $q(X)$ as the matrix

$$D = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -a_{r-1} \end{pmatrix}.$$

If we denote by w the endomorphism of R^r given by D in the canonical base, then the $R[X]$-module $(R^r)_w$ is cyclic and consequently we have

$$\mathrm{Ann}_{R[X]}(R^r)_w = \mathscr{F}_0((R^r)_w) = (q(X)).$$

THEOREM 4.7. *Let R be an integral domain, and let M and u be as in Theorem 4.3 with M a torsion free R-module. Let $\{d_i(u, X)\}_{1 \leqslant i \leqslant t}$ be the invariant factors of u, and m_i the degree of $d_i(u, X)$. Then there exist submodules $M_1, M_2, \ldots, M_t$ of M verifying:*

(i) *M_i is a free R-module of rank m_i invariant with respect to u,* i.e. *$u(M_i) \subseteq M_i$, for $1 \leqslant i \leqslant t$.*

(ii) *M_i is a cyclic R-module for u,* i.e., *$(M_i)_{u|_{M_i}}$ is a cyclic $R[X]$-module, where $u|_{M_i}$ is the restriction of u to M_i. Hence*

$$\mathrm{Ann}_{R[X]}(M_i)_{u|_{M_i}} = (d_i(u, X)).$$

(iii) *$M_i \cap M_j = (0)$ for $i \neq j$, and the quotient R-module $M/\bigoplus_{i=1}^t M_i$ has a finite free resolution and Euler characteristic zero.*

Proof. Consider the endomorphism w of R^n given, with respect to the canonical base, by the matrix

$$D = \begin{pmatrix} D_1 & & \\ & \ddots & \\ & & D_t \end{pmatrix},$$

where $n = \mathrm{Char}_R\, M$ and D_i is the companion matrix of $d_i(u, X)$ for $1 \leqslant i \leqslant t$. If we denote by K the quotient field of R, then since

$\mathrm{Hom}_K(K^n, M_{(K)}) \cong (\mathrm{Hom}_R(R^n, M))_{(K)}$, it follows that there exist $s \in R$ with $s \neq 0$ and $f \in \mathrm{Hom}_R(R^n, M)$ such that the diagram

$$\begin{array}{ccc} K^n & \xrightarrow{f/s} & M_{(K)} \\ \Big\downarrow{\scriptstyle w_{(K)}} & & \Big\downarrow{\scriptstyle u_{(K)}} \\ K^n & \xrightarrow{f/s} & M_{(K)} \end{array}$$

is commutative and f/s is an isomorphism.

Since M is a torsion free R-module, the diagram

$$\begin{array}{ccc} R^n & \xrightarrow{f} & M \\ \Big\downarrow{\scriptstyle w} & & \Big\downarrow{\scriptstyle u} \\ R^n & \xrightarrow{f} & M \end{array}$$

is commutative. Because f/s is injective, it follows that f is injective. Hence we have that the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & R^n & \xrightarrow{f} & M & \longrightarrow & \mathrm{Coker}\, f & \longrightarrow & 0 \\ & & \Big\downarrow{\scriptstyle w} & & \Big\downarrow{\scriptstyle u} & & \Big\downarrow & & \\ 0 & \longrightarrow & R^n & \xrightarrow{f} & M & \longrightarrow & \mathrm{Coker}\, f & \longrightarrow & 0 \end{array}$$

is commutative. By [8, pp. 73, 95], $\mathrm{Coker}\, f$ has a finite free resolution and

$$\mathrm{Char}_R \, \mathrm{Coker}\, f = \mathrm{Char}_R \, M - \mathrm{Char}_R \, R^n = 0.$$

Now if S_i is the free R^n-submodule of rank m_i associated to the matrix D_i, we consider the submodule of M defined by $M_i = f(S_i)$ for $1 \leqslant i \leqslant t$. Consideration of the submodules S_i and the injectivity of f, which ensures that the R-modules S_i and M_i are isomorphic, shows the statements of the theorem. ∎

REMARK 4.8. If R is a reduced ring with a finite number of minimal prime ideals $\{\mathfrak{p}_j\}_{1 \leqslant j \leqslant p}$, then the total quotient ring is isomorphic to a product of fields

$$T(R) \cong R_{\mathfrak{p}_1} \times \cdots \times R_{\mathfrak{p}_p}.$$

Now if M and u are as in Theorem 4.3, we have

$$d_i(u(\mathfrak{p}_j), X) = \pi_{\mathfrak{p}_j}(d_i(u, X))$$

for $1 \leqslant i \leqslant t$ and $1 \leqslant j \leqslant p$. Following the notation of the previous theorem, the canonical form of the homomorphism $u(\mathfrak{p}_j)$ is

$$D = \begin{pmatrix} D_1 & & \\ & \ddots & \\ & & D_t \end{pmatrix}$$

for $1 \leqslant j \leqslant p$. Hence there exists an isomorphism f/s that makes the diagram

$$\begin{array}{ccc} T(R)^n & \xrightarrow{f/s} & M_{(T(R))} \\ \downarrow{\scriptstyle w_{(T(R))}} & & \downarrow{\scriptstyle u_{(T(R))}} \\ T(R)^n & \xrightarrow{f/s} & M_{(T(R))} \end{array}$$

commutative. Applying the same techniques as in the previous theorem, we obtain a similar result.

REFERENCES

1 G. Almkvist, Endomorphisms of finitely generated modules over a commutative ring, *Ark. Mat.* 2:263–301 (1973).
2 N. Bourbaki, *Eléments de Mathématique: Algèbre I, Ch. 1 à 3*, Hermann, Paris, 1970.
3 H. Fitting, Die determinantenideale eines moduls, *Jahresbericht Deutsch. Math.-Verein* 46:195–228 (1936).
4 O. Goldman, Determinants in projective modules, *Nagoya Math. J.* 18:27–36 (1961).
5 R. M. Guralnick, Matrix equivalence and isomorphism of modules, *Linear Algebra Appl.* 43:125–136 (1982).
6 R. E. MacRae, On an application of Fitting invariants, *J. Algebra* 2(2):153–169 (1965).
7 B. R. McDonald, *Linear Algebra over Commutative Rings*, Marcel Dekker, 1984.
8 D. G. Northcott, *Finite Free Resolutions*, Cambridge U.P., 1976.
9 M. Pisonero, Invariantes asociados a endomorfismos de modulos que admiten resoluciones libres finitas, Tesis Doctoral, Univ. Valladolid, 1990.

Received 5 June 1992; final manuscript accepted 18 August 1992