No.08: ring of Witt vectors (1) Preparations

From here on, we make use of several notions of category theory. Readers who are unfamiliar with the subject is advised to see a book such as [**?**] for basic definitions and first properties.

Let p be a prime number. For any commutative ring k of characteristic $p \neq 0$, we want to construct a ring $W(k)$ of characteristic 0 in such a way that:

(1) $W(\mathbb{F}_p) = \mathbb{Z}_p$.
(2) $W(\bullet)$ is a functor. That means,
   (a) For any ring homomorphism $\varphi : k_1 \to k_2$ between rings of characterisic p, there is given a unique ring homomorphism $W(\varphi) : W(k_1) \to W(k_2)$.
   (b) $W(\bullet)$ should furthermore commutes with compositions of homomorphisms.

To construct $W(k)$, we construct a new addition and multiplication on a k-module $\prod_{j=1}^{\infty} k$. The ring $W(k)$ will then be called the ring of Witt vectors. The treatment here essentially follows the treatment which appears in [**?**, VI,Ex.46-49], with a slight modification (which may or may not be good–it may even be wrong) by the author.

We first introduce a nice idea of Witt.

DEFINITION 8.1. Let A be a ring (of any characteristic). Let T be an indeterminate. We define the following copy of $A^{\mathbb{Z}_{>0}}$.

$$\mathcal{W}_1(A) = 1 + TA[[T]] = \left\{ 1 + \sum_{j=1}^{\infty} y_j T^j \ ; \ x_n \in A(\forall n) \right\}$$

(as a set.)

For each element $a(T) \in 1 + TA[[T]]$, we will denote by $(a(T))_W$ the corresponding element in $W_1(A)$.

We will equip $\mathcal{W}_1(A)$ with a ring structure. To do so we first make use of "log". 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 8.2. *There is an well-defined map*

$$\mathcal{L}_A = -T\frac{d}{dT}\log(\bullet) : 1 + TA[[T]] \to TA[[T]].$$

If A contains an copy of $\mathbb{Q}$, then the map is a bijection. The inverse is given by

$$Tg(T) \mapsto \exp\left(-\int_0^T g(s)ds \right).$$

PROOF. To see that $\mathcal{L}$ is well defined (that is, "defined over $\mathbb{Z}$"), we compute as follows.

$$-T\frac{d}{dT}\log(1+Tf_1) = -T(f_1'+f_1)(1+Tf_1)^{-1} = -T(f_1'+f_1)\sum_{j=1}^{\infty}(-Tf_1)^j$$

The rest should be obvious.

Note: the condition $A \supset \mathbb{Q}$ is required to guarantee exictence of exponential

$$\exp(\bullet) = \sum_{j=0}^{\infty} \frac{1}{j!} \bullet^j$$

and existence of the integration $\int_0^T g(s)ds$. □

DEFINITION 8.3. We equip $TA[[T]]$ with the usual addition and the following (unusual) "coefficient-wise" multiplication:

$$\left(\sum_{j=1}^{\infty} a^{(j)} T^j\right) * \left(\sum_{j=1}^{\infty} b^{(j)} T^j\right) = \sum_{j=1}^{\infty} (a^{(j)} b^{(j)}) T^j$$

It is easy to see that $\mathfrak{T}A[[T]]$ forms a (unital associative) commutative ring with these binary operations.

DEFINITION 8.4. Let A be a ring which contains a copy of $\mathbb{Q}$. Then we define ring structure on $\mathcal{W}_1(A)$ by putting

$$(f)_W + (g)_W = \mathcal{L}_A^{-1}(\mathcal{L}_A(f) + \mathcal{L}_A(g)), \quad (f)_W \cdot (g)_W = \mathcal{L}_A^{-1}(\mathcal{L}_A(f) * \mathcal{L}_A(g)).$$

LEMMA 8.5. *Let A be a ring which contains a copy of $\mathbb{Q}$. For any $f, g \in \mathcal{W}_1(A)$, we have*

$$(f)_W + (g)_W = (fg)_W.$$

In particular, addition in $\mathcal{W}_1(A)$ is defined over $\mathbb{Z}$.

PROOF. easy □

We may thus extend the definition $+_{\mathcal{L}}$ on $\mathcal{W}_1(A)$ to cases where the condition $A \supset \mathbb{Q}$ is no longer satisfied.

We next see that the multiplication of $\mathcal{W}_1(A)$ is also defined over $\mathbb{Z}$. To do so, we need the following lemma.

LEMMA 8.6. *Let A be any commutative ring. Then every element of $1 + TA[[T]]$ is written uniquely as*

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

PROOF. We may use an expansion

$$\prod_{j=1}^{\infty} (1 - x_j T^j) \equiv -x_n T^n + poly(x_1, \ldots, x_{n-1}, T) \pmod{T^{n+1}}$$

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

$$f_n(X_1, \ldots, X_{n-1}) = \mathrm{coeff}\left(\prod_{j=1}^{n-1} (1 - X_j T^j), T^n\right)$$

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

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

Then it is easy to verify that an equation

$$1 + \sum_{j=1}^{\infty} y_j T^j = \prod_{j=1}^{\infty} (1 - x_j T^j)$$

holds. □

COROLLARY 8.7. *$\mathcal{W}_1(A) = 1 + TA[[T]]$ is topologically generated by*

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

LEMMA 8.8. *Let d, e be positive integers. Let m be the least common multiple of d, e. Then for any $x, y \in A$, we have*

$$\begin{aligned}(1 - xT^d)_W \cdot (1 - yT^e)_W &= \left((1 - x^{m/d} y^{m/e} T^m)^{de/m}\right)_W \\ &= (\frac{de}{m}) \cdot \left(1 - x^{m/d} y^{m/e} T^m\right)_W .\end{aligned}$$

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

$$\mathcal{L}(1 - xT^d) * \mathcal{L}(1 - yT^e) = \frac{dxT^d}{1 - xT^d} * \frac{eyT^e}{1 - yT^e} = de(\sum_{i=1}^{\infty} (xT^d)^i * \sum_{j=1}^{\infty} (yT^e)^j)$$

$$= de \sum_{u=1}^{\infty} x^{mu/d} y^{mu/e} T^{mu} = \frac{dex^{m/d} y^{m/e} T^m}{1 - x^{m/d} y^{m/e} T^m} = -\frac{de}{m} \frac{d}{dT} \log(1 - x^{m/d} y^{m/e} T^m)$$

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

□

DEFINITION 8.9. Let A be any commutative ring. Then we define an addition $+$ and a multiplication $\cdot$ on $\mathcal{W}_1(A)$ who satisfy the following requirements:

(1) $(f)_W + (g)_W = (fg)_W$.
(2) For any positive integer d, e, Let m be the least common multiple of d, e. Then for any $x, y \in A$, we have
$$(1 - xT^d)_W \cdot (1 - yT^e)_W = \left(\left(1 - x^{m/d} y^{m/e} T^m\right)^{\frac{de}{m}}\right)_W .$$
(3) the summation and the multiplication operations are continuous.

(Note that Lemma 8.6 guarantees the existence and the uniqueness of such multiplication.)

THEOREM 8.10. *Let A be any commutative ring. Then:*

(1) *Any element of $\mathcal{W}_1(A)$ is written uniquely as*
$$\sum_{j=1}^{\infty} (1 - x_j T^j)_W.$$
(2) *$\mathcal{W}_1(A)$ is a commutative ring.*
(3) *When $A \supset \mathbb{Q}$, the ring $\mathcal{W}_1(A)$ is isomorphic to the ring $(TA[[T]], +, *)$ 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 8.11. For any commutative ring A, elements of $\mathcal{W}_1(A)$ are called **universal Witt vectors** over A. The ring $\mathcal{W}_1(A)$ is called **the ring of universal Witt vectors** over A.

PROPOSITION 8.12. *$\mathcal{W}_1(\bullet)$ is uniquely determined by the following properties.*

(1) $(f)_W + (g)_W = (fg)_W \qquad (\forall f, g \in 1 + TA[[T]])$.
(2)
(3) $(1 - xT)_W(1 - yT)_W = (1 - (xy)T)_W \qquad (\forall x, y \in A)$.
(4) *The multiplication map is continuous.*
(5) *The multiplication map is functorial.*

PROOF. We only need to prove the requirement (2) of Definition 8.9. With the help of distributive law, the requirement is satisfied if an equation

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

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.

$$\begin{aligned}
&(1 - xT^a)_W(1 - yT^b)_W \\
=&\sum\nolimits_{j,l}(1 - \zeta_a^j(\alpha)T)_W(1 - \zeta_b^l(\beta)T)_W \\
=&\sum\nolimits_{j,l}(1 - \zeta_a^j\zeta_b^l\alpha\beta T)_W \\
=&\left(\prod_l(1 - \zeta_b^{al}\alpha^a\beta^aT^a)\right)_W \\
=&\left(\prod_{l'}(1 - x\beta^aT^a\zeta_{b/d}^{l'})^d\right)_W \qquad (d = \gcd(a,b)) \\
=&\left((1 - x^{a/d}y^{b/d}T^{ab/d})^d\right)_W.
\end{aligned}$$

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

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

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. □