$\mathbb{Z}_p$, $\mathbb{Q}_p$, AND THE RING OF WITT VECTORS

No.8:

$\boxed{\text{The ring of Witt vectors when } A \text{ is a ring of characteristic } p \neq 0.}$ Recall $\Lambda(A) = 1 + A[[T]]T$ for a formal variable T. To clearly describe the variable, we will denote it as $\Lambda_{(T)}(A)$. It is additively topologically generated by $\{[a]_T = 1 - aT; a \in A\}$. the set of all Teichmüller lift of the elements $a \in A$.

8.1. $\Lambda(A)$ **as a λ-ring.** The treatment in this subsection essentially follows `https://encyclopediaofmath.org/wiki/Lambda-ring`. (But a caution is advised: some signatures are different from the article cited above.)

Definition 8.1. $(A, \lambda_T : A \to \Lambda_T(A))$ is called a pre-λ-ring if

- A is a commutative ring.
- λ_T:$A \to \Lambda_{(T)}(A)$ is an additive map.

Let us write $\lambda_T(f)$ for $f \in A$ as $\lambda_T(f) = (\sum_j \lambda^j(f)T^j)_W$. Then the additivity of λ_T can be expressed as identities of $\{\lambda^j\}$ of the following form:

- $\lambda^0(f) = 1 \quad (\forall f \in A)$.
- $\lambda^1(f) = f \quad (\forall f \in A)$.
- $\lambda^n(f+g) = \sum_{i+j=n} \lambda^{(}f)\lambda^j(g) \quad \forall f, g \in A$.

(Note that λ^j is **not** a "j-th power of λ" in any sence.)

Definition 8.2. Let $R = (R, \lambda^R_{(T)} : R \to \Lambda_T(R))$, $S = (S, \lambda^S_{(T)} : S \to \Lambda_T(S))$ be pre-lambda rings. Then a λ-ring homomorphism from R to S is a ring homomorphism $\varphi : R \to$ such that the following diagram commutes.

$$\begin{tikzcd}
R \arrow[r, "\lambda^R_{(T)}"] \arrow[d, "\varphi"'] & \Lambda_{(T)}(R) \arrow[d, "\Lambda_{(T)}(\varphi)"] \\
S \arrow[r, "\lambda^S_{(T)}"'] & \Lambda_{(T)}(S)
\end{tikzcd}$$

The map $\Lambda_{(T)}(\varphi)$ which appears above is defined as follows:

$$\Lambda_{(T)}(\varphi)((\sum a_j T^j)_W) = (\sum \varphi(a_j)T^j)_W \quad (\{a_j\}_j \subset A)$$

(Yes, we regard $\Lambda_{(T)}(\bullet)$ as a functor.)

We also note, as a consequence of the definition, that we have the following formula for Teichmüller lifts:

$$\Lambda_{(T)}(\varphi)([a]) = [\varphi(a)] \qquad (\forall a \in A)$$

8.2. $\Lambda(A)$ **as a pre-λ-ring.** There exists an additive map $\lambda_S : \Lambda_{(T)}(A) \to \Lambda_{(S)}\Lambda_{(T)}(A)$ defined by

$$\lambda_S([a]_T) = [[a]_T]_S \qquad (\forall a \in A)$$

PROOF. For $\alpha(T) = \prod_i (1 - \xi_i T)$, we have

$$
\begin{aligned}
&\sum_i [[\xi_i]_T]_U \\
=&\prod_i (1 - [\xi_i]_T U))_W \\
=&(\sum_n \sum_{i_1 < i_2 < \ldots i_n} [\xi_{i_1} \ldots \xi_{i_n}]_T (-U)^n)_W \\
=&(\sum_n \sum_{i_1 < i_2 < \ldots i_n} (1 - \xi_{i_1} \ldots \xi_{i_n} T)_W (-U)^n)_W \\
=&(\sum_n (\prod_{i_1 < i_2 < \ldots i_n} (1 - \xi_{i_1} \ldots \xi_{i_n} T))_W (-U)^n)_W \\
=&(\sum_n (\sum_{j=0}^{\infty} L_{j,n}(a) T^j)_W (-U)^n)_W
\end{aligned}
$$

So the required map is given by

$$(\sum_j a_j(T))_W \mapsto (\sum_n \sum_{j=0}^{\infty} (L_{j,n}(a) T^j)_W (-U)^n)_W$$

□

8.3. λ-ring.

DEFINITION 8.3. A pre-λ-ring $A, \lambda_T : A \to \Lambda_{(T)}(A)$ is a λ-ring if $\lambda_T : A \to \Lambda_{(T)}(A)$ is a λ-homomorphism.

PROPOSITION 8.4. *For any commutative ring A, $(\Lambda(A), \lambda_U : \Lambda_{(T)}(A) \to \Lambda_{(U)}\Lambda_{(T)}(A)$ is a λ-ring.*

PROOF. To avoid some confusion, we use lower case letters for indeterminate variables. Moreover, to distinquish all the lambda's around here, we denote by $\mathring{\lambda}$ the lambda operation on $\Lambda(A)$:

$$\mathring{\lambda}_{(t,u)} : \Lambda_{(t)} A \ni [a]_t \mapsto [[a]_t]_u \in \Lambda_{(u)} \Lambda_{(t)} A$$

where $[a]_t$ is the Teichmüller lift of $a \in A$ in $\Lambda_{(t)} A$. We need to verify the commutativity of the following diagram:

$$
\begin{tikzcd}
\Lambda_{(u)}(A) \arrow[r, "\mathring{\lambda}_{(t,u)}"] \arrow[d, "\mathring{\lambda}_{(v,u)}"'] & \Lambda_{(t)}(\Lambda_{(u)} A) \arrow[d, "\Lambda_{(t)}(\mathring{\lambda}_{(v,u)})"] \\
\Lambda_{(v)} \Lambda_{(u)} A \arrow[r, "\mathring{\lambda}_{(t,v)}"'] & \Lambda_{(t)}(\Lambda_{(v)} \Lambda_{(u)} A)
\end{tikzcd}
$$

which can be verified by a diagram chasing for generators $[a]_u (a \in A)$:

$$
\begin{tikzcd}
{[a]_u} \arrow[r, "\mathring{\lambda}_{(t,u)}"] \arrow[d, "\mathring{\lambda}_{(v,u)}"'] & {[[a]_u]_t} \arrow[d, "\Lambda_{(t)}(\mathring{\lambda}_{(v,u)})"] \\
{[[a]_u]_v} \arrow[r, "\lambda_{(t,v)}"'] & {[[[a]_u]_v]_t}
\end{tikzcd}
$$

□

8.4. **Idempotents.** We are going to decompose the ring of Witt vectors $\mathcal{W}_1(A)$. 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 8.5. *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 8.6. 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,

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

DEFINITION 8.7. Let A be a commutative ring. For any $a \in A$, we denote by $[a]$ the element of $\mathcal{W}_1(A)$ defined as follows:
$$[a] = (1 - aT)_W$$
We call $[a]$ *the "Teichmüller lift" of a.*

LEMMA 8.8. *Let A be a commutative ring. Then:*

1. *$\mathcal{W}_1(A)$ is a commutative ring with the zero element $[0]$ and the unity $[1]$.*
2. *For any $a, b \in A$, we have*
$$[a] \cdot [b] = [ab]$$

$\square$

PROPOSITION 8.9. *Let A be a commutative ring. If n is a positive integer which is invertible in A, then n is invertible in $\mathcal{W}_1(A)$. 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
$$(1 + x)^n = (1 - T).$$
It also follows from the next lemma. $\square$

LEMMA 8.10. *Let n be a positive integer. Let k be a non negative integer. Then we have always*
$$\binom{\frac{1}{n}}{k} \in \mathbb{Z}\left[\frac{1}{n}\right].$$

PROOF.

$$\begin{aligned}\binom{\frac{1}{n}}{k} &= \frac{\frac{1}{n}(\frac{1}{n}-1)\cdots(\frac{1}{n}-(k-1))}{k!} \\ &= \frac{1}{n^k}\frac{(1(1-n)(1-2n)\dots(1-(k-1)n)}{k!}\end{aligned}$$

So the result follows from the next sublemma. □

SUBLEMMA 8.11. *Let n be a positive integer. Let k be a non negative integer. Let $\{a_j\}_{j=1}^k \subset \mathbb{Z}$ be an arithmetic progression of common difference n. Then:*

(1) *For any positive integer m which is relatively prime to n, we have*

$$\#\{j;\ m|a_j\ \} \geq \left\lfloor \frac{k}{m} \right\rfloor$$

(2) *For any prime p which does not divide n, let us define*

$$c_{k,p} = \sum_{i=1}^{\infty} \lfloor \frac{k}{p^i} \rfloor$$

(which is evidently a finite sum in practice.) Then

$$p^{c_{k,p}} | \prod_{j=1}^{k} a_j$$

(3)

$$p^{c_{k,p}} | k!, \qquad p^{c_{k,p}+1} \nmid k!$$

(4)

$$\frac{\prod_{j=1}^k a_j}{k!} \in \mathbb{Z}_{(p)}$$

PROOF. (1) Let us put $t = \lfloor \frac{k}{m} \rfloor$. Then we divide the set of first kt-terms of the sequence $\{a_j\}$ into disjoint sets in the following way.

$$\begin{aligned} &S_0 = \{a_1, a_2, \dots, a_m\}, \\ &S_1 = \{a_{m+1}, a_{m+2}, a_{m+m}\}, \\ &S_2 = \{a_{2m+1}, a_{2m+2}, a_{2m+m}\}, \\ &\dots \\ &S_{t-1} = \{a_{(t-1)m+1}, a_{(t-1)m+2}, \dots, a_{(t-1)m+m}\} \end{aligned}$$

Since m is coprime to n, we see that each of the S_u gives a complete representative of $\mathbb{Z}/n\mathbb{Z}$.

(2): Apply (1) to the cases where $m = p, p^2, p^3, \dots$ and count the powers of p which appear in $\prod a_j$.

(3): Easy. (4) is a direct consequence of (2),(3). □

DEFINITION 8.12. 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 8.13. *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 8.14. *Let n be an integer invertible in A. $e_n \cdot \mathcal{W}_1(A) = \{(f)_W | f \in 1 + T^n A[[T^n]]\}$*

PROOF. Easy. Compare with Lemma 8.24 below.
□

8.6. **The ring of p-adic Witt vectors (when the characteristic of the base ring A is p).** Before proceeding further, let me illustrate the idea. Proposition 8.9 tells us an existence of a set $\{e_n; n \in \mathbb{Z}_{>0}, p \nmid n\}$ of idempotents in $\mathcal{W}_1(A)$ such that its order structure is somewhat like the one found on the set $\{n\mathbb{N}; n \in \mathbb{Z}_{>0}, p \nmid n\}$. Knowing that the idempotents correspond to decompositions of $\mathcal{W}_1(A)$, we may ask:

PROBLEM 8.15. What is the partition of $\mathbb{Z}_{>0}$ generated by the subsets $\{n\mathbb{N}; n \in \mathbb{Z}_{>0}\}$?

To answer this problem, it would probably be better to find out, for given positive number n which is coprime to p, what the set
$$S_{n;p} = n\mathbb{N} \setminus (\bigcup_{\substack{n|m \\ n<m \\ p|m}} m\mathbb{N})$$
should be. The answer is given by a fact which we know very well: every positive integer may uniquely be written as
$$p^s k \quad (s \in \mathbb{Z}_{\geq 0}, \quad k \in \mathbb{Z}_{>0}, \quad \gcd(p,k) = 1),$$
Knowing that, we see that the set $S_{n;p}$ as above is equal to
$$\{p^s n; s \in \mathbb{Z}_{\geq 0}\}.$$

The answer to the problem is now given as follows:
$$\mathbb{Z}_{>0} = \coprod_{p \nmid n} \{p^s n; s \in \mathbb{Z}_{\geq 0}\}.$$

The same story applies to the ring $\mathcal{W}_1(A)$ of universal Witt vectors for a ring A of characteristic p. We should have a direct product expansion
$$\mathcal{W}_1(A) = \prod_{p \nmid n} e_{n;p} \mathcal{W}_1(A)$$
where the idempotent $e_{n;p}$ is defined by
$$e_{n;p} = e_n - \bigvee_{\substack{n|m \\ n<m \\ p \nmid m}} e_m$$

Of course we need to consider infimum of infinite idempotents. We leave it to an exercise:

EXERCISE 8.1. Show that the supremum

$$\bigvee_{\substack{n|m\\ n<m\\ p\nmid m}} e_m = e_n - \prod_{\substack{n|m\\ n<m\\ p\nmid m}} (e_n - e_m)$$

exists. In other words, show that the right hand side converges.

PROPOSITION 8.16. *Let p be a prime. Let A be an integral domain of characteristic p. Let us define an idempotent f of $\mathcal{W}_1(A)$ 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

$$\mathcal{W}_1(A) \cong (f \cdot \mathcal{W}_1(A)) \times (([1] - f) \cdot \mathcal{W}_1(A))\,.$$

We call the factor algebra $([1] - f) \cdot \mathcal{W}_1(A)$ **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 8.17. *Let p be a prime. Let A be a commutative ring of characteristic p. For each positive integer k which is not divisible by p, let us define an idempotent f_k of $\mathcal{W}_1(A)$ 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

$$e_k\mathcal{W}_1(A) \cong (f_k \cdot \mathcal{W}_1(A)) \times ((e_k - f_k) \cdot \mathcal{W}_1(A))\,.$$

Furthermore, the factor algebra $(e_k - f_k) \cdot \mathcal{W}_1(A)$ is isomorphic to the ring $\mathcal{W}^{(p)}(A)$ of p-adic Witt vectors. Thus we have a direct product decomposition

$$\mathcal{W}_1(A) \cong \mathcal{W}^{(p)}(A)^{\mathbb{N}}.$$

8.7. **The ring of p-adic Witt vectors for general A.** In the preceding subsection we have described how the ring $\mathcal{W}_1(A)$ of universal Witt vectors decomposes into a countable direct sum of the ring of p-adic Witt vectors. In this subsection we show that the ring $W^{(p)}(A)$ can be defined for any ring A (that means, without the assumption of A being characteristic p).

We need some tools.

DEFINITION 8.18. Let A be any commutative ring. Let n be a positive integer. Let us define additive operators V_n, F_n on $\mathcal{W}_1(A)$ 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 8.19. *Let p be a prime number. Let A be a commutative ring of characteristic p. Then:*

(1) *We have*

$$F_p(f(T))=(f(T^{1/p}))^p \qquad (\forall f\in \mathcal{W}_1(A)).$$

in particular, F_p is an algebra endomorphism of $\mathcal{W}_1(A)$ 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 8.20. Let A be any commutative ring. Let p be a prime number. We denote by

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

and define

$$\pi_p:\mathcal{W}_1(A)\to\mathcal{W}^{(p)}(A)$$

by

$$\pi_p\left(\sum_{j=1}^{\infty}(1-x_jT^j)\right)=(x_1,x_p,x_{p^2},x_{p^3}\dots).$$

LEMMA 8.21. *Let us define polynomials $\alpha_j(X,Y)\in\mathbb{Z}[X,Y]$ by the following relation.*

$$(1-xT)(1-yT)=\prod_{j=1}^{\infty}(1-\alpha_j(x,y)T^j).$$

Then we have the following rule for "carry operation":

$$(1-xT^n)_W+(1-yT^n)_W=\sum_{j=1}^{\infty}(1-\alpha_j(x,y)T^{jn}).$$

PROPOSITION 8.22. *There exist unique binary operators $+$ and $\cdot$ on $\mathcal{W}^{(p)}(A)$ such that the following diagrams commute.*

$$\begin{array}{ccc}
\mathcal{W}_1(A)\times\mathcal{W}_1(A) & \xrightarrow{+} & \mathcal{W}_1(A)\\
{\scriptstyle\pi_p}\downarrow & & {\scriptstyle\pi_p}\downarrow\\
\mathcal{W}^{(p)}(A)\times\mathcal{W}^{(p)}(A) & \xrightarrow{+} & \mathcal{W}^{(p)}(A)
\end{array}$$

$$\begin{array}{ccc}
\mathcal{W}_1(A)\times\mathcal{W}_1(A) & \xrightarrow{\cdot} & \mathcal{W}_1(A)\\
{\scriptstyle\pi_p}\downarrow & & {\scriptstyle\pi_p}\downarrow\\
\mathcal{W}^{(p)}(A)\times\mathcal{W}^{(p)}(A) & \xrightarrow{\cdot} & \mathcal{W}^{(p)}(A)
\end{array}$$

PROOF. Using the rule as in the previous lemma, we see that addition descends to an addition of $\mathcal{W}^{(p)}(A)$. It is easier to see that the multiplication also descends.

□

DEFINITION 8.23. For any commutative ring A, 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 8.24. *Let p be a prime number. Let A be a ring of characteristic p. Then for any n which is not divisible by p, the map*

$$\frac{1}{n} \cdot V_n : \mathcal{W}_1(A) \to \mathcal{W}_1(A)$$

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

$$\text{Image}(\frac{1}{n} \cdot V_n) = e_n \cdot \mathcal{W}_1(A) = \{\sum_j (1 - y_j T^{nj})_W ; y_j \in A\}.$$

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 $f \in \mathcal{W}_1(A)$. The rest is then obvious. $\square$

In preparing from No.7 to No.10 of this lecture, the following reference (especially its appendix) has been useful:

http://www.math.upenn.edu/~chai/course_notes/cartier_12_2004.pdf