GROTHENDIECK RINGS AND WITT VECTORS

Daniel R. Grayson

Columbia University, Barnard College

The purpose of this note is to draw attention to a theorem of Almkvist which explains the ring of Witt vectors in terms of a Grothendieck ring constructed from endomorphisms of free (or projective) modules. From this point of view certain operations on Witt vectors become transparent; for example, multiplication comes from the tensor product of endomorphisms, and the ghost coordinates arise from the traces of powers of an endomorphism. Thus certain computations and definitions may be presented in a way easy to understand and motivate, without appeal to such notions as universal polynomials or the theory of symmetric functions.

It is convenient to introduce the notion of λ-ring; however, the reader may read ring for λ-ring throughout. A <u>λ-ring</u> R is a commutative ring R with 1, together with an operation λ_t which assigns to each element x of R a power series $\lambda_t(x) = 1 + \lambda^1(x)t + \lambda^2(x)t^2 + \cdots$. This operation must obey $\lambda_t(x+y) = \lambda_t(x) \cdot \lambda_t(y)$.

If A is a commutative ring with 1, let $\underline{P}_A$ denote the category of finitely-generated projective A-modules. The category $\underline{P}_A$ is equipped with the usual notions of short exact sequence, tensor product, and exterior product. The Grothendieck group $K_0 A = K_0\underline{P}_A$ becomes a λ-ring if we define $[P][Q] = [P \otimes_A Q]$ and $\lambda_t^n([P]) = [\Lambda^n{}_A P]$, in light of the isomorphisms $P \otimes_A (Q \oplus Q') = (P \otimes_A Q) \oplus (P \otimes_A Q')$ and $\Lambda^n(P \oplus P') = \bigoplus_{i+j=n} \Lambda^i P \otimes \Lambda^j P'$. For instance, if A is a field, then $K_0 A = \mathbb{Z}$, the ring of integers, and $\lambda_t(n) = (1+t)^n$.

Let $\underline{\mathrm{End}}_A$ denote the category whose objects are all pairs (P, f), where $P \in \underline{P}_A$ and f is an endomorphism of P. The arrows $(P, f) \longrightarrow (P', f')$ are all maps $g : P \longrightarrow P'$ such that $gf = f'g$. An exact sequence in $\underline{\mathrm{End}}_A$ is one whose underlying sequence of A-modules is exact. We make $K_0\underline{\mathrm{End}}_A$ into a λ-ring by defining $[P, f][Q, g] = [P \otimes_A Q, f \otimes g]$ and $\lambda^n[P, f] = [\Lambda^n P, \Lambda^n f]$. The ideal generated by the idempotent $[A, 0]$ is isomorphic to $K_0 A$; we denote the quotient λ-ring by W(A). It is convenient to think of W as a covariant functor on the category of rings A.

The additivity of the characteristic polynomial with respect to short exact sequences means that $L[P, f] = \det(1_P - Tf)$ defines a map $L : W(A) \longrightarrow \hat{W}(A)$. Here $\hat{W}(A)$ denotes the multiplicative group of power series in A[[T]] with constant term 1.

The group $\hat{W}(A)$ is the underlying (additive) group of the ring of Witt vectors. The λ-ring operations on $\hat{W}(A)$ are the unique operations which are continuous, functorial in A, and satisfy :

i) $(1 - aT) * (1 - bT) = 1 - abT$

ii) $\lambda_t(1 - aT) = 1 + (1 - aT)t$

The theorem of Almkvist states that L is an injective ring homomorphism whose image consists of all Witt vectors which are quotients of polynomials ([1], [2], [3]). In fact, L is a λ-ring homomorphism, so we have

$$(*) \quad W(A) \text{ is a dense sub-}\lambda\text{-ring of } \hat{W}(A).$$

The hard part of the theorem is the injectivity. When A is a field the injectivity follows immediately from the existence of the rational canonical form for a matrix. The result is surprising when A is not a field.

Here is an example of a computation in $\hat{W}(A)$ which is tedious unless we perform it in $W(A)$:

$$(1-aT^2) * (1-bT^2) = L(\begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix}) * L(\begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix})$$

$$= L(\begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}) = L\left(\begin{pmatrix} 0 & 0 & 0 & ab \\ 0 & 0 & b & 0 \\ 0 & a & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}\right)$$

$$= 1 - 2abT^2 + a^2b^2T^4.$$

There are certain auxiliary operations defined on $\hat{W}(A)$ which can also be computed in $W(A)$. They are :

1) the n^{th} ghost coordinate $gh_n = \hat{W}(A) \longrightarrow A$. It is the unique continuous natural additive map which sends $1-aT$ to a^n.

2) the Frobenius endomorphism $F_n : \hat{W}(A) \longrightarrow \hat{W}(A)$. It is the unique continuous natural additive map which sends $1-aT$ to $1-a^nT$.

3) the Verschiebung endomorphism $V_n : \hat{W}(A) \longrightarrow \hat{W}(A)$. It is the unique continuous natural additive map which sends $1-aT$ to $1-aT^n$.

We define similar operations on W(A) as follows :

1) $gh_n[P, f] = tr(f^n)$,

2) $F_n[P, f] = [P, f^n]$, and

3) $V_n[P, f] = [P^{\oplus n}, v_n f]$,

where $v_n f$ is represented by

$$\begin{pmatrix} 0 & & & & f \\ 1 & 0 & & & \\ & \ddots & \ddots & & \\ & & \ddots & \ddots & \\ & & & & 0 \\ & & & & 1 \; 0 \end{pmatrix}$$

with 1's on the subdiagonal and f in the opposite corner. The matrix $v_n f$ is close to an n^{th}-root of f, in the sense that it describes the endomorphism X on the module $P[X]/X^n-f \cong P^{\oplus n}$.

One easily checks that the operations just defined are additive with respect to short exact sequences in $\underline{End}_A$, and thus are well-defined on W(A). We will demonstrate the compatibility with the operations on W(A) later.

Since $W(A) \subset \hat{W}(A)$ is dense and the operations gh_n, F_n, and V_n are continuous, identities among them may be verified on $\hat{W}(A)$ by checking them on W(A). Examples where this is easy are :

a) $F_n(v * w) = F_n v * F_n w$,

b) $gh_n(v * w) = gh_n v * gh_n w$,

c) $F_n V_n = n$,

d) $gh_n V_d(v) = \begin{cases} d\, gh_{n/d}(v) & \text{if } d \mid n \\ 0 & \text{if } d \nmid n. \end{cases}$

The corresponding matrix identities are :

a') $(f \otimes g)^n = f^n \otimes g^n$

b') $\mathrm{tr}((f \otimes g)^n) = \mathrm{tr}\, f^n \cdot \mathrm{tr}\, g^n$

c') $(v_n f)^n = \begin{pmatrix} f & & \\ & \ddots & \\ & & f \end{pmatrix}$

d') $\mathrm{tr}((v_d f)^n) = \begin{cases} d\, \mathrm{tr}(f^{n/d}) & \text{if } d \mid n, \\ 0 & \text{if } d \nmid n. \end{cases}$

From (d) we may recover the usual expression of the ghost coordinates in terms of the Witt coordinates. The Witt coordinates of a vector v are the coefficients in the expansion

$$v = \prod_{i=1} (1 - a_i T^i) = \prod_{i=1} V_i (1 - a_i T).$$

We obtain $gh_n(v) = \sum_{d \mid n} d\, a_d^{n/d}$. Many modern treatments of the subject of Witt vectors take this latter expression as the starting point of the theory ! It is easy to see why such an approach can cause confusion.

The logarithmic derivative of $1 - a_d T^d$ is $-\sum_{m=1}^{\infty} d\, a_d{}^m\, T^{dm-1}$, so we obtain the formula :

e) $$T v^{-1}\, dv/dT = -\sum_{n=1}^{\infty} gh_n(v)\, T^n$$

which yields the exponential trace formula :

e') $$T\, L(P, f)^{-1}\, d(L(P, f))/dT = -\sum_{n=1}^{\infty} \mathrm{tr}(f^n) \cdot T^n.$$

For example, when rank $P = 2$, we have $tr(f^2) = (tr\, f)^2 - 2 \det f$.

The rest of the paper is devoted to the proof of compatibility of the operations on $W(A)$ and $\hat{W}(A)$. The proof uses the following basic principle from the theory of Witt vectors : to demonstrate certain equations it suffices to check them on vectors of the form $1 - aT$.

To be precise, we see that the functor W satisfies :

i) If $A \to B$ is a surjective ring homomorphism, then $W(A) \to W(B)$ is surjective. (This follows from the fact that an endomorphism of $B^{\oplus n}$ lifts to an endomorphism of $A^{\oplus n}$.)

ii) If A is an algebraically closed field, then the group W(A) is generated by elements of the form [A, a]. (This holds because any matrix over A is trigonalizable.)

Suppose V is another functor which satisfies :

iii) If $A \to B$ is injective, then $V(A) \to V(B)$ is injective.

For the functor V we have in mind $\hat{W}$ or $\hat{W}(\hat{W})$. In fact, by (*), V = W satisfies (iii), but we will not use this.

<u>Basic Principle</u>: If $g, h : W^{\times n} \to V$ are two multi-$\mathbb{Z}$-linear natural transformations, such that for all A and all $a_1, \cdots, a_n \in A$ $g([A, a_1], \cdots, [A, a_n]) = h([A, a_1], \cdots, [A, a_n])$, then $g = h$.

The principle is an easy consequence of the fact that every ring is a quotient ring of a subring of an algebraically closed field.

The compatibility for product, gh_n, F_n, V_n, and λ_t reduces to the following verifications :

0) $(A \otimes A,\ a_1 \otimes a_2) \cong (A,\ a_1 a_2)$

1) $tr((a)^n) = a^n$

2) $L(A,\ a^n) = 1 - a^n T$

3) $L(A^{\oplus n},\ v_n(a)) = 1 - a T^n$

4) $\lambda_t[A,\ a] = 1 + [A,\ a]t$

REFERENCES

1. G. Almkvist, Endomorphisms of finitely generated projective modules over a commutative ring, Arkiv. för Math., 11 (1973) 263-301.

2. G. Almkvist, The Grothendieck Ring of the Category of Endomorphisms, J. Alg., 28 (1974) 375-388.

3. D. Grayson, The K-theory of Endomorphisms, to appear.