No.07: $\boxed{\text{ring of Witt vectors (1) Preparations}}$

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 [1] 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 [2, 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 7.1. Let A be a ring (of any characteristic). Let T be an indeterminate. We define the following copies of $A^{\mathbb{Z}_{>0}}$.

$$\mathcal{W}_0(A) = TA[[T]] = \left\{ \sum_{j=1}^{\infty} x^{(j)} T^j \ ; \ x^{(n)} \in A (\forall n) \right\}$$

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

Lemma 7.2. *$\mathcal{W}_0$ and $\mathcal{W}_1$ are functors from the category of rings to the category of sets. They are represented by "polynomial rings in infinite indeterminates"*

$$A_{\mathcal{W}_0} = \mathbb{Z}[X^{(1)}, X^{(2)}, X^{(3)}, \dots]$$

and

$$A_{\mathcal{W}_1} = \mathbb{Z}[Y_1, Y_2, Y_3, \dots].$$

That means, there are functorial bijections

$$\mathrm{Hom}_{\mathrm{ring}}(A_{\mathcal{W}_0}, A) \cong \mathcal{W}_0(A)$$

and

$$\mathrm{Hom}_{\mathrm{ring}}(A_{\mathcal{W}_1}, A) \cong \mathcal{W}_1(A).$$

Definition 7.3. We define the following "universal elements".

$$v_0 = \sum_{j=1}^{\infty} X^{(j)} T^j \in \mathcal{W}_0(A_{\mathcal{W}_0}),$$

$$v_1 = 1 + \sum_{j=1}^{\infty} Y_j T^j \in \mathcal{W}_1(A_{\mathcal{W}_1}).$$

LEMMA 7.4. *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 7.5. We equip $\mathcal{W}_0(A) = TA[[T]]$ with the usual addition and the following (unusual) 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 $\mathcal{W}_0(A)$ forms a (unital associative) commutative ring with these binary operations.

DEFINITION 7.6. Let A be a ring which contains a copy of $\mathbb{Q}$. Then we define ring structure on $\mathcal{W}_1(A)$ by putting

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

LEMMA 7.7. *Let A be a ring which contains a copy of $\mathbb{Q}$. For any $f, g \in \mathcal{W}_1(A)$, we have*

$$f +_{\mathcal{L}} g = fg.$$

In particular, addition $+_{\mathcal{L}}$ 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.

REFERENCES

[1] S. S. Mac Lane, *Categories for the working mathematicians*, Springer Verlag, 1971.

[2] S. Lang, *Algebra (graduate texts in mathematics)*, Springer Verlag, 2002.