No.7:

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

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 topological-algebraically generated by $\{[a]_T = 1 - aT; a \in A\}$. the set of all Teichmüller lift of the elements $a \in A$.

In summary, subsections 7.1-7.3 Tells:

- λ-ring can be defined by using $\Lambda(A)$.
- For any ring A, $\Lambda(A)$ itself gives an example of λ-ring.

But we do not use these sections this year.

7.1. $\Lambda(A)$ **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 7.1. $(A, \lambda_T : A \to \Lambda_T(A))$ 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 7.2. 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:

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

7.2. $\Lambda(A)$ **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

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

□

7.3. **λ-ring.**

DEFINITION 7.3. 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 7.4. *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 $[a]_u (a \in A)$:

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

$\square$

7.4. **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 7.5. *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 7.6. 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,

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

DEFINITION 7.7. 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 7.8. *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*

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

$\square$

PROPOSITION 7.9. *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

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

Indeed, assume we already know that there exists

$$\{b_1, b_2, \dots b_k\} \subset A$$

such that we have

$$(1 + \sum_{j=1}^{k} b_j T^j)^n \equiv (1-T) \mod T^{k+1}.$$

(The elements $\{b_j\}$ can actually be computed by the binomial theorem, but we don't care.) Then there exists $a_{k+1} \in A$ such that

$$(1 + \sum_{j=1}^{k} b_j T^j)^n \equiv (1-T) + a_{k+1}T^{k+1} \mod T^{k+2}.$$

Now, let us put $c = -\frac{1}{n} \cdot a_{k+1}$. By our assumption, the element c is an element of A. We compute:

$$\begin{aligned} &(1 + \sum_{j=1}^{k} b_j T^j + cT^{k+1})^n \\ =&(1 + \sum_{j=1}^{k} b_j T^j)^n + n(1 + \sum_{j=1}^{k} b_j T^j)^{n-1} \cdot cT^{k+1} \\ \equiv&(1 + \sum_{j=1}^{k} b_j T^j)^n + ncT^{k+1} \equiv 1 - T^{k+1} \mod T^{k+2} \end{aligned}$$

So we may proceed with induction. □

DEFINITION 7.10. 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 7.11. *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 7.12. *Let n be an integer invertible in A. Then we have $e_n \cdot \Lambda(A) = \{(f)_W | f \in 1 + T^n A[[T^n]]\}$*

PROOF. Easy. Compare with Lemma 7.14 below.

□

DEFINITION 7.13. 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 is called Verschiebung map. F_n is called "Frobenius"" map.)

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

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

(The formulae in parentheses in 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

$$F_n((1-aT^m)_)) = d\cdot(1-a^{n'}T^{m'})_W$$

$(n, m \in \mathbb{Z}, d = \gcd(n,m), l = \mathrm{lcm}(n,m), n = n'd, m = m'd (n', m' \in \mathbb{Z}))$

See Proposition 6.3. for details of computations.)

LEMMA 7.14. *Let A be a ring. Then for any n which is not divisible by p, Then for any $n \in \mathbb{Z}_{>0}$ which is invertible in A, 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,

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

In other words, $\frac{1}{n}\cdot V_n$ gives a usual(i.e. unital) isomorphism between $\Lambda(A)$ and $e_n\cdot\Lambda(A)$.

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, let us write $d = \gcd(a,b), a = a'd, b = b'd (a', b' \in \mathbb{Z})$ with $l = \mathrm{lcm}(a,b)(= a'b'd)$. Then for any element $x, y \in A$, by using Proposition 6.3, we have:

$$\begin{aligned}
&(\frac{1}{n}\cdot V_n((1-xT^a)_W))\cdot(\frac{1}{n}\cdot V_n((1-yT^b)_W))\\
=&(\frac{1}{n}\cdot(1-xT^{an})_W)\cdot(\frac{1}{n}\cdot(1-yT^{bn})_W)\\
=&\frac{1}{n^2}\cdot d\left((1-x^{b'}y^{a'}T^{nl})\right)_W\\
=&\frac{1}{n}\cdot V_n(((1-xT^a)_W\cdot(1-yT^b)_W)
\end{aligned}$$

(We actually can save this computation by using "splitting method"+ functoriality+T-addic completion arguements)

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 $\frac{1}{n}V(e_nf) = e_nf$ for any $f \in \Lambda(A)$. The rest is then obvious. $\square$

7.6. **The ring of p-adic Witt vectors (when the characteristic of the base ring A is p).**

LEMMA 7.15. *Let p be a prime number. Let A be a commutative ring of characteristic p. Then:*

(1) *We have*

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

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

(2)

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

By using a boolean-algebra-type argument, we have:

PROPOSITION 7.16. *Let p be a prime number. Let A be a commutative ring of characteristic p. We have a direct product expansion*

$$\Lambda(A) = \prod_{\{n; p \nmid n\}} e_{n;p}\Lambda(A)$$

where the idempotent $e_{n;p}$ is defined by

$$e_{n;p} = e_n - \bigvee_{\{m; n|m, n<m, p\nmid m\}} e_m$$

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

EXERCISE 7.1. Show that the supremum $\displaystyle\bigvee_{\{m; n|m, n<m, p\nmid m\}} e_m$ exists.

Hint: Put $S_p = \{q; prime, q \neq p\}$. then:

$$\begin{aligned}
e_n - \bigvee_{\{m; n|m, n<m, p\nmid m\}} e_m &= e_n - \bigvee_{q \in S_p} e_{nq} = \bigwedge_{q \in S_p} (e_n - e_{nq}) \\
&= e_n \bigwedge_{\{q; \text{prime}, q \neq p\}} (1 - e_{nq}) \\
&= e_n \prod_{q \in S_p} (1 - e_{nq}) \\
&= e_n \begin{pmatrix} 1 - \sum_{q_1 \in S_p} (1 - e_{nq_1}) + \sum_{q_1, q_2 \S_p, q_1 < q_2} (1 - e_{nq_1} e_{nq_2}) \\ - \sum_{q_1, q_2, q_3 \S_p, q_1 < q_2 < q_3} (1 - e_{nq_1} e_{nq_2} e_{nq_3}) + \dots \end{pmatrix}
\end{aligned}$$

The $n = 1$ case is the most important. We note that $e_1 = [1]$.

PROPOSITION 7.17. *Let p be a prime. Let A be an integral domain of characteristic p.*

Then $e_{1;p}$ defines a direct product decomposition

$$\Lambda(A) \cong (e_{1,p} \cdot \Lambda(A)) \times (([1] - e_{1,p}) \cdot \Lambda(A)).$$

We call the factor algebra $e_{1;p} \cdot \Lambda(A)$ **the ring $\Lambda^{(p)}(A)$ of p-adic Witt vectors**.

For any $n > \mathbb{Z}_{>0} \setminus p\mathbb{Z}$, our idempotent $e_{n,p}$ can be described by $e_{1;p}$ using the Verschiebung V_n:

PROPOSITION 7.18.

$$e_{n;p} = V_n(e_{1,p})$$

7.7. The ring of p-adic Witt vectors for general A. In the preceding subsection we have described how the ring $\Lambda(A)$ 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 $\Lambda^{(p)}(A)$ can be defined for any ring A (that means, without the assumption of A being characteristic p).

Image(V_n) plays a role of substitute for Image e_n. It's even better in the sence that $(1 - cT^n)_W \in \text{Image}(V_n)$ may not be a elemnt of the form $n(1 - aT^n)_W$ for any $a \in A$. We have:

PROPOSITION 7.19. *$I_n = \text{Image}(V_n)$ is an ideal of $\Lambda(A)$.*

PROOF. Let us calculate a multiplication of additive generators (as topological modules) of $\Lambda(A)$ and I_n :

$$\begin{aligned} ((1 - aT^k)_W) \cdot V_n((1 - bT^m)_W) &= ((1 - aT^k)_W) \cdot ((1 - bT^{nm})_W) \\ &= d(1 - a^*b^*T^l)_W \in I_n \\ &\quad (d = \gcd(k, nm), l = \operatorname{lcm}(k, nm)) \end{aligned}$$

□

DEFINITION 7.20. Let A be any commutative ring. Let p be a prime number. Let us put $S_p = \{q; prime, q \neq p\}$. Let $I_{(p)}$ be the (topological) closure of the ideal $\langle \cup_{q \in S_p} \text{Image}(V_q) \rangle$ generated by $\cup_{q \in S_p} \text{Image}(V_q)$.

Then we define

$$\Lambda^{(p)}(A) \stackrel{\text{def}}{=} \Lambda(A)/I_{(p)}$$

LEMMA 7.21.

$$A^{\mathbb{N}} \ni (x_1, x_p, x_{p^2}, x_{p^3} \ldots) \mapsto \sum_{k=0}^{\infty} (1 - x_{p^k} T^{p^k})_W \mod I_{(p)} \in \Lambda^{(p)}(A)$$

is a bijection.

LEMMA 7.22. *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":

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

DEFINITION 7.23. For any commutative ring A, elements of $\Lambda^{(p)}(A)$ are called **p-adic Witt vectors** over A. The ring $(\Lambda^{(p)}(A), +, \cdot)$ is called **the ring of p-adic Witt vectors** over A.