No.08: ring of Witt vectors (2) The ring of universal Witt vectors

In the following, we use infinite sums and infinite products of elements of $\mathcal{W}_1(A) = 1+TA[[T]]$. They are defined as limits of sums and products with respect to the filtration topology defined in the usual way.

LEMMA 8.1. *Let A be any commutative ring. Then every element of $1+TA[[T]]$ is written uniquely as*

$$\prod_{j=1}^{\infty}(1-x_jT^j) \qquad (x_j \in A).$$

PROOF. We may use an expansion

$$\prod_{j=1}^{\infty}(1-x_jT^j) \equiv -x_nT^n + poly(x_1,\dots,x_{n-1},T) \pmod{T^{n+1}}$$

to inductively determine x_j. More precisely, for each $n \in \mathbb{Z}_{>0}$, let us define a polynomial $f_n(X_1,X_2,\dots,X_{n-1})$ in the following way:

$$f_n(X_1,\dots,X_{n-1}) = \mathrm{coeff}(\prod_{j=1}^{n-1}(1-X_jT^j), T^n)$$

Then for any element $1+\sum_{j=1}^{\infty}y_jT^j \in 1+TA[[T]]$, we define

$$x_1 = -y_1, \quad x_n = -y_n + f_n(x_1,\dots,x_{n-1}) \quad (\forall n > 1).$$

Then it is easy to verify that an equation

$$1+\sum_{j=1}^{\infty}y_jT^j = \prod_{j=1}^{\infty}(1-x_jT^j)$$

holds. □

COROLLARY 8.2. *$\mathcal{W}_1(A) = 1+TA[[T]]$ is topologically generated by*

$$\{(1-x_jT^j); \quad x_j \in A, \quad j = 1,2,3,\dots\}.$$

LEMMA 8.3. *Let d,e be positive integers. Let m be the least common multiple of d,e. Then we have*

$$(1-x_dT^d)*_{\mathcal{L}}(1-x_eT^e) = (1-x_d^{m/d}x_e^{m/e}T^m)^{de/m}(= (\frac{de}{m})\cdot_{\mathcal{L}}\Big(1-x_d^{m/d}x_e^{m/e}T^m\Big)).$$

(Note that $m \geq d,e$.)

PROOF. let d,e be positive integers. Let m be the least common multiple of d,e. We have,

$$\mathcal{L}(1-x_dT^d)*\mathcal{L}(1-x_eT^e) = \frac{dx_dT^d}{1-x_dT^d} * \frac{ex_eT^e}{1-x_eT^e} = de(\sum_{i=1}^{\infty}(x_dT^d)^i * \sum_{j=1}^{\infty}(x_eT^e)^j)$$

$$=de\sum_{u=1}^{\infty}x_d^{mu/d}x_e^{mu/e}T^{mu} = \frac{dex_d^{m/d}x_e^{m/e}T^m}{1-x_d^{m/d}x_e^{m/e}T^m} = -\frac{de}{m}\frac{d}{dT}\log(1-x_d^{m/d}x_e^{m/e}T^m)$$

$$=\mathcal{L}((1-x_d^{m/d}x_e^{m/e}T^m)^{de/m}).$$

□

DEFINITION 8.4. Let A be any commutative ring. Then we define an addition $\boxplus$ and a multiplication $\boxtimes$ on $\mathcal{W}_1(A)$ who satisfy the following requirements:

(1) $f \boxplus g = fg$.
(2) For any positive integer d, e, Let m be the least common multiple of d, e. Then we have
$$(1 - x_d T^d) \boxtimes (1 - x_e T^e) = \left(1 - x_d^{m/d} x_e^{m/e} T^m\right)^{\frac{de}{m}}.$$
(3) for general f, g , the multiplication $f \boxtimes g$ is defined by first expressing f, g as a formal $\boxplus$-sum as in Lemma 8.3 and then applying the rule 2 formally to each "$\boxplus$-summand".

(Note that Lemma 8.1 guarantees the existence and the uniqueness of such multiplication $\boxtimes$.)

THEOREM 8.5. *Let A be any commutative ring. Then:*

(1) *Any element of $\mathcal{W}_1(A)$ is written uniquely as*
$$\sum_{j=1}^{\infty}{}^{\boxplus}(1 - x_j T^j).$$
(2) *$\mathcal{W}_1(A)$ forms a commutative ring under the binary operations $\boxplus$ and $\boxtimes$. More precisely,*
   (a) *$(\mathcal{W}_1(A), \boxplus)$ is an additive group with the zero element 1.*
   (b) *The multiplication $\boxtimes$ is an associative commutative product on $\mathcal{W}_1(A)$ with the unit element $1 - T$.*
   (c) *The distributive law holds.*
(3) *When $A \supset \mathbb{Q}$, the ring $(\mathcal{W}_1(A), \boxplus, \boxtimes)$ is isomorphic to $(\mathcal{W}_0(A), +, *)$ via the map $\mathcal{L}_A = -T\frac{d}{dT}\log(\bullet)$.*

PROOF. When $A \supset \mathbb{Q}$, the statements trivially hold. This implies in particular that rules such as distributivity and associativity hold for universal cases (that means, for formal power series with indeterminate coefficients). Thus we conclude by specialzation arguments that the rule also hold for any ring A.

□

DEFINITION 8.6. For any commutative ring A, elements of $\mathcal{W}_1(A)$ are called **universal Witt vectors** over A. The ring $(\mathcal{W}_1(A), \boxplus, \boxtimes)$ is called **the ring of universal Witt vectors** over A.

PROPOSITION 8.7. *$(\mathcal{W}_1(\bullet), \boxplus, \boxtimes)$ is uniquely determined by the following properties.*

(1) $f \boxplus g = fg \qquad (\forall f, g \in \mathcal{W}_1(A)$.
(2) *The multiplication $\boxtimes$ is $\boxplus$-biadditive. (That means, $\mathcal{W}_1(A), \boxplus, \boxtimes)$ obeys the distributive law.)*
(3) $(1 - xT) \boxtimes (1 - yT) = (1 - (xy)T) \qquad (\forall x, y \in A)$.
(4) *$\boxtimes$ is continuous.*
(5) *$\boxtimes$ is functorial.*

PROOF. We only need to prove the requirement (2) of Definition 8.4. With the help of distributive law, the requirement is satisfied if an equation

$$(\#)\ (1 - xT^a) \boxtimes (1 - yT^b) = (1 - x^{m/a} y^{m/b} T^m)^{ab/m} \quad (m = l.c.m(a, b))$$

holds for each $(a, b) \in (\mathbb{Z}_{>0})^2$.

To that aim, we first deal with a special case where $x = \alpha^a, y = \beta^b$, $A = \mathbb{C}[\alpha, \beta]$, α, β algebraically independent over $\mathbb{C}$. In that case we may easily decompose the polynomials $(1 - xT^a)$ and $(1 - yT^b)$ and then we use the distributive law to see that the requirement actually holds. Indeed, let us put

$$\zeta_k = \exp(2\pi\sqrt{-1}/k)$$

and compute as follows.

$$\begin{aligned}
&(1 - xT^a) \boxtimes (1 - yT^b) \\
=&\sum_{j,l}^{\boxplus} (1 - \zeta_a^j(\alpha)T) \boxtimes (1 - \zeta_b^l(\beta)T) \\
=&\sum_{j,l}^{\boxplus} (1 - \zeta_a^j \zeta_b^l \alpha\beta T) \\
=&\prod_{l} (1 - \zeta_b^{al} \alpha^a \beta^a T^a) \\
=&\prod_{l'} (1 - x\beta^a T^a \zeta_{b/d}^{l'})^d \qquad (d = g.c.d(a, b)) \\
=&(1 - x^{a/d} y^{b/d} T^{ab/d})^d.
\end{aligned}$$

We second deal with a case where $A = \mathbb{Z}[x, y]$, x, y algebraically independent over $\mathbb{C}$. In that case we take a look at an inclusion

$$\iota : \mathbb{Z}[x, y] \hookrightarrow \mathbb{C}[a, b].$$

and consider $\mathcal{W}_1(\iota)$. It is easy to see that $\mathcal{W}_1(\iota)$ is injection so that the equation (#) is also true in this case. The general case now follows from specialization argument. $\square$