A functorial property of nested Witt vectors

Roland Auer

Rijksuniversiteit Groningen, Vakgroep Wiskunde,
Blauwborgje 3, NL-9747 AC Groningen, The Netherlands
E-mail: auer@math.rug.nl

For coprime truncation sets $M, N \subseteq \mathbb{N}$, we establish an isomorphism of functors $\mathbb{W}_N \circ \mathbb{W}_M \simeq \mathbb{W}_{MN}$, where $\mathbb{W}_N(A)$ denotes the ring of N-Witt vectors over a ring A. Further we note that this isomorphism can, under certain restrictions on A, be expressed in terms of Artin-Hasse exponentials.

Key Words: Witt vectors (2000 MSC: 13K05)

INTRODUCTION

From Roberts' paper [4], we can extract the following result. Let p be a prime number, $M = \{1, p, p^2, \dots\}$ and $N \subseteq \mathbb{N}$ the set of positive integers coprime to p. Then, for (commutative) algebras A over the localisation $\mathbb{Z}_{(p)} = \mathbb{Z}[\frac{1}{n} : n \in N]$, there is a functorial isomorphism of rings

$$\mathbb{W}_N(\mathbb{W}_M(A)) \simeq \mathbb{W}_{\mathbb{N}}(A). \tag{1}$$

Here, $\mathbb{W}_N$ denotes the Witt functor on the index set N. (A more precise definition and some basic properties of Witt vectors are given in Section 1.) This result has applications to class field theory by interpreting $\mathbb{W}_{\mathbb{N}}(\mathbb{F}_q)$ as the one-unit group in a local function field (cf. Remark (c) to Proposition 3.1 below).

The question arises whether (1) holds generally for $M \cap N = \{1\}$, $MN = \mathbb{N}$ and arbitrary rings A. We shall answer this question affirmatively in Section 2. The crucial point (as with most proofs concerning Witt vectors) will be to show that certain polynomials over $\mathbb{Q}$ actually have their coefficients in $\mathbb{Z}$. This exposition is concluded in Section 3 by explaining how the isomorphism (1) can be written out using Artin-Hasse exponentials, when returning to the assumption that A is an algebra over $\mathbb{Z}[\frac{1}{n} : n \in N]$.

I am grateful to H. W. Lenstra, who first mentioned to me the result proven here as a conjecture. Also, I want to thank M. van der Put for valuable discussions.

1. PRELIMINARIES

Let us briefly recall the necessary facts about Witt vectors, which we distill from [6] and [3]. In this text, rings and algebras are always commutative with 1, and a morphism of rings $A \to B$ sends 1_A to 1_B. In what follows, A always denotes a ring. For any set N, let Π_N : Rings $\to$ Rings be the functor which associates to A the N-fold direct product ring A^N with the usual componentwise addition and multiplication. Note that Π_N is left represented by the polynomial ring $R_N := \mathbb{Z}[x_n : n \in N]$.
Throughout, $\mathbb{N}$ is the set of positive integers. Now let $N \subseteq \mathbb{N}$ be a **truncation set**, i.e. N contains every positive divisor of each of its elements. We denote by $\mathbb{W}_N$: Rings $\to$ Rings the Witt functor which is also left represented by R_N. However, addition and multiplication in $\mathbb{W}_N(A)$ are defined by requiring that the functorial map

$$\varphi_N(A) : \begin{array}{rcl} \mathbb{W}_N(A) & \to & A^N \\ x = (x_n)_{n\in N} & \mapsto & (x^{(n)})_{n\in N} \end{array}$$

with

$$x^{(n)} := \sum_{d|n} d x_d^{n/d} \tag{2}$$

is a ring morphism. (In other words, $\varphi_N : \mathbb{W}_N \to \Pi_N$ is a natural transformation.)
Set $\mathbb{W} := \mathbb{W}_{\mathbb{N}}$ and let t be a variable. Then the functorial bijection

$$\begin{array}{rcl} \mathbb{W}(A) & \to & \Lambda(A) := 1 + tA[[t]] \\ x = (x_n)_{n\in\mathbb{N}} & \mapsto & f_x := \prod(1 - x_n t^n)^{-1} \end{array}$$

transports the ring structure from $\mathbb{W}(A)$ to $\Lambda(A)$. The map

$$\partial(A) : \begin{array}{rcl} \Lambda(A) & \to & tA[[t]] \\ f & \mapsto & \partial f := t\frac{f'}{f} \end{array}$$

(where f' means the formal derivative w.r.t. the variable t) sends f_x to $\sum_{n\in\mathbb{N}} x^{(n)} t^n$. Hence $(\mathbb{W}(A), +) \to (\Lambda(A), \cdot)$ is an isomorphism of groups. (The multiplication in the ring $\Lambda(A)$ is a bit more complicated.) Below, we shall need some facts and definitions concerning truncation sets and the ring morphisms $\varphi_N(A)$.

Remark/Definition.

(a) If M and N are truncation sets, then $MN := \{mn \,|\, m \in M, n \in N\}$ is a truncation set.

(b) The submonoid of $(\mathbb{N}, \cdot)$ generated by any set of prime numbers is a truncation set. These are precisely the truncation sets which are submonoids of $\mathbb{N}$, and we call them **monoidal**.

(c) For any subset $M \subseteq \mathbb{Z}$, the set $M^\perp := \{n \in \mathbb{N} \,|\, \gcd(m,n) = 1\ \forall m \in M\}$ is a monoidal truncation set. If M is a monoidal truncation set, then $M^\perp$ is uniquely determined by the two identities $M \cap M^\perp = \{1\}$ and $MM^\perp = \mathbb{N}$.

For a (truncation) set $N \subseteq \mathbb{N}$, let $\mathbb{Z}_N := \mathbb{Z}[\frac{1}{n} : n \in N] \subseteq \mathbb{Q}$ denote the localization of $\mathbb{Z}$ by N.

LEMMA 1.1. *Let $M \neq \emptyset$ and N be truncation sets and A a ring. Then we have the following characterizaions.*

(a) *$\varphi_N(A)$ is injective $\iff$ A has no N-torsion.*

(b) *$\varphi_N(A)$ is surjective $\iff$ $\varphi_N(A)$ is bijective $\iff$ A is a $\mathbb{Z}_N$-algebra $\iff$ $\mathbb{W}_M(A)$ is a $\mathbb{Z}_N$-algebra.*

2. MAIN THEOREM

Let M, N be two truncation sets and A a ring. Applying the functoriality of φ_N to the ring morphism $\varphi_M(A) : \mathbb{W}_M(A) \to A^M$ gives the commutative diagram

$$\begin{array}{ccc} \mathbb{W}_N(\mathbb{W}_M(A)) & \xrightarrow{\varphi_N(\mathbb{W}_M(A))} & \mathbb{W}_M(A)^N \\ {\scriptstyle \mathbb{W}_N(\varphi_M(A))}\downarrow & & \downarrow{\scriptstyle \varphi_M(A)^N} \\ \mathbb{W}_N(A^M) & \xrightarrow{\varphi_N(A^M)} & (A^M)^N. \end{array}$$

The resulting ring morphism $\varphi_{M,N}(A) : \mathbb{W}_N(\mathbb{W}_M(A)) \to (A^M)^N$ takes $x = (x_{m,n})_{\substack{m\in M \\ n \in N}}$ to $(x^{(m,n)})_{\substack{m\in M \\ n \in N}}$ where

$$x^{(m,n)} := \left(x^{(n)}\right)^{(m)} = \sum_{d|n} d\Big(\sum_{c|m} c x_{c,d}^{m/c}\Big)^{n/d}. \tag{3}$$

Note that $M \times N \simeq MN$ in case $M \cap N = \{1\}$, so that we can identify $(A^M)^N = A^{M\times N} = A^{MN}$. Our main theorem now reads as follows.

THEOREM 2.1. *Let M, N be two truncation sets with $M \cap N = \{1\}$. Then there is a unique functorial isomorphism (or: natural equivalence of func-*

tors)

$$\omega_{M,N} : \mathbb{W}_N \circ \mathbb{W}_M \to \mathbb{W}_{MN}$$

satisfying $\varphi_{M,N} = \varphi_{MN} \circ \omega_{M,N}$.

We want to give an elementary proof of this theorem by imitating an idea from Witt's original paper [5], where we find a special case of the following

LEMMA 2.1. *Let A be a ring, $q \in \mathbb{Z}$ and $Q \subseteq \mathbb{N}$ the monoid generated by all prime numbers dividing q. Factor each $n \in \mathbb{N}$ as $n = n'n^*$ with $n' \in Q$ and $n^* \in Q^\perp$.*

(a) *If $a, b \in A$ satisfy $q|b-a$, then $n'q|b^n - a^n$ for every $n \in \mathbb{N}$.*

(b) *Let N be a truncation set such that A has no torsion by $N \cap Q$. For $x = (x_n)_{n\in N}, y = (y_n)_{n\in N} \in \mathbb{W}_N(A)$, we then have the equivalence*

$$q|y_n - x_n \ \forall n \in N \iff n'q|y^{(n)} - x^{(n)} \ \forall n \in N.$$

Proof.

(a) Since $rsA = rA \cap sA$ for $\gcd(r,s) = 1$, we can reduce to the case $q = p^l$ with $l \in \mathbb{N}$ and p a prime number. Then $n' = p^\nu$ and, proceeding by induction on ν, it suffices to verify the assertion for $n = p$. But writing $b = a + p^l c$ with $c \in A$ yields $b^p - a^p = \sum_{k=1}^{p} \binom{p}{k} p^{kl} c^k a^{p-k} \in p^{l+1}A$.

(b) We may assume N finite and proceed by induction on $|N|$. Suppose one side of the equivalence is true and let $n \in N$. Then, by the induction hypothesis, for all $d|n$ with $d < n$ we have $q|y_d - x_d$, hence $n'q|d(y_d^{n/d} - x_d^{n/d})$, using (a). Since A is n'-torsion free and $\gcd(q, n^*) = 1$, the identity

$$n'n^*(y_n - x_n) + \sum_{\substack{d|n \\ d<n}} d(y_d^{n/d} - x_d^{n/d}) = y^{(n)} - x^{(n)}$$

proves the equivalence for n.
∎

For a prime number p, we denote by v_p the p-adic discrete valuation (on $\mathbb{Q}^*$ with values in $\mathbb{Z}$). Also, for $x = (x_n)_{n\in N} \in \mathbb{W}_N(A)$, we set $F^p x = (x_n^p)_{n\in N}$. (Note that, in general, F^p is not a ring homomorphism.) Then for any $n \in N$ with $\nu := v_p(n) > 0$ we have

$$x^{(n)} = (F^p x)^{(n/p)} + \sum_{\substack{d|n \\ v_p(d)=\nu}} d x_d^{n/d} \equiv (F^p x)^{(n/p)} \mod p^\nu A. \qquad (4)$$

We are now ready to prove Theorem 2.1.

Proof. All three functors, $\mathbb{W}_N \circ \mathbb{W}_M$, $\mathbb{W}_{MN}$ and Π_{MN} are left represented by the polynomial ring $R := \mathbb{Z}[x_{mn} : m \in M, n \in N]$ with variables x_{mn}. Set $x := (x_{mn})_{\substack{m\in M\\ n\in N}} \in \mathbb{W}_N(\mathbb{W}_M(R))$. By Yoneda's Lemma, a functorial map (of sets) $\omega_{M,N} : \mathbb{W}_N \circ \mathbb{W}_M \to \mathbb{W}_{MN}$ satisfying $\varphi_{M,N} = \varphi_{MN} \circ \omega_{M,N}$ corresponds to an element $z = (z_{mn})_{\substack{m\in M\\ n\in N}} \in \mathbb{W}_{MN}(R)$ satisfying $\varphi_{M,N}(x) = \varphi_{MN}(z)$. Moreover $\omega_{M,N}$ will be bijective iff $R = \mathbb{Z}[z_{mn} : m \in M, n \in N]$. Because $\varphi_{M,N}(R \otimes \mathbb{Q})$ and $\varphi_{MN}(R \otimes \mathbb{Q})$ are isomorphisms by Lemma 1.1(b), we clearly must have

$$z = (z_{mn})_{\substack{m\in M\\ n\in N}} := \varphi_{MN}^{-1}(\varphi_{M,N}(x)) \in \mathbb{W}_{MN}(R \otimes \mathbb{Q}),$$

so $\omega_{M,N}$ will be a ring morphism and unique (if it exists). Also, comparing (2) with (3), we find that $z_{mn} - x_{mn} \in \mathbb{Q}[x_{cd} : c|m, d|n, cd < mn]$. Therefore, we are done if we can prove that $z \in \mathbb{W}_{MN}(R)$.
Let p be a prime number, set $\tilde{x} := (x_{mn}^p)_{\substack{m\in M\\ n\in N}} \in \mathbb{W}_N(\mathbb{W}_M(R))$ and $\tilde{z} = (\tilde{z}_{mn})_{\substack{m\in M\\ n\in N}} := \varphi_{MN}^{-1}(\varphi_{M,N}(\tilde{x})) \in \mathbb{W}_{MN}(R \otimes \mathbb{Q})$, and define

$$\begin{gathered} x_n := (x_{mn})_{m\in M}, \tilde{x}_n := (x_{mn}^p)_{m\in M} = F^p x_n \in \mathbb{W}_M(R), \\ y_{mn} := x_n^{(m)}, \tilde{y}_{mn} := \tilde{x}_n^{(m)} \in R, \\ y_m := (y_{mn})_{n\in N}, \tilde{y}_m := (\tilde{y}_{mn})_{n\in N} \in \mathbb{W}_N(R), \end{gathered}$$

then $x^{(m,n)} = y_m^{(n)} = z^{(mn)}$ and $\tilde{x}^{(m,n)} = \tilde{y}_m^{(n)} = \tilde{z}^{(mn)}$.
Now we let $m \in M$, $n \in N$ and show $z_{mn} \in R$ by induction on mn. Suppose $\nu := v_p(mn) > 0$. By the induction hypothesis, we have $z_{cd}, \tilde{z}_{cd} \in R$ and therefore $z_{cd}^p \equiv \tilde{z}_{cd} \mod p$ for all $c|m$ and $d|n$ with $cd < mn$, which implies

$$(F^p z)^{(mn/p)} \equiv \tilde{z}^{(mn/p)} \mod p^\nu \tag{5}$$

according to Lemma 2.1(b). Also, from (2) we conclude that $mnz_{mn} \in R$. Hence, since p was an arbitrary prime number dividing mn, we are done if we can show that $p^\nu | mnz_{mn}$. Now, (4) yields

$$mnz_{mn} \equiv \sum_{\substack{c|m,\ d|n\\ v_p(cd)=\nu}} cdz_{cd}^{\frac{mn}{cd}} = z^{(mn)} - (F^p z)^{(mn/p)} \mod p^\nu.$$

Thus, in view of (5), it remains to verify that $z^{(mn)} \equiv \tilde{z}^{(mn/p)} \mod p^\nu$.
If $p|m$, i.e. $\nu = v_p(m)$, we have $y_{md} = x_d^{(m)} \equiv (F^p x_d)^{(m/p)} = \tilde{y}_{md/p} \mod p^\nu$ for any $d \in N$ by (4). Hence $z^{(mn)} = y_m^{(n)} \equiv \tilde{y}_{m/p}^{(n)} = \tilde{z}^{(mn/p)} \mod p^\nu$ by Lemma 2.1(b).

Now let $p|n$, i.e. $\nu = v_p(n)$. Since $y_{md}^p \equiv \tilde{y}_{md} \mod p$ for any $d \in N$, we conclude $z^{(mn)} = y_m^{(n)} \equiv (F^p y_m)^{(n/p)} \equiv \tilde{y}_m^{(n/p)} = \tilde{z}^{(mn/p)} \mod p^\nu$ by (4) and Lemma 2.1(b). ∎

The isomorphism $\omega_{M,N}$ has many natural properties, e.g. it respects Teichmüller elements and commutes with the Verschiebung V^r for $r \in N$ (but not, in general, for $r \in M$; see [3] for definitions). The interested reader can easily verify this.

3. THE CONNECTION WITH ARTIN-HASSE EXPONENTIALS

In the following, we want to write out the isomorphism in Theorem 2.1 using Artin-Hasse exponentials. Let μ be the Möbius function, M a monoidal truncation set and A an algebra over $\mathbb{Z}_{M^\perp}$. Then, by Lemma 1.1, we can define the **Artin-Hasse exponential** at M over A (cf. [1] or [6]),

$$E_M(t) := \prod_{d \in M^\perp} (1 - t^d)^{-\mu(d)/d} \in \Lambda(A), \text{ satisfying}$$
$$\partial E_M = \sum_{d \in M^\perp} \mu(d) \sum_{k \in \mathbb{N}} t^{kd} = \sum_{\substack{m \in M \\ n \in M^\perp}} \sum_{d|n} \mu(d) t^{mn} = \sum_{m \in M} t^m.$$

We can thereby generalize the original definition of f_x given in Section 1 to an element $x = (x_m)_{m \in M} \in \mathbb{W}_M(A)$ by setting

$$f_x(t) := \prod_{c \in M} E_M(x_c t^c) \in \Lambda(A), \text{ and then}$$
$$\partial f_x = \sum_{c \in M} c \sum_{n \in M} x_c^n t^{cn} = \sum_{m \in M} x^{(m)} t^m. \tag{6}$$

Proposition 3.1. *Let M, N be truncation sets with $M \cap N = \{1\}$ and $MN = \mathbb{N}$, and let A be a $\mathbb{Z}_N$-algebra. Then the isomorphism $\omega_{M,N}(A)$ in Theorem 2.1 sends $x \in \mathbb{W}_N(\mathbb{W}_M(A))$ to $z \in \mathbb{W}(A)$ with*

$$f_z = \prod_{n \in N} f_{x^{(n)}}(t^n)^{1/n} \in \Lambda(A). \tag{7}$$

Proof. On $\mathbb{Z}_N$-algebras, $\mathbb{W}_N \circ \mathbb{W}_M$, $\mathbb{W} = \mathbb{W}_\mathbb{N}$ and $\Pi_\mathbb{N}$ are represented by the polynomial ring $R := \mathbb{Z}_N[x_{mn} : m \in M, n \in N]$ with variables x_{mn}. Therefore, by Yoneda's Lemma, it suffices to consider $x := (x_{mn})_{\substack{m \in M \\ n \in N}} \in \mathbb{W}_N(\mathbb{W}_M(R))$. Let $f \in \Lambda(R)$ equal the right hand side of (7). Then, by (6), the chain rule and (3), we obtain

$$\partial f = \sum_{n \in N} \sum_{m \in M} x^{(m,n)} t^{mn},$$

and the proposition follows using Theorem 2.1 and the connection between ∂ and $\varphi_{\mathbb{N}}$ mentioned in Section 1. ∎

Remark.

(a) In fact, we have $f \in \Lambda(\mathbb{Z}[x_{mn} : m \in M, n \in N])$, in the above proof, due to Theorem 2.1.

(b) We can use Proposition 3.1 even when $MN \neq \mathbb{N}$, if we keep assuming that A is a $\mathbb{Z}_{M^\perp}$-algebra. In this case, set $\tilde{N} := M^\perp$, $\tilde{M} := \tilde{N}^\perp$ and choose $\tilde{x} \in \mathbb{W}_{\tilde{M}}(\mathbb{W}_{\tilde{N}}(A))$ projecting to $x \in \mathbb{W}_M(\mathbb{W}_N(A))$ (e.g. by filling up with zeros). Then apply the proposition to $\tilde{x}$ and project down to $\mathbb{W}_{MN}(A)$ again.

(c) Under the assumptions of the proposition, $\omega_{M,N}(A)$ factors into two isomorphisms as

$$\mathbb{W}_N(\mathbb{W}_M((A)) \xrightarrow[\varphi_N(\mathbb{W}_M(A))]{\sim} \mathbb{W}_M(A)^N \xrightarrow{\sim} \mathbb{W}(A),$$

the second of which has been used by Lauter [2, p. 60] in the case $A = \mathbb{F}_q$ and $M = \{1, p, p^2, \dots\}$ with $p = \mathrm{char}(A)$, in order to determine the index of certain ray class groups in charecteristic p.

REFERENCES

1. E. Artin and H. Hasse, Die beiden Ergänzungssätze zum Reziprozitätsgesetz der l^n-ten Potenzreste im Körper der l^n-ten Einheitswurzeln, *Hamburger Abh.* **6** (1928), p. 152.
2. K. Lauter, A formula for constructing curves over finite fields with many rational points, *J. Number Theory* **74** (1999), 56–72.
3. D. Mumford, Lectures on curves on an algebraic surface, *Ann. Math. Stud.* **59** (1966), 171–191.
4. L. G. Roberts, The ring of Witt vectors, *Queen's Papers in Pure and Appl. Math.* **105** (1997), 2–36.
5. E. Witt, Zyklische Körper und Algebren der Charakteristik p vom Grad p^n, *J. reine angew. Math.* **176** (1937), 126–140.
6. E. Witt, Vektorkalkül und Endomorphismen der Einspotenzreihengruppe, (1969) *in* I. Kersten (ed.), "Ernst Witt, Collected Papers," Springer, Berlin, 1998, p. 157–164.