No.12.extra: The ring of Witt vectors and $\mathbb{Z}_p$

PROPOSITION 12.1. *Let $a, b \in A$. Assume $n, m \in \mathbb{Z}_{>0}$ such that $\gcd(n, m) = d$, $\mathrm{lcm}(n, m) = l$. Then:*
(1) $(1 - T^n)_W(1 - T^m)_W = d \cdot (1 - T^l)_W$
(2) $(1 - aT^n)_W(1 - bT^m)_W = (1 - a^{l/n}b^{l/m}T^l)^d$

PROOF. We will firstly prove the proposition when $A = \mathbb{C}$. unity in $\mathbb{C}$. (1) Let ζ_n be a primitive root of unity in $\mathbb{C}$. Then we have:

$$(1 - T^n)_W(1 - T^m)_W = \sum_{k=0}^{n-1}(1 - \zeta_n^k T)_W(1 - T^m)_W = \sum_{k=0}^{n-1}(1 - \zeta_n^{km}T^m)_W.$$

Knowing that ζ_n^m is a primitive n'-th root of unity, we get the desited result.
(2)

$$\begin{aligned}&(1 - aT^n)_W(1 - bT^m)_W\\ =&(1 - a^{1/n}T)_W(1 - T^n)_W \cdot (1 - b^{1/m}T)_W(1 - T^l)_W.\end{aligned}$$

By functoriality, we see that the proposition is also valid over the polynomial ring $\mathbb{Z}[a, b]$. Then by functoriality we see that the result is also true for any ring A.

□

LEMMA 12.2. *(=Proosition 8.9) Let n be a positive integer. If n is invertible in A, then it is also invertible in $\Lambda(A)$.*

PROOF. Let us define $\alpha_1 = (1 - \frac{1}{n}T)$. Then we have

$$\alpha_1^n = (1 - \frac{1}{n}T)^n = (1 - T) \pmod{T^2}.$$

Let us now assume that for a postive integer k, we have an polynomial α_k such that

$$\alpha_k^n = (1 - T) \pmod{T^{k+1}}$$

holds. Then there exists an element $c_k \in A$ such that

$$\alpha_k^n = (1 - T) + c_k T^{k+1} \pmod{T^{k+2}}.$$

Let us put $\alpha_{k+1} = \alpha_k - \frac{1}{n}c_k T^{k+1}$.

$$\alpha_{k+1}^n \equiv \alpha_k^n - c_k T^{k+1} \equiv 1 \pmod{T^{k+2}}.$$

The statement now follows by the induction.

□

PROPOSITION 12.3. *Let n be a positive integer which is invertible in A. The range $e_n\Lambda(R)$ of the idempotent e_n is isomorphic to $(1 + T^n A[[T^n]])$ via V_n*

Ring of Witt vectors

Let A be a ring. Then

$$A^{\mathbb{Z}_{>0}} \ni (a_1, a_2, \dots) \mapsto \sum_{j=1}^{\infty} (1 - a_j T^j)_W \in \Lambda(A)$$

is a bijection. In other words, $\{a_j\}$ plays the role of a coordinate of $\Lambda(A)$. We call the ring $\Lambda(A)$ with the coordinate given this way **the ring of Witt vectors**. In this lecture, we do not distinguish too much between $W(A)$ and $\Lambda(A)$.

Verschiebung and Frobenius map.

DEFINITION 12.4. We define:

(1) Verschiebung. $V_n : \Lambda(A) \ni (f(T))_W \mapsto (f(T^n))_W \in \Lambda(A)$
(2) Frobenius map. $F_n : (1 - aT)_W \mapsto (1 - a^n T)_W$

PROPOSITION 12.5. *Let A be a ring. Let n be a positive integer such that it is invertible in A. Then $e_n = \frac{1}{n}(1 - T^n)_W$ is an idempotent in $\Lambda(A)$. $e_n \Lambda(A)$ is equal to the image* $\mathrm{Image}(V_n)$ *of the Verschiebung map. In other words, it is isomorphic to $\Lambda(A)$ itself via the non-unital isomorphism V_n.*