An Algebraist's View of the Linear Recurrence Relations

Nikolai V. Ivanov

The key ingredients of our approach to the linear recurrence relations are: a fragment of the *theory of representations of one endomorphism*; the *left shift operator*; the *derivatives of sequences*. As a side benefit, this approach provides more general results than various standard expositions. The logic of exposition should serve as the motivation; there are no artificial motivational discussions. For the author, this little theory is beautiful by itself and requires no further motivation.

In this paper we denote by $\mathbf{Z}$ *the set of all integers and by* $\mathbf{N}$ *the set of non-negative integers. We denote by* $\Bbbk$ *a fixed entire ring, i.e. a commutative ring with a unit without zero divisors and such that its zero and its unit are not equal. The ring* $\Bbbk$ *will be called* ***the base ring****. There is a canonical ring homomorphism* $\mathbf{Z} \to \Bbbk$ *taking* $0, 1 \in \mathbf{Z}$ *to the zero and the unit of* $\Bbbk$ *respectively, making* $\Bbbk$ *into a* $\mathbf{Z}$*-algebra. We identify* $0, 1 \in \mathbf{Z}$ *with their images in* $\Bbbk$*.*

If the homomorphism $\mathbf{Z} \to \Bbbk$ *is injective, we say that the characteristic of* $\Bbbk$ *is equal to* 0*. If it is not injective, then its kernel is equal to* $p\mathbf{Z}$ *for some prime* p*. In this case we say that the characteristic of* $\Bbbk$ *is equal to* p*. The characteristic of* $\Bbbk$ *is denoted by* $\operatorname{char}\Bbbk$*.*

1. Modules

In this section K denotes a commutative ring with a unit such that $0 \neq 1$, where 0 and 1 are the zero and the unit of K, and M denotes a K-module.

 Neither the work reported in this paper, nor its preparation were supported by any governmental or non-governmental agency, foundation, or institution.

1.1. Lemma. *Suppose that* $v_0, v_1, \dots, v_a$ *are free generators of a free* K*-submodule of* M*. Suppose that* $w_0, w_1, \dots, w_a$ *are elements of* M *such that for each* $i = 0, 1, \dots, a$ *the element* v_i *has the form* $v_i = c_i w_i$ *for some* $c_i \in K$*. Then the homomorphism* $K^{a+1} \to M$ *defined by*

$$(x_0, x_1, \dots, x_a) \mapsto x_0 w_0 + x_1 w_1 + \dots + x_a w_a$$

is an isomorphism onto its image. In particular, $w_0, w_1, \dots, w_a$ *are free generators of a free* K*-submodule of* M*.*

Proof. It is sufficient to prove that our homomorphism $K^{a+1} \to M$ is injective. In other terms, it is sufficient to prove that if

(1) $\quad x_0 w_0 + x_1 w_1 + \dots + x_a w_a = 0$

for some $x_0, x_1, \dots, x_a \in K$, then $x_0 = x_1 = \dots = x_a = 0$.

Suppose that (1) holds and $x_j \neq 0$ for some j. Let $c = c_1 c_2 \dots c_a$. Note that $v_i \neq 0$ implies that $c_i \neq 0$. Therefore $c \neq 0$. The equality (1) implies that

(2) $\quad c x_0 w_0 + c x_1 w_1 + \dots + c x_a w_a = 0.$

For each $i = 0, 1, \dots, a$, let $\widehat{c_i}$ be the product of all c_j with $0 \leqslant j \leqslant a$ and $j \neq i$. Then $c = \widehat{c_i} c_i$ for all i. In addition, $\widehat{c_i}, c_i \neq 0$ for all i because $c \neq 0$. The equality (2) implies

(3) $\quad \widehat{c_0} x_0 c_0 w_0 + \widehat{c_1} x_1 c_1 w_1 + \dots + \widehat{c_a} x_a c_a w_a = 0.$

For each $i = 0, 1, \dots, a$, let $\widehat{x_i} = \widehat{c_i} x_i$. Since $c_i w_i = v_i$ for all i, (3) can be rewritten as

$$\widehat{x_0} v_0 + \widehat{x_1} v_1 + \dots + \widehat{x_a} v_a = 0.$$

Since $\widehat{c_i} \neq 0$ for all i and $x_j \neq 0$ for some j, $\widehat{x_j} \neq 0$ for some j. Hence the last equation contradicts to the lemma. ■

Torsion free and torsion modules. A K-module M is called *torsion-free,* if $xm = 0$ implies that either $x = 0$, or $m = 0$, where $x \in K$ and $m \in M$. Since K is assumed to be a ring without zero divisors, K^n is a torsion free module for any non-zero $n \in \mathbf{N}$.

An element $m \in M$ is called a *torsion element* of M, if $xm = 0$ for some non-zero $x \in K$. A module is called a *torsion module* if every element of M is a torsion element.

1.2. Lemma. *Suppose that* K *is a commutative ring with a unit such that* $0 \neq 1$*, where* 0 *and* 1 *are the zero and the unit of* K*. Suppose that, in addition,* K *is a ring without zero divisors. Let* $n \in \mathbf{N}$*. If* M *is a* K*-submodule of a* K*-module* N *and both* M *and* N *are isomorphic to* K^n*, then the quotient* N/M *is a torsion module. Moreover, there is an element* $x \in K$ *such that* $x \neq 0$ *and* $x(N/M) = 0$*, i.e.* $xv = 0$ *for all* $v \in N/M$*.*

Proof. Suppose that N/M is not a torsion module. Then there is an element $v \in N/M$ such that $xv \neq 0$ if $x \neq 0$. For such a v the map $x \mapsto xv$ is an injective homomorphism of K-modules $K \to N/M$. Let us lift $v \in N/M$ to an element $v_0 \in N$, so v is the image of v_0 under the canonical surjection $N \to N/M$. Then the map $x \mapsto xv_0$ is an injective homomorphism of K-modules $K \to N$.

Clearly, if $v_1, v_2, \ldots, v_n$ is a basis of M (which exists because M is isomorphic to K^n), then $v_0, v_1, \ldots, v_n$ is a basis of $Kv_0 + M$. Therefore, $Kv_0 + M$ is a submodule isomorphic to K^{n+1} of the module N isomorphic to K^n. In particular, there exist an injective K-module homomorphism $J\colon K^{n+1} \to K^n$.

Since the ring K has no zero divisors, it can be embedded into its field of fractions, which we will denote by F. Moreover, the K-module homomorphism $K^{n+1} \to K^n$ extends to an F-linear map $F^{n+1} \to F^n$, which we will denote by J_F.

Claim. J_F *is injective.*

Proof of the claim. Suppose $(y_0, y_1, \ldots, y_n) \in F^{n+1}$ is non-zero and belongs to the kernel of J_F. Since F is the field of fractions of K, there is an element $z \in K$ such that $zy_0, zy_1, \ldots, zy_n \in K$. For such a $z \in K$ the $(n+1)$-tuple $(zy_0, zy_1, \ldots, zy_n)$ belongs to K^{n+1}, and

$$\begin{aligned} J(zy_0, zy_1, \ldots, zy_n) &= J_F(zy_0, zy_1, \ldots, zy_n) \\ &= zJ_F(y_0, y_1, \ldots, y_n) = z0 = 0 \end{aligned}$$

Since F is the field of fractions of K, $(y_0, y_1, \ldots, y_n) \neq 0$ implies that the $(n+1)$-tuple $(zy_0, zy_1, \ldots, zy_n) \neq 0$. At the same time this $(n+1)$-tuple belongs to the kernel of J, in contradiction with the injectivity of J. The claim follows. □

As is well known, for a field F there are no injective F-linear maps $F^{n+1} \to F^n$. The contradiction with the above claim proves that N/M is indeed a torsion module.

It remains to prove the existence of a non-zero $x \in K$ such that $x(N/M) = 0$. Since N is finitely generated, N/M is also finitely generated. Suppose that $w_1, \ldots, w_m \in N/M$ generate N/M. Since, as we just proved, N/M is a torsion module, there are non-zero elements $x_1, \ldots, x_m \in K$ such that $x_i w_i = 0$ for all $i = 1, 2, \ldots, m$. Then $x = x_1 x_2 \ldots x_m$ has the required property. ■

2. Endomorphisms

Representation of the polynomial algebra defined by an endomorphism. Let x be a variable, and let $\Bbbk[x]$ be the $\Bbbk$-algebra of polynomials in x with coefficients in $\Bbbk$. Let

M be a $\Bbbk$-module. The $\Bbbk$-endomorphisms $M \to M$ form a $\Bbbk$-algebra $\mathbf{End}\, M$ with the composition as the multiplication. For every $\Bbbk$-endomorphism $E\colon M \to M$ and every $n \in \mathbf{N}$ we will denote by E^n the n-fold composition $E \circ E \circ \ldots \circ E$. As usual, we interpret the 0-fold composition E^0 as the identity endomorphism $\mathrm{id} = \mathrm{id}_M \in \mathbf{End}\, M$, and the 1-fold composition E^1 as E.

For a $\Bbbk$-module endomorphism $E\colon M \to M$ and a polynomial

$$f(x) = c_0 x^n + c_1 x^{n-1} + c_2 x^{n-2} + \ldots + c_n \in \Bbbk[x] \tag{4}$$

one can define an endomorphism $f(E)\colon M \to M$ by the formula

$$f(E) = c_0 E^n + c_1 E^{n-1} + c_2 E^{n-2} + \ldots + c_n. \tag{5}$$

The map $f(x) \mapsto f(E)$ is a homomorphism $\Bbbk[x] \to \mathbf{End}\, M$ of $\Bbbk$-algebras. This follows from the obvious identities $x^n x^m = x^{n+m}$ and $E^n \circ E^m = E^{n+m}$. This homomorphism defines a structure of $\Bbbk[x]$-module on M. Of course, this structure depends on E.

We will denote by $\Bbbk[E]$ the image of the homomorphism $f(x) \mapsto f(E)$. Since $\Bbbk[x]$ is commutative, the image $\Bbbk[E]$ is a commutative subalgebra of $\mathbf{End}\, M$.

If a homomorphism $\Bbbk[x] \to \mathbf{End}\, M$ of $\Bbbk$-algebras takes x to E, then it is equal to $f(x) \mapsto f(E)$. Indeed, the definition of homomorphisms of $\Bbbk$-algebras implies that the value of such a homomorphism on a polynomial (4) should be equal to the right hand side of (5).

Eigenvalues. Suppose that a $\Bbbk$-module endomorphism $E\colon M \to M$ is fixed.

Let $\alpha \in \Bbbk$. The kernel $\mathrm{Ker}(E - \alpha)$ is called the *eigenmodule of* E *corresponding to* α and will be often denoted by E_α. Clearly, E_α is a $\Bbbk$-submodule of M. An element $\alpha \in \Bbbk$ is called an *eigenvalue of* E if the kernel $E_\alpha = \mathrm{Ker}(E - \alpha) \neq 0$.

The set of elements $v \in M$ such than $(E - \alpha)^i(v) = 0$ for some $i \in \mathbf{N}$ is called the *extended eigenmodule of* E *corresponding to* α and is denoted by $\mathrm{Nil}(\alpha)$. Clearly, $\mathrm{Nil}(\alpha)$ is a $\Bbbk$-submodule of M.

2.1. Lemma. *Let $\alpha \in \Bbbk$. Then the following statements hold.*

(i) The submodules E_α and $\mathrm{Nil}(\alpha)$ are E-invariant.

(ii) E_α and $\mathrm{Nil}(\alpha)$ are $\Bbbk[x]$-submodules of M.

(iii) The submodule $\mathrm{Nil}(\alpha)$ is non-zero if and only if α is an eigenvalue.

Proof. Let us prove (i), (ii) first. Note that $(E-\alpha)^i \circ E = E \circ (E-\alpha)^i$ for every $i \in \mathbf{N}$, because $\Bbbk[E]$ is a commutative subalgebra of $\mathbf{End}\, M$. Therefore, if $(E-\alpha)^i(v) = 0$, then

$$(E-\alpha)^i\,(E(v)) = \Big((E-\alpha)^i \circ E\Big)\,(v) = \Big(E \circ (E-\alpha)^i\Big)\,(v) = E\,\Big((E-\alpha)^i(v)\Big) = 0.$$

In the case $i = 1$ this implies that $E(E_\alpha) \subset E_\alpha$. In general, this implies that

$$E(\mathrm{Ker}\,(E-\alpha)^i) \subset \mathrm{Ker}\,(E-\alpha)^i,$$

and hence $E(\mathrm{Nil}(\alpha)) \subset \mathrm{Nil}(\alpha)$. This proves (i), and (ii) immediately follows.

Finally, let us prove (iii). Suppose that $v \neq 0$ and $(E-\alpha)^i(v) = 0$. Let i be the smallest integer such that $(E-\alpha)^i(v) = 0$. Note that $i > 0$ because $v \neq 0$. Let $w = (E-\alpha)^{i-1}(v)$. Then $w \neq 0$ and $(E-\alpha)(w) = 0$. Therefore $E_\alpha = \mathrm{Ker}\,(E-\alpha) \neq 0$. This proves (iii). ■

For the rest of this section we will assume that M ***is a torsion free module.***

2.2. *Lemma.* *Let* $\alpha_1, \alpha_2, \ldots, \alpha_n$ *be distinct eigenvalues of an endomorphism* $E\colon M \to M$. *Let* $\mathrm{Ker}_1, \mathrm{Ker}_2, \ldots, \mathrm{Ker}_n$ *be the corresponding eigenmodules, i.e.* $\mathrm{Ker}_i = \mathrm{Ker}\,(E-\alpha_i)$ *for each* $i = 1, 2, \ldots, n$. *Then the sum of these eigenmodules is a direct sum, i.e. an element*

$$v \in \mathrm{Ker}_1 + \mathrm{Ker}_2 + \ldots + \mathrm{Ker}_n \text{ admits only one presentation } v = v_1 + v_2 + \ldots + v_n$$

with $v_i \in \mathrm{Ker}_i$ *for all* $i = 1, 2, \ldots, n$.

Proof. It is sufficient to prove that if $v_1 + v_2 + \ldots + v_n = 0$ and $v_i \in \mathrm{Ker}_i$ for all i, then $v_1 = v_2 = \ldots = v_n = 0$. We will argue by contradiction and suppose that there are elements $v_1 \in \mathrm{Ker}_1$, $v_2 \in \mathrm{Ker}_2$, $\ldots$, $v_n \in \mathrm{Ker}_n$ such that

$$v_1 + v_2 + \ldots + v_n = 0.$$

and not all v_i are equal to 0. Let m be the minimal integer $m \leqslant n$ such that

(6) $\quad v_1 + v_2 + \ldots + v_m = 0 \quad$ and $\quad v_m \neq 0$

for some elements $v_1 \in \mathrm{Ker}_1$, $v_2 \in \mathrm{Ker}_2$, $\ldots$, $v_m \in \mathrm{Ker}_m$. Note that (6) implies that $v_i \neq 0$ also for some $i < m$. By applying $E - \alpha_m$ to (6), we get

$$(E-\alpha_m)(v_1) + \ldots + (E-\alpha_m)(v_{m-1}) + (E-\alpha_m)(v_m) = 0.$$

Since $v_i \in \mathrm{Ker}_i = \mathrm{Ker}\,(E-\alpha_i)$ and hence $E(v_i) = \alpha_i v_i$ for all $i = 1, 2, \ldots, n$, we see that

(7) $\quad (\alpha_1 - \alpha_m)v_1 + \ldots + (\alpha_{m-1} - \alpha_m)v_{m-1} + (\alpha_m - \alpha_m)v_m = 0.$

It follows that

(8) $(\alpha_1-\alpha_m)v_1+\ldots+(\alpha_{m-1}-\alpha_m)v_{m-1}=0.$

Since the eigenvalues α_i are distinct, $\alpha_i-\alpha_m\neq 0$ for $i<m$. For each for $i<m$, let $w_i=(\alpha_i-\alpha_m)v_i$. Then $w_i\in \mathrm{Ker}_i$ for each for $i<m$, and since M is assumed to be torsion free, $w_i\neq 0$ if $v_i\neq 0$. As we noted above, $v_i\neq 0$ for some $i<m$. Hence, $w_i\neq 0$ for some $i<m$. Let l be the maximal integer such that $l<m$ and $w_l\neq 0$. Then

(9) $w_1+w_2+\ldots+w_l=0$ and $w_l\neq 0$

Since $l<m$, the equality (9) contradicts to the choice of m. This contradiction proves the lemma. ■

2.3. Lemma. *Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be distinct eigenvalues of an endomorphism $E\colon M\to M$. Let $\mathrm{Nil}_1, \mathrm{Nil}_2, \ldots, \mathrm{Nil}_n$ be the corresponding extended eigenmodules, i.e. $\mathrm{Nil}_i=\mathrm{Nil}(\alpha_i)$ for $i=1, 2, \ldots, n$. Then the sum of these extended eigenmodules is a direct sum, i.e. an element*

$v\in \mathrm{Nil}_1+\mathrm{Nil}_2+\ldots+\mathrm{Nil}_n$ *admits only one presentation* $v=v_1+v_2+\ldots+v_n$

with $v_i\in \mathrm{Nil}_i$ for all $i=1, 2, \ldots, n$.

Proof. It is sufficient to prove that if $v_1+v_2+\ldots+v_n=0$ and $v_i\in \mathrm{Nil}_i$ for all i, then $v_1=v_2=\ldots=v_n=0$. Suppose that $v_1+v_2+\ldots+v_n=0$, $v_i\in \mathrm{Nil}_i$ for all i, and not all v_i are equal to 0. The proof proceeds by replacing, in several steps (no more than n), the original elements v_i by new ones in such a way that eventually not only $v_i\in \mathrm{Nil}_i$, but, moreover, $v_i\in \mathrm{Ker}_i=\mathrm{Ker}(E-\alpha_i)$, and still not all v_i are equal to 0. Obviously, this will contradict to Lemma 2.2.

For each $i=1, 2, \ldots, n$, let $E_i=E-\alpha_i$. Then $E_i^0(v_i)=v_i$ and $E_i^N(v_i)=0$ for some integer $N\geqslant 1$ (depending on i). If $v_i\neq 0$, then we define a_i as the largest integer $a\geqslant 0$ such $E_i^a(v_i)\neq 0$. Then $E_i^{a_i}(v_i)\neq 0$ and $E_i^{a_i+1}(v_i)=0$. In particular,

$$(E-\alpha_i)(E_i^{a_i}(v_i))=E_i(E_i^{a_i}(v_i))=E_i^{a_i+1}(v_i)=0,$$

and hence $E_i^{a_i}(v_i)\in \mathrm{Ker}_i$. If $v_i=0$, then we set $a_i=0$ and $E_i^{a_i}(v_i)\in \mathrm{Ker}_i$ is still true.

Let us fix an integer k between 1 and n. Let $w_i=E_k^{a_k}(v_i)$, where $i=1, 2, \ldots, n$. By applying $E_k^{a_k}$ to $v_1+v_2+\ldots+v_n=0$, we conclude $w_1+w_2+\ldots+w_n=0$. Note that since the submodules Nil_i are E-invariant by Lemma 2.1, $w_i\in \mathrm{Nil}_i$ for every i.

Claim 1. *If $v_i\neq 0$, then $w_i\neq 0$.*

Proof of Claim 1. If $i=k$ and $v_i=v_k\neq 0$, then $w_i=w_k=E_k^{a_k}(v_k)\neq 0$ by the choice of a_k. Suppose that $i\neq k$ and $v_i\neq 0$. Then

$$E_i^{a_i}(w_i)=E_i^{a_i}\left(E_k^{a_k}(v_i)\right)=E_k^{a_k}\left(E_i^{a_i}(v_i)\right)$$

But $E_i^{a_i}(v_i) \in \mathrm{Ker}_i$ and $E_i^{a_i}(v_i) \neq 0$ by the choice of a_i. Since E acts of Ker_i as the multiplication by α_i, we have

$$E_k^{a_k}\left(E_i^{a_i}(v_i)\right) = (E-\alpha_k)^{a_k}\left(E_i^{a_i}(v_i)\right) = (\alpha_i-\alpha_k)^{a_k}\left(E_i^{a_i}(v_i)\right).$$

Since $\alpha_i \neq \alpha_k$ and $\Bbbk$ is a ring withour zero divisors, $(\alpha_i-\alpha_k)^{a_k} \neq 0$. Since M is a torsion free k-module and $E_i^{a_i}(v_i) \neq 0$, this implies that $(\alpha_i-\alpha_k)^{a_k}\left(E_i^{a_i}(v_i)\right) \neq 0$. It follows that

$$E_i^{a_i}(w_i) = (\alpha_i-\alpha_k)^{a_k}\left(E_i^{a_i}(v_i)\right) \neq 0.$$

It follows that $w_i \neq 0$. This completes the proof of the claim. □

Claim 2. *If* $v_i \in \mathrm{Ker}_i$, *then* $w_i \in \mathrm{Ker}_i$.

Proof of Claim 2. Since the endomorphism E acts on Ker_i as the multiplication by α_i, the endomorphism $E-\alpha_k$ acts on Ker_i as the multiplication by $\alpha_i-\alpha_k$. Hence

$$E_k^{a_k}(v_i) = (E-\alpha_k)^{a_k}(v_i) = (\alpha_i-\alpha_k)^{a_k}(v_i).$$

The last formula allows us to compute $E(w_i)$:

$$\begin{aligned} E(w_i) &= E\left(E_k^{a_k}(v_i)\right) = E\left((\alpha_i-\alpha_k)^{a_k}(v_i)\right) = (\alpha_i-\alpha_k)^{a_k} E(v_i) \\ &= (\alpha_i-\alpha_k)^{a_k}\alpha_i v_i = \alpha_i(\alpha_i-\alpha_k)^{a_k} v_i = \alpha_i E_k^{a_k}(v_i) = \alpha_i w_i. \end{aligned}$$

The result of this computation shows that, indeed, $w_i \in \ker(E-\alpha_i) = \mathrm{Ker}_i$, and, hence, completes the proof of the claim. □

To sum up, we see that by applying $E_k^{a_k}$ to the equality $v_1+v_2+\ldots+v_n=0$ with $v_i \in \mathrm{Nil}_i$ for all i we get another equality $w_1+w_2+\ldots+w_n=0$ such that for all i:

(i) $w_i \in \mathrm{Nil}_i$;

(ii) *if* $v_i \neq 0$, *then* $w_i \neq 0$;

(iii) *if* $v_i \in \mathrm{Ker}_i$, *then* $w_i \in \mathrm{Ker}_i$.

In addition, $w_k = E_k^{a_k}(v_k) \in \mathrm{Ker}_k$ even if $v_k \notin \mathrm{Ker}_k$. Therefore, if $v_k \notin \mathrm{Ker}_k$, then by taking $w_1, w_2, \ldots, w_n$ as the new $v_1, v_2, \ldots, v_n$, we will increase the number of elements v_i such that $v_i \in \mathrm{Ker}_i$.

It follows that by starting with the equality $v_1+v_2+\ldots+v_n=0$ and consequtively applying endomorphisms $E_k^{a_k}$ for $k=1, 2, \ldots, n$, we will eventually prove the equality $v_1+v_2+\ldots+v_n=0$ for some new vectors v_i such that $v_i \in \mathrm{Ker}_i$ for all i, and still not all v_i are equal to 0. The contradiction with Lemma 2.2 completes the proof. ■

2.4. Lemma. *Let* $E\colon M \to M$ *be an endomorphism of* M *and let* α *be an eigenvalue of* E. *Suppose that* $v \in \mathrm{Nil}(\alpha)$. *Let* $a \geqslant 0$ *be the largest integer such that* $(E-\alpha)^a(v) \neq 0$, *and let* $v_i = (E-\alpha)^i(v)$ *for* $i = 0, 1, \ldots, a$. *Then the homomorphism* $\Bbbk^{a+1} \to M$ *defined by*

$$(x_0, x_1, \ldots, x_a) \mapsto x_0 v_0 + x_1 v_1 + \ldots + x_a v_a$$

is an isomorphism onto its image. In particular, $v_0, v_1, \ldots, v_a$ *are free generators of a free* $\Bbbk$*-submodule of* M.

Proof. It is sufficient to prove that our homomorphism is injective. In other terms, it is sufficient to prove that if

(10) $\quad x_0 v_0 + x_1 v_1 + \ldots + x_a v_a = 0$

for some $x_0, x_1, \ldots, x_a \in \Bbbk$, then $x_0 = x_1 = \ldots = x_a = 0$. Suppose that (10) holds and $x_i \neq 0$ for some i. Let $b \in \mathbf{N}$ be the minimal integer with the property $x_b \neq 0$. Let us apply $(E-\alpha)^{a-b}$ to (10). Note that if $i > b$, then

$$(E-\alpha)^{a-b}(v_i) = (E-\alpha)^{a-b}\Big((E-\alpha)^i(v)\Big) = (E-\alpha)^{a-b+i}(v) = 0$$

because $a-b+i > a$ and $(E-\alpha)^n(v) = 0$ for $n > a$ by the choice of a. Therefore, the operator $(E-\alpha)^{a-b}$ takes the left hand side of (10) to

$$x_b(E-\alpha)^{a-b}(v_b) = (E-\alpha)^{a-b}\Big((E-\alpha)^b(v)\Big) = (E-\alpha)^{a-b+b}(v) = (E-\alpha)^a(v),$$

and hence the result of application of $(E-\alpha)^{a-b}$ to (10) is

(11) $\quad x_b(E-\alpha)^a(v) = 0.$

But $(E-\alpha)^a(v) \neq 0$ by the choice of a, and $x_b \neq 0$ by the choice of b. Since the module M is assumed to be torsion free, these facts together with (11) lead to a contradiction. This contradictions shows that (10) may be true only if $x_i = 0$ for all i. ■

3. Sequences

Sequences. For a set X, a function $s\colon \mathbf{N} \to X$ is also called a *sequence* s *of elements of* X. A sequence of elements of the base ring $\Bbbk$ will be called simply a *sequence*. For $i \in \mathbf{N}$ we usually denote the value $s(i)$ by s_i and call it the i-th *term* of s. Each subset $A \subset \mathbf{N}$ defines a sequence $\varphi_A\colon \mathbf{N} \to \{0,1\}$, namely, the *characteristic function* of A:

$$\varphi_A(i) = 1 \text{ for } i \in A, \quad \varphi_A(i) = 0 \text{ for } i \notin A.$$

The following sequences of elements of $\mathbf{N}$ will play a special role:

$$\mathbf{1} = \varphi_{\mathbf{N}}; \quad \mathbf{1}^0 = \varphi_{\mathbf{N}\setminus\{0\}}; \quad \mathbf{I} = \mathrm{id}_{\mathbf{N}} \ \text{ (so } \mathbf{I}_n = n \text{ for all } n \in \mathbf{N}).$$

The $\Bbbk$-module of sequences. The set $\mathfrak{S}_\Bbbk$ of all sequences is a $\Bbbk$-module. The $\Bbbk$-module structure on $\mathfrak{S}_\Bbbk$ is given by the term-wise addition of sequences and the term-wise multiplication of sequences by elements of $\Bbbk$, which are defined as follows. The *term-wise sum* $r+s$ *of sequences* r, s is defined by $(r+s)_i = r_i + s_i$, and the *term-wise product* bs *of* $b \in \Bbbk$ *and a sequence* s is defined by $(bs)_i = bs_i$.

Since $\Bbbk$ is assumed to be an entire ring, and, in particular, $\Bbbk$ has no zero divisors, $bs \neq 0$ if $b \neq 0$ and $s \neq 0$. Therefore, $\mathfrak{S}_\Bbbk$ is a torsion free $\Bbbk$-module. In particular, we can apply the results of Section 2 to $\mathfrak{S}_\Bbbk$ and to submodules of $\mathfrak{S}_\Bbbk$ in the role of M.

The $\Bbbk$-endomorphisms $\mathfrak{S}_\Bbbk \to \mathfrak{S}_\Bbbk$ form a $\Bbbk$-algebra $\mathbf{End}\,\mathfrak{S}_\Bbbk$ with the composition as the multiplication. For an endomorphism $E \in \mathbf{End}\,\mathfrak{S}_\Bbbk$ and a sequence $s \in \mathfrak{S}_\Bbbk$ we usually denote the value $E(s)$ by Es.

The multiplication operators. The *term-wise product* $r \cdot s$ *of sequences* r, s is defined by $(r \cdot s)_i = r_i s_i$. Obviously, the term-wise product is associative and distributive with respect to the term-wise addition. For a sequence r we denote by $r\cdot : \mathfrak{S}_\Bbbk \to \mathfrak{S}_\Bbbk$ the operation of term-wise multiplication by r on the left. In other terms, $r\cdot(s) = r \cdot s$. Since the ring $\Bbbk$ is commutative, $r\cdot$ is a $\Bbbk$-module endmorphism of $\mathfrak{S}_\Bbbk$.

As an example, we point out an obvious identity: $\mathbf{I} \cdot \mathbf{1}^0 = \mathbf{I}$.

The shift operators. The *left and right shift operators* $L, R \colon \mathfrak{S}_\Bbbk \to \mathfrak{S}_\Bbbk$ are defined by

$$\begin{aligned} (Ls)_i &= s_{i+1} \quad \text{for all } i \in \mathbf{N}, \\ (Rs)_0 &= 0, \qquad \text{and } (Rs)_i = s_{i-1} \text{ for } i \in \mathbf{N},\ i \geqslant 1. \end{aligned}$$

Some obvious properties of the operators L, R are listed in the next lemma. In particular, this lemma shows that the operators L and R are almost inverses of each other.

3.1. Lemma. $L \circ R = \mathrm{id}$, $R \circ L = \mathbf{1}^0\cdot$, $L(\mathbf{I}) = \mathbf{I} + \mathbf{1}$. ■

The representation defined by the left shift. Recall that if a $\Bbbk$-module M and an endomorphism $E \colon M \to M$ are given, then $f(x) \mapsto f(E)$ is representation $\Bbbk[x] \to \mathbf{End}\,M$. In particular, the left shift operator $L \colon \mathfrak{S}_\Bbbk \to \mathfrak{S}_\Bbbk$ defines a representation $h_L \colon \Bbbk[x] \to \mathfrak{S}_\Bbbk$. It takes $f(x) \in \Bbbk[x]$ to $f(L)$.

Linear requrrence relations. Suppose that $f(x) = c_0x^n + c_1x^{n-1} + c_2x^{n-2} + \ldots + c_n \in \Bbbk[x]$, and suppose that $c_n \neq 0$ and c_0 is invertible in $\Bbbk$. If a sequence $s \in \mathfrak{S}_\Bbbk$ belongs to the kernel $\mathrm{Ker}\, f(L)$, i.e. if $f(L)s = f(L)(s) = 0$, then we say that s satisfies a *linear recurrence relation* and that $f(x)$ is *the characteristic polynomial* of this relation. A sequence $s \in \mathfrak{S}_\Bbbk$ is said to be a *linearly recurrent sequence* if s satisfies a linear recurrence relation with some characteristic polynomial $f(x)$ as above.

The classical form of the linear recurrence relations. Let us compute the terms of $f(L)s$:

$$\begin{aligned}(f(L)s)_i &= ((c_0L^n + c_1L^{n-1} + c_2L^{n-2} + \ldots + c_n)s)_i \\ &= c_0(L^n s)_i + c_1(L^{n-1}s)_i + c_2(L^{n-2}s)_i + \ldots + c_n(L^0 s)_i \\ &= c_0 s_{i+n} + c_1 s_{i+n-1} + c_2 s_{i+n-2} + \ldots + c_n s_i.\end{aligned}$$

This calculation shows that $s \in \operatorname{Ker} f(L)$ if and only if the equation

$$(\sigma_i) \quad c_0 s_{i+n} + c_1 s_{i+n-1} + c_2 s_{i+n-2} + \ldots + c_n s_i = 0.$$

holds for all $i \geqslant 0$. Since c_0 is assumed to be invertible in $\Bbbk$, we can divide (σ_i) by c_0. After doing this and moving all terms except s_{i+n} to the right hand side, (σ_i) turns into an equation expressing s_{i+n} as a linear combination of n preceding terms with the coefficients not depending on i.

3.2. Lemma. *The map* $s \mapsto (s_0, s_1, \ldots, s_{n-1})$ *establishes an isomorphism* $\operatorname{Ker} f(L) \to \Bbbk^n$. *In particular, in this case* $\operatorname{Ker} f(L)$ *is a free* $\Bbbk$*-module of rank* n.

Proof. Clearly, the equations (σ_i) for $i \geqslant 0$ do not impose any restrictions on the first n terms $s_0, s_1, \ldots, s_{n-1}$ of s. Since c_0 is assumed to be invertible in $\Bbbk$, the terms s_i with $i \geqslant n$ are recursively determined by the equations (σ_0), (σ_1), etc. The lemma follows. ■

4. Derivatives

Derivatives of polynomials. The derivative of a polynomial

$$f(x) = c_0x^n + c_1x^{n-1} + c_2x^{n-2} + \ldots + c_n \in \Bbbk[x]$$

is *defined* as the polynomial

$$f'(x) = c_0nx^{n-1} + c_1(n-1)x^{n-2} + \ldots + c_{n-1} \in \Bbbk[x].$$

If it is clear from the context what is the variable, then it may be omitted from the notations and the derivative of $f \in \Bbbk[x]$ may be denoted by $f' \in \Bbbk[x]$. The usual properties of derivatives, such as the linearity and the Leibniz formula, can be verified by straightforward computations. Let $d\colon \Bbbk[x] \to \Bbbk[x]$ be the endomorphism of the $\Bbbk$-module $\Bbbk[x]$ defined by $f(x) \mapsto f'(x)$. Then $d(f(x)) = f'(x)$, or, what is the same, $d(f) = f'$. For $a \in \mathbf{N}$ the a-fold composition $d^a = d \circ \ldots \circ d$ is nothing else but the operation of taking the a-th derivative of f. In particular, $d^1 f = df = f'$ and $d^0 f = f$ for all $f \in \Bbbk[x]$.

Derivatives of sequences. The *derivative operator* $D\colon \mathfrak{S}_{\Bbbk} \to \mathfrak{S}_{\Bbbk}$ is defined as the composition $D = (\mathbf{I}\cdot) \circ R$. Equivalently, $D(s) = \mathbf{I}\cdot(R(s))$ for all $s \in \mathfrak{S}_{\Bbbk}$. Using our agreements from Section 3, we may omit parentheses in this formula and write it as $Ds = \mathbf{I}\cdot Rs$.

The value $D(s)$ is called the *derivative* of s. Obviously, the i-th term $(Ds)_i$ of the derivative Ds is equal to is_{i-1} for $i \geqslant 1$, and to 0 for $i = 0$. This implies, in particular, that if $i > 0$ and $s_i \neq 0$, then $(Ds)_{i+1} \neq 0$.

For $a \in \mathbf{N}$, the a-fold composition $D^a = D \circ \ldots \circ D$ is called the a-th derivative operator, or, when the value of a is not relevant, a *higher derivative operator*. The value $D^a s$ is called the a-th derivative of s.

4.1. Lemma. *Let $\alpha \in \Bbbk$. Then*

$$D(Ls) = L(Ds) - s \quad \textit{and} \quad D((L-\alpha)s) = (L-\alpha)(Ds) - s \tag{12}$$

for every $s \in \mathfrak{S}_{\Bbbk}$. Equivalently,

$$D \circ L = L \circ D - \mathrm{id} \quad \textit{and} \quad D \circ (L-\alpha) = (L-\alpha) \circ D - \mathrm{id}. \tag{13}$$

Proof. Let us start with two observations: $\mathbf{I}\cdot 1^0 = \mathbf{I}$; $L(\mathbf{I}) = \mathbf{I}+1$. By using these observations together with Lemma 3.1, we see that:

$$D(Ls) = \mathbf{I}\cdot(R\circ L(s)) = \mathbf{I}\cdot(1^0\cdot s) = (\mathbf{I}\cdot 1^0)\cdot s = \mathbf{I}\cdot s;$$
$$L(Ds) = L(\mathbf{I}\cdot R(s)) = L(\mathbf{I})\cdot L(R(s)) = (L(\mathbf{I}))\cdot(L\circ R(s)) = (\mathbf{I}+1)\cdot s.$$

It follows that $D(Ls) = \mathbf{I}\cdot s = (\mathbf{I}+1)\cdot s - 1\cdot s = L(Ds) - s$. Therefore, $D(Ls) = L(Ds) - s$ for all s. Since D is $\Bbbk$-linear, we have $\alpha Ds = D(\alpha s)$. By subtracting $\alpha Ds = D(\alpha s)$ from $L(Ds) = D(Ls) + s$ we see that

$$(L-\alpha)(Ds) = D((L-\alpha)s) + s$$

for all s. This proves (12) for all s. Clearly, (13) is equivalent to (12). ■

4.2. Lemma. $D \circ L^n = L^n \circ D - nL^{n-1}$, *i.e.* $D(L^n s) = L^n(Ds) - nL^{n-1}s$ *for every $s \in \mathfrak{S}_{\Bbbk}$ and $n \in \mathbf{N}$, $n \geqslant 1$.*

Proof. We will use an induction by n. For $n = 1$ the lemma reduces to Lemma 4.1. Suppose that the lemma is already proved for $n = m-1$. Lemma 4.1 applied to $L^{m-1}s$ in the role of s implies that

$$D(L^m s) = D(L(L^{m-1}s)) = L(D(L^{m-1}s)) - L^{m-1}s.$$

By the case $n = m-1$ of the lemma, $D(L^{m-1}s) = L^{m-1}(Ds) - (m-1)L^{m-2}s$, and hence

$$\begin{aligned} D(L^m s) &= L\,(D(L^{m-1}s)) - L^{m-1}s \\ &= L\,(L^{m-1}(Ds) - (m-1)L^{m-2}s) - L^{m-1}s \\ &= L^m(Ds) - (m-1)L^{m-1}s - L^{m-1}s \\ &= L^m(Ds) - mL^{m-1}s. \end{aligned}$$

The lemma follows. ■

4.3. Corollary. *Let* $f(x) = x^n$, *where* $n \in \mathbf{N}$. *Then for every* $s \in \mathfrak{S}_{\Bbbk}$ *we have*

$$D(f(L)s) = f(L)(Ds) - f'(L)s.$$

Proof. If $n = 0$, then $f(x) = 1$, $f'(x) = 0$, and hence $f(L) = \mathrm{id}$, $f'(L) = 0$. Hence, in this case our identity reduces to $Ds = Ds$. For $n \geqslant 1$, it is sufficient to combine the lemma with $(x^n)' = nx^{n-1}$. ■

4.4. Corollary. *Let* $f(x) \in \Bbbk[x]$. *Then for every* $s \in \mathfrak{S}_{\Bbbk}$ *we have*

$$D(f(L)s) = f(L)(Ds) - f'(L)s.$$

Proof. For monomials $f(x) = cx^n$, where $c \in \Bbbk$, this immediately follows from Corollary 4.3. It remains to notice that every polynomial is a finite sum of such monomials and all involved operations are linear in f. ■

4.5. Lemma. *Let* $f(x) \in \Bbbk[x]$ *and* $s \in \mathfrak{S}_{\Bbbk}$. *If* $f(L)s = 0$ *and* $f'(L)s = 0$, *then* $f(L)(Ds) = 0$.

Proof. If $f(L)s = 0$, then $D(f(L)s) = 0$. Since $f'(L)s = 0$ by the assumption, this means that two terms of the identity of Corollary 4.4 are equal to 0. Therefore, the third term is also equal to 0, i.e. $f(L)(Ds) = 0$. ■

4.6. Lemma *Let* $f(x) \in \Bbbk[x]$ *and* $s \in \mathfrak{S}_{\Bbbk}$. *Suppose that* $\mu \in \mathbf{N}$, $\mu \geqslant 1$, *and that* $(d^a f)(L)s = 0$ *for all* $a = 0, 1, \ldots, \mu$. *Then* $f(L)(D^a s) = 0$ *for* $a = 0, 1, \ldots, \mu$.

Proof. We will use an induction by μ. For $\mu = 1$ the lemma reduces to Lemma 4.5. Suppose that the lemma is already proved for $\mu \leqslant \nu$, where $\nu \in \mathbf{N}$, $\nu \geqslant 1$, and suppose that $(d^a f)(L)s = 0$ for $a = 0, 1, \ldots, \nu+1$.

Note that $d^a f'(X) = d^{a+1} f(x)$ for all $a \in \mathbf{N}$. Therefore, $d^a f'(L)s = 0$ for $a = 0, 1, \ldots, \mu$. By applying the case $\mu = \nu$ of the lemma to s and $f'(x)$ we conclude that $f'(L)(D^a s) = 0$ for all $a = 0, 1, \ldots, \mu$. In particular, $f'(L)(D^\mu s) = 0$.

By applying the case $\mu = \nu$ of the lemma to s and $f(x)$, we conclude that $f(L)(D^a s) = 0$ for all $a = 0, 1, \ldots, \mu$. In particular, $f(L)(D^\mu s) = 0$.

Therefore, $f(L)(D^\mu s) = 0$ and $f'(L)(D^\mu s) = 0$. Hence $f(L)(DD^\mu s) = 0$ by Lemma 4.5. But $DD^\mu = D^{\mu+1}$, and hence $f(L)(D^{\mu+1} s) = 0$. By combining this with the previous paragraph, we see that $f(L)(D^a s) = 0$ for all $a = 0, 1, \ldots, \mu, \mu+1$. This completes the step of the induction, and hence the proof of the lemma. ■

5. Powers

Sequences of powers $s(\alpha)$ ***and their derivatives*** $s_D(\alpha, n)$**.** Given $\alpha \in \Bbbk$, let $s(\alpha)$ be the sequence defined by

(14) $s(\alpha)_i = \alpha^i$ for all $i \in \mathbf{N}$.

Obviously, $Ls(\alpha) = \alpha s(\alpha)$, or, equivalently,

(15) $(L - \alpha)s(\alpha) = 0$.

The sequence $s_D(\alpha, n)$, where $n \in \mathbf{N}$, is defined as the n-th derivative of $s(\alpha)$:

(16) $s_D(\alpha, n) = D^n s(\alpha)$.

5.1. Lemma *If* $\alpha \neq 0$, *then* $s_D(\alpha, n) \neq 0$ *for all* $n \in \mathbf{N}$.

Proof. By a remark after the definition of the derivative D (see Section 4), $(Ds)_{i+1} \neq 0$ if $i > 0$ and $s_i \neq 0$. An induction by n shows that $(D^n s)_{i+n} \neq 0$ if $n \geqslant 1$, $i > 0$ and $s_i \neq 0$. Since all terms of $s_D(\alpha, n)$ are non-zero if α is non-zero, the lemma follows. ■

5.2. Lemma. $(L - \alpha)s_D(\alpha, 0) = 0$ *and* $(L - \alpha)s_D(\alpha, n) = n s_D(\alpha, n-1)$ *if* $n \in \mathbf{Z}$, $n \geqslant 1$.

Proof. By the definition $s_D(\alpha, 0) = D^0 s(\alpha) = s(\alpha)$. Therefore, (15) implies the first statement of the lemma. The second statement is proved by induction. For $n = 1$, we have

$$s_D(\alpha, n) = s_D(\alpha, 1) = D^1 s(\alpha) = Ds(\alpha),$$
$$s_D(\alpha, n-1) = s_D(\alpha, 1-1) = s_D(\alpha, 0) = D^0 s(\alpha) = s(\alpha).$$

Therefore, for $n = 1$ the lemma reduces to the equality $(L - \alpha)(Ds(\alpha)) = s(\alpha)$, which follows from Lemma 4.1 together with (15).

Suppose that the lemma holds for a fixed $n \geqslant 1$. Then

$$\begin{aligned}(L-\alpha)s_D(\alpha,n+1) &= (L-\alpha)\left(D^{n+1}s(\alpha)\right)\\ &= (L-\alpha)\left(DD^n s(\alpha)\right)\\ &= \left((L-\alpha)D\right)\left(D^n s(\alpha)\right)\end{aligned}$$

Now we can apply Lemma 4.1 and conclude that the last expression is equal to

$$\begin{aligned}\left(D(L-\alpha)+\mathrm{id}\right)\left(D^n s(\alpha)\right) &= D\left((L-\alpha)D^n s(\alpha)\right)+D^n s(\alpha)\\ &= D\left(nD^{n-1}s(\alpha)\right)+D^n s(\alpha) \quad \text{(by the assumption)}\\ &= nD^n s(\alpha)+D^n s(\alpha)\\ &= (n+1)D^n s(\alpha) = (n+1)s_D(\alpha,n).\end{aligned}$$

It follows that the second statement holds for $n+1$ in the role of n. An application of the induction completes the proof. ■

Falling powers. Let x be a variable, a let $a\in\mathbf{N}$. The a-th *falling power* $\Delta^a_x\in\mathbf{Z}[x]$ of x is a polynomial in x with integer coefficients defined by

$$\Delta^0_x = 1, \quad \textit{and} \quad \Delta^a_x = x(x-1)\dots(x-a+1) \quad \textit{for} \quad a\geqslant 1.$$

For an integer $n\in\mathbf{Z}$ we denote by Δ^a_n the value of the polynomial Δ^a_x at $x=n$. The following properties of falling powers follow immediately from the definition.

(17) $\Delta^{a+1}_x = \Delta^a_x(x-a)$.

(18) *If* $n\in\mathbf{N}$ *and* $a>n$, *then* $\Delta^a_n=0$.

5.3. Lemma. *If* $a,n\in\mathbf{N}$ *and* $a\leqslant n$, *then* $(L-\alpha)^a s_D(\alpha,n) = \Delta^a_n s_D(\alpha,n-a)$.

Proof. Since $(L-\alpha)^0=\mathrm{id}$ and $\Delta^0_n=1$, for $a=0$ the lemma is trivial. For $a=1$ the lemma follows from Lemma 5.2 together with the obvious identity $\Delta^1_n=n$. In order to prove the lemma for all $a\geqslant 1$ we use induction by a. The step of the induction follows from Lemma 5.2 together with (17). ■

5.4. Corollary. *Suppose that* $\alpha\neq 0$. *If* $a>n$, *then* $(L-\alpha)^a s_D(\alpha,n)=0$. *If* $0\leqslant a\leqslant n$ *and* $\operatorname{char}\Bbbk=0$ *or* $\operatorname{char}\Bbbk\geqslant\mu$, *then* $(L-\alpha)^a s_D(\alpha,n)\neq 0$.

Proof. The first statement immediately follows from (18). Let us prove the second one.

Since $\alpha\neq 0$, all sequences $s_D(\alpha,n)$ are not equal to 0 by Lemma 5.1. Note that under our assumptions about $\operatorname{char}\Bbbk$ the image of Δ^a_n in $\Bbbk$ is not equal to 0. Since $\mathfrak{S}_\Bbbk$ is a torsion free $\Bbbk$-module, the second statement follows from Lemma 5.3. ■

6. Theorems

6.1. Theorem. *Suppose that* $f(x) \in \Bbbk[x]$ *and that* $\alpha \in \Bbbk$ *is a root of the polynomial* $f(x)$ *of the multiplicity* μ. *Then* $f(L)(s_D(\alpha, a)) = 0$ *for* $a = 0, 1, \dots, \mu - 1$.

Proof. First, recall that if α is a root of $f(x)$, then $f(x) = g(x)(x - \alpha)$ for some polynomial $g(x)$. Therefore, (15) implies that $f(L)(s(\alpha)) = g(L)((L - \alpha)s(\alpha)) = g(L)(0) = 0$.

Recall that the multiplicity of a root is $\geqslant 1$. It is well known that a root of the multiplicity μ of $f(x)$ is also a root of the derivatives $d^a f$ of $f(x)$ of order $a \leqslant \mu - 1$. Therefore, $d^a f(\alpha) = 0$ for $a = 0, 1, \dots, \mu - 1$. In view of the result of the previous paragraph, this implies that $d^a f(L)(s(\alpha)) = 0$ for $a = 0, 1, \dots, \mu - 1$.

Now, Lemma 4.6 implies that $f(L)(D^a s(\alpha)) = 0$ for $a = 0, 1, \dots, \mu - 1$. Since $s_D(\alpha, a) = D^a s(\alpha)$ by the definition (16), this proves that $f(L)(s_D(\alpha, a)) = 0$. ■

The framework. In the remaining part of the paper we consider a fixed polynomial $f(x) \in \Bbbk[x]$. We assume that $\Bbbk$ contains all roots of $f(x)$. In other terms, we will assume that $f(x)$ is a product of a constant $c_0 \in \Bbbk$, $c \neq 0$, and several linear factors of the form $(x - \alpha)$ with $\alpha \in \Bbbk[x]$. Clearly, c_0 is the leading coefficient of $f(x)$, i.e. the coefficient in front of highest power of x entering $f(x)$ with a non-zero coeffiecient.

As in the definition of the linear recurrence relations (see Section 3), we will assume that this leading coefficient c_0 is invertible in $\Bbbk$, and that the free term of $f(x)$ is non-zero.

Let $n = \deg f(x)$ be the degree of $f(x)$. Let k be the number of distinct roots of $f(x)$ has k, and let $\alpha_1, \alpha_2, \dots, \alpha_k \in \Bbbk$ be these roots. For $i = 1, 2, , \dots, k$, we will denote by μ_i be the multiplicity of the root α_i. Then $n = \deg f(x) = \mu_1 + \mu_2 + \dots + \mu_k$. We will denote by μ the maximum of the multiplicities of the roots, namely, the maximum of the numbers $\mu_1, \mu_2, \dots \mu_k$.

The assumption that the free term of $f(x)$ is non-zero is equivalent to 0 not being a root of $f(x)$. In other terms, none of α_i (where $i = 1, 2, , \dots, k$) is equal to 0.

For the rest of thus section we will assume that either $\operatorname{char} \Bbbk = 0$ ***or*** $\operatorname{char} \Bbbk > \mu$.

6.2. Theorem. *The sequences* $s_D(\alpha_u, a)$ *with* $1 \leqslant u \leqslant k$ *and* $0 \leqslant a \leqslant \mu_u - 1$ *are free generators of a free* $\Bbbk$*-submodule of* $\operatorname{Ker} f(L)$.

Proof. By Theorem 6.1, all these sequences belong to $\operatorname{Ker} f(L)$. In order to prove the rest, let us consider the $\Bbbk$-module $\operatorname{Ker} f(L)$. The left shift operator L induces an endomorphism of $\operatorname{Ker} f(L)$. Indeed, if $s \in \operatorname{Ker} f(L)$, then $f(L)s = 0$ and

$$f(L)(Ls) = f(L)L(s) = Lf(L)(s) = L(f(L)s) = Lo = o.$$

It follows that $\mathrm{Ker}\, f(L)$ is L-invariant, i.e. L induces an endomorphism of $\mathrm{Ker}\, f(L)$.

Let $1 \leqslant u \leqslant k$. Since $\alpha_u \neq o$ by our assumptions, Corollary 5.4 implies that

$$(L-\alpha_u)^a s_D(\alpha_u, \mu_u - 1) \neq o \quad \text{if} \quad o \leqslant a \leqslant \mu_u - 1, \quad \text{and}$$

$$(L-\alpha_u)^a s_D(\alpha_u, \mu_u - 1) = o \quad \text{if} \quad a = \mu_u.$$

Therefore $s_D(\alpha_u, \mu_u - 1)$ belongs to the extended eigenmodule of L considered as an endomorphism of $\mathrm{Ker}\, f(L)$ corresponding to the eigenvalue μ_u. In other terms,

$$s_D(\alpha_u, \mu_u - 1) \in \mathrm{Nil}(\alpha_u).$$

In addition, $a = \mu_u - 1$ is the largest integer a such that $(L-\alpha_u)^a s_D(\alpha_u, \mu_u - 1) \neq o$.

Now, Lemma 2.4 implies that the sequences

$$(L-\alpha_u)^a s_D(\alpha_u, \mu_u - 1)$$

with $a = o, 1, \ldots, \mu_u - 1$ form a basis of a free submodule of $\mathrm{Nil}(\alpha_u) \subset \mathrm{Ker}\, f(L)$. In view of Lemma 5.3, this means that the sequences

$$\Delta^a_{\mu_u - 1}\, s_D(\alpha_u, \mu_u - 1 - a)$$

with $a = o, 1, \ldots, \mu_u - 1$ form a basis of a free submodule of $\mathrm{Nil}(\alpha_u) \subset \mathrm{Ker}\, f(L)$.

By combining the result of the last paragraph with Lemma 1.1, we see that the n sequences $s_D(\alpha_u, a)$ from the theorem form a basis of a free submodulte of $\mathrm{Ker}\, f(L)$. This completes the proof of the theorem. ■

6.3. Theorem. *Let $S_D \subset \mathrm{Ker}\, f(L)$ be the free $\Bbbk$-module generated by the n sequences $s_D(\alpha_u, a)$ from Theorem 6.2. Then the quotient $\Bbbk$-module $(\mathrm{Ker}\, f(L))/S_D$ is a torsion module. Moreover, $x(\mathrm{Ker}\, f(L))/S_D = o$ for some non-zero $x \in \Bbbk$.*

Proof. By Lemma 3.2, $\mathrm{Ker}\, f(L)$ is a free module of rank n, i.e. is isomorphic to $\Bbbk^n$. Since $n = \mu_1 + \ldots + \mu_k$, we have exactly n sequences $s_D(\alpha_u, a)$. By Theorem 6.2, they are free generators of S_D. In particular, S_D is also isomorphic to $\Bbbk^n$. It remains to apply Lemma 1.2 (with $\Bbbk$ in the role of K). ■

6.4. Theorem. *If $\Bbbk$ is a field, then $S_D = \mathrm{Ker}\, f(L)$.*

Proof. A torsion module over a field is equal to o. ■

Remark. Of course, Theorem 6.4 immediately follows from Theorem 6.2 without the detour through Lemma 1.2 and Theorem 6.3.

Remark. Theorems 6.2, 6.3, and 6.4 are not true without the assumption that either $\operatorname{char} \Bbbk = 0$ or $\operatorname{char} \Bbbk > \mu$. In fact, if $\operatorname{char} \Bbbk \neq 0$ and $a \geqslant \operatorname{char} \Bbbk$, then $s_D(\alpha, a) = 0$ for all $\alpha \in \Bbbk$.

December 14, 2014

http://nikolaivivanov.com