No.14:

$\boxed{\text{The ring of Witt vectors when } A \text{ is a ring of characteristic } p \neq 0.}$

14.1. **Idempotents.**

We are going to decompose the ring of Witt vectors $\Lambda(A)$. Before doing that, we review facts on idempotents. Recall that an element x of a ring is said to be **idempotent** if $x^2 = x$.

THEOREM 14.1. *Let R be a commutative ring. Let $e \in R$ be an idempotent. Then:*

(1) *$\tilde{e} = 1 - e$ is also an idempotent. (We call it the* **complementary idempotent** *of e.)*
(2) *$e, \tilde{e}$ satisfies the following relations:*

$$e^2 = 1, \quad \tilde{e}^2 = 1, \quad e\tilde{e} = 0.$$

(3) *R admits an direct product decomposition:*

$$R = (Re) \times (R\tilde{e})$$

DEFINITION 14.2. For any ring R, we define a partial order on the idempotents of if as follows:

$$e \succeq f \iff ef = f$$

It is easy to verify that the relation $\succeq$ is indeed a partial order. We note also that, having defined the order on the idempotents, for any given family $\{e_\lambda\}$ of idempotents we may refer to its "supremum" $\vee e_\lambda$ and its"infimum" $\wedge e_\lambda$. (We are not saying that they always exist: they may or may not exist.) When the ring R is topologized, then we may also discuss them by using limits. Note that our $\Lambda(A)$ for any ring A has the "T-adic topology".

14.2. **Playing with idempotents in the ring of Witt vectors.**

DEFINITION 14.3. Let A be a commutative ring. For any $a \in A$, we denote by $[a]$ the element of $\Lambda(A)$ defined as follows:

$$[a] = (1 - aT)_W$$

We call $[a]$ *the "Teichmüller lift" of a.*

LEMMA 14.4. *Let A be a commutative ring. Then:*

(1) *$\Lambda(A)$ is a commutative ring with the zero element $[0]$ and the unity $[1]$.*
(2) *For any $a, b \in A$, we have*

$$[a] \cdot [b] = [ab]$$

□

PROPOSITION 14.5. *Let A be a commutative ring. If n is a positive integer which is invertible in A, then n is invertible in $\Lambda(A)$. To be more precise, we have*

$$\frac{1}{n} \cdot [1] = \left((1-T)^{\frac{1}{n}}\right)_W = \left((1 + \sum_{j=1}^{\infty} \binom{\frac{1}{n}}{j} (-T)^j\right)_W.$$

PROOF. It is easy to find out, by using iterative approximation, an element x of $A[[T]]$ such that

$$(1+x)^n = (1-T).$$

□

DEFINITION 14.6. For any positive integer n which is invertible in a commutative ring A, we define an element e_n as follows:

$$e_n = \frac{1}{n} \cdot (1-T^n)_W.$$

LEMMA 14.7. *Let A be a commutative ring. Then for any positive integer n which is invertible in A, we have:*

(1) *e_n is an idempotent.*
(2)
$$e_n = (1 - \frac{1}{n}T^n + \textit{(higher order terms)})_W$$
(3) *If $n|m$, with m invertible in A, then $e_n \geq e_m$ in the order of idempotents.*

PROOF. if $n|m$, then we have

$$e_n \cdot e_m = e_m.$$

□

It should be important to note that the range of the projection e_n is easy to describe.

PROPOSITION 14.8. *Let n be an integer invertible in A. $e_n \cdot \Lambda(A) = \{(f)_W | f \in 1 + T^n A[[T^n]]\}$*

PROOF. Easy. Compare with Lemma 14.15 below.

□

14.3. **The ring of p-adic Witt vectors (when the characteristic of the base ring A is p).** In this subsection we assume our ring A satisfies $pA = 0$. Note that in that case $\mathbb{F}_p \subset A$ and that every integer m is invertible in A unless $p|m$.

PROPOSITION 14.9. *Let p be a prime. Let A be a ring with $pA = 0$. Let us define an idempotent f of $\Lambda(A)$ as follows.*

$$f = \bigvee_{\substack{n>1 \\ p\nmid n}} e_n (= [1] - \prod_{\substack{p\nmid n \\ n>1}} ([1] - e_n))$$

Then f defines a direct product decomposition

$$\Lambda(A) \cong (f \cdot \Lambda(A)) \times (([1]-f) \cdot \Lambda(A)).$$

We call the factor algebra $([1]-f)\cdot\Lambda(A)$ **the ring $\mathcal{W}^{(p)}(A)$ of p-adic Witt vectors**.

The following proposition tells us the importance of the ring of p-adic Witt vectors.

PROPOSITION 14.10. *Let p be a prime. Let A be a commutative ring with $pA = 0$. For each positive integer k which is not divisible by p, let us define an idempotent f_k of $\Lambda(A)$ as follows.*

$$f_k = \bigvee_{\substack{p\nmid n \\ n>1}} e_{kn} (= e_k - \prod_{\substack{p\nmid n \\ n>1}} (e_k - e_{kn}))$$

Then f_k defines a direct product decomposition

$$e_k\Lambda(A) \cong (f_k \cdot \Lambda(A)) \times ((e_k - f_k) \cdot \Lambda(A)) .$$

Furthermore, the factor algebra $(e_k - f_k) \cdot \Lambda(A)$ is isomorphic to the ring $\mathcal{W}^{(p)}(A)$ of p-adic Witt vectors. Thus we have a direct product decomposition

$$\Lambda(A) \cong \mathcal{W}^{(p)}(A)^{\mathbb{N}}.$$

PROPOSITION 14.11. *There exists a bijection $\varphi : A^{\mathbb{N}} \ni (a_r)_{r\in\mathbb{N}} \mapsto \sum_r (1 - a_r T^{p^r})_W \in \mathcal{W}^{(p)}(A)$. We may thus regard $(a_r)_{r\in N}$ as a coordinate of $\varphi((a_r)) \in \mathcal{W}^{(p)}(A)$.*

14.4. **Some operations on $\Lambda(A)$.**

DEFINITION 14.12. Let A be any commutative ring. Let n be a positive integer. Let us define additive operators V_n, F_n on $\Lambda(A)$ by the following formula.

$$V_n((f(T))_W) = (f(T^n))_W.$$

$$F_n((f(T))_W) = (\prod_{\zeta\in\mu_n} f(\zeta T^{1/n}))_W$$

(The latter definition is a formal one. It certainly makes sense when A is an algebra over $\mathbb{C}$. Then the definition descends to a formal law defined over $\mathbb{Z}$ so that F_n is defined for any ring A. In other words, F_n is actually defined to be the unique continuous additive map which satisfies

$$F_n((1 - aT^l)_) = ((1 - a^{m/l} T^{m/n})^{ln/m})_W \qquad (m = \mathrm{lcm}(n, l)).$$

)

LEMMA 14.13. *Let p be a prime number. Let A be a commutative ring with $pA = 0$. Then:*

(1) *We have*

$$F_p(f(T)) = (f(T^{1/p}))^p \qquad (\forall f \in \Lambda(A)).$$

in particular, F_p is an algebra endomorphism of $\Lambda(A)$ in this case.

(2)

$$V_p(F_p((f)_W) = F_p(V_p((f)_W)) = (f(T)^p)_W = p \cdot (f(T))_W$$

DEFINITION 14.14. For any commutative ring A with $pA = 0$, elements of $W^{(p)}(A)$ are called **p-adic Witt vectors** over A. The ring $(W^{(p)}(A), +, \cdot)$ is called **the ring of p-adic Witt vectors** over A.

LEMMA 14.15. *Let p be a prime number. Let A be a ring with $pA = 0$. Then for any n which is not divisible by p, the map*

$$\frac{1}{n} \cdot V_n : \Lambda(A) \to \Lambda(A)$$

is a "non-unital ring homomorphism". Its image is equal to the range of the idempotent e_n. That means,

$$\mathrm{Image}(\frac{1}{n} \cdot V_n) = e_n \cdot \Lambda(A) = \{\sum_j (1 - y_j T^{nj})_W; y_j \in A\}.$$

PROOF. V_n is already shown to be additive. The following calculation shows that $\frac{1}{n} \cdot V_n$ preserves the multiplication: for any positive integer a, b with lcm m and for any element $x, y \in A$, we have:

$$\begin{aligned}
&(\frac{1}{n} \cdot V_n((1-xT^a)_W)) \cdot (\frac{1}{n} \cdot V_n((1-yT^b)_W)) \\
=&(\frac{1}{n} \cdot (1-xT^{an})_W) \cdot (\frac{1}{n} \cdot (1-yT^{bn})_W) \\
=&\frac{1}{n^2} \cdot \frac{an \cdot bn}{nm} \left((1-x^{m/a}y^{m/b}T^{nm})^d\right)_W \\
=&\frac{1}{n} \cdot V_n(((1-xT^a)_W \cdot (1-yT^b)_W)
\end{aligned}$$

We then notice that the image of the unit element [1] of the Witt algebra is equal to $\frac{1}{n}V_n([1]) = e_n$ and that $\frac{1}{n}V(e_n f) = e_n f$ for any $f \in \Lambda(A)$. The rest is then obvious. $\square$