

¹ Math. Inst. University of Münster
Einsteinstr. 62
D - 48149 Münster
Germany ischebe@uni-muenster.de

Modules of Witt Vectors

Friedrich Ischebeck and Volker Kokot

Abstract

Parallel to the construction of the (big or small) Witt vectors ring $\Lambda(R)$ resp. $W^{(p)}(R)$ over a commutative ring R we construct a module $L(A)$ and $L(p, A)$ over $\Lambda(R)$, resp. $W^{(p)}(R)$ if a graded R -algebra A is given.

Introduction

The original ring of Witt vectors $W(R) = W^{(p)}(R)$, the ‘small Witt vectors ring’ is a functor from the category of commutative rings R to itself, defined with respect to a fixed prime number p . It has the following remarkable property: If K is a field of characteristic p , then $W(K)$ is a complete local domain of characteristic 0 with residue class field K . Moreover, if K is perfect of characteristic p , then $W(K)$ is a discrete valuation ring with maximal ideal $pW(K)$ and $W(K)/pW(K) = K$.

The ‘big (or universal) Witt vectors ring’ $\Lambda(R)$ was constructed much later independently by several authors, including Witt himself. The small Witt rings $W^{(p)}(R)$, for all prime numbers p , are residue class rings of $\Lambda(R)$. The additive group of $\Lambda(R)$ is isomorphic to the subgroup $1 + TR[[T]]$ of the unit group of the formal power series ring $R[[T]]$ (in one variable). (In [1] one finds the notation $U(R)$ for the big Witt vectors ring, whereas $\Lambda(R)$ in [1] denotes its underlying additive subgroup.)

In this paper we consider the analogous group $L(A) := 1 + \prod_{j \geq 1} A_j$ for any ‘product’-graded R -algebra $A = \prod_{j \geq 0} A_j$ (see 1.1) and equip it with the structure of a $\Lambda(R)$ -module.

*Sponsored by the DFG

Analogously to the small Witt vectors ring $W^{(p)}(R)$, attached to the prime number p , we construct the small Witt vectors module $L(p, A)$ as a residue class module of $L(A)$, in a manner that $L(p, A)$ also becomes a $W^{(p)}(R)$ -module.

Our construction is functorial in (R, A) .

If A is reduced of characteristic p , then $L(p, A)$ is \mathbb{Z} -torsion free, which generalizes the fact that $W^{(p)}(K)$ is of characteristic 0, if K is a field of characteristic p . (See Proposition 3.6.)

If R is a domain of characteristic p and A reduced, then $L(p, A)$ is torsion free over $W^{(p)}(R)$.

Let K be a perfect field of characteristic $p > 0$. Then it is easily seen that for every finitely generated $W(K)$ -module N there is a product graded K -algebra A with $L(p, A) \cong N$. On the other hand, the quotient field of $W(K)$ as a $W(K)$ -module is not of this form.

By \mathbb{N} we denote the set of integers ≥ 0 , by \mathbb{N}_1 the set of integers ≥ 1 , by \mathbb{P} the set of prime numbers.

We thank Hendrik W. Lenstra, who allows us to use freely ideas we found on his web site. Also we thank Dale Husemöller for advice.

1 Fundamental Constructions

1.1. Here we consider ‘product graded’ rings $A = \prod_{j \in \mathbb{N}} A_j$. This notion means a variation of the notion ‘graded ring’ insofar as we consider $\prod_{j \in \mathbb{N}} A_j$ instead of $\bigoplus_{j \in \mathbb{N}} A_j$. The elements of A can be uniquely written as formal infinite series $\sum_{n \in \mathbb{N}} f_n$ with $f_n \in A_n$. Multiplication is given by the Cauchy product $(\sum_{n \in \mathbb{N}} f_n)(\sum_{n \in \mathbb{N}} g_n) = \sum_{n \in \mathbb{N}} (\sum_{i+j=n} f_i g_j)$. In a canonical way A_0 is a subring of $\prod A_i$ and we require that A_0 has a 1 which is also the 1 of $\prod A_i$. A morphism of product graded rings $\alpha : \prod_j A_j \rightarrow \prod_j A'_j$ is a ring homomorphism with $\alpha(1) = 1$, $\alpha(A_j) \subset A'_j$ and $\alpha(\sum_{j \in \mathbb{N}} f_j) = \sum_{j \in \mathbb{N}} \alpha(f_j)$.

Let A_+ denote the (‘irrelevant’) ideal $\prod_{j \geq 1} A_j$ of $A = \prod_{j \geq 0} A_j$. We equip A with the A_+ -adic topology. The subgroup $1 + A_+ = \{1 + \sum_{j \geq 1} f_j \mid f_j \in A_j\}$ of the group of units A^\times of A will here

be denoted by $L(A)$. If $A = R[[T]]$ (with one indeterminate and the canonical graduation) we will write $\Lambda(R) := L(R[[T]]) = 1 + TR[[T]]$. This is compatible with Exercice 42) of §1 in [1] p. 56, and also with [4].

In the case where A_0 , hence A , is an R -algebra we will define a product $*$: $\Lambda(R) \times L(A) \rightarrow L(A)$, which in the case $A = R[[T]]$ gives $\Lambda(R)$ the structure of a ring (clearly the known one) and, for general A , equips $L(A)$ with a $\Lambda(R)$ -module structure.

1.2. Every element of $L(A)$ can be uniquely written as an infinite product of the form

$$\prod_{j \geq 1} (1 - f_j) \text{ with } f_j \in A_j.$$

(This follows from the fact that $(1 + f_n)^{-1}(1 + f_n + f_{n+1} + \dots)$ with $f_i \in A_i$ is of the form $1 + g_{n+1} + g_{n+2} + \dots$ with $g_i \in A_i$.) This means that $L(A)$ is topologically generated by the $(1 - f_j)^{-1}$ with homogeneous f_j of positive degree with respect to the A_+ -adic topology.

Note that one can construct an extension of the ring R over which the term $1 - aT^j$ splits into a product of linear factors. Therefore we will first define the $*$ -product in the special case $(1 - aT)^{-1} * u$ with $u \in L(A)$, and see then that this forces the definition in the general case $\alpha * u$ with $\alpha \in \Lambda(R), u \in L(A)$.

Let $a \in R, u := 1 + \sum_{j \geq 1} f_j \in L(A), f_j \in A_j$ (where the case $A = R[[T]]$ clearly is not excluded). For these special left factors our definition of ' $*$ ' is

$$(1 - aT)^{-1} * u := 1 + \sum_{j \geq 1} a^j f_j .$$

Note 1.3. For $A = R[[T]], u = (1 - bT)^{-1}$ this means $(1 - aT)^{-1} * (1 - bT)^{-1} = (1 - abT)^{-1}$.

It is **not** possible to give $L(A)$ – for general A – the structure of a ring in this way. One would come into trouble with graduation: Try e.g. $(1 - f)^{-1} * (1 - g)^{-1} = (1 - fg)^{-1}$ for $f, g \in A_1$. Applied to $A = R[[T]]$ this would give $(1 - aT)^{-1} * (1 - bT)^{-1} = (1 - abT^2)^{-1} \neq (1 - abT)^{-1}$.

Definitions 1.4. a) By \mathbb{A} we denote the category of pairs (R, A) where R is a commutative ring and A is a commutative product graded R -algebra, the R -algebra structure of A given by one of its zeroth part

A_0 . A morphism $(R, A) \rightarrow (R', A')$ is a pair of a ring homomorphism $\rho : R \rightarrow R'$ and a morphism of product graded rings $\alpha : A \rightarrow A'$ that are compatible with the algebra structures.

b) By \mathbb{M} we denote the category of pairs (R, M) where R is a commutative ring and M an R -module. A morphism $(R, M) \rightarrow (R', M')$ is a pair of a ring homomorphism $\rho : R \rightarrow R'$ and an R -module homomorphism $\mu : M \rightarrow M'$ where the R -module structure of M' is induced by its R' -module structure and ρ .

Theorem 1.5. For $(R, A) \in \text{Ob}(\mathbb{A})$ there are biadditive maps

$$* : \Lambda(R) \times \Lambda(R) \rightarrow \Lambda(R) \text{ and } * : \Lambda(R) \times L(A) \rightarrow L(A)$$

which are continuous with respect to the topologies defined by the irrelevant ideals $TR[[T]]$ and A_+ , such that

$$\mathbb{A} \rightarrow \mathbb{M}, (R, A) \mapsto (\Lambda(R), L(A))$$

is a functor and

$$(1 - aT)^{-1} * (1 + \sum_{j \geq 1} b_j T^j) = 1 + \sum_{j \geq 1} a^j b_j T^j,$$

$$(1 - aT)^{-1} * (1 + \sum_{j \geq 1} f_j) = 1 + \sum_{j \geq 1} a^j f_j$$

for $a, b_j \in R$, $f_j \in A_j$.

We will prove this in the remaining part of the section.

1.6. We will compute and argue modulo $\prod_{j > n} A_j$ in $L(A)$ resp. modulo T^{n+1} in $\Lambda(R)$. It is not difficult to see $L(A)/(1 + \prod_{j > n} A_j) \cong L(A/\prod_{j > n} A_j)$. We define $L_n(A) := L(A/\prod_{j > n} A_j)$ and $\Lambda_n(R) := L(R[[T]]/(T^{n+1}))$. Taking inverse limits and using continuity, we will get definitions and statements for $\Lambda(R)$ and $L(A)$.

We will not be too pedantic in our notations. So we will write $\sum_{j=1}^n f_j$ and also $(1 - aT^m)^{-1}$ for their residue classes modulo $\prod_{j > n} A_j$. Also if R' is a nongraded R -algebra we will write $L_n(R' \otimes A) := L_n(\prod_{j \geq 0} (R' \otimes_R A_j))$. (There may be some justification in the fact that one may identify $L_n(A)$ with $\bigoplus_{j=0}^n A_j$ with an adjusted multiplication. Also one may regard A as the sequence of the A_j instead of their product.)

Definition 1.7. Let $a \in R$, $u := 1 + \sum_{j=1}^n f_j \in L_n(A)$. Then define

$$\varphi_a(u) := (1 - aT)^{-1} * u = 1 + \sum_{j=1}^n a^j f_j$$

Remark 1.8. The following is easily verified: φ_a is a group endomorphism of $L_n(A)$ and for $a, b \in R$ we have $\varphi_a \circ \varphi_b = \varphi_{ab}$.

1.9. By $\mathbb{Z}[R] := \mathbb{Z}[(R, \cdot)]$ we denote the monoid ring over \mathbb{Z} of the multiplicative monoid of R . Then, $a \in R$ operating as φ_a , the group $L_n(A)$ becomes a $\mathbb{Z}[R]$ -module.

Considering the case $A = R[[T]]$, we get a $\mathbb{Z}[R]$ -module homomorphism $\mathbb{Z}[R] \rightarrow \Lambda_n(R)$, defined by $1 \mapsto (1 - T)^{-1}$. Its kernel is an ideal. Therefore its image, denoted by $M_n(R)$, has the structure of a ring. And $L_n(A)$ is a module over that ring. Note that

(*) the assignment $(R, A) \mapsto (M_n(R), L_n(A))$ is a functor.

There is a ring extension $R \subset \bar{R}$ such that every nonconstant polynomial over \bar{R} splits into linear factors. One can even choose \bar{R} so that it is free over R with a basis containing 1.

To see this, note that $R[X]/(f)$ is free over R with basis the classes $\bar{1}, \bar{X}, \dots, \bar{X}^{n-1}$, if f is monic of degree n .

The rest of the construction is similar to that of an algebraically closed extension field in [3] V, Theorem 2.5.

1.10. Note that if over some ring one has $X^m - a = (X - \alpha_1) \cdots (X - \alpha_m)$ then $1 - aT^m = (1 - \alpha_1 T) \cdots (1 - \alpha_m T)$. Therefore $M_n(\bar{R}) = \Lambda_n(\bar{R})$. So there is a product $\Lambda_n(\bar{R}) \times L_n(A \otimes_r \bar{R}) \rightarrow L_n(A \otimes_R \bar{R})$, $(\lambda, u) \mapsto \lambda * u$.

The following lemma (of Lenstra) now is crucial:

Lemma 1.11. Let $R \subset R'$ be a ring extension and $\lambda \in \Lambda(R)$, $u \in L_n(A)$ such that $\lambda \in M_n(R')$. Then $\lambda *_{\bar{R}} u = \lambda *_{R'} u \in L_n(A)$.

Proof. Let $R' \subset R''$ be a ring extension. Then by functoriality, 1.9 (*), we have $\lambda *_{R'} u = \lambda *_{R''} u$. Apply this to the case $R'' = R' \otimes_R \bar{R}$. Write

$\overline{R} = \bigoplus_{i \in I} R e_i$ with $e_0 = 1$. Then $R'' = \bigoplus_{i \in I} R' e_i$. Considering R', \overline{R} canonically as subrings of R'' (especially $R' = R' e_0$), one has $R' \cap \overline{R} = R$.

So one has $\lambda *'_R u = \lambda *_{R''} u = \lambda *_{\overline{R}} u$, and this element lies in $L_n(R' \otimes A) \cap L_n(\overline{R} \otimes A) = L_n(A)$. \square

This means there is a unique possibility to define the $*$ -multiplication with those properties, which are required in the Theorem.

2 Elementary Properties

Proposition 2.1. *Let $d, e \in \mathbb{N}_1$, $\mu := \text{lcm}(d, e)$, $\delta := \text{gcd}(d, e)$ and $a \in R$, $f \in A_e$. Then*

$$(1 - aT^d)^{-1} * (1 - f)^{-1} = (1 - a^{\mu/d} f^{\mu/e})^{-de/\mu} = (1 - a^{e/\delta} f^{d/\delta})^{-\delta}. \quad (1)$$

Especially for $A = R[[T]]$ the $$ -product is commutative.*

Proof. Let $\zeta \in \mathbb{C}$ be a primitive d -th root of unity. One knows that $\mathbb{Z}[\zeta]$ is free over \mathbb{Z} with basis $1, \zeta, \dots, \zeta^{\varphi(d)-1}$. Now let $R' \supset R$ be a ring extension (with R') containing a d -th root α of a .

Then we may write $R' \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta] = R' \oplus R' \zeta \oplus \dots \oplus R' \zeta^{\varphi(d)-1}$. (Especially we write $\alpha \zeta^j$ instead of $\alpha \otimes \zeta^j$.)

From $\prod_{j=1}^d (1 - \zeta^j T) = 1 - T^d$ in $\mathbb{Z}[\zeta][T]$ one derives $\prod_{j=1}^d (1 - \alpha \zeta^j T) = 1 - aT^d$ in $(R' \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta])[T]$. By distributivity of ' $*$ ' with respect to ' \cdot ' we see

$$(1 - aT^d)^{-1} * (1 - f)^{-1} = \prod_{j=1}^d \left((1 - \alpha \zeta^j T)^{-1} * (1 - f)^{-1} \right) = \prod_{j=1}^d (1 - \alpha^e \zeta^{ej} f)^{-1} = \left(\prod_{j=1}^{d/\delta} (1 - \alpha^e \zeta^{ej} f) \right)^{-\delta}.$$

The last equality holds, since the series $(\zeta^{ej})_j$ has the period d/δ , i.e. ζ^e is a primitive (d/δ) -th root of unity. Since further $(\alpha^e)^{d/\delta} = a^{e/\delta}$ we see

$$\left(\prod_{j=1}^{d/\delta} (1 - \alpha^e \zeta^{ej} f) \right)^{-\delta} = (1 - a^{e/\delta} f^{d/\delta})^{-\delta}.$$

□

Note 2.2. Before we knew of Lenstra's notices [4] we defined the $*$ -product by equation (1). This defines ' $*$ ' for general factors by biadditivity and continuity, which means biadditivity with respect to infinite series. To show the ring, resp. module axioms we first considered the case $A = R[[X_1, \dots, X_n]]$. We used formal logarithmic derivations with respect to T and the X_j . The general case was then handled, using homomorphisms $R[[X_1, \dots, X_n]] \rightarrow A$.

Remarks 2.3. We compute some $*$ -products.

α) $(1 - aT^d)^{-1} * (1 - f)^{-1} = (1 - a^e f^d)^{-1}$, if $f \in A_e$ and $\gcd(d, e) = 1$.

β) Let $j, k, p \in \mathbb{N}$ and $p > 1$, further $f \in A_{p^k}$. Then

$$(1 - aT^{p^j})^{-1} * (1 - f)^{-1} = \begin{cases} (1 - a^{p^{k-j}} f)^{-p^j} & \text{if } j \leq k \\ (1 - a f^{p^{j-k}})^{-p^k} & \text{if } j \geq k \end{cases}$$

γ) In addition to the assumptions of β) let p be a prime number and R (hence also A) be of characteristic p . Then β) reduces to the simple formula

$$(1 - aT^{p^j})^{-1} * (1 - f)^{-1} = (1 - a^{p^k} f^{p^j})^{-1}.$$

The rest of this section does not concern the $*$ -product.

2.4. a) The order of $(1 - T)^{-1}$ in the group $\Lambda(R)$, i.e. the additive order of the (unit element) $\mathbf{1}$ in the ring $\Lambda(R)$, is ∞ , if $R \neq 0$. I.e. the canonical ring homomorphism $\mathbb{Z} \rightarrow \Lambda(R)$ is injective for $R \neq 0$.

b) When is $L(A)$ torsion free as abelian group? Not always:

If in $A_+ = \prod_{j \geq 1} A_j$ there is a nilpotent nonzero element f of finite additive order, then $L(A)$ has torsion.

Namely some power $g = f^m$ has the property $g \neq 0$, $g^2 = 0$. Let $n > 0$ and $nf = 0$. Then $ng = nf \cdot f^{m-1} = 0$. So $1 + g \neq 1$, but $(1 + g)^n = 1 + ng + \binom{n}{2}g^2 + \dots = 1$.

Especially, if in A_+ there is an element whose order is not squarefree then $L(A)$ is not torsion free. For in this case there is a $g \in A_+$ of order m^2 with some $m \geq 2$. Then $mg \neq 0$, $m(mg) = 0 = (mg)^2$.

Proposition 2.5. *Let A be a product graded ring such that for every $p \in \mathbb{P}$, $j \geq 1$ there is no $f \in A_j - \{0\}$ with both $pf = 0$ and $f^p \in pA_{pj}$.*

Then $L(A)$ is \mathbb{Z} -torsion free.

Note that in this paper we use no double indices, especially the index pj above means $p \cdot j$.

Proof. If in $L(A)$ there is an element of finite order, there is also one whose order is a prime number p . So let $u = 1 + f_k + f_{k+1} + \dots$ be such that $f_j \in A_j, f_k \neq 0$. We have to show $u^p \neq 1$.

Otherwise we would first obtain $pf_k = 0$ by considering the k -th homogeneous part of u^p . Then considering its pk -th homogeneous part, we would see that $-f_k^p$ would be a sum of some $\binom{p}{r} f_j^r$ with $k < j \leq pk, 1 \leq r < p$. Since the coefficients are divisible by p , we would see $f_k^p \in pA_{pk}$ whence $f_k = 0$. \square

Corollary 2.6. *a) If A is \mathbb{Z} -torsion free, then $L(A)$ is \mathbb{Z} -torsion free.*

b) Let A be an \mathbb{F}_p -algebra for some $p \in \mathbb{P}$. Then $L(A)$ is \mathbb{Z} -torsion free, iff A_+ is reduced.

c) Let every element of A_+ be of finite squarefree order. Then $L(A)$ is \mathbb{Z} -torsion free, iff A_+ is reduced.

Proof. We have only to show one direction of c). So let p be a prime number. The elements of order p , resp. of order prime to p form graded ideals J , resp. I with $A = J \oplus I$, such that A as a ring is isomorphic to $(A/I) \times (A/J)$. Etc. \square

3 Universally Defined Submodules and Ideals

Definition 3.1. *A subset S of \mathbb{N}_1 is called divisor closed if the divisors of every $n \in S$ also belong to S .*

Equivalently this means that its complement $S^c := \mathbb{N}_1 - S$ has the (ideal like) property $\mathbb{N}_1 S^c \subset S^c$.

Examples 3.2. The mostly used examples of divisor closed sets are

- a) $\{1, 2, \dots, n\}$,
- b) $\langle p \rangle := \{1, p, p^2, \dots\}$ for $p \in \mathbb{P}$,
- c) $\{1, p, p^2, \dots, p^n\}$ for $p \in \mathbb{P}$,
- d) $S := \bigcup_{p \in \mathbb{P}} \langle p \rangle$.

Lemma 3.3. *Let $S \subset \mathbb{N}_1$ be divisor closed.*

a) *The following subsets of $L(A)$ are equal:*

(i) *the set of the (converging) products $\prod_{j=1}^{\infty} (1 - f_j)^{-1} \in L(A)$ with homogeneous f_j whose degrees are elements of S^c ;*

(ii) *the set of the $\prod_{j=1}^{\infty} (1 - g_j)^{-1}$ with g_j homogeneous of degree j and $g_j = 0$ if $j \in S$.*

b) *The set defined by (i) or (ii) is a $\Lambda(R)$ -submodule of $L(A)$, which we denote by $E_S(A)$. In the case $A = R[[T]]$ this means that $E_S(A)$ is an ideal of $\Lambda(R)$.*

(Note that $E_S(A)$ in general is **not** the set of series $1 + \sum_{j \notin S} f_j$ with $f_j \in A_j$. The latter nearly never is closed with respect to multiplication in A , i.e. addition in $L(A)$.)

Proof. Let $f, g \in A_r$ with $r \notin S$. Then $(1 - f)^{-1}$ and $(1 - f)^{-1}(1 - g)^{-1}$ are of the form $1 + \sum_{j \geq 1} h_j$, with $h_j \in A_{rj}$ i.e. of the form $\prod_{j \geq 1} (1 - h'_j)$ with $h'_j \in A_{rj}$. (Recall that rj is not a double index, but means $r \cdot j$.) Since $r \notin S$ and S is divisor closed, also $rj \notin S$. Both claims of the Lemma follow easily from this observation. \square

Definition 3.4. *We write $L(S, A) := L(A)/E_S(A)$ and $\Lambda(S, R) = \Lambda(R)/E_S(R[[T]])$.*

Further for a prime number p we write $E_p(A) := E_S(A)$ and $L(p, A) := L(S, A)$ if $S = \langle p \rangle$, the multiplicative subset of \mathbb{N}_1 , generated by p .

To adapt the classical notation we write $W(R) = W^{(p)}(R) := \Lambda(S, R)$ in the case $S = \langle p \rangle$. Note that $W^{(p)}(R)$ is the classical (small) ring of Witt vectors.

Remarks 3.5. a) $L(S, A)$ is a $\Lambda(S, R)$ -module.

b) A class modulo $E_S(A)$ in $L(A)$ can be represented canonically by an element of the form $w = \prod_{j \in S} (1 - f_j)^{-1}$ where f_j is homogeneous of degree j . The set U_S of these representants is mapped bijectively onto $L(S, A)$ by the canonical projection (residue class map) $\kappa : L(A) \rightarrow L(S, A)$. (In the case $S = \langle p \rangle$ the set $U_p := U_S$ consists of the $w = \prod_{k=0}^{\infty} (1 - f_k)^{-1}$ where f_k is homogeneous of degree p^k .)

Representing a residue class modulo $E_S(A)$ in this way, we obtain a set theoretical cross-section (right inverse) $\sigma : L(S, A) \rightarrow L(A)$ to the canonical projection $\kappa : L(A) \rightarrow L(S, A)$.

c) Note that σ is not generally an additive group homomorphism. Namely U_S is not always a subgroup of $L(A)$. For example let $p > 2$ be prime, $S = \langle p \rangle$, A of characteristic 2 and $a \in A$ homogeneous of degree p and not nilpotent. Then $(1 - a)^2 = 1 - a^2$, where a^2 is homogeneous of degree $2p \neq p^k$ for any k .

Also if $\lambda \in \Lambda(S, R)$ and $w \in L(S, A)$, then generally $\sigma(\lambda * w) \neq \sigma(\lambda) * \sigma(w)$. For example let $R = \mathbb{Z}, A = \mathbb{Z}[[T]], S = \langle 3 \rangle$. Then $(1 - T^3)^{-1} * (1 - T^3)^{-1} = (1 - T^3)^{-3} = (1 - 3T^3)^{-1}(1 + 3T^6)^{-1} \dots \neq (1 - a_0T)^{-1}(1 - a_1T^3)^{-1}(1 - a_2T^9)^{-1} \dots$, so it is not a canonical representant.

d) But if p is a prime number, $S = \langle p \rangle$ and $\text{char}(R) = p$, then by Remark 2.3 γ)

$$\sigma(\lambda * w) = \sigma(\lambda) * \sigma(w).$$

Especially in this case the subset $\{\prod_{j \geq 0} (1 - a_j T^{p^j})^{-1}\}$ of $\Lambda(R)$ is closed with respect to $*$ -multiplication.

e) Let $S = \{1\}$. The submodule $E_{\{1\}}(A)$ consists of the elements of the form $\prod_{j \geq 2} (1 - f_j)^{-1}$ with $f_j \in A_j$. One sees easily that $L(\{1\}, A)$ as a module over $R = \Lambda(\{1\}, R)$ is isomorphic to the R -module A_1 .

f) Every small Witt vectors ring $W^{(p)}(R)$ is a residue class ring of $\Lambda(S, R)$, where S is defined as under 3.2 d).

Proposition 3.6. *Let A be a reduced product graded ring of characteristic $p \in \mathbb{P}$. Then $L(p, A)$ is \mathbb{Z} -torsion free.*

Proof. If $L(p, A)$ had \mathbb{Z} -torsion elements, there would be a prime number q and a class $\bar{w} \in L(p, A)$ of order q where $w = \prod_{k=0}^{\infty} (1 - f_k)^{-1}$ with $f_k \in A_{p^k}$ and not all $f_k = 0$.

1-st case: $q = p$. Then $w^p = \prod_{k=0}^{\infty} (1 - f_k)^{-p} = \prod_{k=0}^{\infty} (1 - f_k^p)^{-1}$, and every f_k^p is homogeneous of degree p^{k+1} . Further $f_k^p \neq 0$ if $f_k \neq 0$, since A is reduced.

2-nd case: $q \neq p$. Let m be minimal under the k with $f_k \neq 0$. Then

$$w^{-q} = 1 - qf_m + \text{terms of higher degrees} = (1 - qf_m)^{-1} \prod_{j>p^m} (1 - g_j)^{-1}$$

with $g_j \in A_j$ and $qf_m \neq 0$. So $q \cdot \bar{w} \neq 0$ in $L(p, A)$. \square

Lemma 3.7. *Let $q \in \mathbb{P}$, $m, k \in \mathbb{N}_1, k \leq q^m$. Then $q^m \mid \binom{q^m}{k}$, iff $q \nmid k$.*

Clearly we believe that this is well-known, but we do not know a source.

Proof. Let v_q denote the q -adic valuation of \mathbb{Q} . We have to show that $v_q\left(\binom{q^m}{k}\right) = m$ iff $q \nmid k$. One knows

$$v_q\left(\binom{n}{k}\right) = v_q(n!) - v_q(k!) - v_q((n-k)!) = \sum_{j \geq 1} \left(\left[\frac{n}{q^j} \right] - \left[\frac{k}{q^j} \right] - \left[\frac{n-k}{q^j} \right] \right)$$

with Gauss brackets $[\]$. The statement now follows from the simple facts that $[a+b] - [a] - [b] = 1$, if $a, b \in \mathbb{R} - \mathbb{Z}$, $a+b \in \mathbb{Z}$ and that $[a+b] - [a] - [b] = 0$, if $a, b \in \mathbb{Z}$. \square

Proposition 3.8. *Let $n \in \mathbb{N}_1$ and $S \subset \mathbb{N}_1$ be a divisor closed set such that no divisor > 1 of n belongs to S . If A is annihilated by n , then so is $L(S, A)$.*

Epecially, if q, p are different prime numbers and A is of characteristic q , then $L(p, A)$ is a (\mathbb{Z}/q) -vector space.

Proof. A splits into finitely many direct factors which are annihilated by prime powers dividing n . So it is enough to show the statement under the hypothesis that $n = q^m$ with $q \in \mathbb{P} - S$. Let $f \in A_r$. By the Lemma $(1-f)^{q^m} = 1 + g_1 + g_2 + \dots$, where $g_j \in A_{jq}$, since the summands $\in A_k$ with $q \nmid k$ disappear. So $(1-f)^{q^m} \in E_S(A)$. \square

4 Small Witt Vectors

In this section let p be a prime number and $W(R) := W^{(p)}(R)$. Further let R be a ring of characteristic p , i.e. a nonzero \mathbb{Z}/p -algebra. Let further A be a nonzero product graded R -algebra (such that also $\text{char}(A) = p$).

The results are well-known as far as only $W(R)$ is regarded, but are here reproved without referring to the classical theory of Witt vectors, as developed for instance in [1] Section 1.

Proposition 4.1. *If R is a domain of characteristic p and A is reduced and R -torsion free, then $L(p, A)$ is $W(R)$ -torsion free.*

Proof. Let $f \in A_{p^k}$ and $a \in R$. Then by Example 2.3 γ)

$$(1 - aT^{p^j})^{-1} * (1 - f)^{-1} = (1 - a^{p^k} f^{p^j})^{-1} \quad (*)$$

The element $a^{p^k} f^{p^j} \in A$ is homogeneous of degree p^{j+k} and not zero, if a and f are not. Now let a nonzero element of $W(R)$ resp. one of $L(p, A)$ be represented by

$$\prod_{j=0}^{\infty} (1 - a_j T^{p^j})^{-1}, \text{ resp. } \prod_{k=1}^{\infty} (1 - f_k) \quad (**)$$

with $f_k \in A_{p^k}$. The $*$ -product of those factors $(1 - a_j T^{p^j})^{-1}$, $(1 - f_k)^{-1}$ in $(**)$ where j, k are minimal with $a_j \neq 0$ resp. $f_k \neq 0$ is nontrivial and not affected by the other $*$ -products of the factors in $(**)$.

So the $*$ -product of the above representants represents a nonzero element of $L(A)/E_p(A)$. \square

Corollary 4.2. *If R is a domain of characteristic p , then $W(R)$ is a domain of characteristic 0.*

Definition 4.3. *Define $V_1(R)$ to be the ideal consisting of all elements, represented by*

$$\prod_{j=1}^{\infty} (1 - a_j T^{p^j})^{-1} \text{ (i.e. } a_0 = 0 \text{)} .$$

Indeed $V_1(R)$ is an ideal of $W(R)$. Moreover $W(R)/V_1(R) \cong \Lambda(\{1\}, R) \cong R$

Proposition 4.4. $V_1(R)$ is contained in the Jacobson radical of $W(R)$.

Proof. We have to show that $1+\alpha$ is a unit in $W(R)$ for every $\alpha \in V_1(R)$. In $\Lambda(R)$ the element representing $1+\alpha$ is written as

$$(1-T)^{-1}(1-a_1T^p)^{-1}(1-a_2T^{p^2})^{-1}\dots = (1-T)^{-1}\prod_{j \geq 1}(1-a_jT^{p^j})^{-1}$$

We will find successively elements $b_1, b_2, \dots \in R$, such that

$$\left((1-T)\prod_{j \geq 1}(1-a_jT^{p^j})\right)^{-1} * \left((1-T)\prod_{j \geq 1}(1-b_jT^{p^j})\right)^{-1} \equiv (1-T)^{-1}$$

modulo $E_p(R[[T]])$.

Assume we have found already $b_1, \dots, b_k \in R$ such that the $*$ -product

$$\left((1-T)\prod_{j \geq 1}(1-a_jT^{p^j})\right)^{-1} * \left((1-T)\prod_{j=1}^k(1-b_jT^{p^j})\right)^{-1}$$

modulo $E_p(R[[T]])$ is congruent to

$$(1-T)^{-1}\prod_{j \geq k+1}(1-c_jT^{p^j})^{-1}$$

Then, setting $b_{k+1} := -c_{k+1}$, we obtain modulo $E_p(R[[T]])$ by the distributivity of ' $*$ ' with respect to ' \cdot '

$$\begin{aligned} & \left((1-T)\prod_{j \geq 1}(1-a_jT^{p^j})\right)^{-1} * \left((1-T)\prod_{j=1}^{k+1}(1-b_jT^{p^j})\right)^{-1} \equiv \\ & \left((1-T)\prod_{j \geq k+1}(1-c_jT^{p^j})\right)^{-1} \left(\left((1-T)\prod_{j \geq 1}(1-a_jT^{p^j})\right)^{-1} * (1-b_{k+1}T^{p^{k+1}})^{-1}\right) \\ & \equiv \left((1-T)\prod_{j \geq k+1}(1-c_jT^{p^j})\right)^{-1} \left((1-b_{k+1}T^{p^{k+1}})\prod_{j \geq k+2}(1+d_jT^{p^j})\right)^{-1} \end{aligned}$$

with suitable $d_j \in R$ for $j \geq k+2$. Now since $b_{k+1} = -c_{k+1}$, we have

$$(1 - c_{k+1}T^{p^{k+1}})(1 - b_{k+1}T^{p^{k+1}}) = 1 + b_{k+1}^2 T^{2p^{k+1}} \equiv 1 \quad \text{or} \quad 1 + b_{k+1}^2 T^{2p^{k+2}}$$

the latter being the case if $p = 2$.

So successively we can choose the b_j in such a way that this product becomes congruent to $(1 - T)^{-1}$ modulo $E_p(R[[T]])$. \square

Corollary 4.5. *Let $R = K$ be a field (of characteristic p , not necessarily perfect). Then $W(K)/V_1(K) \cong K$. So $V_1(K)$ is a maximal ideal of $W(K)$ and by the proposition it is unique.*

4.6. Let $\prod_{j=0}^{\infty} (1 - a_j T^{p^j})^{-1}$ represent an element $\alpha \in W(R)$. Then $p \cdot \alpha$, i.e. the sum of p summands α is represented by $\prod_{j=0}^{\infty} (1 - a_j^p T^{p^{j+1}}) - 1$.

So if R is perfect, i.e. every $b \in R$ of the form $b = a^p$, then $p \cdot W(R) = V_1(R)$. If R is not perfect then $V_1(R)$ is not finitely generated as an ideal of $W(R)$.

Proposition 4.7. *Let K be a perfect field of characteristic p . Then $W(K)$ is a complete discrete valuation ring of characteristic 0 with maximal ideal $pW(K)$ and residue class field K .*

Proof. We know already that $W(K)$ is local with maximal ideal $p \cdot W(K)$ and residue class field K , and that further it is a domain of characteristic 0. But we do not yet know that $W(K)$ is Noetherian.

To show that $W(K)$ is a discrete valuation ring, we prove that every nonzero element of it is of the form $p^n \cdot u$ with $n \in \mathbb{N}$ and a unit u . This means that in $\Lambda(K)$ modulo $E_p(K[[T]])$ every element $\neq 1$ is of the form

$$(1 - T^{p^n})^{-1} * \prod_{j=0}^{\infty} (1 - b_j T^{p^j})^{-1} \quad \text{with } b_0 \neq 0.$$

Let $w \in W(R)$ be represented by $\prod_{j \geq 0} (1 - a_j T^{p^j})^{-1}$, and assume n is minimal under the j with $a_j \neq 0$. Choose by perfectness $b_j \in R$ so that $b_j^{p^n} = a_{n+j}$. Then

$$\prod_{j=0}^{\infty} (1 - a_j T^{p^j})^{-1} = \prod_{j \geq 0} (1 - b_j^{p^n} T^{p^{j+n}})^{-1} = \left(\prod_{j \geq 0} (1 - b_j T^{p^j}) \right)^{-p^n}$$

$$= (1 - T^{p^n})^{-1} * \prod_{j=0}^{\infty} (1 - b_j T^{p^j})^{-1} \text{ with } b_0 \neq 0 .$$

The completeness follows from the fact that in $\Lambda(K)$ the infinite product $\prod_{k=0}^{\infty} f_k$ makes sense if the $f_k \in \Lambda(K)$ are of the form

$$f_k = \prod_{j=0}^{\infty} (1 - a_{k,j} T^{p^j})^{-1} \text{ with } a_{k,j} = 0 \text{ for } j < n_k$$

where $(n_k)_{k \in \mathbb{N}}$ is a sequence in \mathbb{N} with limit ∞ . □

Corollary 4.8. *If K is as above and A a reduced product graded K -algebra, then $L(p, A)$ is flat over $W(K)$.*

Namely we know that $L(p, A)$ is torsion free over the discrete valuation ring $W(K)$.

Definition 4.9. *Let $A^{(j)} = \prod_{n \geq 0} A_n^{(j)}$ for $j \in J$ be product graded R -algebras. Then we define $\prod_{j \in J} A^{(j)}$ by $(\prod_{j \in J} A^{(j)})_n := \prod_{j \in J} A_n^{(j)}$ for $n \geq 1$. One may set either $(\prod_{j \in J} A^{(j)})_0 = R$ or $(\prod_{j \in J} A^{(j)})_0 = \prod_{j \in J} A_0^{(j)}$.*

4.10. It is clear that for any family $(A^{(j)})_{j \in J}$ there is a natural isomorphism

$$L(p, \prod_{j \in J} A^{(j)}) = \prod_{j \in J} L(p, A^{(j)})$$

Proposition 4.11. *Let K be a perfect field of characteristic $p > 0$ and $W(K) = W(p, K)$. Then every finitely generated $W(K)$ -module is of the form $L(p, A)$ for some product graded K -algebra A .*

Proof. Since $L(p, K[[T]]) = W(K)$ and $L(p, K[[T]]/(T^{p^n})) \cong W(K)/p^n W(K)$, this follows from (4.10) and the structure theory of finitely generated modules over a principal ring. □

4.12. On the other hand not every $W(K)$ -module is of the form $L(p, A)$ for some A . Namely let Q be the quotient field of $W(K)$ considered as $W(K)$ -module. Then $p \cdot Q = Q$. But $p \cdot L(p, A) \neq L(p, A)$, if $L(p, A) \neq 0$. For, let m be the minimal j with $A_{p^j} \neq 0$ and $f \in A_{p^m} - \{0\}$. Then $1 - f$ is no p -th power of any element of A .

References

- [1] N. Bourbaki: Algèbre Commutative, Chapitre 9
- [2] V. Kokot: Moduln von Wittvektoren, Dissertation Münster, 2000
- [3] S. Lang: Algebra
- [4] H. Lenstra: Construction of the Ring of Witt Vectors. Preprint 2002