No.06: $\boxed{\text{ring of Witt vectors (2)}}$

6.1. $\Lambda(A)$ **for arbitrary commutative ring** A. In the previous lecture we defined the ring structure on $\Lambda(A)$ for $A = \Omega$, a field of characteristic 0. Now we want to define the structure for arbitrary commutative ring A. Note that addition is already known:

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

We would like to know the product $(f)_W(g)_W$. Before doing that, we consider "universal" power serieses:

$$a(T) = 1 + a_1T + a_2T^2 + a_3T^3 + \dots,$$
$$b(T) = 1 + b_1T + b_2T^2 + b_3T^3 + \dots,$$

with $a_1, a_2, \dots, b_1, b_2, b_3, \dots$ be all independent variables. We need a fairly large field Ω, namely,

$$\Omega = \overline{\mathbb{Q}(a_1, a_2, \dots, b_1, b_2, \dots)},$$

the algebraic closure of an infinite trancendent extension of $\mathbb{Q}$. We find:

$$(a(T))_W(b(T))_W = (m_{a,b}(T))_W$$

where

$$m_{a,b}(T) = 1 + m_{a,b;1}T + m_{a,b;2}T^2 + m_{a,b;3}T^3 + \dots$$

with $m_{a,b;k} \in \Omega$.

By using computer algebra system, we obtain:

$$m_{a,b,1} = -a_1 b_1$$
$$m_{a,b,2} = -2\, a_2\, b_2 + a_1^2\, b_2 + a_2\, b_1^2$$
$$m_{a,b,3} = -3\, a_3\, b_3 + 3\, a_1\, a_2\, b_3 - a_1^3\, b_3 + 3\, a_3\, b_1\, b_2 - a_1\, a_2\, b_1\, b_2 - a_3\, b_1^3$$
$$\begin{aligned} m_{a,b,4} = &- 4\, a_4\, b_4 + 4\, a_1\, a_3\, b_4 + 2\, a_2^2\, b_4 - 4\, a_1^2\, a_2\, b_4 + a_1^4\, b_4 \\ &+ 4\, a_4\, b_1\, b_3 - a_1\, a_3\, b_1\, b_3 - 2\, a_2^2\, b_1\, b_3 + a_1^2\, a_2\, b_1\, b_3 + 2\, a_4\, b_2^2 \\ &- 2\, a_1\, a_3\, b_2^2 + a_2^2\, b_2^2 - 4\, a_4\, b_1^2\, b_2 + a_1\, a_3\, b_1^2\, b_2 + a_4\, b_1^4 \end{aligned}$$

We also see:

- For fixed a, $m_{a,b,k}$ only depend on $b_1, b_2, b_3, \dots, b_k$. (In other words, it is an element of $\overline{\mathbb{Q}(a_1, \dots, a_k, b_1, b_2, \dots, b_k)}$.
- By using a Galois-theoretic arguments (or by using arguments on symmetric polynomials,) we see that $m_{a,b,k}$ actually lie in $\mathbb{Q}(a_1, a_2, \dots, a_k, b_1, b_2, \dots, b_k)$.
- $m_{a,b,k}$ is integral over the polynomial ring $\mathbb{Z}[a_1, a_2, \dots, a_k, b_1, b_2, \dots, b_k]$. It is thus itself belongs to the ring $\mathbb{Z}[a_1, a_2, \dots, a_k, b_1, b_2, \dots, b_k]$.
- The fact that $\Lambda(\Omega)$ obeys each of the axioms of ring, such as

  $$((a)_W(b)_W)(c)_W = (a)_W((b)_W(c)_W)$$

  (associativity), gives a set of polynomial identities in $a, b, c, m_{ab;k}, m_{bc,k}$. Such identities in term guarantees that for any ring A, $\Lambda(A)$ satisfy such axiom.

PROPOSITION 6.1. *For any commutative ring A, $\Lambda(A)$ carries the structure of a ring.*

6.2. Yet another way to deal with the multiplication of $\Lambda(A)$.

PROPOSITION 6.2. *$\Lambda(A)$ is generated by $\{(1-cT^n)_W; c \in A, n \in \mathbb{N}\}$ as a topological additve group.*

PROOF. Induction. (We leave it as Exercise 6.1) $\square$

PROPOSITION 6.3. *Let $a, b \in A$. Assume $n, m \in \mathbb{Z}_{>0}$. PUt $d = \gcd(n, m)$. We have $n = n'd, m = m'd \quad (\exists n', \exists m' \in \mathbb{Z}_{>0})$. We furether put $l \stackrel{\text{def}}{=} n'm'(= \operatorname{lcm}(n, m))$. Then:*

$$(1 - aT^n)_W (1 - bT^m)_W = d \cdot (1 - a^{m'} b^{n'} T^l)_W$$

PROOF. (Exercise 6.2) $\square$

COROLLARY 6.4. *The multiplication of $\Lambda(A)$ surely remain in $\Lambda(A)$ as it should be.*