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

No.10:
$\boxed{\text{The ring of Witt vectors when } A \text{ is a ring of characteristic } p \neq 0.}$

DEFINITION 10.1. 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:

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

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

LEMMA 10.2. *Let A be a commutative ring. Then:*

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

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

□

PROPOSITION 10.3. *Let p be a prime number. Let A be a ring of characteristic p. Then:*

(1) *If n is a positive integer which is not divisible by p, then n is invertible in $\mathcal{W}_1(A)$. To be more precise,*

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

(2) $p\boxdot : \mathcal{W}_1(A) \to \mathcal{W}_1(A)$ *is an injection.*
(3) *For any positive integer n which is not divisible by p, we define*

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

as an element of $\mathcal{W}_1(A)$.
(4) *For any positive integer n, e_n is an idempotent. (That means, $e_n^{\boxtimes 2} = e_n$.)*
(5) *If $n|m$, then $e_n \succeq e_m$ in the order of idempotents. That means, $e_n \boxtimes e_m = e_m$.*

PROOF. (1) follows from the next lemma. □

LEMMA 10.4. *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.

$$\begin{aligned} &\binom{\frac{1}{n}}{k} \in \mathbb{Z}\left[\frac{1}{n}\right] \\ =&\frac{\frac{1}{n}(\frac{1}{n}-1)\cdots(\frac{1}{n}-(k-1))}{k!} \\ =&\frac{1}{n^k}\frac{(1(1-n)(1-2n)\dots(1-(k-1)n)}{k!} \end{aligned}$$

So the result follows from the next sublemma. □

SUBLEMMA 10.5. *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)

$$p^{c_{k,p}}|k!, \qquad p^{c_{k,p}+1} \not| k!$$

(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.

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

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 $m = p, p^2, p^3, \ldots$ and count the powers of p which appear in $\prod a_j$.

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

PROPOSITION 10.6. *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.*

$$f = \bigvee_{\substack{n>1 \\ p\not| n}} e_n (= [1] \boxminus \prod_{\substack{p\not| n \\ n>1}}^{\boxtimes} ([1] \boxminus e_n))$$

Then f defines a direct product decomposition

$$\mathcal{W}_1(A) \cong (f \boxtimes \mathcal{W}_1(A)) \times ((1 \boxminus f) \boxtimes \mathcal{W}_1(A)).$$

Furthermore, the factor algebra $(1 \boxminus f) \boxtimes \mathcal{W}_1(A)$ is isomorphic to 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 10.7. *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.*

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

Then f_k defines a direct product decomposition

$$e_k \mathcal{W}_1(A) \cong (f_k \boxtimes \mathcal{W}_1(A)) \times ((1 \boxminus f_k) \boxtimes \mathcal{W}_1(A)).$$

Furthermore, the factor algebra $(1 \boxminus f_k) \boxtimes \mathcal{W}_1(A)$ is isomorphic to the ring $\mathcal{W}^{(p)}(A)$ of p-adic Witt vectors. Thus we have a direct product decomposition

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

To understand the mechanism which appears in the proposition above, it would be better to prove the following

LEMMA 10.8. *Let p be a prime number. Let A be a ring of characteristic p. Then for any n which is not divisible by p, a map*

$$\frac{1}{n} \boxdot V_n : (\mathcal{W}_1(A), \boxplus, \boxtimes) \to (\mathcal{W}_1(A), \boxplus, \boxtimes)$$

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

$$\mathrm{Image}(\frac{1}{n} \boxdot V_n) = e_n \boxtimes \mathcal{W}_1(A) = \{ \sum_j^{\boxplus} (1 - y_j T^{nj}); y_j \in A \}.$$

PROOF. V_n is already shown to be additive. The following calculation shows that $\frac{1}{n} \cdot V_n$ preserves the $\boxtimes$-multiplication.

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

□

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`