European Journal of Mathematics (2019) 5:1234–1241
https://doi.org/10.1007/s40879-018-0294-1

RESEARCH ARTICLE

Construction of the ring of Witt vectors

Hendrik W. Lenstra[1]

Received: 18 November 2015 / Accepted: 25 February 2016 / Published online: 15 October 2018

Abstract
The paper contains an intelligible construction of the ring $W(A)$ of Witt vectors over an arbitrary commutative ring A.

Keywords Witt vectors · Rings of power series · Zeta functions of varieties over finite fields

Mathematics Subject Classification 13F35 · 11G25

I will describe a functor $A \mapsto W(A)$ from the category of commutative rings to itself. The ring $W(A)$ of 'Witt vectors' over A has many applications (to algebraic geometry, local rings, etc.), but I won't discuss those. Convention: rings have 1's that are respected by ring homomorphisms. By A I will always denote a commutative ring.

The literature on the functor W is in a somewhat unsatisfactory state: nobody seems to have any interest in Witt vectors beyond applying them for a purpose, and they are often treated in appendices to papers devoted to something else; also, the construction usually depends on a set of implicit or unintelligible formulae. Apparently, anybody who wishes to understand Witt vectors needs to construct them personally. That is what is now happening to myself.

One may compare the construction of $W(A)$ to the construction of the polynomial ring $A[X]$: the ring operations in the latter are also defined by formulae, but those are both explicit and intelligible. In addition, $A[X]$ can be thought of in a conceptual way: it is an A-algebra that represents the forgetful functor from the category of A-algebras to the category of sets. It is quite possible that $W(A)$ also represents some functor,

Editor's note. This paper is published here exactly as it had appeared (as a preprint) in 2002 and therefore may be viewed also as a historical document. The abstract, MSC codes and keywords were provided by the editor.

Based on notes made by John Voight (jvoight@math.berkeley.edu) from two lectures on February 27 and March 1, 2002, in the Number Theory Seminar, University of California, Berkeley.

✉ Hendrik W. Lenstra
hwl@math.leidenuniv.nl

[1] Mathematisch Instituut, Universiteit Leiden, Niels Bohrweg 1, 2333 CA Leiden, The Netherlands

and that this helps in constructing W; but I never saw a satisfactory treatment along these lines. For $W(A)$, the arrows run in the opposite direction: A is a $W(A)$-algebra rather than the other way around, and if $W(A)$ represents a functor then most likely it is a contravariant one.

If the only available way to construct W is by implicit formulae, then one is doomed to using those formulae whenever one wishes to prove any result about Witt vectors. The theory as found in the literature is indeed formula-ridden.

My treatment depends also on a formula (see (ii) below), but it is both explicit and intelligible. One may be hopeful that my approach will pass the test of allowing a smooth development of the entire theory of Witt vectors. For example, one can use it to construct an important morphism $W \to W \circ W$ that turns each $W(A)$ into a 'lambda-ring'.

I start by defining a ring $\Lambda(A)$ that is isomorphic to $W(A)$, the only difference being notational. Let $A[[T]]$ be the ring of power series in one indeterminate T over A. Let the A-algebra homomorphism $A[[T]] \to A$ map T to 0, and hence any power series to its constant coefficient. It induces a homomorphism $A[[T]]^* \to A^*$ on the unit groups, and I define

$$\Lambda(A) = \ker(A[[T]]^* \to A^*) = 1 + TA[[T]].$$

This is a multiplicative group, and Λ is a functor from the category of commutative rings to the category of abelian groups. The multiplication on $\Lambda(A)$ will serve as the "addition" in a new ring structure to be defined on $\Lambda(A)$.

Theorem *There is a unique system of maps*

$$* = *_A : \Lambda(A) \times \Lambda(A) \to \Lambda(A),$$

one for each commutative ring A, such that:

(i) $*$ *is left and right distributive with respect to* $\times$*;*

(ii) *for all A and all* $a, b \in A$*, one has*

$$(1 - aT)^{-1} * (1 - bT)^{-1} = (1 - abT)^{-1};$$

and

(iii) $*_A$ *is functorial in A; that is, for each homomorphism* $f : A \to B$ *of commutative rings, the diagram*

$$\begin{array}{ccc} \Lambda(A) \times \Lambda(A) & \xrightarrow{*_A} & \Lambda(A) \\ {\scriptstyle (\Lambda(f), \Lambda(f))}\downarrow & & \downarrow{\scriptstyle \Lambda(f)} \\ \Lambda(B) \times \Lambda(B) & \xrightarrow{*_B} & \Lambda(B) \end{array}$$

commutes.

For each A, the map $*_A$ is T-adically continuous and makes $\Lambda(A)$ into a commutative ring with addition $\times$, multiplication $*$ and unit element $(1-T)^{-1}$.

Finally, Λ is a functor from the category of commutative rings to itself.

The elements occurring in (ii) are sums of geometric progressions:

$$(1-aT)^{-1} = \sum_{i=0}^{\infty} a^i T^i.$$

Thus, on elements of this form, the operation $*$ is given by coefficientwise multiplication, the "Hadamard product".

The unit element $(1-T)^{-1}$ has all coefficients equal to 1. One finds also other normalizations in the literature, leading to unit element $1-T$ (invert all elements of $\Lambda(A)$) or $1+T$ (substitute $-T$ for T). My convention keeps the formulae simple, and leads for zeta functions of varieties X, Y over a finite field k to the pleasing formula $Z(X \times_k Y/k) = Z(X/k) *_{\mathbb{Z}} Z(Y/k)$.

I now first prove existence of the operations $*_A$. For each $n \geqslant 0$, put

$$\Lambda_n(A) = \ker\left((A[T]/(T^{n+1}))^* \to A^*\right)$$

(by the map $T \mapsto 0$), so that one has $\Lambda(A) = \varprojlim_n \Lambda_n(A)$. Define

$$M_n(A) \subset \Lambda_n(A)$$

to be the subgroup of $\Lambda_n(A)$ generated by $\{1-aT : a \in A\}$. The strategy is to first make each $M_n(A)$ into a ring, next extend the ring structure to $\Lambda_n(A)$ (this will require varying A), and finally pass to $\Lambda(A)$ by taking the projective limit.

Lemma 1 *For each commutative ring A and non-negative integer n, the abelian group $M_n(A)$ has a unique composition $*_A$ satisfying property* (ii) *and making $M_n(A)$ into a commutative ring; also, M_n is a functor from the category of commutative rings to itself, and the natural maps $M_{n+1} \to M_n$ are morphisms of functors.*

Example The map $A \to M_1(A)$ sending a to $1 + aT \pmod{T^2}$ is bijective, and the ring structure on $M_1(A)$ makes it into an isomorphism of rings.

Proof For $a \in A$, the A-algebra endomorphism

$$\begin{aligned} A[T]/(T^{n+1}) &\to A[T]/(T^{n+1}) \\ T &\mapsto aT \end{aligned}$$

induces an element φ_a of the endomorphism ring $\mathrm{End}\,\Lambda_n(A)$ of $\Lambda_n(A)$. Clearly one has $\varphi_a \varphi_b = \varphi_{ab}$ for $a, b \in A$. Hence, if $E \subset \mathrm{End}\,\Lambda_n(A)$ denotes the additive subgroup generated by $\{\varphi_a : a \in A\}$, then E is a commutative subring of $\mathrm{End}\,\Lambda_n(A)$. The natural action of E on $\Lambda_n(A)$ makes $\Lambda_n(A)$ into an E-module, and I write the action exponentially.

The map

$$E \to \Lambda_n(A)$$
$$e \mapsto (1-T)^{-e}$$

is an E-module homomorphism that sends φ_a to $(1-aT)^{-1}$. The image of this E-module homomorphism is $M_n(A)$, since it is generated by the images of generators. The kernel is a left ideal I of E, and one obtains a group isomorphism

$$E/I \simeq M_n(A).$$

Since E is commutative, I is a two-sided ideal of E, so E/I has a ring structure. One can now transport the ring structure from E/I to $M_n(A)$. All assertions in the lemma are then straightforward to verify. □

Next I pass from $M_n(A)$ to $\Lambda_n(A)$. It would be convenient if every monic polynomial over A were a product of linear factors, since then one had identities like

$$1 + a_1T + \cdots + a_nT^n = (1-\alpha_1T)(1-\alpha_2T)\cdots(1-\alpha_nT),$$

showing that $\Lambda_n(A) = M_n(A)$. This is true, for example, if A is an algebraically closed field. Also for $A = \mathbb{R}$ one can show that $\Lambda_n(A) = M_n(A)$. In general one must vary the ring.

Lemma 2 *For each A, there is an A-algebra $\overline{A}$ such that*

(i) *for all n, one has $\Lambda_n(\overline{A}) = M_n(\overline{A})$;*
(ii) *as an A-module, $\overline{A}$ has a basis containing the unit element.*

From (ii) one sees that $\overline{A}$ is free as an A-module, and that the map from A to $\overline{A}$ is injective.

The lemma is much stronger than what I need. It would be enough to show that for each n and for each finite subset $F \subset \Lambda_n(A)$ there exists a faithfully flat A-algebra $A_{F,n}$ with $F \subset M_n(A_{F,n})$.

Proof Let

$$\mathcal{M}(A) = \{f \in A[X] : f \text{ monic, } \deg f > 0\}$$

and put

$$A' = \bigotimes_{f\in\mathcal{M}(A)} A[X]/(f) = A[X_f : f \in \mathcal{M}(A)]/\big(f(X_f) : f \in \mathcal{M}(A)\big).$$

Every $f \in \mathcal{M}(A)$ has the linear factor $X - \alpha_f$ in $A'[X]$, where α_f denotes the image of X_f in A'. Also, the collection of elements $\prod_{f\in\mathcal{M}(A)} \alpha_f^{i(f)}$ with $0 \leqslant i(f) < \deg f$ for all f and $i(f) = 0$ for almost all f, is a basis for A' as an A-module, so $A \subset A'$.

Repeating the construction, write $A'' = (A')'$, and inductively $A^{(n)} = (A^{(n-1)})'$ (where $A^{(0)} = A$). It is now routine to verify that the A-algebra

$$\overline{A} = \varinjlim_n A^{(n)}$$

has the properties stated in the lemma. □

There are many ways of making other rings that do the job just as well, but the following lemma shows that there is no reason to care about this at all.

Lemma 3 *Let $A \subset B$ be commutative rings, $n \geqslant 0$, and let $u, v \in \Lambda_n(A)$ be such that $u, v \in M_n(B)$. Then $u *_B v$ and $u *_{\overline{A}} v$ lie in $\Lambda_n(A)$ and are equal.*

Proof If $B \subset C$, then $u *_B v = u *_C v$ since $*$ is functorial. Choose $C = B \otimes_A \overline{A}$. Since one can write $\overline{A} = \bigoplus_{i \in I} Ae_i$ with $e_0 = 1$, one has $C = \bigoplus_{i \in I} Be_i$. From this one sees that there are inclusions $B, \overline{A} \subset C$, and that inside C one has $B \cap \overline{A} = A$ (elements of B can only at e_0 have a non-zero coefficient).

Therefore one has $u *_B v = u *_C v = u *_{\overline{A}} v$, and this element lies in $\Lambda_n(B) \cap \Lambda_n(\overline{A}) = \Lambda_n(A)$. □

Since a ring B as in the lemma exists for every n, u, v (take for example $B = \overline{A}$), one concludes that $\Lambda_n(A)$ is a subring of $\Lambda_n(\overline{A})$ for every n. This gives a ring structure on $\Lambda_n(A)$. It is functorial in A; that is, if $f\colon A \to B$ is a homomorphism of commutative rings, then the map $\Lambda_n(A) \to \Lambda_n(B)$ induced by f is a ring homomorphism. To prove this, let $u, v \in \Lambda_n(A)$. Then u, v are in $M_n(\overline{A})$, so the images $\tilde{u}$ and $\tilde{v}$ of u and v in $\Lambda_n(B)$ are in $M_n(B \otimes_A \overline{A})$. Applying Lemma 3 to the inclusion $B \subset B \otimes_A \overline{A}$ in the role of $A \subset B$, one sees that the product $\tilde{u} *_B \tilde{v}$ can be computed in $M_n(B \otimes_A \overline{A})$; since M_n is a functor one concludes that this product equals the image of $u *_{\overline{A}} v = u *_A v$ in $\Lambda_n(B)$, as required.

Each Λ_n is a functor from the category of commutative rings to itself, and the natural maps $\Lambda_{n+1} \to \Lambda_n$ are morphisms of functors. Thus $\Lambda(A) = \varprojlim_n \Lambda_n(A)$ now gets a ring structure. This proves the existence part of the theorem, and also shows the additional properties of $*_A$. The only thing left to prove is uniqueness.

Lemma 4 *Let I and J be sets, and let*

$$\vartheta_A\colon A^I \to A^J$$

be a map, one for each commutative ring A, functorial in A. Then each ϑ_A is continuous (where A has the discrete topology and A^I and A^J the product topologies); more precisely, for each $j \in J$ there is a finite subset $I_j \subset I$ such that for all A there exists a commutative diagram

$$\begin{array}{ccc} A^I & \xrightarrow{\vartheta_A} & A^J \\ {\scriptstyle \pi_{I_j}}\downarrow & & \downarrow{\scriptstyle \pi_j} \\ A^{I_j} & \dashrightarrow & A, \end{array}$$

the vertical maps being the obvious projections.

Proof The functor $-^I$ (taking $A \mapsto A^I$) from the category of commutative rings to the category of sets is isomorphic to the functor $\mathrm{Rhom}(\mathbb{Z}[X_i : i \in I], -)$ (taking A to the set of ring homomorphisms $\mathbb{Z}[X_i : i \in I] \to A$). By Yoneda's lemma, the system of maps ϑ_A corresponds to a ring homomorphism $\mathbb{Z}[X_i : i \in I] \leftarrow \mathbb{Z}[X_j : j \in J]$. Lemma 4 now comes down to the statement that for every $j \in J$ there is a finite subset $I_j \subset I$ such that the image of X_j is in the subring $\mathbb{Z}[X_i : i \in I_j]$ of $\mathbb{Z}[X_i : i \in I]$, and this is clear. □

To prove the uniqueness statement in the theorem, suppose that $\# = \#_A : \Lambda(A) \times \Lambda(A) \to \Lambda(A)$ satisfies conditions (i), (ii), and (iii). Applying the lemma to $\vartheta_A = \#_A$, with $J = \mathbb{Z}_{>0}$ and I equal to the disjoint union of two copies of $\mathbb{Z}_{>0}$, one sees that $\#_A$ is T-adically continuous. Let $M(A) \subset \Lambda(A)$ be the subgroup generated by $\{1 - aT : a \in A\}$. Then $\#$ and $*$ agree on $M(A) \times M(A)$ by (ii) and (i), and since $\Lambda(A)$ is Hausdorff, they also agree on $\overline{M(A)} \times \overline{M(A)}$; here $\overline{M(A)}$ denotes the closure of $M(A)$ in $\Lambda(A)$, which equals $\varprojlim_n M_n(A)$. Applying this result to $\overline{A}$ one sees that $\# = *$ on $\Lambda(\overline{A})$ and hence on the subring $\Lambda(A)$. This completes the proof of the theorem.

By way of exercises I list some identities in $\Lambda(A)$.

(1) For all $a \in A$ and $u \in \Lambda(A)$ one has $(1 - aT)^{-1} * u = u(aT)$; i.e.

$$\left(\sum_{i=0}^{\infty} a^i T^i\right) * \left(\sum_{i=0}^{\infty} b_i T^i\right) = \sum_{i=0}^{\infty} a^i b_i T^i$$

(the Hadamard product!). From this one can deduce that the ideal I occurring in the proof of Lemma 1 is 0.

(2) For $a_1, a_2, b_1, b_2 \in A$ one has

$$\begin{aligned}(1 + a_1 T + a_2 T^2) * (1 + b_1 T + b_2 T^2) \\ = 1 + a_1 b_1 T + \big(a_2 b_2 + (a_2 - a_1^2)(b_2 - b_1^2)\big) T^2\end{aligned}$$

in $\Lambda_2(A)$. Also, one has $\Lambda_2(A) = M_2(A)$.

(3) Let m, n be positive integers, and put $l = \mathrm{lcm}(m, n)$, $g = \gcd(m, n)$. Then for $a, b \in A$, one has

$$(1 - aT^m)^{-1} * (1 - bT^n)^{-1} = \big(1 - a^{l/m} b^{l/n} T^l\big)^{-g}.$$

Equivalently: if two collections of α's and β's satisfy

$$X^m - a = \prod\nolimits_{\alpha} (X - \alpha), \qquad X^n - b = \prod\nolimits_{\beta} (X - \beta),$$

then one has

$$\prod\nolimits_{\alpha,\beta} (X - \alpha\beta) = \big(X^l - a^{l/m} b^{l/n}\big)^g.$$

This is particularly easy to see if A is a field of characteristic 0.

(4) For relatively prime positive integers m, n one has

$$\frac{(1-T^m)^n}{1-T^{mn}} * \frac{(1-T^n)^m}{1-T^{mn}} = 1.$$

This is best understood through an interpretation of $\Lambda(\mathbb{Z})$ as a Burnside ring. Taking $m = 14, n = 15$ one concludes that $\Lambda(A)$ is not a domain for any A.

To conclude, I exhibit the relationship between the given construction of Witt vectors and the standard one.

Define the maps $\gamma_n : \Lambda(A) \to A$ by

$$\frac{Tu'}{u} = \sum_{n=1}^{\infty} \gamma_n(u) T^n$$

where u' is the formal derivative of u with respect to T.

Proposition *Each γ_n is a ring homomorphism, functorial in A. The ring structure on the set $\Lambda(A)$ is characterized by being functorial in A and all γ_n being ring homomorphisms.*

Proof It is well-known that the logarithmic derivative $u \mapsto u'/u$ transforms multiplication into addition. For $u = (1-aT)^{-1}$ one has

$$\frac{Tu'}{u} = \frac{aT}{1-aT}$$

so

$$\gamma_n((1-aT)^{-1}) = a^n.$$

This is multiplicative in a, so on elements of the form $(1-aT)^{-1}$ each γ_n transforms $*$ into multiplication. Using functoriality and continuity one concludes that it gives a ring homomorphism. As for the last statement, with Yoneda's lemma one reduces the proof to the case of polynomial rings over $\mathbb{Z}$, and one uses that for those rings the map $u \mapsto Tu'/u$ is injective; the details are left to the reader. □

Lemma 5 *For each commutative ring A, the maps*

$$\prod_{m=1}^{n} A \to \Lambda_n(A)$$

$$(a_m)_{m=1}^n \mapsto \prod_{m=1}^{n} (1-a_m T^m)^{-1}$$

for $n = 0, 1, 2, \ldots$ as well as the map

$$\varphi\colon \prod_{m=1}^{\infty} A \to \Lambda(A)$$
$$(a_m)_{m\geqslant 1} \mapsto \prod_{m\geqslant 1} (1 - a_m T^m)^{-1}$$

are bijective.

The proof is routine.

I can now relate the standard definition of $W(A)$ to the construction given.

Definition The Witt ring $W(A)$ is the set $\prod_{m\geqslant 1} A$ with ring structure $v + w = \varphi^{-1}(\varphi(v)\varphi(w))$, $vw = \varphi^{-1}(\varphi(v) * \varphi(w))$, where φ is as in Lemma 5.

Here is a diagram in the category of commutative rings that is important in the theory of Witt vectors:

$$\begin{array}{ccc} W(A) & \xrightarrow{\sim} & \Lambda(A) \\ \downarrow & & \downarrow \\ \prod_{n=1}^{\infty} A & \xrightarrow{\sim} & TA[[T]]. \end{array}$$

The top horizontal map is φ. The right vertical map sends u to Tu'/u; by the proposition, it is a ring homomorphism if $TA[[T]]$ has the usual addition and Hadamard multiplication. The bottom horizontal map sends $(a_n)_{n\geqslant 1}$ to $\sum_{n=1}^{\infty} a_n T^n$; it is a ring isomorphism if $\prod_{n=1}^{\infty} A$ has componentwise ring operations. The left vertical map is defined by the commutativity of the diagram. By a straightforward computation, it sends $(a_n)_{n=1}^{\infty}$ to $(a^{(n)})_{n=1}^{\infty}$, where the "ghost components" $a^{(n)}$ are given by

$$a^{(n)} = \sum_{d|n} d a_d^{n/d}.$$

By the proposition, the ring structure on $W(A)$ is characterized by functoriality and by the ghost components being ring homomorphisms $W(A) \to A$. This is often taken as the definition of $W(A)$.

March 4, 2002