Introduction to p-adic Hodge theory 6

—— Witt vectors

§1. Big Witt ring

Let R be a commutative ring.

The big Witt ring of R, denoted by $W(R)$ is defined as follows:

- as a set, $W(R) = R^{\mathbb{N}}$; an element in $W(R)$ is written as $a = (a_1, a_2, \cdots)$
  (or a power series $1 + a_1 t + a_2 t^2 + \cdots$)
  ↑ called a Witt vector
- there's a ghost map $w = (w_1, w_2, \cdots) : W(R) \longrightarrow R^{\mathbb{N}}$
  given by $w_1(a) = a_1$, $w_2(a) = a_1^2 + 2a_2 \cdots$
  $$w_n(a) = \sum_{d|n} d \cdot a_d^{n/d}$$
- Basically, the $+, \cdot$ on $W(R)$ are functorially pulled back from coordinatewise operation on $R^{\mathbb{N}}$.

e.g. $(a_1, a_2, a_3, \cdots) \xmapsto{w} a_1, a_1^2 + 2a_2, a_1^3 + 3a_3, \cdots$

$(b_1, b_2, b_3, \cdots) \xmapsto{w} b_1, b_1^2 + 2b_2, b_1^3 + 3b_3, \cdots$

↓ addition

$$(a_1 + b_1, a_2 + b_2 - a_1 b_1, a_3 + b_3 + \frac{a_1^3 + b_1^3 - (a_1 + b_1)^3}{3}, \cdots) \rightsquigarrow a_1 + b_1, a_1^2 + b_1^2 + 2a_2 + 2b_2, a_1^3 + b_1^3 + 3a_3 + 3b_3$$

solve for $(a_1 + b_1)^2 + 2x_2 = a_1^2 + b_1^2 + 2a_2 + 2b_2$

- Rigorous speaking, first prove that in the universal case
  $R^{univ} = \mathbb{Z}[x_1, x_2, \cdots, y_1, y_2, \cdots]$ and $x = (x_1, x_2, \cdots)$, $y = (y_1, y_2, \cdots)$,

(*) $w(x) + w(y)$ and $w(x)w(y)$ belongs to Image(w)

They are represented by $S = (S_1(x, y), S_2(x, y), \cdots)$ and $P = (P_1(x, y), P_2(x, y), \cdots)$

- In the general case, $\exists\, \psi : R^{univ} \longrightarrow R$ s.t. $\psi(x) = a$, $\psi(y) = b$

by functoriality, define $a+b := \psi(S(x,y))$, $a\cdot b := \psi(P(x,y))$

- Proof of (*): In the universal case, $\forall$ prime p, there's an operator

$$\varphi_p : R^{univ} \longrightarrow R^{univ} \qquad \varphi_p(a_n) = a_n^p \ \forall n.$$

Claim: A sequence $(f_1, f_2, \cdots) \in Im(w)$ if and only if $\forall p \nmid d$, $\alpha \geq 1$, $f_{p^\alpha d} \equiv \varphi_p(f_{p^{\alpha-1}d}) \pmod{p^\alpha}$

Pf: Indeed, $\forall (f_1, f_2, \cdots) \in (R^{univ})^{\mathbb{N}}$, $\exists!\ (a_1, a_2, \cdots) \in (R^{univ} \otimes \mathbb{Q})^{\mathbb{N}}$ s.t. $w(\underline{a}) = \underline{f}$.

NTS: $\underline{a} \in (R^{univ})^{\mathbb{N}} \iff \forall n$, $p^\alpha \| n$ with $\alpha \geq 1$, $f_n \equiv \varphi_p(f_{n/p}) \pmod{p^\alpha}$

"$\Rightarrow$" $\varphi_p(f_{n/p}) = \sum_{d \mid \frac{n}{p}} d\, \varphi_p(a_d^{n/pd}) \equiv \sum_{d \mid \frac{n}{p}} d \cdot (a_d^{n/pd})^p \equiv \sum_{d \mid \frac{n}{p}} d \cdot a_d^{n/d} \equiv f_n \pmod{p^\alpha}$.

↑ uses: $\varphi_p(a_d) \equiv a_d^p \bmod p$

$\Rightarrow \varphi_p(a_d)^{n/pd} \equiv (a_d^p)^{n/pd} \bmod p^{v\left(\frac{n}{pd}\right)+1}$

"$\Leftarrow$" Conversely, the congruence above $\Rightarrow$ when inductively determine a_n by

$$n a_n = f_n - \sum_{\substack{d \mid n \\ d \neq n}} d \cdot a_d^{n/d}$$

$$\equiv \varphi_p(f_{n/p}) - \sum \cdots \equiv 0 \bmod p^\alpha \text{ for any } p^\alpha \| n. \qquad \square$$

Corollary. A ring homomorphism $R \to R'$ induces a homomorphism $W(R) \to W(R')$.

§2 p-typical Witt vectors

Let p be a prime. The p-typical Witt vectors $W(R)$ is the components of $W(R)$ indexed by p-powers

Still write $\underline{a} = (a_0, a_1, a_2, \cdots)$ to mean a_1, a_p, a_{p^2} in $W(R)$.

p-Ghost map is $w(\underline{a}) = (a_0,\ a_0^p + p a_1,\ a_0^{p^2} + p a_1^p + p^2 a_2, \cdots)$

- The element $p \in W(R)$ is $w^{-1}(p, p, p, \cdots)$

$$= (p,\ 1 - p^{p-1},\ p \cdot *, \cdots)$$

From now on, assume that $\operatorname{char} R = p > 0$

- p is represented by $(0, 1, 0, \cdots)$ in $W(R)$

In general, $\mathfrak{p}\cdot(a_0, a_1, \cdots) = (0, a_0^{\mathfrak{p}}, a_1^{\mathfrak{p}}, \cdots)$ shift to the right and then

- When R is perfect, $W(R)/\mathfrak{p}W(R) \cong R$
- If $a \in R$, the element $[a] := (a, 0, 0, \cdots)$ is called the <u>Teichmüller lift</u> of R.

  it is multiplicative : $(R, \cdot) \longrightarrow (W(R), \cdot)$

<u>Example</u> : $W(\mathbb{F}_p) = \mathbb{Z}_p$, $W(\mathbb{F}_{p^n})$ = unram. extension of $\mathbb{Z}_p$ of deg n.

The Teichmüller map defines $\mathbb{F}_p^\times \xrightarrow{\sim} \mu_{p-1} \subseteq \mathbb{Z}_p^\times$.

- When R is perfect, every element in $W(R)$ admits a power series expansion

$$(a_0, a_1, a_2, \cdots) = [a_0] + \mathfrak{p}[a_1^{1/p}] + \mathfrak{p}^2[a_2^{1/p^2}] + \cdots$$

b/c RHS under ghost is $a_0 + \mathfrak{p}a_1^{1/p} + \mathfrak{p}^2 a_2^{1/p^2} + \cdots \equiv a_0 \bmod \mathfrak{p}$

$a_0^{\mathfrak{p}} + \mathfrak{p}a_1 + \mathfrak{p}^2 a_2^{1/p} + \cdots \equiv a_0^{\mathfrak{p}} + \mathfrak{p}a_1 \bmod \mathfrak{p}^2$

- By functoriality of Witt rings, the Frobenius map on R induces a natural map

$$F : W(R) \longrightarrow W(R), \quad F(a_0, a_1, \cdots) = (a_0^{\mathfrak{p}}, a_1^{\mathfrak{p}}, \cdots)$$

<u>Theorem</u>. If A is a ring complete for $\mathfrak{p}$-adic topology and if R is a perfect ring in char $\mathfrak{p}$.

then a map $f : R \to A/\mathfrak{p}A$ lifts uniquely to $\tilde{f} : W(R) \to A$.

Proof: For $x \in R$, denote $x^{(n)} := \mathfrak{p}^n$th root of x.

First pick any set-theoretic lift $\hat{f} : R \to A$ of f.

Define $\tilde{f}([x]) := \lim_{m \to +\infty} \hat{f}(x^{(m)})^{\mathfrak{p}^m}$ (and $\hat{f}(x^{1/\mathfrak{p}^m})^{\mathfrak{p}^m} \bmod \mathfrak{p}^{m+1}$ is well-defined.)

This converges b/c $\hat{f}(x^{(m+1)})^{\mathfrak{p}} \equiv \hat{f}(x^{(m)}) \bmod \mathfrak{p}$ implies that $\hat{f}(x^{(m+1)})^{\mathfrak{p}^{m+1}} \equiv \hat{f}(x^{(m)}) \bmod \mathfrak{p}^{m+1}$.

In general, define for $a = \sum_{n \geq 0} \mathfrak{p}^n [a_n] \in W(R)$: $\tilde{f}(a) = \sum_{n \geq 0} \mathfrak{p}^n \hat{f}([a_n])$.

Clearly, $\hat{f}([a]) \cdot \hat{f}([b]) = \hat{f}([ab])$

We need to show $\tilde{f}([a]) + \tilde{f}([b]) = \tilde{f}([a] + [b])$ (*) (this proof reveals the defn of Witt vectors)

For this, we consider the universal case $R_{univ} = \mathbb{Z}[x^{1/p^\infty}, y^{1/p^\infty}] \twoheadrightarrow \bar{R}_{univ} = \mathbb{F}_p[x^{1/p^\infty}, y^{1/p^\infty}]$

we have $[x] + [y] = [S_0(x,y)] + p\cdot[S_1(x,y)] + p^2\cdot[S_2(x,y)] + \cdots$

- Proof of (*) mod p: $\hat{f}(x) + \hat{f}(y) = \hat{f}(S_0(x,y)) \Rightarrow S_0(x,y) \equiv x+y \bmod p$
- Proof of (*) mod p^2: $\hat{f}(x^{1/p})^p + \hat{f}(y^{1/p})^p = \hat{f}(S_0(x,y^{1/p})^p + p\hat{f}(S_1(x,y)) \bmod p^2$

But $(x^{1/p})^p + (y^{1/p})^p = (S_0(x^{1/p}, y^{1/p}))^p + pS_1(x,y) \bmod p^2$ is known.

(This can be seen as $\mathbb{Z}[x^{1/p}, y^{1/p}] \xrightarrow{\hat{\hat{f}}} A$, pick any lift, with $\mathbb{Z}[x^{1/p}, y^{1/p}] \to \mathbb{F}_p[x^{1/p}, y^{1/p}] \to R \to A/pA$

$\Rightarrow \hat{\hat{f}}(x^{1/p})^p + \hat{\hat{f}}(y^{1/p})^p = \hat{\hat{f}}(S_0(x^{1/p}, y^{1/p}))^p + p\hat{\hat{f}}(S_1(x,y))$

But (*) mod p^2 does not depend on $\hat{f}$. So okay.)

···· By induction, we proved the theorem. (and we see "why Witt vector is defined as this.") □

Perfectoid fields.

Definition A complete valued field K is called a perfectoid field if $\exists$ an element $\varpi \in \mathfrak{m}_K$ s.t. (1) $\varpi^p \mid p$.

(2) The Frobenius $\sigma: \mathcal{O}_K/\varpi \xrightarrow{\sim} \mathcal{O}_K/\varpi^p$ is an isomorphism.

Remarks: ① (2) is equivalent to $\sigma: \mathcal{O}_K/\varpi^p \to \mathcal{O}_K/\varpi^p$ is surjective.

b/c it automatically factors through $\mathcal{O}_K/\varpi$

② K perfectoid $\Rightarrow v(K^\times) \subseteq \mathbb{R}$ must be dense! (so certainly not a CDVF.)

b/c keep taking inverses of σ, we get elements of norm $\frac{1}{p^m} v(\varpi)$.

Examples:

① $k((t, t^{1/p^\infty})) = K$. $k[[t^{1/p^\infty}]]$ σ $k[[t^{1/p^\infty}]]$

k perfect of char $p>0$ $\qquad (t) \xrightarrow{\simeq} (t^p)$

② $\mathbb{Q}_p(\zeta_{p^\infty}) = K_\infty$ $\quad \dfrac{\mathcal{O}_{K_\infty}}{(\zeta_p - 1)\mathcal{O}_{K_\infty}} = \bigcup_{n\geq 1} \dfrac{\mathbb{Z}_p[\zeta_{p^n}-1]}{(\zeta_p-1)\mathbb{Z}_p[\zeta_{p^n}-1]} \xrightarrow{\text{setting } x_n = \zeta_{p^n}-1} \bigcup_{n\geq 1} \dfrac{\mathbb{F}_p[x_n]}{(x_n^{p^{n-1}})}$

Yet note that $x_{n+1} = \zeta_{p^{n+1}} - 1$; $x_n = (1+x_{n+1})^p - 1 \equiv x_{n+1}^p \bmod p$

so $\mathcal{O}_{K_\infty}/(\zeta_p - 1)\mathcal{O}_{K_\infty} \simeq \mathbb{F}_p[x_1^{1/p^\infty}]/(x_1)$

↑ as rings

By exactly same argument above, ✓

③ $K/\mathbb{Q}_p$ finite. ϖ = uniformizer, $f \in F_\varpi$, F_f, ϖ_n primitive root of $[\varpi^n](X)$

We have $x_n = [\varpi]_f(x_{n+1}) \equiv x_{n+1}^q \bmod \varpi$

$$\frac{\mathcal{O}_{K_\infty}}{x_1 \mathcal{O}_{K_\infty}} \simeq \mathbb{F}_q[x_1^{1/q^\infty}]/(x_1)$$