A Cayley-Hamilton-type theorem

for locally finite polynomial endomorphisms

A Bachelor thesis by

Lorijn van Rooijen

Under supervision of

Dr. Stefan Maubach

March 25, 2009

Contents

1 Introduction

The following theorem is well-known from linear algebra.

Theorem 1. [Cayley-Hamilton][1] Let ℓ be a linear endomorphism of a finite dimensional vector space, and $\mathcal{X}_\ell(T) = \det(TI - \ell)$ its characteristic polynomial. Then $\mathcal{X}_\ell$ vanishes when applied to ℓ itself: $\mathcal{X}_\ell(\ell) = 0$.

The characteristic polynomial of ℓ thus provides us with a relation of the form $\ell^n = a_0 + a_1 \cdot \ell + \ldots + a_{n-1} \cdot \ell^{n-1}$. This relation is useful, eg. for finding the inverse of ℓ, or calculating high powers of ℓ.

In this thesis, we will look at polynomial endomorphisms of $\mathbb{C}[x_1, \ldots, x_N]$.

Definition 2. A polynomial endomorphism of $\mathbb{C}[x_1, \ldots, x_N]$ is a map F: $\mathbb{C}^N \to \mathbb{C}^N$ that is an N-tuple of functions: $F = (F_1, \ldots, F_N)$, where every $F_i \in \mathbb{C}[x_1, \ldots, x_N]$. The F_i are called coordinate functions. Thus,

$$F : (x_1, \ldots, x_N) \mapsto (F_1(x_1, \ldots, x_N), \ldots, F_N(x_1, \ldots, x_N)).$$

The identity mapping, which maps $(x_1, \ldots, x_N)$ to $(x_1, \ldots, x_N)$, is denoted by I. We define $\deg F$ as $\max_{1 \leq i \leq N} \deg F_i$ and $F^i = \underbrace{F \circ F \circ \ldots \circ F}_{i}$.

For some polynomial endomorphisms of $\mathbb{C}[x_1, \ldots, x_N]$, it is easy to see that there also exists a relation of the form $F^n = a_0 + \ldots + a_{n-1} \cdot F^{n-1}$.

For example, let

$$F(x, y) = (x + y^2, y).$$

Then

$$F^2(x, y) = (x + 2y^2, y),$$

and we see that

$$(F^2 - 2 \cdot F + I)(x, y) = (0, 0)$$

From now on the all zero vector will be denoted by 0.

Another example of a polynomial endomorphism is the Nagata automorphism [2], defined as

$$F(x, y, z) = (x - 2y\Delta - z\Delta^2, y + z\Delta, z), \text{where } \Delta = xz + y^2.$$

Then

$$F^2(x,y,z) = (x - 4y\Delta - 4z\Delta^2, y + 2z\Delta, z),$$
$$F^3(x,y,z) = (x - 6y\Delta - 9z\Delta^2, y + 3z\Delta, z).$$

This leads to the relation

$$(-F^3 + 3F^2 - 3F + I)(x,y,z) = 0.$$

The question arises, how to find such a non-trivial relation for an arbitrary polynomial endomorphism, if it exists, without having to try a lot of possibilities. In the case of a linear endomorphism ℓ, the relation is easily obtained from the characteristic polynomial, which depends only on the eigenvalues of ℓ. If a polynomial endomorphism F satisfies such a relation, one would expect that, in a way similar to the linear case, there would exist a closed formula depending only on the eigenvalues of the linear part of F. Thus, we want to find a formula $p \in \mathbb{C}[T]$, $p(T) = \sum_{i=0}^{m} p_i \cdot T^i$, such that $\sum_{i=0}^{m} p_i \cdot F^i = 0$.

In [3], a closed formula for a vanishing polynomial of F is discusssed, for F a locally finite polynomial endomorphism (LFPE, see definition 5), with $F(0) = 0$. This closed formula turns out to depend on the eigenvalues of the linear part of F, and on $\sup_{n\in\mathbb{N}} \deg F^n$. This thesis comprises a proof that this closed formula (see proposition 18), being

$$p(T) = \prod_{|\alpha| \leq \sup_{n\in\mathbb{N}} \deg F^n} (T - \lambda^\alpha),$$

with λ_i the eigenvalues of the linear part of F, is a vanishing polynomial for F. This means that $p(F) = \sum_{i=0}^{m} p_i \cdot F^i = 0$.

2 Locally finite polynomial endomorphisms

Recall from definition 2 that a polynomial endomorphism of $\mathbb{C}^N$ is a map $F\colon \mathbb{C}^N \to \mathbb{C}^N$ that is an N-tuple of coordinate functions: $F = (F_1, \ldots, F_N)$, where every $F_i \in \mathbb{C}[x_1, \ldots, x_N]$. From now on, we denote the polynomial endomorphism $(x_1, x_2, \ldots, x_N)$ by X. The set of all polynomial endomorphisms of $\mathbb{C}^N$ is denoted by $\mathrm{End}(\mathbb{C}^N)$.

For each $F \in \mathrm{End}(\mathbb{C}^N)$, we define $F^\#$ to be the map

$$\begin{aligned} F^\# : \quad & \mathbb{C}[x_1, \ldots, x_N] \to \mathbb{C}[x_1, \ldots, x_N], \\ & r \mapsto r \circ F. \end{aligned}$$

This means that for every $i \in \{1, \ldots, N\}$, $F^\#$ replaces every occurrence of x_i in r by the i-th coordinate function of F. The map $F^\#$ is a $\mathbb{C}$-linear endomorphism of the vector space $\mathbb{C}[x_1, \ldots, x_N]$, since it clearly holds that $F^\#(r + s) = F^\#(r) + F^\#(s)$, for all $r, s \in \mathbb{C}[x_1, \ldots, x_N]$, and $F^\#(a \cdot r) = a \cdot F^\#(r)$, for all $a \in \mathbb{C}$. Notice that $F^\#(G^\#(r)) = r \circ G(F)$ and thus $(F^\#)^m = (F^m)^\#$. The set of all linear endomorphisms of a vector space V is denoted by $\mathcal{L}(V)$.

Definition 3. A linear endomorphism $\ell \in \mathcal{L}(\mathbb{C}[x_1, \ldots, x_N])$ is called locally finite if for all $r \in \mathbb{C}[x_1, \ldots, x_N]$ holds that $\dim \mathrm{Span}_{n \in \mathbb{N}}\, \ell^n(r) < +\infty$.

For $F \in \mathrm{End}(\mathbb{C}^N)$, and $p \in \mathbb{C}[T], p = \sum_{i=0}^{m} p_i \cdot T^i$, we denote $\sum_{i=0}^{m} p_i \cdot F^i$ by $p(F)$. We define $\mathcal{I}_F := \{p \in \mathbb{C}[T] \mid p(F) = 0\}$.

Proposition 4. For a polynomial endomorphism F, the following conditions are equivalent.

i) $\mathcal{I}_F \neq \{0\}$,

ii) $\sup_{n \in \mathbb{N}} \deg F^n < +\infty$,

iii) $F^\#$ is locally finite.

Proof. i) $\Rightarrow$ ii):
Since $\mathcal{I}_F = \{p \in \mathbb{C}[T] \mid p(F) = 0\} \neq \{0\}$, there exists a $p \in \mathbb{C}[T]$ such that

$p \neq 0$ and $p(F) = 0$. Let m be the degree of p, then $p(F) = \sum_{i=0}^{m} p_i \cdot F^i$, thus

$$F^m = -\sum_{i=0}^{m-1} p_i \cdot F^i.$$

Hence, $F^m \in \mathrm{Span}(F^0, F^1, \ldots, F^{m-1})$. By induction, it follows that $F^n \in \mathrm{Span}(F^0, F^1, \ldots, F^{m-1})$, for every $n \in \mathbb{N}$. Thus,

$$\sup_{n\in\mathbb{N}} \deg F^n \leq \max_{0\leq k\leq m-1} \deg F^k < +\infty.$$

ii) $\Rightarrow$ iii):

From $\sup_{n\in\mathbb{N}} \deg F^n < +\infty$ follows that there exists a $C \in \mathbb{N}$ such that for every $n \in \mathbb{N}$ $\deg F^n \leq C$. For $r \in \mathbb{C}[x_1, \ldots, x_N], r \circ F^n$ is obtained by replacing every occurrence of x_i by the i-th coordinate function of F^n (denoted by $(F^n)_i$), for every $i \in \{1, \ldots, N\}$. The degree of $r \circ F^n$ is equal to the degree in the case that a coordinate function $(F^n)_i$, for which $\deg(F^n)_i = \deg F^n$, is used in a monomial with degree $\deg r$. So,

$$\deg r \circ F^n = \deg r \cdot \deg F^n \leq \deg r \cdot C \quad \Rightarrow \quad \dim \mathrm{Span}_{n\in\mathbb{N}}\, r \circ F^n < +\infty,$$

hence $F^{\#}$ is locally finite.

iii) $\Rightarrow$ i):

Note that $\dim \mathrm{Span}_{n\in\mathbb{N}}\, r \circ F^n < +\infty$, for every $r \in \mathbb{C}[x_1, \ldots, x_N]$, implies that $\dim \mathrm{Span}_{n\in\mathbb{N}}\, F^n < +\infty$. Therefore, there exists a finite set I, such that for every $j \in \mathbb{N}$: there exist coefficients $a_i \in \mathbb{C}$ with $F^j = \sum_{i\in I} a_i \cdot F^i$. Now fix $j \in \mathbb{N}\backslash I$ and fix the a_i's such that $F^j = \sum_{i\in I} a_i \cdot F^i$. Define

$$p(T) := (\sum_{i\in I} a_i \cdot T^i) - T^j.$$

Then

$$p(F) = \sum_{i\in I} a_i \cdot F^i - F^j = 0 \Rightarrow p \in \mathcal{I}_F.$$

Since $j \notin I$, $\sum_{i\in I} a_i \cdot T^i \neq T^j$, so $p \neq 0$. This implies that $\mathcal{I}_F \neq \{0\}$.

□

Definition 5. A polynomial endomorphism $F \in \mathrm{End}(\mathbb{C}^N)$ is called locally finite if F satisfies the conditions in proposition 4.

3 A characteristic polynomial for LFPE's

As mentioned before, we want to find a way to produce for every locally finite polynomial endomorphism F, with $F(0) = 0$, a vanishing polynomial. It turns out that the characteristic polynomial of $F^{\#}$, restricted to a certain vector space W is such a vanishing polynomial for F. We will first define this vector space W.

Definition 6. For $F \in \text{End}(\mathbb{C}^N)$, define $W^i := \text{Span}_{n\in\mathbb{N}}((F^{\#})^n(x_i))$, and $W := W^1 + \ldots + W^N$.

Definition 7. For a linear endomorphism $\ell \in \mathcal{L}(\mathbb{C}[x_1, \ldots, x_N]), \mathcal{F}(\ell)$ denotes the set of finite dimensional subspaces U of $\mathbb{C}[x_1, \ldots, x_N]$ for which $\ell(U) \subseteq U$.

We will use the following two lemmas while proving that ${F^{\#}}_{|W}$ is a vanishing polynomial of F.

Lemma 8. Let $F \in \text{End}(\mathbb{C}^N)$ be locally finite. Then $W \in \mathcal{F}(F^{\#})$.

Proof. By proposition 4, the fact that F is locally finite means that $F^{\#}$ is locally finite. By definition 3, this implies that

$$\forall r \in \mathbb{C}[x_1, \ldots, x_N] : \dim \text{Span}_{n\in\mathbb{N}}\ (F^{\#})^n(r) < +\infty.$$

In particular, for every $i \in \{1, \ldots, N\}$, $\dim W^i = \dim \text{Span}_{n\in\mathbb{N}}\ ((F^{\#})^n(x_i)) < +\infty$. From this follows that $\dim W \leq \sum_{1\leq i\leq N} \dim W^i < +\infty$. Together with the fact that $F^{\#}(W) \subseteq W$, this implies that $W \in \mathcal{F}(F^{\#})$.

□

Lemma 9. Let $F \in \text{End}(\mathbb{C}^N)$ be such that $\forall i \in \{1, \ldots, N\} : F^{\#}(x_i) = 0$. Then $F = 0$.

Proof. For every i-th coordinate function of F, we have $F_i = x_i \circ F = F^{\#}(x_i) = 0$. Thus all coordinate functions of F are zero, i.e. $F = 0$.

□

Lemma 10. Let $F \in \text{End}(\mathbb{C}^N)$. Then $\mathcal{X}_{(F^{\#},W)}$, the characteristic polynomial of ${F^{\#}}_{|W}$, is a vanishing polynomial of F.

Proof. Consider the linear map ${F^\#}_{|W} : W \to W$. Theorem 1 states that $\mathcal{X}_{(F^\#,W)} = \sum_{i=0}^m a_i \cdot T^i$ is a vanishing polynomial for ${F^\#}_{|W}$, hence

$$\begin{aligned} & \mathcal{X}_{(F^\#,W)}({F^\#}_{|W}) = 0 \\ \Rightarrow\ & W \subseteq \ker(\mathcal{X}_{(F^\#,W)}(F^\#)) \\ \Rightarrow\ & (\mathcal{X}_{(F^\#,W)}(F^\#))(x_j) = 0, \forall j \in \{1, \ldots, N\}. \end{aligned}$$

By definition of $F^\#$,

$$0 = (\mathcal{X}_{(F^\#,W)}(F^\#))(x_j) = \sum_{i=0}^m a_i \cdot (F^\#)^i(x_j) = \sum_{i=0}^m a_i \cdot (x_j \circ F^i),$$

which is the j-th coordinate function of $\sum_{i=0}^m a_i \cdot F^i$, and thus is equal to $x_j \circ \mathcal{X}_{(F^\#,W)}(F)$. From lemma 9, it follows that $\mathcal{X}_{(F^\#,W)}(F) = 0$, hence $\mathcal{X}_{(F^\#,W)}$ is a vanishing polynomial of F.

□

Now that we have found that $\mathcal{X}_{(F^\#,W)}(F) = 0$, we will use this in order to find a closed formula giving a vanishing polynomial of F.

We define $\mathcal{M}$ as the linear subspace of $\mathbb{C}[x_1, \ldots, x_N]$ such that $\mathcal{M} = \{r \in \mathbb{C}[x_1, \ldots, x_N] \mid r(0) = 0\}$. More generally, $\mathcal{M}^k$ is the linear subspace of $\mathbb{C}[x_1, \ldots, x_N]$ containing only those polynomials $r \in \mathbb{C}[x_1, \ldots, x_N]$ for which every monomial has degree at least k.

For $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_N) \in \mathbb{N}^N$, we define $F^\alpha := F_1^{\alpha_1} F_2^{\alpha_2} \cdots F_N^{\alpha_N}$, and $|\alpha| := \alpha_1 + \alpha_2 + \ldots + \alpha_N$.

Lemma 11. Let $F \in \mathrm{End}(\mathbb{C}^N)$ be such that $F(0) = 0$, then $\forall k \geq 0$: $F^\#(\mathcal{M}^k) \subseteq \mathcal{M}^k$.

Proof. Since $F(0) = 0$, we have $F_i(0) = 0$, for all $i, 1 \leq i \leq N$. So every $F_i \in \mathcal{M}$. Let r be in $\mathcal{M}^k$, then

$$r = \sum_{\alpha \in \mathbb{N}^N,\ |\alpha| \geq k} r_\alpha \cdot X^\alpha,$$

with $r_\alpha \in \mathbb{C}$. Then

$$F^\#(r) = r \circ F = \sum_{\alpha \in \mathbb{N}^N,\ |\alpha| \geq k} r_\alpha \cdot F^\alpha.$$

From $F^\alpha = F_1^{\alpha_1} F_2^{\alpha_2} \cdots F_N^{\alpha_N}$, $|\alpha| \geq k$, and the fact that every $F_i \in \mathcal{M}$, we see that F^α is a product of at least k elements of $\mathcal{M}$, and thus $F^\alpha \in \mathcal{M}^k$. Since $\mathcal{M}^k$ is closed under addition, it follows that $F^\#(r) \in \mathcal{M}^k$, hence $F^\#(\mathcal{M}^k) \subseteq \mathcal{M}^k$.

□

Recall that $W = \mathrm{Span}_{n\in\mathbb{N}}((F^\#)^n(x_i))_{1\leq i\leq N}$ and $d = \sup_{n\in\mathbb{N}} \deg F^n$. For $1 \leq k \leq d+1$, we define $W_k := W \cap \mathcal{M}^k$.

Lemma 12. Let $F \in \mathrm{End}(\mathbb{C}^N)$ be such that $F(0) = 0$, then $F^\#(W_k) \subseteq W_k, \forall k \geq 0$.

Proof. Note that $F^\#(W_k) = F^\#(W \cap \mathcal{M}^k) \subseteq F^\#(\mathcal{M}^k)$. By lemma 11, we have $F^\#(\mathcal{M}^k) \subseteq \mathcal{M}^k, \forall k \geq 0$. Also, it is obvious that $F^\#(W_k) \subseteq F^\#(W) \subseteq W$. Thus, $F^\#(W_k) \subseteq W \cap M^k = W_k, \forall k \geq 0$.

□

Lemma 13. Let $F \in \mathrm{End}(\mathbb{C}^N)$ be such that $F(0) = 0$, and such that $d = \sup_{n\in\mathbb{N}} \deg F^n < \infty$. Let W_k be defined as above. Then $W = W_1 \supseteq W_2 \supseteq \ldots \supseteq W_{d+1} = \{0\}$.

Proof. Since $\mathcal{M}^k$ is the set of polynomials $r \in \mathbb{C}[x_1, \ldots, x_N]$ for which every monomial has degree at least k, we have that $\mathcal{M}^k \supseteq \mathcal{M}^{k+1}$, for $1 \leq k \leq d$. By definition of W_k, it follows that $W_1 \supseteq W_2 \supseteq \ldots \supseteq W_{d+1}$.
Recall that $x_i \circ F^n$ is the i-th coordinate function of F^n. Since $F(0) = 0$, we have $\deg(x_i \circ F^n) \geq 1$, for $1 \leq i \leq N$ and every $n \in \mathbb{N}$. The set $\{x_i \circ F^n \mid n \in \mathbb{N}, 1 \leq i \leq N\}$ is a spanning set for W. Thus, every element of W is in $\mathcal{M}^1$, and thus $W \subseteq \mathcal{M}^1$. From this, it follows that $W = W \cap \mathcal{M}^1 = W_1$.
For $1 \leq i \leq N$, and every $n \in \mathbb{N}$,

$$\deg(x_i \circ F^n) \leq \max_{1\leq j\leq N} \deg(x_j \circ F^n) = \deg F^n < d+1,$$

since $d = \sup_{n\in\mathbb{N}} \deg F^n$. Thus, every basis element of W has degree less than $d+1$. This implies that every polynomial in W consists of monomials of degree less than $d+1$, except for 0, hence $W_{d+1} = \{0\}$.

□

As we will see in lemma 15, the characteristic polynomial $\mathcal{X}_{(F^\#,W)}$ can be written as a product of other characteristic polynomials. We will use these characteristic polynomials in our search for a closed formula that vanishes for F. Therefore, the following endomorphisms are needed.

Definition 14. For the linear map ${F^\#}_{|W}$, and $i \in \{1, \dots, d\}$, we define L_i to be the endomorphism induced by ${F^\#}_{|W}$ on W_i/W_{i+1}, that is:

$$\begin{aligned} L_i : \quad & W_i/W_{i+1} \to W_i/W_{i+1} \\ & w_i + W_{i+1} \mapsto F^\#(w_i) + W_{i+1}, \end{aligned}$$

where $w_i \in W_i$.

The map L_i is well defined: Let $b \in \overline{a}$. Then $L_i(\overline{b}) = F^\#(b) + W_{i+1}$. Since $F^\#$ is linear, this equals $F^\#(b-a) + F^\#(a) + W_{i+1}$. Using that $b - a \in W_{i+1}$, lemma 12 implies that $F^\#(b-a) \in W_{i+1}$, and thus $L_i(\overline{b}) = F^\#(a) + W_{i+1} = L_i(\overline{a})$. This makes L_i independent of the choice of representatives.

Lemma 15. The characteristic polynomial $\mathcal{X}_{(F^\#,W)}$ of ${F^\#}_{|W}$ can be found using the characteristic polynomials of the linear maps L_i defined above, in the following way:

$$\mathcal{X}_{(F^\#,W)} = \mathcal{X}_{L_1} \cdot \mathcal{X}_{L_2} \cdots \mathcal{X}_{L_d}$$

Proof. Note that lemma 13 implies that $W \cong W_1/W_2 \oplus \ldots \oplus W_d/W_{d+1} =: V$. There is an isomorphism

$$\begin{aligned} \phi : \quad & W \to V \\ & w \mapsto (\overline{w_1}, \dots, \overline{w_d}), \end{aligned}$$

where $\overline{w_i}$ is the coset of w in W_i/W_{i+1}. Define a linear endomorphism L on V, such that $L_{|W_i/W_{i+1}} = L_i$, for every $i \in \{1, \dots, d\}$. By definition of the L_i, we then have $\phi^{-1}\ {F^\#}_{|W}\ \phi = L$. Now $\mathcal{X}_{L_i} \bigm| \mathcal{X}_L$, and $\deg \mathcal{X}_{L_i} = \dim W_i/W_{i+1}$, thus

$$\deg(\prod_{i=1}^{d} \mathcal{X}_{L_i}) = \dim(\prod_{i=1}^{d} W_i/W_{i+1}) = \dim W = \dim V = \deg \mathcal{X}_L.$$

Since characteristic polynomials are monic, this means that $\prod_{i=1}^{d} \mathcal{X}_{L_i} = \mathcal{X}_L = \mathcal{X}_{{F^\#}_{|W}}$.

□

Now, we let $F^{\#}{}_{|\mathcal{M}}$ induce endomorphisms on the spaces $\mathcal{M}^i/\mathcal{M}^{i+1}$, in a way similar to how $F^{\#}{}_{|W}$ induced L_i on W_i/W_{i+1}.

Definition 16. The linear map $F^{\#}{}_{|\mathcal{M}}$ induces an endomorphism K_i on $\mathcal{M}^i/\mathcal{M}^{i+1}$, in the following way:

$$\begin{aligned} K_i: \ & \mathcal{M}^i/\mathcal{M}^{i+1} \to \mathcal{M}^i/\mathcal{M}^{i+1} \\ & m_i + \mathcal{M}^{i+1} \mapsto F^{\#}(m_i) + \mathcal{M}^{i+1}, \end{aligned}$$

where $m_i \in \mathcal{M}^i$.

Similar to definition 14, using lemma 11 we find that the K_i are well defined. Furthermore, definition 16 ensures that $K_{i|W_i/W_{i+1}} = L_i$.

By $\mathcal{L}(F_i)$, we denote the linear part of $F_i \in \mathbb{C}[x_1, \ldots, x_N]$. Also, we call $(\mathcal{L}(F_1), \ldots, \mathcal{L}(F_N))$ the linear part of a polynomial endomorphism F, and denote this by $\mathcal{L}(F)$.

We are now able to show how the characteristic polynomial $\mathcal{X}_{K_i}$ depends on the eigenvalues of F.

Lemma 17. Let the K_i be defined as above, with $F \in \operatorname{End}(\mathbb{C}^N)$ such that $F(0) = 0$. Let $\alpha \in \mathbb{N}^N$, and $\lambda^\alpha = \lambda_1^{\alpha_1} \cdots \lambda_N^{\alpha_N}$, where λ_i is the eigenvalue of the linear part of F_i. Then, for the characteristic polynomial $\mathcal{X}_{K_i}$, the following holds

$$\mathcal{X}_{K_i} = \prod_{|\alpha|=i} (T - \lambda^\alpha).$$

Proof. Assume that $\mathcal{L}(F)$ is represented by a diagonal matrix. The canonical basis for $\mathcal{M}^i/\mathcal{M}^{i+1}$ is

$$\{X^\alpha + \mathcal{M}^{i+1} \bigm| |\alpha| = i\}.$$

For these basis elements,

$$K_i(X^\alpha + \mathcal{M}^{i+1}) = F^{\#}(X^\alpha) + \mathcal{M}^{i+1} = F^\alpha + \mathcal{M}^{i+1}.$$

We can write

$$F^\alpha = (\mathcal{L}(F_1) + H_1)^{\alpha_1} \cdots (\mathcal{L}(F_N) + H_N)^{\alpha_N},$$

where $H_i = F_i - \mathcal{L}(F_i)$, the higher order part of F_i. Notice that $|\alpha| = i$ implies that the terms containing higher order parts will end up in $\mathcal{M}^{i+1}$. Hence

$$F^\alpha = \mathcal{L}(F_1)^{\alpha_1} \cdots \mathcal{L}(F_N)^{\alpha_N} + \mathcal{M}^{i+1}$$

and

$$K_i(X^\alpha + \mathcal{M}^{i+1}) = \mathcal{L}(F)^\alpha + \mathcal{M}^{i+1}.$$

By assumption, $\mathcal{L}(F)$ is represented by a diagonal matrix. Thus, $\mathcal{L}(F) = (\lambda_1 X_1, \ldots, \lambda_N X_N)$ and

$$K_i(X^\alpha + \mathcal{M}^{i+1}) = \lambda_1^{\alpha_1} X_1^{\alpha_1} \cdots \lambda_N^{\alpha_N} X_N^{\alpha_N} + \mathcal{M}^{i+1} = \lambda^\alpha X^\alpha + \mathcal{M}^{i+1}.$$

In particular, $K_i : \overline{X^\alpha} \mapsto \lambda^\alpha \overline{X^\alpha}$, for every $\alpha \in \mathbb{N}^N$ with $|\alpha| = i$. Thus, the matrix of K_i in the canonical basis is a diagonal matrix with the λ^α's on the diagonal. This yields $\prod_{|\alpha|=i}(T - \lambda^\alpha)$ as the characteristic polynomial of K_i. When $\mathcal{L}(F)$ is not represented by a diagonal matrix, one can show with a bit more effort that K_i is conjugated to an upper triangular matrix, with the λ^α on the diagonal. This leads to the same conclusion.

□

The following proposition shows that for each locally finite polynomial endomorphism F, with $F(0) = 0$, a vanishing polynomial exists that depends only on the eigenvalues of F and on $\sup_{n \in \mathbb{N}} \deg F^n$.

Proposition 18. Let $F \in \mathrm{End}(\mathbb{C}^N)$ be such that $F(0) = 0$ and $d = \sup_{n \in \mathbb{N}} \deg F^n < \infty$. Let λ_i denote the eigenvalues of the linear part of F. Then

$$\prod_{|\alpha| \le d} (T - \lambda^\alpha)$$

is a vanishing polynomial of F.

Proof. Lemma 10 states that $\mathcal{X}_{(F^\#, W)}$, the characteristic polynomial of $F^\#{}_{|W}$, is a vanishing polynomial of F. We will show that this polynomial divides the polynomial mentioned in the proposition. It follows from lemma 15 that

$$\mathcal{X}_{(F^\#, W)} = \prod_{i=1}^{d} \mathcal{X}_{L_i}.$$

Notice that, by definition of the K_i, we have that $K_{i|W_i/W_{i+1}} = L_i$. This implies that $\mathcal{X}_{L_i} \mid \mathcal{X}_{K_i}$, for every $i \in \{1, \ldots, d\}$. In lemma 17, we saw that

$$\mathcal{X}_{K_i} = \prod_{|\alpha|=i} (T - \lambda^\alpha).$$

Hence,

$$\prod_{i=1}^{d} \mathcal{X}_{L_i} \;\Big|\; \prod_{i=1}^{d} \mathcal{X}_{K_i} = \prod_{i=1}^{d} \prod_{|\alpha|=i} (T - \lambda^\alpha).$$

This last expression is equal to $\prod_{|\alpha|\leq d}(T - \lambda^\alpha)$, which proves the proposition.

□

References

[1] W. Bosma, *Lineaire Algebra 3 en 4*, Lecture notes, Radboud Universiteit, Nijmegen, 2006.

[2] M. Nagata, *On Automorphism Group of* $k[x,y]$, Department of Mathematics, Kyoto University, Lectures in Mathematics, No. 5. Kinokuniya Book-Store Co. Ltd., Tokyo, 1972.

[3] J.-P. Furter and S. Maubach, *Locally finite polynomial endomorphisms*, J. Pure and Applied Algebra **211** (2007) 445–458.