ECONOMETRIC INSTITUTE

OPERATIONS IN THE K-THEORY OF ENDOMORPHISMS

M. HAZEWINKEL

REPORT 8131/M

ERASMUS UNIVERSITY ROTTERDAM - P.O. BOX 1738 - 3000 DR ROTTERDAM - THE NETHERLANDS

OPERATIONS IN THE K-THEORY OF ENDOMORPHISMS*)

by

Michiel Hazewinkel
Dept. Math., Erasmus Univ. Rotterdam
P.O. Box 1738, 3000 DR ROTTERDAM, The Netherlands

Abstract. For a commutative ring with unity A let End A be the category of all pairs (P,f) where P is a finitely generated projective A-module and f an endomorphism of A. The K-group $K_o(A)$ is a direct summand and ideal of $K_o(\text{End}A)$ and Almkvist showed that the quotient ring $W_o(A) = K_o(\text{End}A)/K_o(A)$ is a functorial subring of the ring of the big Witt vectors W(A). [1]. In this paper I determine the ring of all continuous functorial operations on $W_o(-)$ and the semiring of all operations (and all continuous operations) liftable to End(A). This solves some of the open problems listed in [1].

Contents.

*) During the research for and writing of this paper, the author was visiting the Inst. de Ciencias, Univ. Autonoma de Puebla, whose hospitality and support is gratefully acknowledged.

OPERATIONS IN THE K-THEORY OF ENDOMORPHISMS

Michiel Hazewinkel

1. INTRODUCTION, DEFINITIONS AND STATEMENT OF MAIN RESULTS.

Let A be a commutative ring with unit element. With $\underline{\underline{\mathrm{End}}}$ A we denote the category of pairs (P,f) where P is a finitely generated projective module over A and f an endomorphism of P. A morphism u: (P,f) → (Q,g) is a morphism of A-modules u: P → Q such that gu = uf. There is an obvious notion of short exact sequence in $\underline{\underline{\mathrm{End}}}$ A: it is a commutative diagram with exact rows of the form

$$\begin{array}{ccccccccc} 0 & \to & P & \xrightarrow{u} & Q & \xrightarrow{v} & R & \to & 0 \\ & & \downarrow f & & \downarrow g & & \downarrow h & & \\ 0 & \to & P & \to & Q & \to & R & \to & 0 \end{array} \qquad (1.1)$$

1.2. Definition.[1,2]. $K_0(\underline{\underline{\mathrm{End}}}\ A)$ is the free abelian group generated by all isomorphism classes [P,f] of objects in $\underline{\underline{\mathrm{End}}}$ A modulo the subgroup generated by all elements of the form [Q,g] - [P,f] - [R,h] for all exact sequences (1.1).

The tensor product ((P,f), (Q,g)) → (P⊗Q,f⊗g) induces a ring structure on $K_0(\underline{\underline{\mathrm{End}}}\ A)$ for which the unit element is the class of (A,1). (All tensor products are over A). Further the classes of the form (Q,0) form an ideal in $K_0(\underline{\underline{\mathrm{End}}}\ A)$. This ideal identifies naturally with $K_0(A)$ via P↦ (P,0).

1.3. Definition. The ring of rational Witt vectors. The quotient ring is denoted $K_0(\underline{\underline{\mathrm{End}}}\ A)/K_0(A) = W_0(A)$. I like to call the elements of $W_0(A)$ rational Witt vectors for reasons which will become obvious immediately below.

1.4. The big Witt vectors. For each ring R let W(R) be the abelian group of all power series of the form $1 + r_1t + r_2t^2 + \ldots$, $r_i \in R$. Obviously this functor is represented by the ring $\mathbb{Z}[X_1,X_2,\ldots]$;
i.e. $\underline{\underline{\mathrm{Ring}}}(\mathbb{Z}[X],R) \simeq W(R)$ functorially. The group W(R) also carries a multiplication which is characterized by $(1-r_1t)*(1-r_2t) = 1 - r_1r_2t$ for which 1 - t acts as a unit. This makes W(R) functorially a commutative ring with unit. This functorial ring W(R) admits functorial ring endomorphisms called Frobenius operators which are characterized by $F_n(1-at) = (1-a^nt)$.

Cf. [4, chapter III] for a rather detailed treatment of Witt vectors.

1.5. Almkvist's homomorphism. Let $(P,f) \in \underline{\underline{End}}\ A$. Let Q be a finitely generated projective A-module such that $P \oplus Q$ is free and consider the endomorphism $f \oplus 0$ of $P \oplus Q$. Consider $\det(1+t(f\oplus 0))$. This is a polynomial in t which does not depend on Q. This induces a homomorphism $K_o(\underline{\underline{End}}\ A) \to W(A)$ which is (obviously) zero on $K_o(A)$. It is also obviously additive and multiplicative so that there results a homomorphism of rings

$$(1.6) \qquad c: K_o(\underline{\underline{End}}A)/K_o(A) = W_o(A) \to W(A)$$

which is functorial in A. In [2] Almkvist now proves:

1.7. Theorem [2]. The homomorphism c is injective for all A and the image of c (for a given A) consists of all power series $1 + a_1t + a_2t^2 + \dots$ which can be written in the form

$$1 + a_1t + a_2t^2 + \dots = \frac{1+b_1t+\dots+b_rt^r}{1+d_1t+\dots+d_nt^n}, \quad b_i, d_j \in A$$

(Whence the name rational Witt vectors; the c in (1.6) stands for characteristic polynomial).

1.8. Topology on $W_o(A)$, $W(A)$. Let $W^{(n)}(A)$ be the subgroup of all power series of the form $1 + a_{n+1}t^{n+1} + \dots \in W(A)$. These subgroups define a topology on W(A) and $W_o(A) \subset W(A)$ is given the induced topology. Let $W_o^+(A)$ be the subset of W(A) consisting of all polynomials $1 + a_1t + a_2t^2 + \dots a_rt^r$. Then $W_o^+(A)$ and $W_o(A)$ are dense in W(A). With this definition W_o, W, W_o^+ become functors $\underline{\underline{Ring}} \to \underline{\underline{Top}}$, where $\underline{\underline{Top}}$ is the category of Hausdorff topological spaces. The $W^{(n)}(A)$ are in fact ideals in W(A) so that W_o, W_n can also be considered to take their values in the categories $\underline{\underline{TRng}}$ of topological rings or $\underline{\underline{TAb}}$ of topological abelian groups and W_o^+ can be considered to take its values in the category of topological semigroups.

1.9. Operations. Let F be a functor, e.g. a functor F: Ring → Set. Then an operation for F(-) is a functorial transformation u: F → F. Below I shall determine all operations for the functors W_o and W_o^+ considered as functors Ring → Top, i.e. all functorial transformations of sets $W_o(A) \to W_o(A)$, $W_o^+(A) \to W_o^+(A)$ which are continuous with respect to the topologies on $W_o(A)$, $W_o^+(A)$, and also of W_o as a functor to TAb (additive operations) and as a functor to TRng (multiplicative operations). Here $W_o^+(A)$ is the image of End_A in $W_o(A)$ which via c identifies with the commutative sub-semiring of W(A) consisting of all polynomials $1 + a_1t + \ldots + a_rt^r$. (This is fairly obvious, but cf. also 2.4 below). I shall also determine what various natural operations on End A like exterior products and symmetric products correspond to in W(A). All these questions were posed as problems in [1].

1.10. Two Topologies on the ring $\mathbb{Z}[X]$. Before I can describe the results I have to define two topologies on the ring $\mathbb{Z}[X_1,X_2,X_3,\ldots] = \mathbb{Z}[X]$. For each $n \in \mathbb{N}$ let I_n be the ideal of $\mathbb{Z}[X]$ generated by the elements $X_{n+1}, X_{n+2}, \ldots$ The I-topology on $\mathbb{Z}[X]$ is the one defined by this sequence of ideals. The second and more important topology is also more difficult to describe. Consider the infinite Hankel matrix

$$(1.11) \qquad \begin{pmatrix} 1 & X_1 & X_2 & X_3 & \ldots \\ X_1 & X_2 & X_3 & X_4 & \ldots \\ X_2 & X_3 & X_4 & X_5 & \ldots \\ \cdot & \cdot & \cdot & \cdot & \\ \cdot & \cdot & \cdot & \cdot & \\ \cdot & \cdot & \cdot & \cdot & \end{pmatrix}$$

Now for each $n \in \mathbb{N}$ let J_n be the ideal generated by all the (n+1) x (n+1) minors of this matrix.

Let $\mathbb{Z}_I[X]$ and $\mathbb{Z}_J[X]$ denote the completions of $\mathbb{Z}[X]$ with respect to the I-topology and the J-topology.

The ring of power series in infinitely many variables $\mathbb{Z}[[X]]$ is defined as the ring of all expressions $\sum_\alpha c_\alpha X^\alpha$ where α runs through all multiindices $\alpha = (\alpha_1, \alpha_2, \alpha_3, \ldots)$, $\alpha_i \in \mathbb{N} \cup \{0\}$ such that $\alpha_i = 0$ for all but finitely many i. Here X^α is short for the finite monomial

$$X^\alpha = \prod_{\alpha_i \neq 0} X_i^{\alpha_i}$$

Both $\mathbb{Z}_I[X]$ and $\mathbb{Z}_J[X]$ can be considered as subrings of $\mathbb{Z}[[X]]$. For instance the elements of $\mathbb{Z}_I[X]$ are power series $f(X)$ in $X_1, X_2, \ldots$ with the extra property that $f(X)$ is a polynomial mod I_n for all n. Thus e.g. $X_1X_2 + X_1X_3 + X_1X_4 + X_1X_5 + \ldots$ is in $\mathbb{Z}_I[X]$ but $1 + X_1 + X_1^2 + X_1^3 + \ldots$ is not in $\mathbb{Z}_I[X]$.

We also note that $J_n \subset I_{n-1}$ so that there is a natural inclusion $\mathbb{Z}_J[X] \to \mathbb{Z}_I[X]$.

With these notions we can state the main results as

1.12. Theorem. The continuous operations of $W_o^+(-)$ correspond naturally to ring endomorphisms of $\mathbb{Z}[X]$ which are continuous in the I-topology (on both source and target). The (not necessarily continuous) operations of W_o^+ correspond to naturally to ring endomorphisms of $\mathbb{Z}_I[X]$.

1.13. Theorem.

(i) The continuous operations of $W_o(-)$ correspond naturally to ring endomorphisms of $\mathbb{Z}[X]$, which are continuous in the J-topology (on both source and target)

(ii) The additive continuous operations of $W_o(-)$ correspond to elements $1 + x_1t + x_2t^2 + \ldots \in W(\mathbb{Z}[X])$ such that $\lim_{i\to\infty} x_i = 0$ in the J-topology and $\mu(x_n) = \sum_{i+j=n} x_i \otimes x_j$, where $\mu : \mathbb{Z}[X] \to \mathbb{Z}[X] \otimes \mathbb{Z}[X]$ is the coalgebra structure defined by $X_n \mapsto \sum_{i+j=n} X_i \otimes X_j$.

(iii) The multiplicative and unit preserving continuous operations of $W_o(-)$ are the Frobenius operations.

I would like to thank Ton Vorst for pointing out some gaps in an earlier draft of this paper.

2. REPRESENTING THE FUNCTOR W_o^+

2.1. Universal Examples of Endomorphisms. For each $n \in \mathbb{N}$ let $U_n = \mathbb{Z}[X_1,\dots,X_n]$ and consider the free module $P_n = U_n^n$ with the endomorphism f_n given by the matrix

$$(2.2)\qquad f_n = \begin{pmatrix} X_1 & -1 & 0 & \dots & 0 \\ X_2 & 0 & -1 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ & & & & -1 \\ X_n & 0 & & \dots & 0 \end{pmatrix}$$

Then of course $\det(1+tf_n) = 1 + X_1t + \dots + X_nt^n$. And (P_n,f_n) has the following universality property: for each polynomial of degree $\leq n$, $1 + a_1t + \dots + a_nt^n = a \in W_o^+(A)$ there is a unique homomorphism $\phi_a\colon U_n \to A$ such that $\phi_{a*}\colon W_o^+(U_n) \to W_o^+(A)$ takes $\gamma_n = [P_n,f_n]$ into a. This of course also shows that the image of End A in $W_o(A)$ is precisely the subsemiring of polynomials of the form $1 + a_1t + \dots + a_nt^n$.

The $\gamma_n = [P_n,f_n]$ fit together in the sense that if $\pi_n^{n+1}\colon U_{n+1} \to U_n$ is the projection $X_i \mapsto X_i$ for $i = 1, \dots, n$, $X_{n+1} \mapsto 0$, then

$$(2.3)\qquad (\pi_n^{n+1})_*\gamma_{n+1} = \gamma_n$$

The following proposition follows immediately.

2.4. Proposition. There is a functorial isomorphism between $W_o^+(A)$ and TRng $(\mathbb{Z}_I[X_1,X_2,\dots,], A)$ where TRng stands for continuous ring homomorphisms from $\mathbb{Z}[X_1,X_2,\dots]$ with the I-topology to A with the discrete topology.

Indeed, if $\phi\colon \mathbb{Z}[X] \to A$ is continuous, then there is an I_n such that $\phi(I_n) = 0$, so that ϕ factors through $\pi_n\colon \mathbb{Z}[X] \to U_n$. Let ϕ_n be the induced homomorphism, then the element in $W_o^+(A)$ corresponding to ϕ is $\phi_{n*}\gamma_n$. And inversely if $A(t) \in W_o^+(A)$, $a(t) = 1 + a_1t + \dots + a_nt^n$, let $\phi'_a\colon U_n \to A$ be defined by $\phi'_a(X_i) = a_i$. Then $\phi_a = \phi'_a \circ \pi_n$ is the desired continuous homomorphism $\mathbb{Z}[X] \to A$.

3. THE FATOU PROPERTY.

3.1. Definition.

An integral domain R is said to be Fatou if the following property holds.
For every power series $a(s^{-1}) = \sum_{i=o}^{\infty} a_i s^{-i}$ in s^{-1} with coefficients in R such that there exist polynomials p(s), q(s) with coefficients in the quotient field Q(R) such that $a(s^{-1}) = q(s)^{-1}p(s)$, there exist also polynomials $\bar{p}(s)$, $\bar{q}(s) \in R[s]$ such that $\bar{q}(s)$ has leading coefficient 1 which also satisfy $\bar{q}(s)^{-1}\bar{p}(s) = a(s^{-1})$. (The same property then holds obviously also with respect to Laurent series). The following result comes out of mathematical system theory [7,8].

3.2. Proposition. Every noetherian integral domain R is Fatou.
Proof. Let $a(s^{-1}) = \sum_{i=o}^{\infty} a_i s^{-i}$ be a power series in s^{-1} over R. Write down the Hankel matrix of $a(s^{-1})$.

$$\begin{pmatrix} a_o & a_1 & a_2 & \cdots \\ a_1 & a_2 & a_3 & \cdots \\ a_2 & a_3 & a_4 & \cdots \\ \cdot & \cdot & \cdot & \\ \cdot & \cdot & \cdot & \\ \cdot & \cdot & \cdot & \end{pmatrix} \tag{3.3}$$

Now suppose that $a(s^{-1}) = q(s)^{-1}p(s)$ for certain polynomials over the quotient field Q(R) of R. This means that there is a certain recursion relation

$$q_1 a_{n+t-1} + q_2 a_{n+t-2} + \cdots + q_t a_n = 0 \tag{3.4}$$

between the coefficients a_n for all large enough n, and in turn this means that the rank of the matrix (3.3) is finite. Let this rank be r.

Now consider the A-module M generated by the columns of (3.3). This module can be seen as a submodule of some $b^{-1}R^r$ for some $b \in R$. (For b one can take any nonzero r x r minor of (3.3)). But $b^{-1}R^r$ is a finitely generated R-module and as R is noetherian it follows that M is finitely generated. Now define an endomorphism F of M by $F(a(i)) = a(i+1)$ where $a(i)$ is the column of (3.3) starting with a_i. Let $g = a(0)$ and let $h: M \to R$ be defined by $h(a(i)) = a_i$. Note that because of the structure of (3.3) the endomorphism F is well defined. We note that $hF^i g = a_i$ for all $i = 0,1,2, \ldots$. Now because M is finitely generated there is a surjection of R-modules $\pi : R^m \to M$ for some m. Define $\tilde{h} = h\pi$; let $\tilde{F}$ be any lift of F, i.e. any endomorphism (matrix) of R^m such that $\pi\tilde{F} = F\pi$ and $\tilde{g}$ any element of R^m such that $\pi(\tilde{g}) = g$.
Then $\tilde{h}\tilde{F}^i\tilde{g} = hF^i g = a_i$ for all $i = 0,1,2, \ldots$ and consequently $s\tilde{h}(sI-\tilde{F})^{-1}\tilde{g} = a(s^{-1})$ proving the proposition.

4. "REPRESENTING" THE FUNCTOR W_o.

We are now in a position to represent, in a certain sense, the functor $W_o(-)$.

4.1. Definition of the "universal object". Let J_n be the ideal in $\mathbb{Z}[X]$ defined in the introduction and let $V_n = \mathbb{Z}[X]/J_n$, let $\rho_n\colon \mathbb{Z}[X] \to V_n$ be the natural projection, let $\xi = 1 + X_1t + X_2t^2 + \ldots \in W(\mathbb{Z}[X])$ and let $\xi_n = (\rho_n)_*(1+X_1t+X_2t^2+\ldots) \in W(V_n)$.

4.2. Warning and intermezzo. It is not clear that ξ_n is in $W_o(V_n)$. In fact this is definitely not the case, because there are integral domains which are not Fatou. It also follows that the V_n are examples.

(The V_n are integral by the appendix). It follows that the V_n are not noetherian. Let $\tilde{D}_n$ be the top left nxn minor of (1.11)then as we shall see in 6.10 below ξ_n becomes a rational Witt vector over V_n localized at $(1,D_n,D_n^2,\ldots)$ where $D_n = \rho_n(\tilde{D}_n)$. It is easy to check that the map β_n of diagram (6.11) contains V_n in its image and it follows that the localization $(V_n)_{D_n}$ is noetherian.

It is still not true, however, that ξ_n over $(V_n)_{D_n}$ is universal for rational Witt vectors of numerator degree $\leq n-1$ and denominator degree $\leq n$. To obtain universal rational Witt vectors one needs something like a universal Fatourization construction.

4.5. Theorem. For each $1 + a_1 t + \ldots = a \in W_o(A)$ let $\phi_a : \mathbb{Z}[X] \to A$ be the ring homomorphism defined by $X_i \mapsto a_i$. Then $a(t) \mapsto \phi_a$ is a functorial and injective correspondence from $W_o(A)$ to ring homomorphisms $\mathbb{Z}[X] \to A$ which are continuous with respect to the J-topology on $\mathbb{Z}[X]$ and the discrete topology on A. If A is Fatou, so in particular if A is integral and noetherian, then this induces a functorial isomorphism.

Proof. The rational Witt vector a can be written $a = (1+c_1t+\ldots+c_nt^n)^{-1}$ $(1+b_1t+\ldots+b_{n-1}t^{n-1})$. Consider $\mathbb{Z}[Y_1,\ldots,Y_{n-1}; Z_1,\ldots,Z_n]$ and define $\psi : \mathbb{Z}[Y;Z] \to A$ by $\psi(Y_i) = c_i$ and $\psi(Z_j) = b_j$, $i,j = 1, \ldots, n$. Let δ_n be the rational Witt vector

$$(4.6)\qquad \delta_n = \frac{1+Y_1t+\ldots+Y_{n-1}t^{n-1}}{1+Z_1t+\ldots+Z_nt^n} \in W_o(\mathbb{Z}[Y,Z])$$

Then of course $\psi_*\delta_n = a$ (but there may be several ψ's with this property). Define $\varepsilon_n : \mathbb{Z}[X] \to \mathbb{Z}[Y,Z]$ by $\varepsilon_{n*}\xi = \delta_n$. Then $(\psi\varepsilon_n)_*\xi = a$ so that $\psi\varepsilon_n = \phi_a$. Now δ_n is rational so there is a recursion relation between its coefficients $a_i(Y,Z)$ in

$$(4.7)\qquad \delta_n = 1 + a_1(Y,Z)t + a_2(Y,Z)t^2 + \ldots$$

This in turn means that the rank of the associated Hankel matrix (cf. (3.3)) is finite (over the quotientfield $Q(\mathbb{Z}[Y,Z])$ and because $\mathbb{Z}[Y,Z]$ is an integral domain this means that for some n all minors of the Hankel matrix of (4.6) vanish. Thus $\varepsilon_n(J_m) = 0$ for some m (in fact $m = n$ works) so that a fortiori $\phi_a(J_m) = 0$, i.e. ϕ_a is continuous. The injectivity of $a \mapsto \phi_a$ is obvious, because $\phi_a(X_i) = a_i$.

Now let A be Fatou (and an integral domain). Let $\psi : \mathbb{Z}[X] \to A$ be continuous. Let $a_i = \psi(X_i)$. Then there is an m such that $\psi(I_m) = 0$. Thus all (m+1) x (m+1) minors of the Hankel matrix (3.3) of $a_o = 1, a_1, a_2, \ldots$ vanish so that this matrix is of finite rank. So there are $q_o, \ldots, q_m \in Q(A)$ such that $q_o a(0) + \ldots + q_m a(m) = 0$ where as before $a(i)$ is the i-th column of (3.3). Hence

$$q_o a_t + q_1 a_{t+1} + \ldots + q_m a_{t+m} = 0, \quad t = 0,1,2,\ldots \tag{4.8}$$

so that

$$\frac{p_o + p_1 t + \ldots + p_{m-1} t^{m-1}}{q_m + q_{m-1} t + \ldots + q_o t^m} = 1 + a_1 t + a_2 t^2 + \ldots \tag{4.9}$$

with $p_o = q_m$, $p_1 = q_m a_1 + q_{m-1}$, $\ldots$, $p_{m+1} = q_m a_{m-1} + \ldots + q_1$. Now write $t = s^{-1}$ multiply numerator and denominator of (4.6) with s^m and apply the Fatou property to find an expression

$$\frac{c_n s^n + c_{n-1} s^{n-1} + \ldots + c_1 s + c_o}{s^m + b_{m-1} s^{m-1} + \ldots + b_1 s + b_o} = 1 + a_1 s^{-1} + a_2 s^{-2} + \ldots \tag{4.10}$$

with $c_o, \ldots, c_n, b_o, \ldots, b_{m-1} \in A$. It follows that $n = m$ and $c_n = 1$. Now write $t = s^{-1}$ again and multiply numerator and denominator in (4.10) with t^n to find the desired expression.

5. THE OPERATIONS OF W_o^+.

5.1. Functorial transformations $W_o^+ \to W$. Consider the functor W_o^+ and W as functors Ring → Set, and let u: $W_o^+ \to W$ be a functorial transformation. Consider the element $\gamma_n \in W_o^+(U_n)$, cf. section 2.1 above. Let

$$u(\gamma_n) = 1 + u_1(n)t + u_2(n)t^2 + \ldots \in W(U_n) \tag{5.2}$$

and let $\phi_n: \mathbb{Z}[X] \to U_n = \mathbb{Z}[X_1, \ldots, X_n]$ be the unique homomorphism of rings such that $\phi_n(X_i) = u_i(n)$ for all i. We claim that the ϕ_n are compatible in the sense that

$$\pi_n^{n+1} \phi_{m+1} = \phi_n, \quad n = 1,2, \ldots \tag{5.3}$$

Indeed because u is functorial we have $u(\gamma_n) = u((\pi_n^{n+1})_*\gamma_{n+1}) = (\pi_n^{n+1})_* u(\gamma_{n+1})$ and (5.3) follows. Thus the ϕ_n combine to define a homomorphism of rings

$$(5.4) \qquad \phi_u : \mathbb{Z}[X] \to \mathbb{Z}_I[X] \subset \mathbb{Z}[[X]]$$

Moreover ϕ_u determines u uniquely. Inversely given a ring homomorphism $\phi: \mathbb{Z}[X] \to \mathbb{Z}_I[X]$ there is an induced functorial transformation

$$(5.5) \qquad u_\phi : W_o^+(A) \simeq \underline{\underline{\mathrm{Ring}}}(\mathbb{Z}_I[X],A) \xrightarrow{\phi^*} \underline{\underline{\mathrm{Ring}}}(\mathbb{Z}[X],A) \simeq W(A)$$

Now suppose that $u: W_o^+ \to W$ is continuous. By continuity (because $W_o^+(A)$ is dense in $W(A)$), u extends to a functorial transformation $u: W \to W$. Because $W(A) = \underline{\underline{\mathrm{Ring}}}(\mathbb{Z}[X],A)$, u induces a ring endomorphism $\phi_u: \mathbb{Z}[X] \to \mathbb{Z}[X]$. Inversely every ring endomorphism $\phi: \mathbb{Z}[X] \to \mathbb{Z}[X]$ obviously defines a functorial transformation $u_\phi: W(A) \overset{\sim}{\to} \underline{\underline{\mathrm{Ring}}}(\mathbb{Z}[X],A) \overset{\phi}{\to} \underline{\underline{\mathrm{Ring}}}(\mathbb{Z}[X],A) \simeq W(A)$. This u_ϕ is automatically continuous. Indeed let $a \in W(A)$ and $u_\phi(a) = b$. Given m let $n(m) \in \mathbb{N}$ be such that $\phi(X_1), \ldots, \phi(X_m)$ involve only the indeterminates $X_1, \ldots, X_{n(m)}$. Then if $a' \in W(A)$ is such that the first $n(m)$ coefficients of a' are equal to those of a we have that the first m coefficients of $b' = u_\phi(a')$ are equal to those of b. This proves the continuity of u_ϕ.

Putting all this together we have

5.6. <u>Proposition</u>. Every operation $u: W_o^+ \to W$ corresponds uniquely to a ring homomorphism $\phi_u: \mathbb{Z}[X] \to \mathbb{Z}_I[X]$ and inversely. If the image of ϕ_u is in $\mathbb{Z}[X] \subset \mathbb{Z}_I[X]$ the operation is continuous and extends uniquely to an operation $W \to W$. The continuous operations $W_o^+ \to W$ and the (automatically continuous) operations $W \to W$ correspond bijectively to the ring endomorphisms $\mathbb{Z}[X] \to \mathbb{Z}[X]$.

There are also discontinuous operations $W_o^+ \to W$ and $W_o^+ \to W_o^+$. An example is the one given by the ring homomorphism $X_1 \to X_1X_2 + X_1X_3 + X_1X_4 + \ldots$, $X_i \to 0$ for $i \geq 2$.

5.7. The ring of operations $Op(W_o^+)$. Proof of theorem 1.12. Let $Op(W_o^+)$ be the ring of operations $W_o^+ \to W_o^+$, and let $u \in Op(W_o^+)$. Then $u(\gamma_n)$ (cf. (5.3) above) is a polynomial and it follows that $\phi_n(I_t) = 0$ for t large enough (where I_t is the ideal $(X_{t+1}, X_{t+2}, \ldots) \subset \mathbb{Z}[X]$). Thus ϕ_u satisfies, $\phi_u(I_t) \subset I_n$. There is such a t for every n so that ϕ_u is continuous. Inversely let $\phi: \mathbb{Z}[X] \to \mathbb{Z}[X]$ be continuous, and let $a \in W_o^+(A)$. Let $\phi_a: \mathbb{Z}[X] \to A$ be the classifying homomorphism of a (cf. proposition 2.4). Then $\phi_a(I_r) = 0$ for some r. Because ϕ is continuous there is an m such that $\phi(I_m) \subset I_r$. Now $u_\phi(a) = (\phi_a\phi)_*(\xi)$, $\xi = 1 + X_1 t + X_2 t^2 + \ldots \in W(\mathbb{Z}[X])$ and it follows that $u_\phi(a)$ is in $W_o^+(A) \subset W(A)$. This proves the second statement of theorem 1.12. The first statement follows because for continuous operations u the homomorphism ϕ_u is such that $\mathrm{Im}(\phi_u) \subset \mathbb{Z}[X]$ (by proposition 5.6).

6. THE OPERATIONS OF W_o.

6.1. J-continuous endomorphisms of $\mathbb{Z}[[X]]$ *define operations*. Let $u \in Opc(W_o)$ be a continuous operation of W_o. Then because W_o is dense in W, as in section 5.1 above u defines uniquely an endomorphism of $\mathbb{Z}[X]$. It remains to determine what endomorphisms can arise in this way. The first step is to show that J-continuous endomorphisms give indeed rise to operations.

Let $T_n = \mathbb{Z}[Y_1,\dots,Y_n;\ Z_1,\dots,Z_{n-1}]$ and consider the element

$$(6.2)\qquad \eta_n = \frac{1+Z_1t+\dots+Z_{n-1}t^{n-1}}{1+Y_1t+\dots+Y_nt^n} = 1 + v_1(Y,Z)t \ + \dots \quad \in W_o(T_n)$$

The $v_i(Y,Z) \in T_n$ are easy to calculate explicitly. The result is

$$(6.3)\qquad \begin{aligned}
&v_1 + Y_1 = Z_1\\
&v_2 + v_1Y_1 + Y_2 = Z_2\\
&\quad\vdots\\
&v_{n-1}+v_{n-2}Y_1+\dots+v_1Y_{n-2}+Y_{n-1} = Z_{n-1}\\
&v_n \ +v_{n-1}Y_1+\dots+v_1Y_{n-1}+Y_n = 0\\
&\quad\vdots\\
&v_{n+r}+v_{n+r-1}Y_1+\dots+v_2Y_{n-1}+v_2Y_n = 0\\
&\quad\vdots
\end{aligned}$$

Let $\Delta_n(X)$ be the n x n upper left hand corner submatrix of (1.11), i.e.

$$(6.4)\qquad \Delta_n(X) = \begin{pmatrix} 1 & X_1 & \cdots & X_{n-1}\\ X_1 & X_2 & \cdots & X_n\\ \vdots & \vdots & & \vdots\\ X_{n-1} & X_n & \cdots & X_{2n-2}\end{pmatrix}$$

Finally let $d_n(Y,Z) \in T_n$ be obtained by substituting $v_i(Y,Z)$ for X_i in (6.4) and taking the determinant of the resulting matrix. It is not difficult to see that

$$(6.5)\qquad 0 \neq d_n(Y,Z) \in T_n$$

Indeed take e.g. $Z_1 = \dots = Z_{n-1} = 0$, $Y_1 = \dots = Y_{n-1} = 0$, $Y_n = 1$. Then $v_1 = \dots = v_{n-1} = 0$ $v_n = -1$, $v_{n+1} = \dots = v_{2n-2} = 0$ so that for these values d_n becomes -1 (if $n \geq 2$).

Now let $\sigma_n : \mathbb{Z}[X] \to T_n$ be defined by

$$(6.6)\qquad \sigma_n(X_i) = v_i(Y,Z)$$

Then because the $v_i(Y,Z)$ satisfy the recurrence relations (6.3) we have that $\sigma_n(J_n) = 0$, so that

(6.7) $$J_n \subset \mathrm{Ker}\sigma_n$$

Now let $\phi: \mathbb{Z}[X] \to \mathbb{Z}[X]$ be continuous with respect to the J-topology. Let u_ϕ be the associated functorial transofrmation $W(-) \to W(-)$. Then in particular

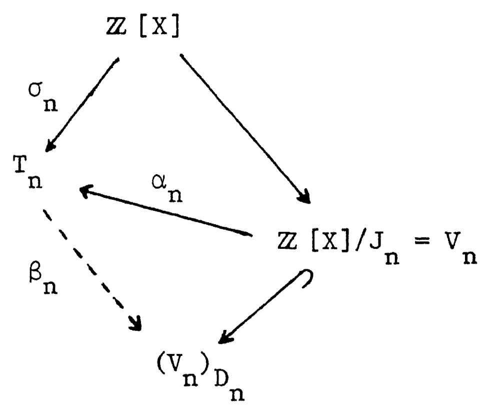
(6.8) $$u_\phi(\eta_n) = (\sigma_n\phi)_*(\xi)$$

Now ϕ is continuous with respect to the J-topology. So there is an $m \in \mathbb{N}$ such that $\phi(J_m) \subset J_n$ and then $(\sigma_n\phi)(J_m) = 0$. Because T_n is Fatou (proposition 3.2) it follows that $u_\phi(\eta_n) \in W_o(T_n) \subset W(T_n)$. It follows that u_ϕ maps $W_o(A) \to W_o(A)$ for all rings A because for every $a \in W_o(A)$ there is a ring homomorphism $\psi: T_n \to A$ for some n such that $\psi_*(\eta_n) = a$.
So we have proved

6.9. Proposition. For every J-continuous ring endomorphism ϕ of $\mathbb{Z}[X]$, the associated functorial transformation $u_\psi: W \to W$ maps W_o into W_o.

6.10. Operations on W_o give rise to J-continuous endomorphisms. To obtain the inverse statement we need the inverse inclusion of (6.7). To that end consider the following diagram

(6.11)



Here the homomorphism in the upper righthand corner is the natural projection π_n. Because $J_n \subset \mathrm{Ker}\sigma_n$, σ_n factors through V_n to give α_n. Finally $V_n \to (V_n)_{D_n}$ is localization with respect to the multiplicative system $(1, D_n, D_n^2, \ldots)$. This is injective because $D_n \neq 0$ (by 6.5)) and because D_n is not a zero divisor; (cf the appendix).

Now we claim that there exists a homomorphism β_n making the lower triangle commutative. To define β_n we try to solve

$$(6.12) \qquad \frac{1+Z_1 t+\ldots+Z_{n-1} t^{n-1}}{1+Y_1 t+\ldots+Y_n t^n} = 1 + X_1 t + X_2 t^2 + \ldots$$

for $Y_1, \ldots, Y_n, Z_1, \ldots, Z_{n-1}$ in terms of the X's. Substituting X_i for v_i in the equations (6.3) this gives in particular

$$\begin{pmatrix} 1 & X_1 & \cdots & X_{n-1} \\ X_1 & X_2 & \cdots & X_n \\ \vdots & \vdots & & \vdots \\ X_{n-1} & X_n & \cdots & X_{2n-2} \end{pmatrix} \begin{pmatrix} Y_n \\ Y_{n-1} \\ \vdots \\ Y_1 \end{pmatrix} = \begin{pmatrix} -X_n \\ -X_{n+1} \\ \vdots \\ -X_{2n-1} \end{pmatrix}$$

and from this we can calculate $Y_1, \ldots, Y_n$ as a polynomial $b_i(X)$, $i = 1, \ldots, n$ in $X_1, \ldots, X_{2n-1}$ and $\tilde{D}_n(X)^{-1}$ where $\tilde{D}_n(X)$ is the determinant of (6.4). Given the $Y_1, \ldots, Y_{n-1}$ the $Z_1, \ldots, Z_{n-1}$ follow directly from the first n-1 equations of (6.3), and are also polynomials $c_i(X)$ in $X_1, \ldots, X_{2n-1}$ and $\tilde{D}_n(X)^{-1}$.

It is now straightforward to check that the expression

$$\tilde{D}_n(X)(X_{n+r}+X_{n+r-1}Y_1+\ldots+X_{r-1}Y_{n-1}+X_rY_n), \qquad r \geq n$$

is precisely equal to the minor of the Hankel matrix (1.11) obtained by taking the first n + 1 rows and columns 1,2, ..., n and r + 1. (Alternatively we can use the proof of proposition 3.2 to see that it suffices to invert D_n to be able to solve equations (6.12). Thus we can define $\beta_n : T_n \to (V_n)_{D_n}$ by $Y_i \mapsto b_i(X)$ and $Z_i \mapsto c_i(X)$. The polynomials $b_i(X)$, $c_i(X)$ are unique and it follows that the lower triangle in (6.11) commutes. It follows that α_n is injection so that

(6.13) $$\operatorname{Ker} \sigma_n = J_n$$

Now let $u \in \mathrm{Op}(W_o)$ be a continuous operation and let $\phi_u \in \mathrm{End}(\mathbb{Z}[X])$ be the associated endomorphism. Consider $u(\eta_n) \in W_o(T_n)$. Because $u(\eta_n)$ is rational there is a T_m and a homomorphism of rings $\psi : T_m \to T_n$ such that $\psi_* \eta_m = u(\eta_n)$. Both $\sigma_n \phi_u$ and $\psi \sigma_m$ take $\xi \in W(\mathbb{Z}[X])$ to $u(\eta_n)$ therefore $\sigma_n \phi_u = \psi \sigma_m$

(6.14)
$$\begin{array}{ccc} \mathbb{Z}[X] & \xrightarrow{\ \phi_u\ } & \mathbb{Z}[X] \\ \Big\downarrow \sigma_m & & \Big\downarrow \sigma_n \\ T_m & \xrightarrow{\ \psi\ } & T_n \end{array}$$

It follows that ϕ_u takes the kernel of $\psi\sigma_m$ into the kernel of σ_n. But the kernel of σ_n is J_n and the kernel of σ_m is J_m which is contained in the kernel of $\psi\sigma_m$. Thus $\phi_u(J_m) \subset J_n$. There is such an m for every n which proves that ϕ_u is continuous w.r.t. the J-topology. This finishes the proof of part (i) of theorem 1.13.

6.15. Additive operations in $\mathrm{Opc}(W_o)$. The addition in $W_o(A)$ and $W(A)$ corresponds to a comultiplication on $\mathbb{Z}[X]$. It is in fact (as is very easily verified) the comultiplication $\mu: X_n \mapsto \sum_{i+j=n} X_i \otimes X_j$. There is also a counit $\mathbb{Z}[X] \to \mathbb{Z}$, $X_i \mapsto 0$, and a coinverse. This turns $\mathbb{Z}[X]$ into a Hopf-algebra (with antipode). An operation $u \in \mathrm{Op}(W_o)$ is additive (group structure preserving) iff its associated endomorphism is a Hopf-algebra endomorphism. Now according to Moore [6], $\mathbb{Z}[X]$ is the free Hopf-algebra on the coalgebra $\oplus\, \mathbb{Z} X_i$, $X_n \mapsto \sum_{i+j=n} X_i \oplus X_j$, meaning that for every Hopf-algebra H and coalgebra homomorphism $\oplus\, \mathbb{Z}\, X_i \to H$, there is a unique extension $\mathbb{Z}[X] \to H$ which is a Hopf-algebra endomorphism. Thus the endomorphism of an additive operation u is uniquely specified by the elements $\phi_u(X_i) = x_i$ subject to $\mu x_n = \sum_{i+j=n} x_i \otimes x_j$, and inversely. This proves part (ii) of theorem 1.13.

6.16. Addendum to theorem 1.13 (ii).

Let $\phi \in \mathrm{End}\, \mathbb{Z}[X]$ be a Hopf-algebra endomorphism and suppose it is continuous as a morphism $\mathbb{Z}[X] \to \mathbb{Z}[X]$ with the J-topology on the source and the I-topology on the target. Then, cf. 5.1 above, the associated operation takes $W_o^+(A)$ into $W_o(A)$ and hence by additivity $W_o(A)$ into $W_o(A)$. It follows that ϕ also has the stronger continuity property of being a continuous J-topology endomorphism of $\mathbb{Z}[X]$.

6.17. Splitting principle and Frobenius operators. Before discussing multiplicative operations we need to define the Frobenius operators and the splitting principle. Consider $\mathbb{Z}[X]$ as a subring of $\mathbb{Z}[[\xi_1,\xi_2,\ldots]]$ by viewing X_i as $(-1)^i e_i(\xi_1,\xi_2,\ldots)$ where e_i is the i-th elementary symmetric function in ξ_1, ξ_2, ... Then we can write

$\xi = 1 + X_1t + X_2t^2 + \ldots = \prod_{i=1}^{\infty} (1-\xi_i t)$. It follows that to specify an additive operation on W(-) it suffices to specify what it does to elements of the form $1 + a_1t \in W(A)$, and similarly the functorial multiplication on W(A) is also characterized by the equation $(1-at)*(1-bt) = (1-abt)$. The Frobenius operations are now characterized by

$$F_n(1-at) = (1-a^nt) \tag{6.18}$$

They are functorial ring endomorphisms of W(A) (Cf. e.g. [4, Chapter III]). They are defined on the level of EndA by

$$(P,f) \mapsto (P,f^n) \tag{6.19}$$

6.20. Multiplicative Operations.

Define new coordinates for the Witt vectors by the equation

$$\prod_{i=1}^{\infty} (1-Z_it^i) = 1 + X_1t + X_2t^2 + \ldots \tag{6.21}$$

Then the Z_i can be calculated as polynomials in the X_i and vice versa, defining an isomorphism $\mathbb{Z}[Z] \xrightarrow{\sim} \mathbb{Z}[X]$. Some aspects of the big Witt vectors are more easily discussed using 'Z coordinates' than 'X coordinates'. Let

$$w_n(Z) = \sum_{d|n} dZ^{n/d} \tag{6.22}$$

Then the w_n define a functorial homomorphism of rings $w\colon W(A) \to A^{\mathbb{N}}$, where $\mathbb{N} = \{1,2,\ldots\}$ and if A is a Q-algebra this is an isomorphism. Here $A^{\mathbb{N}}$ is a ring with component wise addition and multiplication. Now let u: $W \to W$ be a transformation of ring valued functors. Then at least for Q-algebra's this induces a transformation on $A^{\mathbb{N}}$, functorial in A. These are easy to describe and are given by an infinite matrix with precisely one 1 in each row and zero's elsewhere. Let $\tau\colon \mathbb{N} \to \mathbb{N}$ be the corresponding mapping. Now if this tranformation comes from one on W(A), there must be polynomials $U_1(Z)$, $U_2(Z), \ldots$ such that

$$(6.23) \qquad w_n(U_1(Z), U_2(Z), \ldots) = w_{\tau(n)}(Z_1, Z_2, \ldots)$$

Taking n = 1 gives $U_1(Z) = w_{\tau(1)}(Z)$. So that this transformation takes an element $(1-at) \in W(A)$ to $(1-a^n t)$. But this determines by the splitting principle the transformation uniquely and moreover there is a multiplicative transformation acting precisely like this. Thus the functorial ring endomorphisms of W(A) are the Frobenius operators F_1, $F_2, \ldots$ and they obviously take $W_o^+(A)$ and $W_o(A)$ into themselves. This proves part (iii) of theorem 1.13.

N.B. Not all mappings $\tau\colon \mathbb{N} \to \mathbb{N}$ give rise to a functorial ring endomorphism of W. For that to happen the polynomials $U_1(Z)$, $U_2(Z)$, ... defined by (6.22) must turn out to have integral coefficients. As it turns out (and this is proved by the preceding) this is the case iff there is a number n such that $\tau(m) = nm$ for all m. This follows because the Frobenius operators F_n satisfy (and are characterized by) $w_m F_n = w_{nm}$, cf. [4, Chapter III].

6.24. Remark. It is not clear (to me at least) whether the (not necessarily continuous) operations $W_o \to W_o$ correspond bijectively to continuous ring endomorphisms $\mathbb{Z}_J[X] \to \mathbb{Z}_J[X]$. Certainly such a ring endomorphism gives rise to an operation $W_o \to W_o$. The opposite is less clear (and in my opinion probably not true). The difficulty is of course that the canonical "representing elements" ξ_n are not in $W_o(V_n)$.

7. THE OPERATIONS Λ^i AND S^i.

There are several operations which are naturally defined on $\underline{\underline{\mathrm{End}}}\,A$ and the question arises to what these correspond in $W_0(A) \subset W(A)$ [1]. On the other hand a number of the more mysterious operations of $W(A)$ have natural interpretation on the level of $\underline{\underline{\mathrm{End}}}\,A$ which sometimes can be used to advantage, [3]. Thus e.g. the Frobenius operator corresponds to $f \mapsto f^n$ (f composed with itself n times) and the Verschiebung operator corresponds to

$$V_n : f \mapsto \begin{pmatrix} 0 & & 0 & f \\ 1 & \ddots & & \\ & \ddots & \ddots & \\ 0 & & 1 & 0 \end{pmatrix} \tag{7.1}$$

In [1] the question was asked to what the exterior and symmetric product correspond. The answer is rather obvious.

$W(A)$ is functorially a λ-ring, with the operations λ^i defined as follows. Because in any λ-ring $\lambda^n(x+y) = \sum_{i+j=n} \lambda^i(x)\lambda^j(y)$ it suffices by the splitting principle to specify the λ^i on elements of the form $(1-at)$. The characterizing definition is now

$$\lambda^1(1-at) = 1 - at, \quad \lambda^i(1-at) = 1 \quad \text{for } i \geq 2 \tag{7.2}$$

(Recall that 1 is the zero element of the abelian group $W(A)$).

Now consider the module with endomorphism (P_n, f_n) over $U_n = \mathbb{Z}[X_1,\dots,X_n]$ of section 2.1. Write $1 + X_1 t + \dots + X_n t^n = \prod_{i=1}^{n} (1-\xi_i t)$. Then over $Q(\xi_1,\dots,\xi_n)$ the module with endomorphism (P_n, f_n) is isomorphic to a free n-dimensional module with diagonal endomorphism with eigenvalues $-\xi_1, \dots, -\xi_n$. Thus there is a splitting principle for $\underline{\underline{\mathrm{End}}}\,A$ also. Now $\Lambda^1 = \mathrm{id}$ and Λ^i (one dimensional module) $= 0$ if $i \geq 2$, and finally if ξ_i is the endomorphism multiplication with ξ_i of A, then $c(\xi_i) = 1 + \xi_i t$. It follows that the Λ^i on $\underline{\underline{\mathrm{End}}}\,A$ correspond to the natural λ-operations on $W(A)$.

7.3. Adams Operations.

Every λ-ring has Adams operations defined on it, which are defined by the formula

$$\frac{d}{dt} \log \lambda_t(x) = \sum_{i=o}^{\infty} (-1)^n \psi^{n+1}(x) t^n \tag{7.4}$$

where $\lambda_t(x) = 1 + \lambda^1(x)t + \lambda^2(x)t^2 + \dots$. Using this one easily checks that the Adams operations ψ^n on $W(A)$ coincide with the Frobenius operations F_n (Adams=Frobenius). It follows that the Adams operations corresponding to the Λ^i on End A are given by $(P,f) \to (P,f^n)$.

7.5. Symmetric Powers. For any projective module P over A there is a wellknown exact sequence of projective modules

$$0 \to S^n P \to S^{n-1}P \otimes \Lambda^1 P \to S^{n-2}P \otimes \Lambda^2 P \to \dots \to S^1 P \otimes \Lambda^{n-1} P \to \Lambda^n P \to 0 \tag{7.6}$$

It follows that the exterior product operations λ^i and the symmetric product operations s^i on $W_o(A) \subset W(A)$ are related by the formula

$$s^n(a) - s^{n-1}(a)\lambda^1(a) + s^{n-2}(a)\lambda^2(a) - \dots + (-1)^{n-1}s^1(a)\lambda^{n-1}(a) + (-1)^n\lambda^n(a) = 0 \tag{7.7}$$

A description for the s^i similar to the one given above for the λ^i is given by

$$s^1((1+at)^{-1}) = (1+at)^{-1}, \quad s^i((1+at)^{-1}) = 0 \text{ for } i \geq 2 \tag{7.8}$$

The s^i of the other elements are determined by this because the s^i also satisfy $s^n(a+b) = \sum_{i+j=n} s^i(a)s^j(b)$ (where + denotes the addition in $W(A)$ and on the right hand side we have both multiplication and addition in $W(A)$. In other words the s^i define a different λ-ring structure (also functorial) on $W(A)$.

This comes about as follows. If the X_i are the elementary symmetric functions in $-\xi_1, -\xi_2, \ldots$ so that $1 + X_1t + X_2t^2 + \ldots = \Pi(1-\xi_i t)$, then the complete symmetric functions h_i in the $-\xi_1, -\xi_2, \ldots$ are given by $1 + h_1t + h_2t^2 + \ldots = \Pi\ (1+\xi_i t)^{-1}$. They are (therefore) related by $\sum_{i=o}^{n} (-1)^i X_i h_{n-i} = 0$, cf (7.7).

Now the functorial λ-ring structure on W(A) is given by certain ring endomorphisms $\phi(\lambda^i)$: $\mathbb{Z}[X] \rightarrow \mathbb{Z}[X]$, or, equivalently, by certain universal polynomials, the $\phi(\lambda^i)(X_j) = \Phi_{ij}(X_1,X_2,\ldots)$. Now recoordinatize $\mathbb{Z}[X]$ and view it as $\mathbb{Z}[h]$. Write down the polynomials $\Phi_{ij}(h_1,h_2,\ldots)$ and substitute the expressions in $X_1, X_2, \ldots$ to which the h_i are equal. Then these new universal polynomials define the new functorial λ-ring structure on W(A) defined by the s^i.

REFERENCES.

1. G. Almkvist, K-theory of endomorphisms, J. of Algebra 55(1978), 308-340.
2. G. Almkvist, The Grothendieck ring of the category of endomorphisms, J. of Algebra 28(1974), 375-388.
3. D. Grayson, The K-theory of endomorphisms, J. of ALgebra 48(1977), 439-446.
4. M. Hazewinkel, Formal groups and applications, Acad. Pr., 1978.
5. A. Liulevicius, Arrows, symmetries and functors, preprint Univ. of Chicago, 1979
6. J.C. Moore, Algèbres de Hopf universelles, Sém. H. Cartan 12(1959/1960), exposé 10.
7. Y. Rouchaleou, B.F. Wyman, R.E. Kalman, Algebraic structure of linear dynamical systems, III: realization theory over a commutative ring, Proc. Nat. Acad. Sci. USA 69(1972), 3404-3406.
8. E.D. Sontag, Linear systems over commutative rings: a survey, Richerche di Automatica 7(1976), 1-14.

APPENDIX. PROOF THAT J_n IS A PRIME IDEAL.

A.1. Sylvester's theorem [10]. Let $x_1, \ldots, x_n$ be n vectors. Denote with $\det(x_1,\ldots,x_n)$ the determinant of the matrix consisting of the columns $x_1, \ldots, x_n$ (in that order). Then Sylvester proved a noteworthy identity concerning products of the form

$$\det(x_1,x_2,\ldots,x_n)\det(y_1,\ldots,y_n) \tag{1}$$

Namely choose any subset of r integers $i_1, \ldots, i_r$, $1 \leq i_k \leq n$. For each r tuple $1 \leq j_1 <\ldots< j_r \leq n$, let

$$\begin{pmatrix} i_1 & \cdots & i_r \\ j_1 & \cdots & j_r \end{pmatrix} \det(x_1,\ldots,x_n)\det(y_1,\ldots,y_n) \tag{2}$$

denote the expression (1) with x_{i_k} interchanged with y_{j_k}, $k = 1,2, \ldots, r$.

Then Sylvester's identity says that for any fixed set $i_1, \ldots, i_r$

$$\det(x_1,\ldots,x_n)\det(y_1,\ldots,y_n) = \Sigma\begin{pmatrix} i_1 & \cdots & i_r \\ j_1 & \cdots & j_r \end{pmatrix} \det(x_1,\ldots,x_n)\det(y_1,\ldots,y_n) \tag{3}$$

where the sum is over all $\binom{n}{r}$ possible choices for $j_1 <\ldots< j_r$.

A.2. Proof that D_n is not a zero divisor in $\mathbb{Z}[X]/J_n$. Consider the semi-infinite matrix

$$\begin{pmatrix} 1 & X_1 & X_2 & X_3 & X_4 & \cdots \\ X_1 & X_2 & X_3 & X_4 & X_5 & \cdots \\ \vdots & \vdots & & & & \\ X_n & X_{n+1} & \cdots & & & \end{pmatrix} \tag{4}$$

Now observe that all the (n+1) x (n+1) minors of the Hankel matrix (1.11) are linear combinations (with integral coefficients) of the minors of the matrix (4). This is essentially also a result from linear system theory, more precisely realization theory, cf. e.g. section 4 of [9]. Let if $m(i_1,\ldots,i_n;\ j_1,\ldots,j_n)$ denotes the determinant of the submatrix of (1.11) whose top row consists of $X_{i_1}, \ldots, X_{i_{n+1}}$ and first column

consists of $X_{j_1}, \ldots, X_{j_{n+1}}$ $(i_1=j_1;\ i_1<\ldots<i_n;\ j_1<\ldots<j_n)$ and $m(j_1,\ldots,j_{n+1})$ denotes the minor of (4) obtained by taking the columns starting with $X_{j_1}, \ldots, X_{j_{n+1}}$. Then for example $m(1,3,5;1,4,7) =$
$m(1,5,9) + m(2,4,9) + m(1,6,8) + 2m(2,5,8) + m(3,4,8) + m(2,6,7) + m(3,5,7)$.

Hence J_n is the ideal generated by all the $(n+1) \times (n+1)$ minors of (4). Recall that $\Delta_n(X)$ is the $n \times n$ upper left hand corner submatrix of (4) and that $\tilde{D}_n$ is the determinant of $\Delta_n(X)$, or, what is the same, the determinant of

(5) $$\begin{pmatrix} 1 & X_1 & \cdots & X_{n-1} & 0 \\ \vdots & & & \vdots & \vdots \\ X_{n-1} & & \cdots & X_{2n-2} & 0 \\ X_n & & \cdots & X_{2n-1} & 1 \end{pmatrix}$$

We shall from now on write D for $\tilde{D}_n$. Let the columns Of (4) be numbered $0,1,\ldots$. Let $m(j_1,\ldots,j_{n+1})$ denote the minor of (4) obtained by taking columns $j_1, \ldots, j_{n+1}$ and let m_s be short for $m(1,2,\ldots,n,s)$, $s > n$. Let J denote the ideal generated by the m_r.

Then by applying Sylvesters identity with $r = n$ and $(i_1,\ldots,i_r) = (1,\ldots,n)$ to the product of the determinant of (5), i.e. D, and $m(j_1,\ldots,j_{n+1})$ we see that

(6) $$D\,J_n \subset J$$

Now suppose that $DP \in J_n$ for some polynomial P. Then we can write

(7) $$D^2P = \sum_{i=1}^{t} f_i m_i$$

for certain polynomials f_i. We can of course even assume that the f_i are monomials. Let f be any monomial and let X_s be the largest X occurring in f. Then we can write if $f = f'X_s$

(8) $$Df = f'DX_s = m_{s-n}f' + p(X_1,\ldots,X_{s-1})f'$$

where p is a polynomial in $X_1, \ldots, X_{s-1}$. Using this repeatedly we obtain from (7) an expression of the form

$$D^k P = \Sigma f_{\underline{i}} m_{\underline{i}} \tag{9}$$

where $\underline{i}$ is a multiindex, $m_{\underline{i}}$ is short for $m_{i_1} m_{i_2} \ldots m_{i_r}$ if $\underline{i} = (i_1, \ldots, i_r)$ and the $f_{\underline{i}}$ are polynomials in $X_1, \ldots, X_{2n-1}$ only.

Let k be minimal such that there exists an expression of the form (9) with the property just mentioned. If $k = 0$ we are through, so assume $k > 0$. The sum in (9) is over multiindices $\underline{i}$ such that $n \leq i_1 \leq \ldots \leq i_r$. Now rewrite (9) as a sum

$$D^k P = \sum_{\underline{j}} g_{\underline{j}} m_{\underline{j}} \tag{10}$$

where the $g_{\underline{j}}$ s are equal to

$$g_{\underline{j}} = \Sigma f_{\underline{i}} m_n^t \tag{11}$$

where the sum is over all $\underline{i}$ such that $i_1 = \ldots = i_t = n < i_{t+1}$ and $\underline{j} = (i_{t+1}, \ldots, i_r)$. The $g_{\underline{j}}$ in (10) depend on $X_1, \ldots, X_{2n}$ but the dependence on X_{2n} occurs only through polynomials in $X_1, \ldots, X_{2n-1}$ and the product DX_{2n}. Now let V(D) be the subvariety of $\mathbb{C}^{2n-2}$ of zero's of D. Let $x \in V(D)$, $x = (x_1, \ldots, x_{2n-2})$ and x_{2n-1} be fixed, $x_{2n-1} \neq 0$. Let $m_{\underline{j}}(x)$ denote the polynomial obtained from $m_{\underline{j}}$ by substituting x_i for X_i, $i = 1, \ldots, 2n-1$. Suppose $D_{n-1}(x) = t \neq 0$. Then the lexicographically largest term in $m_{\underline{j}}(x)$ is, $\underline{j} = (j_1, \ldots, j_s)$, $n < j_1 \leq \ldots \leq j_s$

$$(tx_{2n-1})^s X_{n+j_1-1} X_{n+j_2-1} \ldots X_{n+j_s-1} \tag{12}$$

and these terms are different for different $\underline{j}$. This means that by varying the X_{2n}, X_{2n+1}, ... we can produce a nonsingular N x N matrix of $m_{\underline{j}}$ values where N is the number of terms in (10). Now because $g_{\underline{j}}$ is a polynomial in $X_1, \dots, X_{2n-1}, DX_{2n}$ the $g_j(x)$ do not depend on $x_{2n}, x_{2n+1}, \dots$ (as long as $x \in V(D)$). Therefore $g_j(x) = 0$ for all $x \in V(D)$ such that $D_{n-1}(x) \neq 0$. These x form an open dense subset of V(D) so that $g_{\underline{j}}(x) = 0$ for all $x \in V(D)$. Hence the $g_j(X)$ in (10) are divisible by D so that we can reduce k by 1 and we are through. (D_n is a prime element as an easy induction shows.)

A3. Proof that J_n is a prime ideal. Consider again diagram (6.11). Because D_n is not a zero divisor the lower right hand arrow is injective. Hence α_n is injective so that V_n is a subring of the integral domain T_n which proves that V_n is itself integral and that J_n is a prime ideal.

REFERENCES FOR THE APPENDIX

9. M. Hazewinkel, On the (internal) symmetry groups of linear dynamical systems, In: P. Kramer, M. Dal Cin (eds), Groups, systems and many-body physics, Vieweg 1980, 362-404.

10. J.J. Sylvester, Phil Mag. 4, no. II (1851), 142-145.