ON THE DE RHAM-WITT COMPLEX

by

Özlem Ejder

A Thesis Submitted to the

Graduate School of Sciences and Engineering

in Partial Fulfillment of the Requirements for

the Degree of

Master of Science

in

Mathematics

Koç University

June 2011

Koç University
Graduate School of Sciences and Engineering

This is to certify that I have examined this copy of a master's thesis by
Özlem Ejder

and have found that it is complete and satisfactory in all respects,
and that any and all revisions required by the final
examining committee have been made.

Thesis Committee Members:

Asst. Prof. Sinan Ünver (Advisor)..........................
Asst. Prof. Kazım Büyükboduk.....................................
Assoc. Prof. Sefa Feza Arslan...............................

Date: 09 June 2011

ABSTRACT

The purpose of this study is to give a comprehensive treatment of big Witt vectors and the de Rham-Witt complex.

We begin with an introduction to Witt vectors and cover both the classical p-typical Witt vectors and the big Witt vectors. The latter associates to every ring A and every set S of positive integers stable under division a ring $\mathbb{W}_S(A)$, and the former corresponds to the case where all elements of S are powers of a single prime p. We also give a historical motivation for p-typical Witt vectors.

We continue with the definition of the big de Rham-Witt complex mainly focusing on p-typical de Rham-Witt complex. De Rham-Witt complex is a projective system of differential graded algebras. In degree zero, it is the Witt vectors and the first complex in the inverse limit is de Rham complex. It provides a complex which is explicit and computable. We also give an explicit calculation of p-typical de Rham-Witt complex over $\mathbb{F}_p[T, T^{-1}]$.

ÖZET

Bu tezin asıl amacı Witt vektörleri ve de Rham-Witt kompleks hakkında kapsayıcı bir çalışma sunmaktır. Witt vektörlerine bir giriş ile başlayacak olan bu çalışma hem klasik p-sel Witt vektörlerini hem de büyük Witt vektörlerini kapsayacaktır. Büyük Witt vektörleri her A halkasına ve doğal sayıların bölme altında kapalı her S altkümesine bir halka atarken p-sel Witt vektörleri S kümesinin sadece bir tek p asal sayısının kuvvetlerinden oluştuğu duruma denk gelmektedir.

Ardından büyük de Rham-Witt kompleksin tanımı ile devam etmektedir. Fakat asıl olarak p-sel de Rham-Witt kompleks üzerinde odaklanılmıştır. De Rham-Witt kompleks derecelendirilmiş diferansiyel cebirlerinin bir projektif sistemidir. Bu sistem sıfırıncı derecede Witt vektörlerini verir ve bu projektif sistemdeki ilk nesne de Rham komplekstir. De Rham-Witt kompleks bize kolay ve açık olarak hesaplanabilen bir kompleks sağlar. Bu çalışmada da buna bir örnek olarak $\mathbb{F}_p[T, T^{-1}]$ halkası üzerindeki p-sel de Rham-Witt kompleksin hesaplanışı açık olarak gösterilmiştir.

ACKNOWLEDGEMENTS

My first gratitude is to Assoc. Prof Sinan Ünver, my thesis supervisor, for his support, tolerance and guidance. His efforts and the time he spent were invaluable and the courses we have made were very fruitful.

I would like to thank Assoc. Prof. Sefa Feza Arslan and Asst. Prof. Kazım Büyükboduk and for their participation in my thesis committee.

I also would like to express my thankfulness to Prof. Ali Ülger, the director of the graduate studies of Mathematics Department for his support and guidance.

I thank Pınar Kılıçer for her help and support during typing my thesis, and mostly for her friendship.

I am thankful to my officemates for the friendly atmosphere they provided.

Finally, my deepest gratitude is to my family, for their endavours, love and support. Their presence made everything easier.

Contents

1 Introduction

Aim of this study is to give an explicit calculation of de Rham-Witt complex over a certain ring. For this, first we need to describe Witt vectors and the de Rham-Witt complex. The ring of Witt vectors over A is the direct product of copies of A's as a set. Ring operations are not defined componentwise. The operations are defined such that Witt polynomials $w_n(x)$ are ring homomorphisms.

$$w_0(x) = x_0,\ w_1(x) = x_0^p + px_1,\ w_2(x) = x_0^{p^2} + px_1^p + p^2x_2, \ldots$$

Here one finds the Witt polynomials as mysterious. But historically, this is not the case. The setting is that of the investigations by Helmut Hasse and his students and collaborators into the structure of complete discrete valuation rings A with residue field k. Oswald Teichmüller discovered that in such a situation there is a multiplicative system of representatives, i.e., a multiplicative section of the natural projection $A \to k$. Such a system is unique if k is perfect. These are now called Teichmüller lifts. Every element of A can be written as a power series with coefficients from any chosen system of representatives. As they are already multiplicative the first problem was to figure out how Teichmüller representatives should be added in the arithmetic of the ring. In unequal case, this is a very difficult problem. Teicmüller found a formula for doing this. The formula is,

$$[a] + [b] = \sum [s_n] p^n$$

where $[-]$ denotes Teichmüller representatives and $s_n = r_n(a^{1/p^n}, b^{1/p^n})$ such that

$$r_0(x,y)^{p^n} + pr_1(x,y)^{p^{n-1}} + \ldots + p^n r_n(x,y) = x^{p^n} + y^{p^n}.$$

And here this coefficients coincide with the p-adic Witt polynomials on the left handside of the above equation. After Witt vectors, we describe the de Rham-Witt complex which is a projective system of diferential graded algebras that provides a complex which is explicit and computable. In degree 0, it is the Witt vectors and the first object in the inverse limit is the de Rham complex. Thus the de Rham-Witt complex combines the Witt vectors and the de Rham complex.

2 Preliminaries

Throughout this study, a ring is commutative ring with unity.

2.1 Kähler Differentials

This is an algebraic generalization of differential forms on a manifold.
Let A be a ring and M be an A-module. A Derivation from A to M is a map

$$D : A \longrightarrow M$$

satisfying

$$D(a+b) = D(a) + D(b) \quad \text{and} \quad D(ab) = aD(b) + bD(a)$$

The set of derivations from A to M is denoted as $\mathrm{Der}(A, M)$. Let A be k-algebra and $f : k \longrightarrow A$, we say D is a k-derivation if $D \circ f = 0$.
Note that $D(1 \cdot 1) = D(1) + D(1) = 2D(1)$ and we obtain $D(1) = 0$. So any derivation is a $\mathbb{Z}$-derivation. Now, assume that A is a k-algebra. Define

$$\mu : A \otimes_k A \longrightarrow A$$

$$x \otimes y \mapsto xy.$$

Then μ is a surjective k-algebra homomorphism. Set $I = \ker(\mu)$, $\Omega^1_{A/k} = I/I^2$ and $B = A \otimes_k A/I^2$. Then μ induces

$$\mu' : B \longrightarrow A$$

and we have the exact sequence

$$0 \longrightarrow {\Omega^1}_{A/k} \longrightarrow B \longrightarrow A \longrightarrow 0$$

Define $\lambda_1 : A \longrightarrow B$ by and $\lambda_2 : A \longrightarrow B$ by $a \mapsto 1 \otimes a \pmod{I^2}$ and by $a \mapsto a \otimes 1 \pmod{I^2}$ respectively. Then $\mu'(\lambda_i(a)) = a$ for $i = 1, 2$.
Set $d = \lambda_1 - \lambda_2 : A \longrightarrow \Omega^1_{A/k}$. Firstly, $\Omega^1_{A/k}$ has the A-module structure induced by multiplication by $a \otimes 1 \pmod I$ in $A \otimes A$. i.e., $a \cdot x := (a \otimes 1) \pmod I \cdot x$ for $a \in A$ and

$x \in \Omega^1_{A/k}$. Note that this multiplication can also be defined by using $1 \otimes a$ instead of $a \otimes 1$, since the difference of these two element is in I. Then d is a derivation.

$$\begin{aligned} d(aa') &= \lambda_1(a)\lambda_1(a') - \lambda_2(a)\lambda_2(a') \\ &= \lambda_1(a)\lambda_1(a') - \lambda_1(a)\lambda_2(a') + \lambda_1(a)\lambda_2(a') - \lambda_2(a)\lambda_2(a') \\ &= \lambda_1(a)((\lambda_1 - \lambda_2)(a)) + \lambda_2(a')((\lambda_1 - \lambda_2)(a)) \\ &= a \cdot da' + a' \cdot da \end{aligned}$$

Now we will prove that $(\Omega^1_{A/k}, d)$ satisfies the following universal property : For any A- module M and any derivation $D \in \mathrm{Der}_k(A, M)$, there exist a unique A-linear map $f : \Omega^1_{A/k} \longrightarrow M$ such that $D = f \circ d$.

Let D be in $\mathrm{Der}_k(A, M)$ and we define

$$\varphi : A \otimes_k A \longrightarrow A * M$$

by

$$\varphi(x \otimes y) = (xy, xDy)$$

where $A * M := A \oplus M$ is a k-algebra with multiplication $(a, x) \cdot (a', b') = (aa', ax' + a'x)$ for $a, a' \in A$ and $x, x' \in N$. Then φ is a homomorphism of k-algebras.

$$\begin{aligned} \varphi((a \otimes b)(a' \otimes b')) = \varphi(aa' \otimes bb') &= (aa'bb', aa'D(bb')) \\ &= (aa'bb', aa'bDb' + aa'b'Db) \\ &= (ab, aDb)(a'b', a'Db') \end{aligned}$$

Now, let $\sum_i x_i \otimes y_i \in ker(\mu)$, then

$$\varphi\left(\sum_i x_i \otimes y_i\right) = \left(\sum_i x_i y_i, \sum_i x_i D y_i\right) = \left(0, \sum_i x_i D y_i\right)$$

and since $(0, a)(0, b) = (0, 0)$ for any $a, b \in M$, $\varphi(I^2) = 0$. Therefore φ induce a map

$$f : \Omega^1_{A/k} \longrightarrow M$$

$$f(da) = f(1 \otimes a - a \otimes 1 \pmod{I^2}) = \varphi(1 \otimes a) - \varphi(a \otimes 1)$$
$$= (a, Da) - (a, aD1) = Da$$

So $D = f \circ d$. If $\xi = \sum_i x_i \otimes y_i \pmod{I^2} \in \Omega^1_{A/k}$, then

$$f(a\xi) = f(\sum_i ax_i \otimes y_i \pmod{I^2}) = \sum_i ax_i Dy_i = af(\xi).$$

So f is A-linear. Next thing to show is $\Omega^1_{A/k}$ is generated as an A-module by the set $\{da | a \in A\}$. First we have

$$a \otimes a' = (a \otimes 1)(1 \otimes a' - a' \otimes 1) + aa' \otimes 1 \tag{2.1.1}$$

so that if $\omega = \sum_i x_i \otimes y_i \in I$, then

$$\omega \pmod{I^2} = \sum_i (x_i \otimes 1)(1 \otimes y_i - y_i \otimes 1) + \sum_i x_i y_i \otimes 1 \pmod{I^2} \quad \text{by equation(1.1.3)}$$
$$= \sum_i x_i dy_i.$$

Hence $\Omega^1_{A/k}$ is generated as an A-module by $\{da | a \in A\}$.

The A-module we have just obtained is called Kähler Differentials and for $a \in A$ the element da is called differential of a. From the definition, we see that

$$\mathrm{Der}_k(A, M) \cong \mathrm{Hom}_A(\Omega^1_{A/k}).$$

Example.

If A is generated as a k-algebra by a subset $U \subset A$, then $\Omega^1_{A/k}$ is generated as an A-module by $\{da|\ a \in U\}$. Indeed, if $a \in A$, then there exist $a_i \in U$ and a polynomial $f(x) \in k[x_1, \ldots, x_n]$ such that $a = f(a_1, \ldots, a_n)$. We have

$$da = d(f(a_1, \ldots, a_n) = \sum_i f_i(a_1, \ldots, a_n) da_i$$

where $f_i = \partial f / \partial x_i$. Then consider $\Lambda\Omega^1_C$. We take here the definition of exterior algebra

$\Lambda(\Omega_C{}^1)$ as :

$$\Lambda\Omega_C^1 := (T\Omega_C^1)/\{x \otimes y + y \otimes x |\ x, y \in \Omega_C^1\}$$

where $T(\Omega_C^1)$ denotes the tensor algebra over Ω_C^1.

2.2 Direct and Inverse Limits

We will give universal properties of inverse and direct limits in the ring category.

2.2.1 Direct Limit

Let us start with the definition of a directed system of rings and homomorphisms. Let $< I, \leq >$ be a partially ordered set with the property that for every $i, j \in I$, there exist $k \in I$ with $i \leq k$ and $j \leq k$. Then we say $< I, \leq >$ is a directed set. Let $\{A_i |\ i \in I\}$ be a family of rings indexed by I and $f_{ij} : A_i \to A_j$ be homomorphism for all $i \leq j$ with the following properties:

(i) f_{ii} is the identity homomorphism of A_i.

(ii) $f_{ik} = f_{jk} \circ f_{ij}$ for all $i \leq j \leq k$.

Then the pair $< A_i, f_{ij} >$ is called a directed system over I. The direct limit of the directed system $< A_i, f_{ij} >$ denoted as

$$\varinjlim A_i := \coprod_i A_i / \sim$$

where for $a_i \in A_i$, $a_i \sim a_j$ if there is some $k \in I$ such that $f_{ik}(a_i) = f_{jk}(a_j)$.

2.2.2 Inverse limit

We start with the definition of an inverse (or projective) system of rings and homomorphisms. Let $(I, \leq)$ be a directed partially ordered set. Let $(A_i)_{i \in I}$ be a family of rings and suppose we have a family of homomorphisms $f_{ij} : A_j \to A_i$ for all $i \leq j$ with the following properties:

(i) f_{ii} is the identity in A_i,

(ii)$f_{ik} = f_{ij} o f_{jk}$ for all $i \leq j \leq k$.

Then the pair $((A_i)_{i \in I}, (f_{ij})_{i,j \in I})$ is called an inverse system of rings and morphisms over

I, and the morphisms f_{ij} are called the transition morphisms of the system. We define the inverse limit of the inverse system $((A_i), f_{ij})$ as a particular subring of the direct product of the A_i's:

$$\varprojlim A_i := \{a \in \prod_{i \in I} A_i |\ a_i = f_{ij}(a_j) \text{ for all } i \leq j\}$$

2.3 String p-Rings

Definition 2.3.1. A ring R is strict p-ring if it is Hausdorff and complete for the topology defined by its p-adic filtration and its residue ring A/p is perfect ring of characteristic p.

Proposition 2.3.2. *Let A be a strict p- ring. Then :*

(i) There exist one and only one system of representatives $\tau : \bar{K} \to A$ which commutes with pth powers : $\tau(\lambda^p) = \tau(\lambda)^p$ for all $\lambda \in \bar{K}$.

(ii) In order that $a \in A$ belong to $S = \tau(\bar{K})$, it is necessary and sufficient that a be a p^nth power for all $n \geq 0$.

(iii) This system of representatives is multiplicative, i.e., one has $\tau(\lambda\mu) = \tau(\lambda)\tau(\mu)$ for all $\lambda, \mu \in \bar{K}$.

Proof. Denote $\bar{K} = k$. Let $\lambda \in k$ and set

$$L_n = \{x \in A |\ x \equiv \lambda^{p^{-n}} \pmod p\}$$

$$U_n = \{x^{p^n} |\ x \in L_n\}$$

for all $n \geq 0$.

Let $x \in U_n$. By definition of U_n, $x = y^{p^n}$ for some $y \in L_n$. Then $y \equiv \lambda^{p^{-n}} \pmod p$. This implies $x = y^{p^n} \equiv \lambda (\text{mod } p)$. So $x \in L_0$ and U_n is contained in L_0 for all n. Also U_n's form a decreasing sequence. $x^{p^{n+1}} \in U_{n+1}$ gives $x \equiv \lambda^{p^{-n-1}} \pmod p$ and taking p'th power, $x^p \equiv \lambda^{p^{-n}} (\text{mod p})$ and then $x^p \in L_n$ and $x^{p^{n+1}} \in U_n$. We will show U_n's form a Cauchy filter base, but first we should give the definition of a Cauchy filter base and give some properties.

Definition 2.3.3. Let S be a set and $P(S)$ be the set of all subsets of S. Then $B \subset P(S)$ with the following properties

(i) Intersection of two set of B contains a set of B.

(ii) B is non-empty and empty set is not in B.

is called filter base for S.

Definition 2.3.4. In a topological ring A, a subset S of A is V-small if $x - y \in V$ for all $x, y \in S$ where V is neighborhood of 0. A filter base is Cauchy if it contains a V-small set for every neighborhood V of 0. We say a filter base converges to an element x of A if for any neighborhood V of x, there exist $\beta \in B$ such that $\beta \subset V$.

Since $\{U_n\}$ satisfies above properties, it forms a Cauchy filter base. We will define $\tau(\lambda) = \lim U_n$. But before we need to show this limit exist and it is unique.
In general, in a complete topological ring A, a Cauchy filter base converges :
Let V_n be neighborhood basis of 0. Since filter base is cauchy, for every V_n, there exist V_n-small sets $F_n \in B$. Let

$$x_n \in \bigcap_{k=1}^{n} F_n$$

There exist such an element since a subset of this intersection must be in B and empty set is not in B, it is not empty. If $m \geq n$ and $s \geq n$, x_s and x_m lies in F_n and by definition of F_n, $x_m - x_s \in V_n$,i.e., $\{x_n\}_n$ is a Cauchy sequence in A and A is complete implies $\{x_n\}$ converges to an element x in A. Now take a neighborhood of x, namely $x + V_p$ where V_p is a neighborhood of 0. Then there is an $N \in \mathbb{N}$ such that for all $m \geq N$,

$$x_m \in x + V_p.$$

For any $c \in F_N$ and $m \geq N$,

$$c = c - x_m + x_m - x + x \in V_N + V_p + x.$$

If necessary, choose N bigger than p, then $c \in V_p + x$ i.e $F_N \subseteq V_p + x$ and B converges to x. In addition if topology on A is Hausdorff, then limit is unique. Otherwise let x and y be limits of this filter base. Then we can find two distinct neighborhoods of x and y. Their intersection is emtpy and it must be in B, which is a contradiction.

Define $\tau(\lambda) = \lim U_n(\lambda)$. This defines a system of representatives. If $\lambda = \mu^p$, the pth power operation in A maps $U_n(\mu)$ to $U_{n+1}(\lambda)$. For $x^{p^n} \in U_n(\mu)$,

$$x \equiv \mu^{p^{-n}} \pmod p,$$

$$x \equiv \lambda^{p^{-n-1}} \pmod p,$$

$$x \in L_{n+1}(\lambda),$$

$$(x^{p^n})^p \in U_{n+1}(\lambda).$$

$$\tau(\mu)^p = (\lim U_n(\mu))^p = \lim U_{n+1}(\lambda) = \tau(\lambda) = \tau(\mu^p).$$

If f is a system of representatives having this property, $f(\lambda)$ is p^nth power for all n, since k is perfect. Hence $f(\lambda) \in U_n$ for all n. Then for any neighborhood U of $f(\lambda)$, there is some U_k such that $U_k \subset U$. So $f(\lambda)$ is the limit of $\{U_n\}$. This shows (i) and (ii). If x and y are p^nth power, then xy is also. So $\tau(x)\tau(y)$ is again a representative and since it is equivalent to $xy \pmod p$, it is equal to $\tau(xy)$.

□

Proposition 2.3.5. *Every element a in a string p-ring A can be written uniquely as a convergent series*

$$a = \sum_{n=0}^{\infty} s_n \pi^n, \textit{ with } s_n \in S.$$

Proof. Let $a \in A$. By definition of S, there is an $s_0 \in S$ such that $a \equiv s_0 \pmod p$. If we write $a = s_0 + a_0\pi$ and apply the same procedure we obtain s_1 such that

$$a = s_0 + s_1\pi + a_2\pi^2$$

Continuing this process, we obtain s_n's for all n. The series $\sum_{n=0}^{\infty} s_n\pi^n$ converges to a. Set $S_n = \sum_{i=0}^{n} s_i\pi^i$. For any neighborhood U of 0, there is an N such that $p^N \subseteq U$. Now for all $n, m \geq N$, $S_m - S_n \in p^{n+1} \subseteq p^N \subseteq U$. $\{S_n\}_n$ is a Cauchy sequence in A and since A is complete, the series $\sum s_n\pi^n$ converges to a. Since A is Hausdorff, the limit is unique. Conversely, every series of the form $\sum s_n\pi^n$ converges, since its general term converges to zero and A is complete. □

3 Witt Vectors

3.1 Motivation

Let A be a strict p-ring with residue field k and denote $\tau(a) = [a]$. Suppose

$$\sum_{n=0}^{\infty}[a_n]p^n + \sum_{n=0}^{\infty}[b_n]p^n = \sum_{n=0}^{\infty}[s_n]p^n \tag{3.1.1}$$

We will try to determine s_n in terms of a_i, b_i's inductively. Before that, let us give a lemma which will be useful later.

Lemma 3.1.1. *If $a \equiv b \pmod p$, then $a^{p^n} \equiv b^{p^n} \pmod{p^{n+1}}$.*

Proof. We proceed by induction on n. When $n = 0$, Lemma is clear. So assume the lemma is true for $n-1$. Then $a \equiv b \pmod p$ and by induction hypothesis $a^{p^{n-1}} \equiv b^{p^{n-1}} \pmod{p^n}$.

$$a^{p^n} = (a^{p^{n-1}})^p = (b^{p^{n-1}} + p^n x)^p = b^{p^n} + \sum_{i=0}^{p-1}\binom{p}{i} a^{ip^{n-1}}(p^n x)^{p-i} \equiv b^{p^n} \pmod{p^{n+1}}.$$

since $\binom{p}{i}$ is divisible by p for all i. □

We will begin with finding the sum of two Teichmüller lifts.
Now suppose

$$[a_0] + [b_0] = \sum_{n=0}^{\infty}[s_n]p^n \tag{3.1.2}$$

Then

$$[a_0] + [b_0] \equiv [s_0] \pmod p,$$

$$a_0 + b_0 = s_0,$$

since $[x] \equiv x \pmod p$ for all $x \in k$. Now we will find s_1 in the Equation(2.1.1) . To do this, we should look at the Equation(2.1.2) modulo p^2. So we have

$$\begin{aligned}
[a_0] + [b_0] &\equiv [s_0] + [s_1]p && \pmod{p^2},\\
[s_1]p &\equiv [a_0] + [b_0] - [a_0 + b_0] && \pmod{p^2},\\
[s_1]p &\equiv [a_0^{1/p}]^p + [b_0^{1/p}]^p - [a_0^{1/p} + b_0^{1/p}]^p && \pmod{p^2}.
\end{aligned}$$

Since $[x]+[y]\equiv[x+y] \pmod p$ for all $x,y\in k$ and $a_0^{1/p}+b_0^{1/p}=(a_0+b_0)^{1/p}$, we have

$$([x]+[y])^p\equiv[x+y]^p \pmod{p^2} \text{ by Lemma(2.1.1)}$$

and we obtain

$$\begin{aligned}
[s_1]p &\equiv [a_0^{1/p}]^p+[b_0^{1/p}]^p-([a_0^{1/p}]+[b_0^{1/p}])^p && \pmod{p^2}\\
[s_1]p &\equiv -\sum_{i=1}^{p-1}\binom{p}{i}[a_0]^{\frac{p-i}{p}}[b_0]^{\frac{i}{p}} && \pmod{p^2}
\end{aligned}$$

Since $\binom{p}{i}$ is divisible by p,

$$\begin{aligned}
[s_1] &\equiv -\sum_{i=1}^{p-1}\frac{1}{p}\binom{p}{i}[a_0]^{\frac{p-i}{p}}[b_0]^{\frac{i}{p}} && \pmod p\\
s_1 &= -\sum_{i=1}^{p-1}\frac{1}{p}\binom{p}{i}a_0^{\frac{p-i}{p}}b_0^{\frac{i}{p}}
\end{aligned}$$

And the next step is to find s_2 and to determine this coefficient, we will look at the Equation(2.1.2) modulo p^3.

$$\begin{aligned}
[a_0]+[b_0] &\equiv [s_0]+[s_1]p+[s_2]p^2 && \pmod{p^3}\\
[s_2]p^2 &\equiv [a_0]+[b_0]-[a_0+b_0]-\left[-\sum_{i=1}^{p-1}\frac{1}{p}\binom{p}{i}a_0^{\frac{p-i}{p}}b_0^{\frac{i}{p}}\right]p && \pmod{p^3}\\
[s_2]p^2 &\equiv [a_0^{1/p^2}]^{p^2}+[b_0^{1/p^2}]^{p^2}-\left([a_0^{1/p^2}]+[b_0^{1/p^2}]\right)^{p^2}\\
&\quad -(-1)^p\left(\sum_{i=1}^{p-1}\frac{1}{p}\binom{p}{i}[a_0^{\frac{p-i}{p^2}}][b_0^{\frac{i}{p^2}}]\right)^p p && \pmod{p^3}
\end{aligned}$$

We used here that

$$\begin{aligned}
&[a+b]\equiv[a]+[b]\\
&[a+b]^p\equiv([a]+[b])^p \pmod{p^2} \quad \text{for any} \quad a,b\in k.
\end{aligned}$$

$$[s_2]p^2\equiv-\sum_{i=1}^{p^2-1}\binom{p^2}{i}[a_0]^{\frac{p^2-i}{p^2}}[b_0]^{\frac{i}{p^2}}-(-1)^p\left(\sum_{i=1}^{p-1}\frac{1}{p}\binom{p}{i}[a_0^{\frac{p-i}{p^2}}][b_0^{\frac{i}{p^2}}]\right)^p p \pmod{p^3}$$

To find s_2, we must divide above expression by p^2.

Every term other than terms with coefficients $\binom{p^2}{kp}$ and $((\binom{p}{i}/p)^p p$ is divisible by p^2.

But we have

$$\binom{p^2}{kp} \equiv \left(\frac{\binom{p}{k}}{p}\right)^p p \pmod{p^2} \text{ for } k = 1, \dots, p-1.$$

First, we will show

$$\binom{p^2}{kp} \equiv \binom{p}{k} \pmod{p^2} \tag{3.1.3}$$

$$\binom{p^2}{kp} = \frac{p^2 \cdot (p^2-1)\dots(p^2-p)\dots(p^2-2p)\dots(p^2-(k-1)p)\dots(p^2-kp+1)}{1\cdot 2\cdot 3\dots p\cdot(p+1)\dots(2p)\dots((k-1)p)\dots(kp-1)\cdot(kp)}$$

In above expression, in numerator the only numbers divisible by p are $p^2 - np$, for $n = 1, \dots, (k-1)$. Also in denominator, numbers divisible by p are np for $n = 1, \dots, (k-1)$. So after doing cancellations, we have

$$\frac{\prod_1^{(k-1)}(p-n)}{\prod_1^{(k-1)} n} = \binom{p}{k}$$

and remaining terms

$$\frac{(p^2-1)\dots(p^2-(p-1))\cdot(p^2-(p+1))\dots(p^2-(kp-1))}{1\cdot 2\cdot 3\cdot(p-1)\cdot(p+1)\dots(kp-1)} \equiv 1 \pmod{p^2}$$

Now, we have showed (2.1.3).

$$\frac{\binom{p^2}{kp}}{p} \equiv \frac{\binom{p}{k}}{p} \pmod{p},$$

By Fermat's Little Theorem, we have

$$\frac{\binom{p}{k}}{p} \equiv \left(\frac{\binom{p}{k}}{p}\right)^p \pmod{p},$$

finally combining previous two raw together, we obtain

$$\frac{\binom{p^2}{kp}}{p} \equiv \left(\frac{\binom{p}{k}}{p}\right)^p \pmod{p}$$

Multiplying the last row by p, we obtain

$$\binom{p^2}{kp} \equiv \left(\frac{\binom{p}{k}}{p}\right)^p p \pmod{p^2}$$

So, if p is odd,

$$[s_2] \equiv \frac{1}{p^2}\left(-\sum_{i=1}^{p^2-1}\binom{p^2}{i}[a_0]^{\frac{p^2-i}{p^2}}[b_0]^{\frac{i}{p^2}} + \left(\sum_{i=1}^{p-1}\frac{1}{p}\binom{p}{i}[a_0^{\frac{p-i}{p^2}}][b_0^{\frac{i}{p^2}}]\right)^p p\right) \pmod{p}$$

Now we are in general case.

Note that s_n's are unique for $a_0, \dots a_n$ and $b_0, \dots b_n$. After now, we will use the notation $s_n(a,b)$ for the coefficients in the sum $[a]+[b]$ to avoid any confuse. Let us begin with equation

$$\sum_{n=0}^{\infty}[a_n]p^n + \sum_{n=0}^{\infty}[b_n]p^n = \sum_{n=0}^{\infty}[k_n]p^n. \tag{3.1.4}$$

$$\begin{aligned} a+b \equiv [a_0]+[b_0] &\equiv a_0+b_0 \pmod{p} \\ k_0 &= a_0+b_0 \end{aligned}$$

Looking at Equation (2.1.4) modulo p^2, we have

$$\begin{aligned} [a_0]+[a_1]p+[b_0]+[b_1]p &\equiv [a_0+b_0]+[k_1]p \pmod{p^2} \\ [s_0(a_0,b_0)]+[s_1(a_0,b_0)]p+p[s_0(a_1,b_1)] &\equiv [a_0+b_0]+[k_1]p \pmod{p^2} \\ [s_1(a_0,b_0)]p+p[s_0(a_1,b_1)] &\equiv [k_1]p \pmod{p^2} \\ [k_1]p &\equiv ([s_1(a_0,b_0)]+[s_0(a_1,b_1)])p \pmod{p^2}. \end{aligned}$$

Dividing the last equation by p,

$$k_1 = a_1 + b_1 - \sum_{i=1}^{p-1}\frac{1}{p}\binom{p}{i}a_0^{\frac{p-i}{p}}b_0^{\frac{i}{p}}$$

We see that finding coefficients of sum of two series is not so easy even sum of two Teichmüller lift. But there is another way that gives these coefficients and this is discovered by Ernst Witt.

Now, let X_i, Y_i be indeterminants. Now consider the polynomial

$$w_n(X_0, X_1, \ldots, X_n) = \sum_{i=0}^{n} p^i X_0^{p^{n-i}} \quad \text{for all} \quad n.$$

We can find S_n which satisfies the equation

$$w_n(X_0, X_1, \ldots, X_n) + w_n(Y_0, Y_1, \ldots, Y_n) = w_n(S_0, S_1, \ldots, S_n)$$

for all n inductively. Since the term in the equation involving S_n is $p^n S_n$, S_n's are polynomials of $X_0, \ldots, X_n, Y_0, \ldots, Y_n$ with rational coefficients.

Call $S_n = \varphi_n(X_0, \ldots, X_n; Y_0, \ldots, Y_n)$. Next proposition gives relation with φ_n and s_n in the Equation (2.1.1).

Proposition 3.1.2. *Let A be complete DVR with perfect residue field k of characteristic p and*

$$\sum_{i=0}^{\infty} [a_i] p^i + \sum_{i=0}^{\infty} [b_i] p^i = \sum_{i=0}^{\infty} [s_i] p^i$$

Set

$$r_i = \varphi_i(a_0^{1/p^i}, \ldots, a_j^{1/p^{i-j}}, \ldots, a_i; b_0^{1/p^i}, \ldots, b_j^{1/p^{i-j}}, \ldots, b_i), \quad a_i, b_i \in k$$

where

$$W_n(X_0, \ldots, X_n) + W_n(Y_0, \ldots, Y_n) = W_n(\varphi_0(X_0; Y_0), \ldots, \varphi_n(X_0, \ldots, X_n; Y_0, Y_1, \ldots, Y_n))$$

Then $r_i = s_i$.

Proof.

$$\begin{aligned} r_i^{1/p^{n-i}} &= \varphi_i(a_0^{1/p^n}, \ldots, a_j^{1/p^{n-j}}, \ldots, a_i^{1/p^{n-i}}; b_0^{1/p^n}, \ldots, b_j^{1/p^{n-j}}, \ldots, b_i^{1/p^{n-i}}) \\ [r_i^{1/p^{n-i}}] &\equiv \varphi_i([a_0^{1/p^n}], \ldots, [a_i^{1/p^{n-i}}]; [b_0^{1/p^n}], \ldots, [b_i^{1/p^{n-i}}]) && \pmod p \\ [r_i^{1/p^{n-i}}]^{p^{n-i}} &\equiv \varphi_i^{p^{n-i}}([a_0^{1/p^n}], \ldots, [a_i]^{1/p^{n-i}}; [b_0]^{1/p^n}, \ldots, [b_i]^{1/p^{n-i}}) && \pmod{p^{n-i+1}} \end{aligned}$$

Multiplying by p^i,

$$p^i[r_i] \equiv p^i \varphi_i^{p^{n-i}}([a_0^{1/p^n}], \ldots, [a_i]^{1/p^{n-i}}; [b_0]^{1/p^n}, \ldots, [b_i]^{1/p^{n-i}}) \pmod{p^{n+1}}$$

Evaluating φ_i's at $X_i = [a_i]^{1/p^{n-i}}$, $Y_i = [b_i]^{1/p^{n-i}}$, we obtain

$$[a_0^{1/p^n}]^{p^n} + p[a_1^{1/p^{n-1}}]^{p^{n-1}} + \ldots + p^n[a_n] + [b_0^{1/p^n}]^{p^n} + p[b_1^{1/p^{n-1}}]^{p^{n-1}} + \ldots + p^n[b_n]$$

$$= \varphi_0^{p^n}([a_0^{1/p^n}]; [b_0^{1/p^n}]) + \ldots + p^n \varphi_n([a_0^{1/p^n}], \ldots, [a_n]; [b_0^{1/p^n}], \ldots, [b_n])$$

$$[a_0] + \ldots + [a_n]p^n + [b_0] + \ldots + [b_n]p^n \equiv [r_0] + [r_1]p + \ldots + [r_n]p^n \pmod{p^{n+1}}$$

$$\sum_{i=0}^{n} [a_i]p^i + \sum_{i=0}^{n} [b_i]p^i \equiv \sum_{i=0}^{n} [r_i]p^i \equiv \sum_{i=0}^{n} [s_i]p^i \pmod{p^{n+1}}$$

We will show $r_n = s_n$ for all n by induction on n. For $n = 0$,

$$[r_0] \equiv [s_0] \pmod{p}$$

$$r_0 = s_0$$

Assume $r_i = s_i$ for $i \leq n - 1$.

$$[r_0] + [r_1]p + \ldots + [r_n]p^n \equiv [s_0] + [s_1]p + \ldots + [s_n]p^n \qquad \pmod{p^{n+1}}$$

$$p^n[r_n] \equiv p^n[s_n] \qquad \pmod{p^{n+1}}$$

Dividing by p^n,

$$[r_n] \equiv [s_n] \qquad \pmod{p}$$

$$r_n = s_n$$

$$s_n = \varphi_n(a_0^{1/p^n}, \ldots, a_i^{1/p^{n-i}}, \ldots, a_n; b_0^{1/p^n}, \ldots, b_i^{1/p^{n-i}}, \ldots, b_n)$$

□

3.2 Witt Vectors

Let $\mathbb{N}$ be the set of positive integers, and S be a subset of $\mathbb{N}$ with the property that, if $n \in S$, and if d is a divisor of n, then $d \in S$. We then say that S is a truncation set. $\mathbb{W}_S(A)$ is the set A^S equipped with a ring structure such that the ghost map

$$w : \mathbb{W}_S(A) \to A^S$$

$$(a_n | n \in S) \mapsto (w_n(a) | n \in S),$$

where

$$w_n(a) = \sum_{d|n} d a_d^{n/d}$$

is natural transformation of functors from the category of rings to rings. Here A^S is considered to be a ring with componentwise addition and multiplication.

Lemma 3.2.1. *Suppose that for every prime p, there exist a ring homomorphism $\phi_p : A \to A$ with the property that $\phi_p(a) \equiv a^p \bmod pA$. Then a sequence $(x_n)_{n\in S}$ is in the image of the ghost map*

$$w : \mathbb{W}_S(A) \to A^S$$

if and only if $x_n \equiv \phi_p(x_{n/p}) \pmod{p^{\upsilon_p(n)} A}$, for every prime p, and for every $n \in S$ with $\upsilon_p(n) \geq 1$. Here $\upsilon_p(n)$ denotes the p-adic valuation.

Proof. Assume $x_n = w_n(a)$ for some $a \in \mathbb{W}_S(A)$. Then we have

$$\phi_p(w_{n/p}(a)) = \phi_p(\sum_{d|(n/p)} d a_d^{n/pd}) = \sum_{d|(n/p)} d\phi_p(a_d)^{n/pd} \tag{3.2.1}$$

since $\phi_p(a_d) \equiv a_d^p \pmod{pA}$,

$$\begin{aligned} \phi_p(a_d)^{n/pd} &\equiv a_d^{n/d} && \pmod{p^{\upsilon_p(n)-\upsilon_p(d)} A} \\ d\phi_p(a_d)^{n/pd} &\equiv d a_d^{n/d} && \pmod{p^{\upsilon_p(n)} A} \\ \sum_{d|(n/p)} d\phi_p(a_d)^{n/pd} &\equiv \sum_{d|(n/p)} d a_d^{n/d} && \pmod{p^{\upsilon_p(n)} A} \\ \sum_{d|(n/p)} d a_d^{n/d} &\equiv \phi_p(w_{n/p}(a)) && \pmod{p^{\upsilon_p(n)} A} \end{aligned} \tag{3.2.2}$$

Let $d \in \mathbb{N}$ such that $d|n$ and $d \nmid (n/p)$. Write $d = p^{\upsilon_p(d)}.d'$ where d' is relatively prime to p. Then $p^{\upsilon_p(d)}|(n/d')$ and does not divide (n/pd'). So $\upsilon_p(d) = \upsilon_p(n/d') = \upsilon_p(n)$. Now we have

$$\sum_{d|n, d\nmid(n/p)} da_d^{n/d} \equiv 0 \pmod{p^{\upsilon_p(n)}A},$$

$$w_n(a) = \sum_{d|n} da_d^{n/d} = \sum_{d|(n/p)} da_d^{n/d} + \sum_{d|n,d\nmid(n/p)} da_d^{n/d} \equiv \sum_{d|(n/p)} da_d^{n/d} \pmod{p^{\upsilon_p(n)}A},$$

$$\phi_p(w_{n/p}(a)) \equiv w_n(a) \pmod{p^{\upsilon_p(n)}A}$$

by equation 2.2.2. Conversely, if $(x_n|n \in S) \in A^S$ such that $x_n \equiv \phi_p(x_{n/p}) \pmod{p^{\upsilon_p(n)}A}$. We want to find an $a = (a_n)_{n\in S}$ such that $w_n(a) = x_n$ for all $n \in S$. Let $a_1 = x_1$, and assume for all d/n we have chosen a_d such that $w_d(a) = x_d$.

$$\begin{aligned} x_n \equiv \phi_p(x_{n/p}) = \phi_p(w_{n/p}(a)) = \sum_{d|(n/p)} d\phi_p(a_d)^{n/pd} \equiv \sum_{d|(n/p)} da_d^{n/d} \qquad &\pmod{p^{\upsilon_p(n)}A} \\ \equiv \sum_{d|(n/p)} da_d^{n/d} \equiv \sum_{d|n,d\neq n} da_d^{n/d} \qquad &\pmod{p^{\upsilon_p(n)}A} \end{aligned}$$

Then

$$x_n \equiv \sum_{d|n,d\neq n} da_d^{n/d} \pmod{p^{\upsilon_p(n)}A},$$

for all p dividing n. So by Chinese remainder theorem,

$$x_n - \sum_{d|n,d\neq n} da_d^{n/d} \equiv 0 \pmod{n}$$

Here, the important thing is that above expression is true for all p. Now, we can chose an $a_n \in A$ such that this difference is equal to na_n.

$$x_n = w_n(a)$$

□

Proposition 3.2.2. *There exist a unique ring structure such that ghost map*

$$w : \mathbb{W}_S(A) \to A^S$$

is a natural transformation of functors from rings to rings.

Proof. Assume $A = \mathbb{Z}[x_n; y_n | n \in S]$. We have the map

$$\phi_p : A \to A$$

$$x_n \mapsto x_n^p$$

$$y_n \mapsto y_n^p$$

For any $f \in A$, we have $\phi_p(f) \equiv f^p \pmod{pA}$. Since ϕ_p is additive,

$$\phi_p(w_{n/p}(x)) + \phi_p(w_{n/p}(y)) = \phi_p(w_{n/p}(x) + w_{n/p}(y)).$$

Then

$$w_n(x) + w_n(y) \equiv \phi_p(w_{n/p}(x) + w_{n/p}(y)).$$

So $w_n(x)+w_n(y)$ is in the image of the ghost map by Lemma 3.2.1. Repeating this argument for multiplication, we see that there exist polynomials $\varphi_n(x, y)$ and $\phi_n(x, y)$ such that

$$w_n(x) + w_n(y) = w_n(\varphi(x, y)),$$
$$w_n(x)w_n(y) = w_n(\phi(x, y)).$$

Furthermore these polynomials are unique. If $w_n(x) = w_n(y)$, then $w_1(x) = x_1 = w_1(y) = y_1$. Assume for all $d|n$, $x_d = y_d$. Then

$$\sum_{d|n} dx_d^{n/d} = \sum_{d|n, d\neq n} dx_d^{n/d} + ns_n = \sum_{d|n} dy_d^{n/d} + ny_n = w_n(k),$$

$$nx_n = ny_n.$$

Since A is a torsion free ring, we can cancel n's and we get

$$x_n = y_n$$

So the ghost map is injective when A is torsion free. Let A be any ring and a_n, $b_n \in A$. Let τ be the ring homorphism ,

$$\tau : \mathbb{Z}[x_n; y_n | n \in S] \to A$$

$$\tau : x_n \mapsto a_n, y_n \mapsto b_n$$

Then define addition and multiplication in $\mathbb{W}_S(A)$ as

$$(a_n)_{n\in S} + (b_n)_{n\in S} := (\tau(\varphi_n(x, y))_{n\in S},$$
$$(a_n)_{n\in S}(b_n)_{n\in S} := (\tau(\phi_n(x, y))_{n\in S}.$$

$\mathbb{W}_S(A)$ forms a commutative ring with addition and multiplication defined above. We will only show associativity of addition. First assume $A = \mathbb{Z}[x_n; y_n; z_n | n \in S]$. Then $(x + y) + z = \varphi(x, y) + z = \varphi(\varphi(x, y), z)$ and $x + (y + z) = x + \varphi(y, z) = \varphi(x, \varphi(y, z))$.

$$(w_n(x) + w_n(y)) + w_n(z) = w_n(\varphi(x, y)) + w_n(z) = w_n(\varphi(\varphi(x, y), z))$$
$$w_n(x) + (w_n(y) + w_n(z)) = w_n(x) + w_n(\varphi(y, z) = w_n(\varphi(x, \varphi(y, z)))$$
$$w_n(\varphi(\varphi(x, y), z)) = w_n(\varphi(x, \varphi(y, z)))$$
$$\varphi(\varphi(x, y), z) = \varphi(x, \varphi(y, z))$$
$$(x + y) + z = x + (y + z)$$

Finally, for an arbitrary ring A, $\tau(\varphi_n(\varphi(x, y), z)) = \tau(\varphi_n(x, \varphi(y, z)))$. □

The set A^S equiped with the ring structure given in the Lemma(3.2.2) is called big Witt Vectors.

3.2.1 Verschiebung, Frobenius and Teichmüller Lift

Define

$$[-] : A \longrightarrow \mathbb{W}_S(A)$$

such that

$$[a]_n = \begin{cases} a & \text{if n=1} \\ 0 & \text{otherwise.} \end{cases}$$

This map is called Teichmüller lift and we have an exact sequence of multiplicative groups.

$$0 \longrightarrow A \xrightarrow{[-]} \mathbb{W}_S(A) \xrightarrow{\pi} A \longrightarrow 0.$$

Let $T \subset S$ be truncation sets. Then the forgetful map

$$R_T^S : \mathbb{W}_S(A) \to \mathbb{W}_T(A)$$

$$(a_n)_{n \in S} \mapsto (a_n)_{n \in T}$$

is a ring homomorphism called restriction from S to T. If $n \in \mathbb{N}$, and if $S \subset \mathbb{N}$ is a truncation set, then

$$S/n = \{d \in N | nd \in S\}$$

is again a truncation set. We define n'th Verschiebung map

$$V_n : \mathbb{W}_{S/n}(A) \to \mathbb{W}_S(A)$$

by

$$V_n((a_d | d \in S/n))_m = \begin{cases} a_{m/n} & \text{if } n|m, \\ 0 & \text{otherwise.} \end{cases}$$

Lemma 3.2.3. *The Verschiebung map V_n is additive.*

Proof. There is a commutative diagram

$$\begin{array}{ccc} \mathbb{W}_{S/n}(A) & \xrightarrow{w} & A^{S/n} \\ \downarrow{\scriptstyle V_n} & & \downarrow{\scriptstyle V_n^w} \\ \mathbb{W}_S(A) & \xrightarrow{w} & A^S \end{array}$$

where the map V_n^w is given by

$$V_n^w((x_d|d \in S/n))_m = \begin{cases} nx_{m/n} & \text{if } n|m, \\ 0 & \text{otherwise.} \end{cases}$$

$$(V_n^w(w(a)))_m = nw_{m/n}(a) \quad \text{if} \quad m = nd,$$

$$\begin{aligned} w_m(V_n(a)) &= \sum_{d|m} d(V_n(a))_d{}^{m/d} = \sum_{d|m,n|d} da_{d/n}^{m/d} \\ &= \sum_{d|m,d=nk} nka_k^{m/d} = n\sum_{k|m/n} ka_k^{m/nk} = nw_{m/n}(a) \end{aligned}$$

So the diagram commutes and it is easy to see that V_n^w is additive. Then

$$\begin{aligned} w(V_n(x) + V_n(y)) &= V_n^w(w(x)) + V_n^w(w(y)) = V_n^w(w(x) + w(y)) \\ &= V_n^w(w(x + y)) = w(V_n(x + y)) \end{aligned}$$

for $A = \mathbb{Z}[x_n; y_n|n \in S]$. Since A is torsion free, the ghost map is injective.

$$V_n(x + y) = V_n(x) + V_n(y)$$

If we have a ring homomorphism

$$f : A \to B,$$

define

$$\mathbb{W}_S(f) : \mathbb{W}_S(A) \to \mathbb{W}_S(B)$$

$$(a_n) \mapsto (f(a_n))$$

Since addition and multiplication is defined by polynomials, $\mathbb{W}_S(f)$ is a ring homomorphism. For an arbitrary ring A, let

$$\tau : \mathbb{Z}[X_n; Y_n | n \in S] \to A$$

be as in the proof of the Lemma 3.2.2. Then we have

$$V_n(a+b) = V_n(\mathbb{W}_S(\tau)(x+y)) = \mathbb{W}_S(\tau)(V_n(x+y)) = \mathbb{W}_S(\tau)(V_n(x)+V_n(y)) = V_n(a)+V_n(b)$$

since $\mathbb{W}_S(\tau)(V_n(x))_m = \tau(V_n(x)_m) = \tau(x_{m/n}) = V_n(\mathbb{W}_S(\tau)(x))_m$.

□

Remark 3.2.4. V_n commutes with $\mathbb{W}_S(f)$, where f is any ring homomorphism from A to B. We have the commutative diagram

$$\begin{array}{ccc} \mathbb{W}_{S/n}(A) & \xrightarrow{\mathbb{W}_{S/n}(f)} & \mathbb{W}_{S/n}(B) \\ \downarrow{\scriptstyle V_n} & & \downarrow{\scriptstyle V_n} \\ \mathbb{W}_S(A) & \xrightarrow{\mathbb{W}_S(f)} & \mathbb{W}_S(B) \end{array}$$

$$\begin{aligned} V_n(\mathbb{W}_{S/n}(f)(a))_d &= (\mathbb{W}_{S/n}(f(a)))_{d/n} = f(a_{d/n}) \\ &= f(V_n(a)_d) = \mathbb{W}_S(f)(V_n(a))_d. \end{aligned}$$

Lemma 3.2.5. *There exists a unique natural ring homomorphism*

$$F_n : \mathbb{W}_S(A) \to \mathbb{W}_{S/n}(A)$$

such that the diagram

$$\begin{array}{ccc} \mathbb{W}_S(A) & \xrightarrow{w} & A^S \\ \downarrow{\scriptstyle F_n} & & \downarrow{\scriptstyle F_n^w} \\ \mathbb{W}_{S/n}(A) & \xrightarrow{w} & A^{S/n} \end{array}$$

where $F_n((x_m | m \in S))_d = x_{nd}$, *commutes.*

Proof. Let $A = \mathbb{Z}[x_n | n \in S]$.
$F_n^w(w(x))_d = w_{nd}(x)$ and $F_n^w(w(x))_{d/p} = w_{(nd)/p}(x)$.

$$\phi_p(F_n^w(w(x))_{d/p}) \equiv F_n^w(w(x))_d = w_{nd}(x) \pmod{p^{v_p(d)}A}$$

by Lemma 3.2.1.

So there exists unique f_n's, where

$$F_n(x) = (f_{n,d} | d \in S/n) \in \mathbb{W}_{S/n}(A), \quad \text{such that}$$
$$w(F_n(x)) = F_n^w(w(x)).$$

Now in $\mathbb{Z}[x_n | n \in S]$, F_n exists and the diagram commutes. For an arbitrary ring A, define

$$F_n(a) = \mathbb{W}_{S/n}(\tau)(F_n(x))$$

where $a = (a_n | n \in S) = \mathbb{W}_S(\tau)((x_n | n \in S))$. Then

$$\begin{aligned} F_n^w(w(a))_d = w_n d(a) = (w_{nd}(x)) = \tau(F_n^w(w(x))_d) = \tau(w_d(F_n(x))) \\ = w_d(\mathbb{W}_{S/n}(\tau)(F_n(x))) = w_d(F_n(a)) \end{aligned}$$

So the diagram again commutes.
Since F_n^w is ring homomorphism, F_n is ring homomorphism when $A = \mathbb{Z}[x_n | n \in S]$. In general, we have

$$\begin{aligned} F_n(a)F_n(b) &= \mathbb{W}_{S/n}(\tau)(F_n(x))\mathbb{W}_{S/n}(g)(F_n(y)) \\ &= \mathbb{W}_{S/n}(\tau)(F_n(x)F_n(y)) = \mathbb{W}_{S/n}(\tau)(F_n(xy)) = F_n(ab) \end{aligned}$$

by definition of $F_n(a)$.

□

Regard $\mathbb{W}_S(A)$ as being a topological space with the direct product topology where each copy of A is given the discrete topology. So open sets are of the form

$$\prod_{i\geq 0} V_i$$

where for only finitely many i, $V_i \neq A$.

Since addition and multiplication formulas are given by polynomials in each coordinate. Therefore addition and multiplication is continuous.

We can define this topology by neighborhoods of 0. Let us denote $S(n) = \{k \in S | k \leq n\}$. Then we have the restriction maps for all n,

$$R_n : \mathbb{W}_S(A) \longrightarrow \mathbb{W}_{S(n)}(A),$$

where $Ker(R_n) = \{(x_i) \in \mathbb{W}_S(A) | x_i = 0 \quad \text{for all} \quad i \leq n\}$. For any neighborhood U of 0, only finitely many U_i will be different from A. Let us assume after first n entry, $V_i = A$. Then $Ker(R_n) \subseteq U$. Then $Ker(R_n)$'s form a neighborhood basis for 0.

The restriction maps from $\mathbb{W}_S(A)$ to $\mathbb{W}_{S(n)}(A)$ give the map

$$\mathbb{W}_S(A) \to \varprojlim_{n\in S} \mathbb{W}_{S(n)}(A)$$

$$a = (a_k)_{k\in S} \mapsto (R_n(a))_{S(n)}$$

by universal property of projective limit. Take any sequence in $\varprojlim \mathbb{W}_{S(n)(A)}(A)$, we can construct a witt vector a such that nth component of a is nth component of $a_{S(m)}$ for $n \leq m$. We can choose here any $S(m)$ containing n, since $R^{S(n)}_{S(m)}(a_{s(m)}) = R^{S(n)}_{S(k)}(a_{s(k)})$ by the defining property of inverse limit. This shows surjectivity. Injectivity comes from the fact that $R_n(a) = 0$ for all n implies $a = 0$. So

$$\varprojlim_{n} \mathbb{W}_{S(n)}(A) \cong \mathbb{W}_S(A)$$

Since $\mathbb{W}_S(A)/ker(R_n) \cong \mathbb{W}_{S(n)}(A)$, $W_S(A)$ is complete.

Lemma 3.2.6. *The following relations hold.*

(i) $a = \sum_{n\in S} V_n([a_n]_{S/n})$

(ii) $F_nV_n(a) = na$.

(iii) $aV_n(b) = V_n(F_n(a)b)$.

(iv) $F_mV_n = V_nF_m$ *if* $(n,m) = 1$.

Proof. (i)

$$\begin{aligned} w_d(V_n[x_n]) + w_d(V_m[x_m]) &= nw_{d/n}([x_n]) + mw_{d/m}([x_m]) \\ &= nx_n^{d/n} + mx_m^{d/m} = w_d(x') \end{aligned}$$

where

$$x'_d = \begin{cases} x_m & \text{if } d = m \\ x_n & \text{if } d = n \\ 0 & \text{otherwise} \end{cases}$$

Set $S_n = \sum_{k\geq n\in S} V_k([a_k])$. Then by above calculations, $S_n - S_m = \sum_{k|n,k\nmid m} V_k([a_k])$ is in R_m. Take any neighborhood U of 0, there exist an k such that $R_k \subseteq U$. So for all $m,n \geq k$, $S_m - S_n \in U$. Then $\{S_n\}$ is Cauchy and since $\mathbb{W}_S(A)$ is complete, $\sum_{n\in S} V_n[a_n] = \lim S_n$ exists. Taking any R_n, $a - S_m \in \ker(R_n)$ for all $m \geq n$. This implies the limit of $\{S_n\}$ is a.

So for $A = Z[x_n|n \in S]$, we may write any vector as sum of $V_n([x_n]_{S/n})$'s when n varies. For an arbitrary ring, we have

$$\mathbb{W}_S(\tau) : \mathbb{W}_S(Z[x_n|n \in S]) \longrightarrow \mathbb{W}_S(A)$$

since V_n commuttes with $\mathbb{W}_S(\tau)$, the formula follows in general.

(ii) First assume $A = \mathbb{Z}[x_n; y_n|n \in S]$

$$w_d(F_n(V_n(x))) = F_n^w(w(V_n(x)))_d = w_{nd}(V_n(x)) = V_n^w(w(x))_{nd} = nw_d(x) = w_d(nx)$$

since ghost map is injective in this case,

$$F_n(V_n(x)) = nx$$

In general,

$$F_n(V_n(a)) = F_n(\mathbb{W}_S(\tau)(V_n(x))) = \mathbb{W}_{S/n}(\tau)(F_n(V_n(x))) = \mathbb{W}_{S/n}(\tau)(nx) = na.$$

(iii)

$$\begin{aligned} w_d(V_n(F_n(x)y)) &= nw_{d/n}(F_n(x)y) = w_{d/n}(F_n(x)).w_{d/n}(y) \\ &= nw_d(x)w_{d/n}(y) = w_d(x)V_n^w(w(y))_d \\ &= w_d(x)w_d(V_n(y)) = w_d(xV_n(y)) \quad \text{if} \quad n|d. \end{aligned}$$

Otherwise $V_n(x)_d = 0$.

So

$$xV_n(y) = V_n(F_n(x)y)$$

for $A = \mathbb{Z}[x_n; y_n | n \in S]$.

General case follows from the fact that F_n, V_n commutes with $\mathbb{W}_S(\tau)$.

(iv)

$$w_d(F_mV_nx) = F_m^w(w(V_nx))_d = w_{md}(V_nx) = V_n^w(w(x))_{md} = nw_{md/n}(x)$$

if n divides d, since $(n, m) = 1$.

$$w_d(V_nF_mx) = V_n^w(w(F_mx))_d = nw_{d/n}(F_mx) = nF_m^w(w(x))_{d/n} = nw_{md/n}(x)$$

if n divides d.

$F_mV_n = V_nF_m$ for the ring $\mathbb{Z}[x_n; y_n | n \in S]$. General case follows again since $\mathbb{W}_S(\tau)$ commutes with F_m and V_n.

□

Lemma 3.2.7. *Suppose that A is an $\mathbb{F}_p$-algebra, and let $\varphi : A \to A$ be the Frobenius endomorphism. Then*

$$F_p = R^S_{S/p} \circ \mathbb{W}_S(\varphi)$$

where $R^S_{S/p}$ is the forgetful map from $\mathbb{W}_S(A) \to \mathbb{W}_{S/p}(A)$ takes $(x_d)_{d\in S}$ to $(x_d)_{d\in S/p}$.

Proof. We will call terms of $F_p(a)$ as $f_{p,d}(a)$ and we know by construction of F_p that $w(F_p(a)) = F^w_p(w(a))$.
So we have

$$\sum_{d|n} df_{p,d}(a)^{n/d} = \sum_{d/np} da_d^{np/d}$$

for all $n \in S/p$. Let $A = \mathbb{Z}[x_n; y_n|n \in S]$ and we shall show $f_{p,n}(x) \equiv x_n^p (\mathrm{mod} pA)$.
For $n = 1$, we have

$$f_{p,1}(x) = x_1^p + px_p \equiv x_1^p \pmod{p}$$

Assume for all $d \neq n$ and dividing n,

$$f_{p,d}(x) \equiv x_d^p \pmod{p}.$$

So

$$\begin{aligned} f_{p,d}(x)^{n/d} &\equiv x_d^{np/d} && \pmod{p^{\upsilon_p(n/d)+1}} \\ df_{p,d}(x)^{n/d} &\equiv dx_d^{np/d} && \pmod{p^{\upsilon_p(n/d)+1+\upsilon_p(d)}} \\ \sum_{d|n} df_{p,d}(x)^{n/d} &\equiv \sum_{d|n,d\neq n} dx_d^{np/d} + nf_{p,n}(x) && \pmod{p^{\upsilon_p(n)+1}} \end{aligned}$$

and also

$$\sum_{d/np} dx_d^{np/d} = \sum_{d|n,d\neq n} dx_d^{np/d} + nx_n^p + \sum_{d/np,d\nmid n} dx_d^{np/d}$$

$d|pn$ and $d \nmid n$ implies $\upsilon_p(d) = \upsilon_p(n) + 1$.

$$\begin{aligned} \sum_{d/np} dx_d^{np/d} &\equiv \sum_{d|n,d\neq n} dx_d^{np/d} + nx_n^p && \pmod{p^{\upsilon_p(n)+1}} \\ nf_{p,n}(x) &\equiv nx_n^p && (\mathrm{mod} p^{\upsilon_p(n)+1}). \end{aligned}$$

Dividing by n, we obtain

$$f_{p,n}(x) \equiv x_n^p \qquad (\text{mod} p)$$
$$f_{p,d}(x) \equiv x_d^p \qquad (\text{mod} p)$$

for all $d \in S/p$. If A is $\mathbb{F}_p$ algebra,

$$(F_p(a))_d = a_d^p$$

□

The set $P = \{1, p, .., p^n, ..\}$ is a truncation set that consist of all powers of p, where p is a fixed prime. We call $W(A) := \mathbb{W}_P(A)$ ring of p-typical Witt vectors in A and $W_n(A) = W_{1,p,..,p^{n-1}}(A)$ is called ring of p-typical Witt vectors of lenght n in A. We will show that, for a $\mathbb{Z}_p$-algebra A, $\mathbb{W}_S(A)$ decompose as a product of rings of p-typical Witt vectors.

Lemma 3.2.8. *Let m be an integer and suppose that m is invertible in A. Then m is invertible in $\mathbb{W}_S(A)$.*

Proof. Let S be a finite truncation set. We will prove lemma by induction.
For $S = \{1\}$, $\mathbb{W}_S(A) = A$, so we are done. Then assume for any subset S_0 of S, m is invertible in $\mathbb{W}_{S_0}(A)$. Let n be the maximal element in S. Let us define $T := S - \{n\}$. By induction hypothesis, m in $\mathbb{W}_T(A)$ is invertible. let $a = (a_k)$ be inverse of m in $\mathbb{W}_T(A)$.

$$m((a_0, \dots, a_k, 0) + V_n(x)) = (1, 0, \dots, 0) \tag{3.2.3}$$

We want to solve the equation for $x \in A$.

$$\begin{aligned} m((a_0, \dots, a_k, 0) + V_n(x)) &= (1, 0, \dots, 0, y) + mV^n(x) \quad \text{for some } y \in A \\ &= (1, 0, \dots, 0) \text{ by the Equation (2.2.3)} \end{aligned}$$

Then

$$mV^n(x) = V^n(mx) = (0, \dots, 0, z) = (0, \dots, mx)$$

for some z which is a poynomial of $y, a_0, \ldots, a_k$. Since m is invertible in A, we find $x = zm^{-1}$. Then m is invertible in $\mathbb{W}_S(A)$. Also for any truncation set, we know that $\mathbb{W}_S(A)$ is inverse limit of $\mathcal{W}_{S_0}(A)$ where S_0's are finite subtruncations of S. Since m is invertible in all components of the projective system, it is also invertible in $\mathbb{W}_S(A)$. $\square$

Proposition 3.2.9. *Let p be a prime and A be a $\mathbb{Z}_p$-algebra. S be a truncation set, $I(S) = \{k \in \mathbb{N} | p \nmid k\}$ Then ring $\mathbb{W}_S(A)$ has a natural idempotent decomposition*

$$\mathbb{W}_S(A) = \prod_{k \in I(S)} \mathbb{W}_S(A) e_k$$

where

$$e_k = \prod_{l \in I(S), l \neq 1} \left(\frac{1}{k} V_k([1]_{S/k}) - \frac{1}{kl} V_{kl}([1]_{S/kl})\right)$$

Moreover

$$\mathbb{W}_S(A) e_k \hookrightarrow \mathbb{W}_S(A) \to \mathbb{W}_{S/k}(A) \to \mathbb{W}_{S/k \cap P}(A)$$

is an isomorphism.

Proof. Assume S is finite as the first step.

$$w_n\left(\frac{1}{k} V_k([1]_{S/k})\right) = \begin{cases} 1 & \text{if } n \in S \cap k\mathbb{N} \\ 0 & \text{otherwise} \end{cases}$$

$k \in I(S)$ implies $p \nmid k$ and so k is invertible in A and by the previous lemma, k is invertible in $W_S(A)$.

$$w_n\left(\frac{1}{k}\right) w_n(V_k([1]_{S/k})) = w_n\left(\frac{1}{k}\right) V_k^w(w([1]_{S/k}))_n = k w_n\left(\frac{1}{k}\right) = 1 \text{ if } k|n.$$

If for some $l \in I(S)$ $kl|n$, then

$$w_n\left(\frac{1}{k} V_k([1]_{S/k})\right) = w_n\left(\frac{1}{kl} V_k([1]_{S/kl})\right).$$

So $w_n(e_k) = 0$. If $w_n(e_k) \neq 0$, then for any $l \in I(S)$, $kl \nmid n$. So n does not have any divisor

$d \neq k$ with $(d,p)=1$. i.e $n = kp^s$ for some $s \in \mathbb{N}$. Then $w_n(e_k) = w_n(\frac{1}{k}V_k([1]_{S/k})) = 1$.

$$w_n(e_k) = \begin{cases} 1 & \text{if } n \in S \cap kP \\ 0 & \text{otherwise} \end{cases}$$

$w_n(e_k)w_n(e_k) = w_n(e_k)$ and $w_n(e_je_k) = w_n(e_j)w_n(e_k) = 0$ for all $n \in S$. So $e_je_k = 0$.

It follows that e_k's are orthogonal idempotents in $\mathbb{W}_S(A)$.

$$\mathbb{W}_S(A) = \prod_{k \in I(S)} \mathbb{W}_S(A)e_k$$

We will show $\mathbb{W}_s(A)e_k$ is isomorphic to $\mathbb{W}_{S/k\cap P}$.
$S/k \cap P = (S \cap kP)/k \to S \cap kP$ is isomorphism sending t to kt. $t \in S/k \cap P$ if and only if $kt \in S$ and $t \in P$ if and only if $t \in S \cap kP/k$ and following diagram commutes.

$$\begin{array}{ccc} \mathbb{W}_S(A)e_k & \xrightarrow{w} & A^{S\cap kP} \\ \downarrow{\scriptstyle F_k} & & \downarrow{\scriptstyle F_k^w} \\ \mathbb{W}_{S/k}(A) & \xrightarrow{w} & A^{S/k} \\ \downarrow{\scriptstyle R_{S/k\cap P}} & & \downarrow \\ \mathbb{W}_{S/k\cap P}(A) & \xrightarrow{w} & A^{S/k\cap P} \end{array}$$

We may think as w maps $\mathbb{W}_S(A)e_k$ to $A^{S\cap kP}$ since other components are 0. when $A = \mathbb{Z}[x_n, y_n | n \in S]$, ghost map is injective implies left hand side is also isomorphism. General case follows then since restriction and F_k is compatible with $\mathbb{W}_S(f)$. Now, we need to show the isomorphism

$$\mathbb{W}_S(A) \longrightarrow \prod_{k \in I(S)} \varprojlim_{S(n)} \mathbb{W}_{S(n)/k\cap P}(A)$$

let S_f denote the set of finite subtruncation sets of S and let $T \in S_f$. We have restriction map

$$\prod_{k \in I(S)} W_{S/k\cap P}(A) \longrightarrow \prod_{k \in I(T)} W_{T/k\cap P}(A)$$

$$(a_k) \mapsto (R^{T/k\cap P}_{S/k\cap P}(a_k))$$

This induce a ring homomorphism

$$\prod_{k\in I(S)} W_{S/k\cap P}(A) \longrightarrow \varprojlim_{T\in S_f} \prod_{k\in I(S)} W_{T/k\cap P}(A). \tag{3.2.4}$$

Consider projection map

$$\prod_{k\in I(S)} W_{T/k\cap P}(A) \longrightarrow W_{T/k\cap P}(A)$$

By functoriality of inverse limit, we have

$$\varprojlim_{T\in S_f} \prod_{k\in I(T)} W_{T/k\cap P}(A) \longrightarrow \varprojlim_{T\in S_f} W_{T/k\cap P}(A)$$

Now, inverse limit on the right hand side is isomorphic to $W_{S/k\cap P}$ for all $k \in I(T)$ and all $T \in S_f$.

$$\varprojlim_{T\in S_f} \prod_{k\in I(T)} W_{T/k\cap P}(A) \longrightarrow \prod_{k\in I(S)} W_{S/k\cap P}(A) \tag{3.2.5}$$

The maps in (3.2.4) and (3.2.5) are inverses of each other. So the proof is done.

□

We will now consider ring of p-typical Witt vectors in more detail. The ghost map

$$w : W_n(A) \longrightarrow A^n$$

takes the vector $(a_0, a_1, \ldots, a_{n-1}) \longrightarrow (w_o, \ldots, w_{n-1})$ where

$$w_i = a_0^{p^i} + pa_1^{p^{i-1}} + \ldots + p^i a_i$$

We write

$$[-] : A \to W_n(A)$$

$$F : W_n(A) \to W_{n-1}(A)$$

$$V : W_n(A) \to W_{n+1}(A)$$

for the pth Frobenius and pth Verschiebung.

Lemma 3.2.10. *If A is an $\mathbb{F}_p$-algebra, then $VF = FV = p$.*

Proof. We know by lemma 3.2.7 that $F = R_S^{S/p} \circ \mathbb{W}_S(\varphi)$,

$$FV(x) = (R_S^{S/p} \circ \mathbb{W}_S(\varphi) \circ V)(x) = (R_S^{S/p} \circ V \circ \mathbb{W}_{S/p}(\varphi))(x) = (V \circ R_{(S/p)}^{(S/p)/p} \circ \mathbb{W}_{S/p}(\varphi))(x)$$

$$= VF(x), \;\; x \in \mathbb{W}_{S/p}(A)$$

since V is compatible with restriction map and $\mathbb{W}_S(\varphi)$.

$$\begin{array}{ccc} \mathbb{W}_{S/n}(A) & \xrightarrow{R_{S/n}^{(S/n)/n}} & \mathbb{W}_{(S/n)/n}(A) \\ \big\downarrow V_n & & \big\downarrow V_n \\ \mathbb{W}_S(A) & \xrightarrow{R_S^{S/n}} & \mathbb{W}_{S/n}(A) \end{array}$$

$$(R_S^{S/n} \circ V_n(x))_d = V_n(x)_d = x_{d/n}, \;\; d \in S/n, \; x \in \mathbb{W}_{S/n}(A)$$

$$(V_n \circ R_{(S/n)}^{(S/n)/n}(x))_d = R_{(S/n)}^{(S/n)/n}(x)_{d/n} = x_{d/n}, \;\; d \in S/n, \; x \in \mathbb{W}_{S/n}(A)$$

and V commutes with $\mathbb{W}_S(\varphi)$ follows from the Remark 3.2.4.

□

This lemma states that for a ring A of characteristic p,

$$F(a_0, \ldots, a_n) = (a_0^p, \ldots, a_{n-1}^p), \quad \text{in particular, } F[a] = [a^p]$$

Suppose A is a p-torsion free ring and there exist a ring homomorphism

$$\phi : A \to A$$

such that

$$\phi(a) \equiv a^p \pmod{pA}, \quad a \in A$$

Consider the sequence $x = (a, \phi(a), \phi^2(a), ..) \in A^P$.

$$\phi(x_{p^n/p}) = \phi(x_{p^{n-1}}) = \phi(\phi^{n-1}(a)) = \phi^n(a) = x_{p^n}$$

By Lemma 3.2.1, there exist an element in $W(A)$ whose image under the ghost map is $(a, \phi(a), \phi^2(a), ..)$. Furthermore since A is p-torsion free, this element is unique.
So there exist a ring homomorphism s_ϕ such that

$$w(s_\phi(a)) = (a, \phi(a), \phi^2(a), ..)$$

$$A \xrightarrow{s_\phi} W(A) \xrightarrow{w} A^P$$

which maps

$$a \mapsto (a, \phi(a), \phi^2(a), ..)$$

We then define

$$t_\phi : A \to W(A/pA)$$

such that $t_\phi = W(\pi) \circ s_\phi$, where

$$\pi : A \to A/pA$$

is canonical projection of A onto A/pA.
We recall that a ring A is perfect if frobenius endomorphism $\varphi : A \to A$ is an automorphism.

Proposition 3.2.11. *Let A be p-torsion free ring and $\phi : A \to A$ be a ring homomorphism such that $\phi(a) \equiv a^p \pmod{pA}$. Suppose that A/pA is perfect $\mathbb{F}_p$ algebra, then the map t_ϕ induces an isomorphism*

$$A/p^nA \to W_n(A/pA) \quad \textit{for all} \quad n \geq 1$$

Proof. Since A/pA is perfect $\mathbb{F}_p$ algebra,

$$\begin{aligned} V^n(W(A/pA)) &= V^n(\varphi^n(W(A/pA))) \\ &= V^nF^nW(A/pA) = p^nW(A/pA) \end{aligned}$$

So

$$A \xrightarrow{s_\phi} W(A) \xrightarrow{W(\pi)} W(A/pA) \xrightarrow{R} W_n(A/pA)$$

$$p^n a \mapsto p^n s_\phi(a) \mapsto p^n t_\phi(a) \mapsto 0$$

Now $p^n t_\phi(a) \in V(W(A/pA)$ and R maps it to 0 since R(the restriction map) restricts a vector to its first n term and any element in $V(W(A/pA)$ has first n term 0.
So t_ϕ factors as in the statement of the proposition.

We will prove rest by induction on n. For $n = 1$, $W_1(A/pA)$ is isomorphic to A/pA. So assume for all $k < n$, t_ϕ gives isomorphism.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A/pA & \xrightarrow{p^{n-1}} & A/p^nA & \xrightarrow{\pi} & A/p^{n-1}A & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \varphi^{n-1}} & & \downarrow{\scriptstyle t_\phi} & & \downarrow{\scriptstyle t_\phi} & & \\
0 & \longrightarrow & A/pA & \xrightarrow{V^{n-1}} & W_n(A/pA) & \xrightarrow{R} & W_{n-1}(A/pA) & \longrightarrow & 0
\end{array}$$

$$R \circ V^n(a_0, ..a_n, ...) = R(0, ..0, a_0, ..) = (0, ., 0), \quad V^n(a)_d = 0 \quad \text{for all} d \geq n-1$$

The horizantal sequences are exact, since A is p torsion free, left-hand vertical map is isomorphism and by induction hypothesis right-hand side vertical map is also isomorphism. So middle vertical map is also isomorphism. □

Corollary 3.2.12.

$$W(\mathbb{F}_p) \cong \mathbb{Z}_p$$

Proof. We have $W_n(\mathbb{F}_p) \cong \mathbb{Z}/p^n\mathbb{Z}$ from the previous lemma.If we take inverse limit of two side of the equation, we obtain the corrolary. Note that restriction maps on each side are compatible with each other. □

In general, let k be a perfect field of char p. Since $FV = p$, $px = (0, x_0^p, x_1^p, \ldots, x_n^p, \ldots)$ and in particular $p = (0, 1, \ldots, 0, \ldots)$ for $x \in W(k)$. Since k is perfect,we have $VW(k) = pW(k)$. Let us denote the ideal $VW(k)$ as V. Then V-adic topology on $W(k)$ coincide with p-adic topology. Consider the projection map

$$\pi : W(k) \to k$$

that maps $(a_0, \ldots, a_n, \ldots) \mapsto a_0$. Kernel of this map is $VW(k)$. So $V = p$ is a maximal ideal of $W(k)$. $W(k)$ is inverse limit of $W_n(k) = W(k)/V^nW(k)$. So it is complete with respect to p-adic topology. We will show that $W(k)$ is principal ideal domain with unique prime element. Let $x \in W(k)$ be a unit. Then its first entry is unit and non-zero since $(x_0, \ldots)(y_0, \ldots) = (x_0y_0, \ldots)$. Conversely let $x \in W(k)$ be such that its first entry $x_0 \neq 0$. Then write x as $[x_0] + V(y)$ where $y = (x_1, \ldots, y_n, \ldots)$.

$$[x_0] + V(y) = [x_0](1 + [x_0^{-1}]V(y))$$

and denote $[x_0^{-1}]V(y)$ as a. Then $1 - a + a^2 + \ldots + (-1)^n a^n + \ldots$ is the inverse of $1 + a$. Since $a^n = ([x_0^{-1}]V(y))^n = [x_0^{-n}]V(y)^n \in (VW(k))^n = p^nW(k)$, this sequence is Cauchy. The fact that $W(k)$ is complete implies it converges to an element in $W(k)$. So the units in $W(k)$ are those whose first entry are non-zero. So V is the only maximal ideal. Let I be a non-trivial ideal of $W(k)$ and m be the non-zero integer such that for any $x \in I$, $x_n = 0$ for $n < m$. Then we claim that $I = V^m$.
Choose $x \in I$ such that $x_m \neq 0$. Then $x = V^m(x_m, x_{m+1}, \ldots) = p^m u$ for some unit $u \in W(k)$. So we can obtain all the elements in the ideal $p^nW(k)$ multiplying x by certain units. Then $I = p^n = (x)$. This shows $W(k)$ is a pid and has a unique prime element p. So we have proved that :

Lemma 3.2.13. *Let k be a perfect field of char p. Then $W(k)$ is a complete discrete valuation ring with residue field k.*

3.2.2 A Different Characterization of Witt Vectors

If we set $S = \mathbb{N}$, we call $\mathbb{W}_{\mathbb{N}}$ as big Witt vectors and denote it as $\mathbb{W}(A)$.

We write $(1 + tA[[t]])^*$ for the multiplicative group of power series over A with constant term 1.

Proposition 3.2.14. *There is a natural commutative diagram*

$$\begin{array}{ccc} \mathbb{W}(A) & \xrightarrow{\gamma} & (1 + tA[[t]])^* \\ \downarrow{\scriptstyle w} & & \downarrow{\scriptstyle t\frac{d}{dt}log} \\ A^N & \xrightarrow{\gamma^w} & tA[[t]] \end{array}$$

where

$$\gamma(a_1, a_2, ..) = \prod_{n\geq 1}(1 - a_n t^n)^{-1}$$

$$\gamma^w(x_1, x_2, ..) = \sum_{n\geq 1} x_n t^n$$

and the horizontal maps are isomorphisms of abelian groups.

Proof. Let f be any element of $(1 + tA[[t]])^*$. Then $f = 1 + a_1 t + a_2 t^2 + ...$ We will show that $f = \prod_{n\geq 0}(1 - b_n t^n)$ for some unique $\{b_i\}'s$..

Assume $f/\prod_{i=0}^{n-1}(1 - b_i t^i) = 1 + y_n t^n + O(t^{n+1})$ where $b_0 = 0$. For $n = 1$, it is clear. We will prove by induction on n.

$$(1 + y_n t^n + O(t^{n+1}))(1 - (-y)t^n)^{-1} = (1 + y_n t^n + O(t^{n+1}))(1 - yt^n + y^2 t^{2n} - y^3 t^{3n} + ...)$$

In this multiplication, coefficient of t^n is $y - y = 0$. So setting $b_n = y$, using induction hypothesis, $f/\prod_{i=0}^{n-1}(1 - b_i t^i) = 1 + O(t^{n+1})$
since $O(t^{n+1}) \to 0$ when $n \to \infty$, (here we give to the ring of formal power series the topology that neighborhoods of 0 are the ideals (t^n) for all n.)

$$f = \prod_{i\geq 1}(1 - b_i t^i)$$

and by construction these b_i's are unique. Since f is a unit, there exist an $h = (1 + h_1 t + h_2 t^2 + ...) \in (1 + tA[[t]])^*$ such that $fh = 1$.

$$\begin{aligned} f = (1 + g_1 t + g_2 t^2 + ...)^{-1} &= (\prod_{n\geq 1}(1 - b_n t^n))^{-1} \\ &= \prod_{n\geq 1}(1 - b_n t^n)^{-1} \end{aligned}$$

So γ in the diagram defines a bijection. Let $a \in \mathbb{W}(A)$.

$$t\frac{d}{dt}\log(\gamma(a)) = t\frac{d}{dt}\log(\prod_{n\geq 1}(1 - a_n t^n)^{-1}) = -t\frac{d}{dt}\sum_{n\geq 1}\log(1 - a_n t^n)$$

$$
\begin{aligned}
&= -t \sum_{n\geq 1} \frac{d}{dt} \log(1-a_n t^n) = -t \sum_{n\geq 1} \frac{-n a_n t^{n-1}}{1-a_n t^n} \\
&= \sum_{n\geq 1} \frac{n a_n t^n}{1-a_n t^n}
\end{aligned}
$$

If we set $1/(1-a_nt^n) = 1 + a_nt^n + a_{2n}t^{2n} + \ldots$ in the equation above, we obtain

$$
\begin{aligned}
&= \sum_{n\geq 1}\sum_{s\geq 0} n a_n t^n {a_n}^s t^{sn} = \sum_{n\geq 1}\sum_{s\geq 0} n {a_n}^{s+1} t^{n(s+1)} \\
&= \sum_{n\geq 1}\sum_{q\geq 1} n {a_n}^q t^{nq} = \sum_{m\geq 1} \left(\sum_{n|m} n {a_n}^{m/n} \right) t^m \\
&= \sum_{n\geq 1} w_n(a) t^n = \gamma^w(w(a))
\end{aligned}
$$

Assume A is torsion free, then the ghost map is injective. Then γ is homomorphism. In general, we have $\mathbb{W}(g)$ as in the proof of the Proposition3.2.2 and we can extend $g : A \to A'$ to $A[[t]] \to A'[[t]]$ and then restrict g to

$$
g : (1 + tA[[t]])^* \longrightarrow (1 + tA[[t]])^*
$$

$$
1 + a_1t + a_2t^2 + .. \mapsto 1 + g(a_1)t + g(a_2)t^2 + ...
$$

$$
\gamma(a) = \gamma(\mathbb{W}(g)(x)) = \prod_{n\geq 1} (1 - g(x_n)t^n)^{-1} = g(\gamma(x))
$$

$$
\gamma(a+b) = \gamma(\mathbb{W}(g)(x+y)) = g(\gamma(x+y)) = g(\gamma(x)\gamma(y)) = g(\gamma(x))g(\gamma(y))
$$

$$
= \gamma(\mathbb{W}(g)(x))\gamma(\mathbb{W}(g)(y)) = \gamma(a)\gamma(b)
$$

This finishes the proof. □

4 The de Rham-Witt Complex

Definition 4.0.15. A differential graded algebra is a graded algebra with a degree -1 map d satisfying

(i) $d \circ d = 0$

(ii)$d(xy) = (dx)y + (-1)^{degx} xdy$ (Leibniz rule)

We denote the category of differential $\mathbb{Z}$-algebras by DGA.

4.1 The Category of V-Complexes

Definition 4.1.1. Let A be a ring. A V-complex over A is a contravariant functor

$$E : J \to DGA$$

which transforms direct limits to inverse ones and posses the following structure : We denote the elements of degree i in the dga $E(S)$ by $E(S)^i$, there is a natural transformation of rings

$$\lambda : \mathbb{W}_S(A) \to E(S)^{\cdot}, \text{for all } S \in J,$$

and for all $n \in N$, natural transformation of graded $\mathbb{Z}$-modules

$$V_n : E(S/n) \to E(S) \text{ for all } S \in J,$$

satisfying
(i) $V_1 = id$, $V_n \circ V_m = V_{nm}$, and $V_n \circ \lambda = \lambda \circ V_n$, where the latter V_n is the Verchiebung map on $\mathbb{W}_S(A)$.
(ii) $V_n(xdy) = V_n(x)dV_n(y)$, for all $x \in E(S/n)^i$ and $y \in E(S/n)^j$, for all i, j.
(iii) $V_n(x)d\lambda([a]) = V_n(x\lambda([a])^{n-1})d\lambda V_n([a])$, for all $x \in E(S/n)^i$, $a \in A$.

A morphism of V-complexes, $f : E \to E'$ is a natural transformation of differential graded algebras in degree 0,that is compatible with the V_n's and λ's.
If we denote $P = \{1, p, p^2, ..\}$ and we take the restricted category $J_p$instead of J, we call such a functor p-typical De Rham-Witt Complex.

Proposition 4.1.2. *Let A be a ring. Then there exist an initial object in the category of V-complexes,*

$$S \mapsto \mathbb{W}_S\Omega^{\cdot}_A,$$

which we call the de Rham-Witt complex. If S is a finite truncation set, then there is an *epimorphism of differential graded algebras*

$$\Omega^{\cdot}_{\mathbb{W}_S(A)/\mathbb{Z}} \to \mathbb{W}_S\Omega^{\cdot}_A$$

Furthermore,

$$\mathbb{W}_{\{1\}}\Omega^{\cdot}_A = \Omega^{\cdot}_{A/\mathbb{Z}}, \textit{ and } \quad \mathbb{W}_S\Omega^0_A = \mathbb{W}_S(A)$$

Proof. We begin with construction for finite truncation sets. For $S = \{1\}$, set

$$\mathbb{W}_{\{1\}}\Omega^{\cdot}_A = \Omega^{\cdot}_{A/\mathbb{Z}}$$

Now assume we have constructed $\mathbb{W}_{S_0}\Omega^{\cdot}_A$ for all subtrucations S_0 of S,and assume they satisfy

(a) $\mathbb{W}_{S_0}\Omega^0_A = \mathbb{W}_{S_0}(A)$, V_n's and restriction maps coincide on each side.

(b) $V_1 = id$, $V_n \circ V_m = V_{nm}$

(c)$V_n(xdy) = V_n(x)dV_n(y)$ for all $x \in \mathbb{W}_{S_0/n}\Omega^i_A$, $y \in \mathbb{W}_{S_0/n}\Omega^j_A$

(d)$V_n(x)d[a] = V_n(x[a]^{n-1})d(V_n([a])$, for all $x \in \mathbb{W}_{S_0/n}\Omega^i_A$ and $a \in A$.

(e)We have an epimorphism $\pi : \Omega^{\cdot}_{\mathbb{W}_{S_0}(A)/\mathbb{Z}} \to \mathbb{W}_{S_0}\Omega^{\cdot}_A$

Note that $S_0 = \{1\}$ satisfies (a),(b),(c),(d) and (e).

Now $N^{\cdot}_S \subset \Omega^{\cdot}_{\mathbb{W}_S(A)}$ to be the differential ideal generated by the following elements, for all $n > 1$,

(I_n)

$$\sum_j V_n(x_j)dV_n(y_{1j})...dV_n(y_{ij})$$

for all $x_j, y_{kj} \in \mathbb{W}_{S/n}\Omega^0_A = \mathbb{W}_{S/n}(A)$ with $\sum_j x_j dy_{1j}...dy_{ij} = 0$ in $\mathbb{W}_{S/n}\Omega^{\cdot}_A$.

(II_n)

$$V_n(x)d[a] - V_n(x[a]^{n-1})dV_n([a])$$

for all $x \in \mathbb{W}_{S/n}\Omega^0_A = \mathbb{W}_{S/n}(A)$ and for all $a \in A$.

We define

$$\mathbb{W}_S\Omega^{\cdot}_A = \Omega^{\cdot}_{\mathbb{W}_S(A)/\mathbb{Z}}/N^{\cdot}_S$$

which is again a differential graded algebra. $S_0 \subset S$ be a truncation set. We have such diagram

$$\begin{array}{ccc} \mathbb{W}_S(A) & \xrightarrow{R^S_{S_0}} & \mathbb{W}_{S_0}(A) \\ \downarrow d & & \downarrow d \\ \Omega^1_{\mathbb{W}_S(A)} & \longrightarrow & \Omega^1_{\mathbb{W}_{S_0}(A)} \end{array}$$

Since $d \circ R^S_{S_0}$ is a derivation from $\mathbb{W}_S(A)$ to $\Omega^1_{\mathbb{W}_{S_0}(A)}$.(As $\mathbb{W}_S(A)$ module), It decomposes to give a linear map $R : \Omega^1_{\mathbb{W}_S(A)} \to \Omega^1_{\mathbb{W}_{S_0}(A)}$.
by functoriality of Λ, we have a map

$$\Lambda\Omega^1_{\mathbb{W}_S(A)} \to \Lambda\Omega^1_{\mathbb{W}_{S_0}(A)}$$

So we have an algebra homomorphism

$$\Omega^{\cdot}_{\mathbb{W}_S(A)} \to \Omega^{\cdot}_{\mathbb{W}_{S_0}(A)} \to \mathbb{W}_{S_0}\Omega^{\cdot}_A$$

We may write for R instead of $R^{S_0}_S$ to make easier the notation.

$$xdy_1...dy_k \mapsto R(x)dR(y_1)..dR(y_k)$$

since in $\mathbb{W}_S(A)$, V_n and R commutes and $R[a]$ is again a teichmüller lift,

$$R(V_n(x)dV_ny_1..dV_ny_k) = RV_n(x)dRV_ny_1...dRV_ny_k = V_n(R(x))dV_nRy_1...dV_nRy_k.$$

$$R(V_n(x)d[a] - V_n(xd[a]^{n-1})dV_n([a])) = V_n(R(x))dR[a] - V_n(R(x)dR([a])^{n-1}))$$

So $R(N^{\cdot}_S) = 0$ in $\mathbb{W}_{S_0}\Omega^{\cdot}_A$.

We have a map of DGAs.

$$R : \mathbb{W}_S\Omega^{\cdot}_A \to \mathbb{W}_{S_0}\Omega^{\cdot}_A$$

Now, we obtained a contravariant functor,

$$J_S \to DGA$$

$$S_0 \mapsto \mathbb{W}_{S_0}\Omega^{\cdot}_A$$

where J_S denotes set of subtruncation sets of S. Define for each n,

$$V_n : \mathbb{W}_{S/n}\Omega^{\cdot}_A \to \mathbb{W}_S\Omega^{\cdot}_A$$

$$xdy_1...dy_k \mapsto V_n(x)dV_n(y_1)..dV_n(y_k)$$

for all $x, y_i \in \mathbb{W}_{S/n}(A)$. Now we have constructed $\mathbb{W}_S\Omega^{\cdot}_A$ and it satisfies (a),(b),(c),(d),(e).

(a),(b) and (e) follows from the definition.

(c)V_n is well-defined by construction. Let $x = x_1dx_2..dx_k$ and $y = y_1dy_2..dy_s$. Then

$$V_n(xdy) = V_n(x_1dx_2..dx_kdy_1dy_2..dy_s) = V_n(x_1)dV_n(x_2)...dV_n(y_k)$$
$$= V_n(x)d(V_n(y_1)dV_n(y_2)..dV_n(y_k)) = V_n(x)dV_n(y)$$

(d)For $a \in A$,

$$V_n(x)d[a] = V_n(x_1)dV_n(x_2)..dV_n(x_k)d[a] = dV_n(x_2)..dV_n(x_k)V_n(x_1)d[a]$$

$$= dV_n(x_2)..dV_n(x_k)V_n(x_1[a]^{n-1})dV_n([a]) = V_n(x[a]^{n-1})dV_n([a]).$$

Now take any $S \in J$, we write J^f_S for the category of finite subtruncation sets contained in S. Then define in DGA,

$$\mathbb{W}_S\Omega^{\cdot}_A = \varprojlim_{S_0 \in J^f_S} \mathbb{W}_{S_0}\Omega^{\cdot}_A$$

$\mathbb{W}_S\Omega^{\cdot}_A$ is again a differential graded algebra since d is compatible with restriction map. We get a functor

$$J \to DGA$$

$$S \mapsto \mathbb{W}_S\Omega^{\cdot}_A$$

Notice $J^f_{S/n} = \{S_0/n | S_0 \in J^f_S\}$, thus we can write

$$\mathbb{W}_{S/n}\Omega^{\cdot}_A = \varprojlim_{S_0 \in J^f_S} \mathbb{W}_{S_0/n}\Omega^{\cdot}_A$$

and the map V_n for finite truncation sets induce a map of abelian groups,

$$V_n : \mathbb{W}_{S/n}\Omega^{\cdot}_A \to \mathbb{W}_S\Omega^{\cdot}_A$$

since V_n commutes with restriction map.

Thus we get a $V-$complex. Finally, we'll show de Rham-Witt Complex is the initial object in the category of V-complexes. Take a $V-$complex E and a finite truncation set S, then the map $\lambda : \mathbb{W}_S(A) \to E(S)^0$ induces a homomorphism $\Omega^{\cdot}_{\mathbb{W}_S(A)} \to E(S)^{\cdot}$,

If $S = \{1\}$, we are done. So assume for all proper subtruncations S_0 of S, there is a map $\mathbb{W}_{S_0}\Omega^{\cdot}_A \to E(S_0)^{\cdot}$. Then

$$\lambda(\sum_i V_n(x_i)dV_n(y_{i1})..dV_n(y_{ik})) = \sum_i \lambda(V_n(x_i)dV_n(y_{i1})..dV_n(y_{ik}))$$

$$= \sum_i V_n(\lambda x_i)dV_n(\lambda y_{i1})..dV_n(\lambda y_{ik}) = V_n(\sum_i (\lambda x_i)d\lambda y_{i1}...d\lambda y_{ik}) = 0$$

where $\sum_i x_i dy_{i1}..dy_{ik} = 0$.

$$\lambda(V_n(x)d[a] - V_n(x[a]^{n-1})dV_n[a]) = V_n(\lambda(x))d\lambda[a] - V_n(\lambda(x)\lambda[a]^{n-1})dV_n([a])$$

So λ maps $N^{\cdot}_S$ to 0. We have a map

$$\lambda : \mathbb{W}_S\Omega^{\cdot}_A \to E(S)^{\cdot}$$

$$xdy_1..dy_k \mapsto \lambda(x)d\lambda(y_1)..d\lambda(y_k)\ x, y_i \in \mathbb{W}_S(A).$$

Now an arbitrary S is the direct limit of S_0's where $S_0 \in J^f_S$ and E transforms the direct limit to inverse one and we have

$$\lambda : \varprojlim_{S_0 \in J^f_S} \mathbb{W}_{S_0}\Omega^{\cdot}_A \to \varprojlim_{S_0 \in J^f_S} E(S_0)$$

since λ commutes with the restriction map. Then we obtain the map

$$\lambda : \mathbb{W}_S\Omega^{\cdot}_A \longrightarrow E(S)^{\cdot}.$$

□

4.2 The Category of Witt Complexes

Definition 4.2.1. Let A be a ring. A Witt complex over A is a contravariant functor

$$E : J \to DGA$$

which transforms direct limits to inverse ones and together with natural transformation of graded rings

$$F_n : E(S)^{\cdot} \to E(S/n)^{\cdot}, \text{for all } \; S \in J, \;\; \text{for all } \; n \in \mathbb{N},$$

and natural transformation of graded groups

$$V_n : E(S/n) \to E(S) \text{for all } \; S \in J, \;\; \text{for all } \; n \in \mathbb{N},$$

Furthermore there is a natural transformation of rings,

$$\lambda : \mathbb{W}_S(A) \to E(S)^0$$

which commutes with F_n and V_n and satisfies

(i)$F_1 = V_1 = id$, $F_n \circ F_m = F_{nm}$, $V_n \circ V_m = V_{nm}$
(ii)$F_n V_n = n$ and if $(m, n) = 1$, then $F_m V_n = V_n F_m$
(iii)$V_n(F_n(x)y) = xV_n(y)$ for all $x \in E(S)^{\cdot}$, $y \in E(S/n)^{\cdot}$ and all $n \in \mathbb{N}$.
(iv)$F_m dV_n = kdF_{m/c}V_{n/c} + lF_{m/c}V_{n/c}d$, where $\gcd(m, n) = c$ and $km + ln = (m, n)$, $k, l \in \mathbb{N}$.
(v)$F_n d\lambda([a]) = \lambda([a])^{n-1} d\lambda([a])$

A morphism of Witt complexes is a natural transformation of differential graded algebras, compatible with the V_n's,F_m's λ's.
Again if we take the restricted category J_p instead of the category J, we call such a functor p-typical Witt complex.

Lemma 4.2.2. *Let E be a Witt complex over a ring A. Then the following equalities hold, for all $n \in \mathbb{N}$, $S \in J$, $x, y \in E(S/n)$ and all $a \in A$.*

(a)$F_n dV_n = d$

(b)$V_n(xdy) = V_n(x)dV_n(y)$, $V_n(x)d\lambda([a]) = V_n(x\lambda([a]^{n-1}))d\lambda(V_n([a]))$.

(c)$dF_n = nF_n d$, $V_n d = ndV_n$

(d) $F_m dV_n(\lambda([a])) = kdV_{n/c}(\lambda([a])^{m/c}) + lV_{n/c}(\lambda([a])^{m/c-1})dV_{n/c}(\lambda([a]))$

where $c = (m,n)$ *and* $k, l \in \mathbb{Z}$ *are arbitrary with* $km + ln = (m,n)$.

Proof. (a)$F_n dV_n = kdF_{m/c}V_{n/c} + lF_{m/c}V_{n/c}d$ where $c = n$, $k = 0$, $l = 1$.

$F_n dV_n = d$.

(b)

$$V_n(x)dV_n(y) \overset{(iii)}{=} V_n(xF_n(dV_n(y))) \overset{(a)}{=} V_n(xdy).$$

$$V_n(x)d\lambda[a] \overset{(iii)}{=} V_n(xF_n(d\lambda[a])) \overset{(v)}{=} V_n(x\lambda[a]^{n-1}d\lambda[a]) = V_n(x\lambda([a])^{n-1})dV_n(\lambda[a])$$

(c)

$$V_n(dx) = V_n(1dx) = V_n(1)dV_n(x) = V_n(1)dV_n(x) + \underbrace{dV_n(1)V_n(x)}_{V_n(xd(1))=0} = d(V_n(1)V_n(x))$$

$$= d(V_n(1.F_n(V_n(x)))) = d(V_n(nx)) = ndV_n(x)$$

$$dF_n(x) \overset{(a)}{=} F_n dV_n(F_n(x)) = F_n dV_n(1.F_n(x)) \overset{(iii)}{=} F_n d(V_n(1)x) = F_n(dV_n(1)x) + F_n(V_n(1)dx)$$

$$= F_n(dV_n(1))F_n(x) + F_nV_n(1)F_n(dx) = \underbrace{d(1)}_{0}F_n(x) + nF_n(x) = nF_n d(x)$$

(d)Assume $(m,n) = 1$,

$$F_m dV_n(\lambda[a]) = kdF_mV_n(\lambda[a]) + lF_mV_nd(\lambda[a]) = kdV_nF_m(\lambda[a]) + lV_n(F_m(d\lambda[a]))$$

$$= kdV_nF_m(\lambda[a]) + lV_n((\lambda[a])^{m-1}d\lambda[a]) = kdV_n((\lambda[a])^m) + lV_n((\lambda[a])^{m-1})dV_n(\lambda[a])$$

since F_n commutes with λ and $F_m[a] = [a]^m$. If $(m,n) = c$,

$$F_m dV_n = F_{m/c} \circ F_c dV_c \circ V_{m/c} = F_{m/c}dV_{m/c} = kdV_{n/c}(\lambda[a])^{m/c} + lV_{n/c}((\lambda[a])^{m/c-1})dV_{n/c}(\lambda[a])$$

□

The lemma4.2.2 (c) shows if we forget F_n, a Witt-complex turn into a V-complex.

So we have a forgetful functor from the category of Witt-complexes to V-complexes.

Definition 4.2.3. If we take $P = \{1, p, p^2, .., p^n, ..\}$ and the restricted category J_P instead of J, we call such a V-complex as p-typical V-complex. We denote F_p and V_p by F and V, respectively.

So $F_{p^n} = F^n$ and $V_{p^n} = V^n$ for any n, since $F_n \circ F_m = F_{nm}$ and $V_n \circ V_m = V_{nm}$.

Theorem 4.2.4. *Let p be an odd prime and A be a $\mathbb{Z}_(p)$- algebra. Then there is a map of of projective systems of graded rings*

$$F : \mathbb{W}_{.}\Omega^{\cdot}_A \to \mathbb{W}_{.-1}\Omega^{\cdot}_A$$

which is in degree zero the Frobenius of the Witt ring over A and satisfies

$$FdV = d, FV = p, V(F(x)y) = xV(y),$$

for all $x \in \mathbb{W}_n\Omega^{\cdot}_A$, $y \in \mathbb{W}_{n-1}\Omega^{\cdot}_A$ and

$$Fd[a] = [a]^{p-1}d[a], \text{ for all } a \in A$$

.

Proof.

$$\begin{array}{ccc} \mathbb{W}_n(A) & \xrightarrow{F} & \mathbb{W}_{n-1}(A) \\ \downarrow d & & \downarrow d \\ \Omega^1_{\mathbb{W}_n(A)} & \xrightarrow{F'} & \Omega^1_{\mathbb{W}_{n-1}(A)} \end{array}$$

Define multiplication $x\alpha := F(x)\alpha$ for $x \in \mathbb{W}_n(A)$ and $\alpha \in \Omega^1_{\mathbb{W}_{n-1}(A)}$. By this multiplication we can regard $\Omega^1_{\mathbb{W}_{n-1}(A)}$ as $W_n(A)$ module.
$d \circ F(a + b) = d \circ F(a) + d \circ F(a)$ and

$$d \circ F(ab) = d(F(a)F(b)) = d(F(a))F(b) + F(a)dF(b) = b.d \circ F(a) + a.d \circ F(b)$$

for a,b $\in \mathbb{W}_n(A)$.
So $d \circ F$ gives a derivation. By the universal property of $\Omega^1_{\mathbb{W}_n(A)}$, $d \circ F$ decompose as in the

above diagram.

We have $\mathbb{W}_n(A)$ module homomorphism

$$F' : \Omega^1_{\mathbb{W}_n(A)} \to \Omega^1_{\mathbb{W}_{n-1}(A)}$$

$$\sum_i a_i dx_i \mapsto \sum_i F(a_i)dF(x_i), \quad x_i, a_i \in \mathbb{W}_n(A)$$

Now $F'(d[a]) = dF[a] = d[a]^p = p[a]^{p-1}d[a]$ and $F'(dV(x)) = dFV(x) = pdx$, $x \in \mathbb{W}_n(A)$, $a \in A$.

$$F'(dx) = dF(\sum V^i([x_i])) = dF[x_0] + pd[x_1] + ... + pdV^{n-2}[x_{n-1}]$$

$$= p[x_0]^{p-1}d[x_0] + pd[x_1] + ... + pdV^{n-2}[x_{n-1}]$$

$$p([x_0]^{p-1}d[x_0] + d[x_1] + ... + dV^{n-2}[x_{n-1}])$$

Assume $A = \mathbb{Z}[x_n; y_n | n \in \mathbb{N}]$,

Define

$$F : \Omega^1_{\mathbb{W}_n(A)} \to \Omega^1_{\mathbb{W}_{n-1}(A)}$$

$$F : dy \mapsto [y_0]^{p-1}d[y_0] + d[y_1] + ... + dV^{n-2}[y_{n-1}]$$

where $y \in \mathbb{W}_n(A)$.

F is well-defined module homomorphism since A is torsion free.(we cancelled p's.)

We know that Teichmuller lift and Verchiebung map is compatible with $\mathbb{W}(\tau)$. So we can define

$$F(da) = [a_0]^{p-1}d[a_0] + d[a_1] + ... + dV^{n-2}[a_{n-1}]$$

for an arbitrary ring A and it is well defined.

We may extend F to an algebra homomorphism such that

$$F : \Omega^{\cdot}_{\mathbb{W}_n(A)} \to \Omega^{\cdot}_{\mathbb{W}_{n-1}(A)}$$

and composing with the map $\pi : \Omega^{\cdot}_{\mathbb{W}_{n-1}(A)} \to \mathbb{W}_{n-1}\Omega^{\cdot}_{A}$, we have the map

$$\pi \circ F : \Omega^{\cdot}_{\mathbb{W}_{n}(A)} \to \mathbb{W}_{n-1}\Omega^{\cdot}_{A}$$

$$\pi \circ F : xdy_1...dy_k \mapsto F(x)F(dy_1)...F(dy_k)$$

So we need to check that $\pi \circ F$ maps N_S, differential ideal constructed in proof of the proposition 4.1, to 0. First we will show $FdV = d$.

$$FdV([a]) = d[a], \;\; FdV(V^i[a]) = dV^i[a]$$

So

$$FdV(x) = FdV(\sum V^i([x_i])) = d\sum V^i([x_i]) = dx.$$

$$F(\sum_j V^m(x_j)dV^m(y_{1j})...dV^m(y_{kj})) = \sum_j FV^m(x_j)Fd(V^m y_{1j})...FdV^m(y_{kj})$$

$$= p\sum_j V^{m-1}(x_j)dV^{m-1}(y_{1j})...dV^{m-1}(y_{kj}) = pV^{m-1}(\sum_j x_j dy_{1j}..dy_{kj})$$

So if $\sum_j x_j dy_{1j}..dy_{kj} = 0$, $\;F(\sum_j V^m(x_j)dV^m(y_{1j})...dV^m(y_{kj})) = 0$. In particular when $m = 1$, we have showed $FV = p$.

$$F(V(x)d[a] - V(x[a]^{p-1})dV[a]) = FV(x)Fd[a] - FV(x[a]^{p-1})FdV([a])$$

$$= px[a]^{p-1}d[a] - px[a]^{p-1}d[a] = 0$$

So we have

$$F : \mathbb{W}_n\Omega^{\cdot}_{A} \to \mathbb{W}_{n-1}\Omega^{\cdot}_{A}$$

such that

$$FdV = d, FV = p,$$

and taking the inverse limit, we have a map of projective systems of graded rings.

$$F : \mathbb{W}_{.}\Omega^{\cdot}_{A} \to \mathbb{W}_{.-1}\Omega^{\cdot}_{A}$$

We will show F satisfies the projection formula $V(F(x)y) = xV(y)$ for $x \in \mathbb{W}_n\Omega^{\cdot}_{A}$,

$y \in \mathbb{W}_{n-1}\Omega^{\cdot}_A$. First

$$V(xF(dy) = V(x([y_0]^{p-1}d[y_0] + d[y_1] + ... + dV^{n-2}[y_{n-1}]))$$

$$= V(x[y_0]^{p-1}dV([y_0])) + V(x)dV[y_1] + ... + dV^{n-1}[y_{n-1}])$$

$$= V(x)d[y_0] + V(x)dV[y_1] + ... + dV^{n-1}[y_{n-1}] = V(x)dy$$

Inductively assume $V(xF(y_0dy_1..dy_{k-1})) = V(x)y_0dy_1..dy_{k-1}$. Then

$$V(xF(y_0dy_1..dy_k)) = V(xF(y_0)F(dy_1)..F(dy_k)) = V(xF(y_0)F(dy_1)..dy_{k-1})dy_k$$

$$= V(x)y_0dy_1..dy_{k-1}dy_k = V(x)y$$

□

Corollary 4.1. $\mathbb{W}_{.}\Omega^{\cdot}_A$ is the initial object in the category of p-typical Witt complexes.

Proof. First we'll show $\mathbb{W}_{.}\Omega^{\cdot}_A$ is a Witt complex. We already know that it is V-complex. So we need to check
(iii) $V^s(F^s(x)y) = xV^s(y)$ (in proposition we already showed.)
(iv) $F^s dV^t(a) = F^s dV^s(V^{t-s}(a)) = dV^{t-s}(a)$ if $(p^s, p^t) = p^s$.
Otherwise $F^s dV^t(a) = F^{s-t}(F^t dV^t a) = F^{s-t}(da)$.
(v)$Fd[a] = [a]^{p-1}d[a]$ comes from the definition.
So $\mathbb{W}_{.}\Omega^{\cdot}_A$ is a p-typical Witt complex. Assume E is a p-typical Witt complex. as they are both V-complexes, we have a morphism

$$\lambda : \mathbb{W}_{.}\Omega^{\cdot}_A \to E^{\cdot}$$

λ is compatible with F: $E^{\cdot}$ is a Witt complex. So F on $E^{\cdot}$ is compatible with λ in degree 0.

$$\lambda Fd[a] = \lambda([a^{p-1}]d[a]) = \lambda[a^{p-1}]d\lambda[a] = Fd\lambda[a]$$

by definition of Witt complex.

$$\lambda F dV^n[a] = \lambda dV^{n-1}[a] = dV^{n-1}\lambda[a] = FdV^n\lambda[a] = F(\lambda dV^n[a])$$

Here we used the fact that λ is compatible with V^n's and d. Then

$$\lambda : W_n\Omega^{\cdot}_A \longrightarrow E^{\cdot}_n$$

is compatible with F for all n. Since F is a natural transformation of graded rings both on de Rham Witt and $E^{\cdot}$, it is compatible with restriction maps. So we can take inverse limit and $\lambda : W\Omega^{\cdot}_A \longrightarrow E^{\cdot}$ will also be compatible with F. □

4.3 Calculation of de Rham-Witt Complex

Let $A = \mathbb{F}[T, T^{-1}]$. We will give an explicit description of the de Rham-Witt complex $W\Omega^{\cdot}_A$. First introduce rings

$$B = \mathbb{Z}_p[T, T^{-1}]$$

$$C = \varinjlim_r \mathbb{Q}_p[T^{p^{-r}}, T^{-p^{-r}}]$$

Then $\Omega^1_{C/\mathbb{Q}_p}$ is generated by $\{da | a \in C\}$ as a C-module. Since we have

$$d(T^{p^{-r}}) = p^{-r}T^{p^{-r}}\frac{dT}{T},$$

any element $x \in \Omega_C$ can be written as

$$x = \sum_i a_i(T)\text{dlog}T, \quad a_i(t) \in C$$

where dlog$T$ denotes $\frac{dT}{T}$. The polynomials a_i's are called coordinates of x. We define x as entire if its coordinates have coefficients from $\mathbb{Z}_p$. Now, we can define

$$E^m = \{x \in \Omega^m_C | \text{x and dx is entire}\}.$$

Through this section we will write shortly Ω^1_C for $\Omega^1_{C/\mathbb{Q}_p}$. Let $x \in E^m$. Then dx is entire by definition of E^m and $d(dx) = 0$. Therefore $d(E^m) \subseteq E^{m+1}$ and E^m's form a subcomplex of $\Omega^{\cdot}_C$.

Now we will define Frobenius and Verchiebung map on C and Ω^1_C respectively. Define $\mathbb{Q}_p$-algebra automorphism F of C,

$$F : C \longrightarrow C$$

$$T^{p^{-r}} \mapsto T^{p^{-r+1}}$$

and define endomorphism $V = pF^{-1}$.

We can extend F to $\Omega_C{}^1$ by universal property of $\Omega_C{}^1$.

$$F' : \Omega^1_C \longrightarrow \Omega^1_C$$

$$dT \mapsto dT^p = pT^p \mathrm{dlog} T$$

Define

$$F : \sum_k a_k T^k dT \mapsto \sum_k a_k T^{kp} T^{p-1} dT.$$

In fact we obtained this map by dividing F' by p. But we need to show this is a well-defined map. For this, we will define a derivation and then we will use universal property of Ω_C to obtain F.

Define $Fd : C \longrightarrow \Omega_C$ as

$$Fd(aT^k) = kaT^{pk-1}dT, \quad a \in \mathbb{Q}_p, \ \ k \in \mathbb{Z}[\frac{1}{p}].$$

Then Fd is a derivation of C as via-F module. For $a, b \in \mathbb{Q}_p$ and $k, s \in \mathbb{Z}[\frac{1}{p}]$,

$$Fd(aT^k bT^s) = (k+s)abT^{pk+ps-1}dT = saT^{pk}bT^{ps-1}dT + kbT^{ps}aT^{pk-1}dT$$

$$= F(aT^k)Fd(bT^s) + F(bT^s)Fd(aT^k)$$

So $Fd : C \longrightarrow \Omega_C{}^1$ decomposes to give a linear map of C-modules

$$F : \Omega_C \longrightarrow \Omega_C.$$

$$\sum_i a_i(T) \mathrm{dlog} T \mapsto F(a_i(T)) \mathrm{dlog} T \tag{4.3.1}$$

Then define $V = pF^{-1}$ again. We may define V in this way since F gives an automorphism of Ω_C.

$$V\left(\sum_i a_i(T)\mathrm{dlog}T\right) = pF^{-1}\left(\sum_i a_i(T)\mathrm{dlog}T\right) = p\sum_i F^{-1}\left(a_i(T)\mathrm{dlog}T\right)$$
$$= \sum_i V(a_i(T))\mathrm{dlog}T \tag{4.3.2}$$

Lemma 4.3.1. *We have the following equalities*
$dF = pFd, \quad Vd = pdV, \quad V(F(x)y) = xV(y), \quad V(xdy) = V(x)dV(y).$

Proof. Let $aT^k \in C$.

$$dF(aT^k) = adT^{kp} = kpaT^{kp}\mathrm{dlog}T = pF(aT^k\mathrm{dlog}T) = pFdaT^k$$

This shows $dF = pFd$.

$$Vd(aT^k) = V(aT^k\mathrm{dlog}T) = paT^{k/p}\mathrm{dlog}T = paT^{k/p-1}dT = pdV(T^k)$$

So $Vd = pdV$. Let $x, y \in \Omega^1_C$. Then

$$V(xF(y)) = pF^{-1}(xF(y)) = pF^{-1}(x)y = V(x)y$$
$$V(xdy) = V(aT^k dbT^s) = V(sabT^kT^{s-1}dT) = V(sabT^{k+s})\mathrm{dlog}T = psabT^{k+s/p}\mathrm{dlog}T$$
$$= V(aT^k)sbT^{s/p}\mathrm{dlog}T = V(x)dVy$$

∎

Proposition 4.3.2. *(i) $x \in E^0$ is of the form $\sum_k a_kT^k$, where $a_k \in Z_p$ for all k and pth power in the denominator of k divides a_k.*

(ii) $E^0 = \sum_{n\geq 0} V^n(B)$

(iii) $\bigcap_{n\geq 0} V^nE^0 = 0$

(iv) $B \cap V^nE^0 = p^nB$

(vi) There is a unique $\mathbb{Z}_p$-algebra homomorphism $\tau : E^0 \longrightarrow W(A)$

Proof. (i) Let $x = \sum_k a_k T^k \in E^0$. Then x and dx is entire. This implies a_k and ka_k are in $\mathbb{Z}_p$. Then denominator of k divides a_k.

(ii) Let $x = aT^k \in E^0$. If k is in$\mathbb{Z}$, then $x \in B$. So assume $\upsilon_p(k) \leq 0$ and $k = \frac{k_1}{p^s}$. Then $x = aT^k = p^s a_1 T^{k_1/p^s} = V^s(a_1 T^{k_1}) \in V^s(B)$ where $a_1 \in \mathbb{Z}_p$ and $p \nmid k_1$, $k_1 \in \mathbb{Z}$. If $x \in V^s(B)$, $x = V^s(bT^k) = p^s b T^{k/p^s} \in E^0$.

(iii) If $x = \sum_k a_k T^k \in V^n(E^0)$ for all n, p^n divides a_k for all n. Then x must be 0.

(iv) Let $x = V^n(\sum_k a_k T^k) = \sum_k p^n a_k T^{k/p^n} \in B$. This implies $\frac{k}{p^n} \in \mathbb{Z}$, and $a_k \in \mathbb{Z}_p$. Then $x \in p^n B$. Obviously $p^n B \subseteq B \cap V^n(E^0)$.

(v) Let us define new rings $\bar{B}$ and $\bar{A}$ as

$$\bar{B} = \varinjlim_r \mathbb{Z}_p[T^{p^{-r}}, T^{-p^{-r}}]$$

$$\bar{A} = \varinjlim_r \mathbb{F}_p[T^{p^{-r}}, T^{-p^{-r}}]$$

Define

$$\bar{\tau} : \bar{B} \longrightarrow W(\bar{A})$$

$$T^{p^{-r}} \mapsto [T^{p^{-r}}].$$

Then $\bar{\tau}$ is compatible with F.

$$F(\bar{\tau}(T^{p^{-r}})) = [T^{p^{-r+1}}] = \bar{\tau}F(T^{p^{-r}})$$

Since $V = pF^{-1}$, $\bar{\tau}$ is also compatible with V and since only elements that have p^nth roots for all n are Teichmller lift of pth power of T's, $\bar{\tau}$ is unique. $\bar{\tau}$ induces a map

$$\tau : E^0 \longrightarrow \mathbb{W}(\bar{A})$$

$$aT^{p^{-r}} \mapsto \phi(a)[T^{p^{-r}}]$$

where $\phi : \mathbb{Z}_p \longrightarrow W(\mathbb{F}_p)$ taking $a = \sum [a_i] p^i$ to $(a_0, a_1, .., a_n, ..)$.

$$\tau(V^r(T)) = p^r[T^{p^{-r}}] = V^r F^r([T^{p^{-r}}]) = V^r([T])$$

So indeed $\bar{\tau}$ induce a map $E^0 \longrightarrow \mathbb{W}(A)$.

$$\tau : p^s T^{\frac{k}{p^s}} \mapsto V^s[T^k] \quad \text{for } s \in \mathbb{Z}_{\geq 0}$$

□

Lemma 4.3.3. *For $r \geq 0$, $E^0/V^r E^0 \longrightarrow W(A))/V^r(W(A)$ is isomorphism.*

Proof. $F_*^r A$ means we consider A as an A-module restricting scalars to F^r. First we will show that $F_*^r A \longrightarrow V^r(W(A)/V^{r+1}(W(A))$ for $r \geq 0$ is isomorphism.

$$\phi : a \mapsto V^r[a] \ (\text{mod} V^{r+1}(W(A)) \text{ for } a \in A$$

is a module homomorphism. Let $a, b \in A$. Then

$$\phi(a) + \phi(b) \equiv V^r[a] + V^r[b] \ \equiv V^r([a] + [b]) \equiv \ V^r([a+b] \ (\text{mod } V^{r+1}W(A))$$

$$\phi(F^r(a)b) \equiv V^r[F^r(a)b] \equiv V^r(F^r[a][b]) \equiv [a]V^r[b] = [a]\phi[b] \ (\text{mod } V^{r+1}W(A))$$

ϕ is injective and since any witt vector can be written as a sum of $V^n[a_n]$'s,

$$x = V^r(\sum_{n \geq 0} V^n[a_n]) = V^r([a_0]) + V^{r+1}(\sum_{s \geq 0} V^s[a_{s+1}]) \equiv V^r([a_0]) \ (\text{mod } V^{r+1}(\mathbb{W}(A)))$$

So $x = \phi(a_0)$ and ϕ is surjective. So ϕ is isomorphism.

$F_*^r A$ is also isomorhic to $V^r(E_0)/V^{r+1}(E_0)$.

$$\psi : F_*^r A \longrightarrow V^r(E_0)/V^{r+1}(E_0)$$

$$aT^k \mapsto V^r([a]T^k) \ \ (\text{mod} \ \ V^{r+1}(E_0))$$

where $[a]$ denotes the representative of $a \in \mathbb{F}_p$ in $\mathbb{Z}_p$.(Remember that there is a unique multiplicative representative system which commutes with pth power.)
Since $V^r(p^s T^{k/p^s}) = V^r(V^s(T^k)) = V^{r+1}(p^{s-1} a_0 T^{k_0 p^{-s+1}})$.

$$V^r(aT^k) \bmod V^{r+1}(E^0) = \psi(\bar{a}T^k)$$

where p-adic valuation of a is 0. Finally ψ is F^r- linear.

$$W(A)/V^rW(A) \longrightarrow W(A)/VW(A) \cdots \oplus V^{r-1}W(A)/V^rW(A)$$

$$\sum V^n[a_n] \pmod{V^rW(A)} \mapsto ([a_0], V[a_1], .., V^{r-1}[a_{r-1}])$$

$$E^0/V^rE^0 \longrightarrow \sum_{i=0}^{r-1} V^iE^0/V^{i+1}E^0$$

$$aT^k \mapsto (0, 0, .., V^s(a_0T^{kp^s}), .., 0)$$

where $aT^k = a_0p^sT^k$, $\upsilon_p(k) = -s$ and $(a_0, p) = 1$. and since τ is compatible with V, we have induced a map betweeen $W(A)/V^rW(A)$ and E^0/V^rE^0. By the above isomorphisms , this map is also an isomorphism. □

Then $\varprojlim_r E^0/V^r(E_0)$ is isomorphic to $W(A) = \varprojlim_r W_r(A)$. We have the maps

$$E^0 \longrightarrow E^0/V^rE^0$$

we have the canonical map

$$E^0 \longrightarrow \varprojlim_r E^0/V^rE^0$$

and this map is injective, since kernel is $\bigcap_r V^rE^0 = 0$. So we have the injective map $E^0 \longrightarrow W(A)$.

4.4 Filtration on E

Define for $r \geq 0$, $\mathrm{Fil}^rE^i = V^rE^i + dV^rE^{i-1}$ and set $\mathrm{Fil}^rE = \bigoplus_i \mathrm{Fil}^rE^i$.

$$d\mathrm{Fil}^rE^i = d(V^rE^i + dV^rE^{i-1}) = dV^rE^i \subset \mathrm{Fil}^rE^{i+1}$$

and

$$xV^r(y) = V^r(F^r(x)y) \in \mathrm{Fil}^rE$$

$$xdV^ry = d(xV^ry) - V^r(y)dx = dV^r(F^r(x)y) - V^r(F^r(dx)y) \in \mathrm{Fil}^rE$$

for $x, y \in E$. Then $\mathrm{Fil}^r E^i$ forms a diferential graded ideal $\mathrm{Fil}^r E$ of E. We have

$$\mathrm{Fil}^0 E = E \subset \mathrm{Fil}^1 E \subset ... \subset \mathrm{Fil}^r E \subset \mathrm{Fil}^{r+1} E$$

and we can define

$$E_r := E/\mathrm{Fil}^r E^i \cong \bigoplus_{i \geq 0} E^i/\mathrm{Fil}^r E^i$$

and then we still have Verchiebung and Frobenious maps on E_r. Since $V(\mathrm{Fil}^r E) = V^{r+1}E^i + VdV^r E^{i-1} \subset V^{r+1}E^i + pdV^{r+1}E^{-1} \subset \mathrm{Fil}^{r+1}E^i$ and $F(\mathrm{Fil}^{r+1}E^i) = FV^{r+1}E^i + FdV^{r+1}E^{i-1} = pV^r E^i + dV^r E^{i-1} \subset \mathrm{Fil}^r E^i$. So we have induced maps

$$V : E_r \longrightarrow E_{r+1}$$

$$F : E_{r+1} \longrightarrow E_r$$

and satisfy

$$dF = pFd, \;\; Vd = pdV$$

$$xVy = V(Fxy), x \in E_{r+1}, y \in E_r$$

$$V(xdy) = V(x)dV(y), x, y \in E_r$$

We will show that $(E.)$ forms a projective system and it is in fact a V-complex over A. Then we will prove the theorem below. But proof requires to show some preliminaries on the structure of $E.$.

Theorem 4.4.1. *(i) The projective system $(E_.)$, with operators V, and isomorphism of E^0_r and $W_r(A)$ for $r \geq 1$ given by τ is a V-complex.*

(ii) The arrow of V-complexes

$$W_.\Omega^{\cdot}_A \longrightarrow E_.$$

extending the same arrow $\tau : E^0_. \to W_.(A)$ is an isomorphism.

4.5 Grading on $E^{\cdot}$

The ring C posseses a natural grading type $\mathbb{Z}[1/p]$. Extending this grading to $\Omega^{\cdot}_{C}$ such that $x \in \Omega^{\cdot}_{C}$ is of degree k if its coordinate has degree k. Set

$$ {}_{k}E = E \cap {}_{k}\Omega^{\cdot}_{C}, \quad {}_{k}E^{i} = E^{i} \cap_{k} \Omega^{\cdot}_{C} $$

Note that F multiply the degree by p and V divides the degree by p.

Proposition 4.5.1. *Let $k \in \mathbb{Z}[1/p]$. The $\mathbb{Z}_p$-module ${}_{k}E^{0}$ is generated by $e_0(k)$ and ${}_{k}E^{1}$ is generated by $e_1(k)$ where*

$$ e_0(k) = \begin{cases} p^{-\upsilon_p(k)}T^k & \text{if } k \notin \mathbb{Z} \\ T^k & \text{otherwise} \end{cases} \tag{4.5.1} $$

and

$$ e_1(k) = T^k dlogT \tag{4.5.2} $$

Proof. Let $x \in {}_{k}E^{0}$. If $k \notin \mathbb{Z}$,

$$ x = aT^k = p^s a_0 T^k = a_0 e_0(k) $$

where $a_0 \in \mathbb{Z}_p$ and $s = -\upsilon_p(k)$. Otherwise $x = ae_0(k)$. If $x \in {}_{k}E^{1}$, then

$$ x = aT^k \text{dlog} T = ae_1(k) $$

□

Proposition 4.5.2. *E is generated as $\mathbb{Z}_p$-dga by E^0.*

Proof. Since $E^i = 0$ for $i \geq 2$. We only need to deal with E^1. If $k \in \mathbb{Z}$

$$ e_1(k) = T^k \text{dlog} T = T^{k-1} dT = e_0(k-1) d(e_0(1)) \tag{4.5.3} $$

and otherwise

$$ e_1(k) = k_0 p^{-s} p^s k_0^{-1} T^k \text{dlog} T = k_0^{-1} d(p^s T^k) = k_0^{-1} d(e_0(k)) \tag{4.5.4} $$

where $s = -\upsilon_p(k)$ and $k = k_0 p^{-s}$(k_0 is unit in $\mathbb{Z}_p$). □

Now we calculate how $e_i(k)$ behave under the operations d, V, F respectively.

Proposition 4.5.3.

$$de_0(k) = \begin{cases} k_0 e_1(k) & \mathit{if}\, k \notin \mathbb{Z}, k = \frac{k_0}{p^s},\ s \geq 0 \\ ke_1(k) & \mathit{otherwise} \end{cases} \tag{4.5.5}$$

$$de_1(k) = 0$$

$$V(e_0(k)) = \begin{cases} e_0(k/p) & \mathit{if}\, (k/p) \notin \mathbb{Z} \\ pe_0(k/p) & \mathit{otherwise} \end{cases} \tag{4.5.6}$$

$$V(e_1(k)) = pe_1(k/p)$$

$$F(e_0(k)) = \begin{cases} pe_0(kp) & \mathit{if}\, k \notin \mathbb{Z} \\ e_0(kp) & \mathit{otherwise} \end{cases} \tag{4.5.7}$$

$$F(e_1(k) = e_1(kp)$$

Proof. If $k \notin \mathbb{Z}$, $de_0(k) = d(p^{-\upsilon_p(k)} T^k) = kp^{-\upsilon_p(k)} T^k \text{dlog} T$.

If $k \in \mathbb{Z}$, $de_0(k) = dT^k = kT^k \text{dlog} T = ke_1(k)$.

If $k \notin \mathbb{Z}$ and $k/p \notin \mathbb{Z}$,

$V(e_0(k)) = V(p^{-\upsilon_p(k)} T^k) = p^{-\upsilon_p(k)}.pT^{k/p} = p^{-\upsilon_p(k/p)} T^{k/p} = e_0(k)$. If $k \in \mathbb{Z}$ and $k/p \notin \mathbb{Z}$,

$V(e_0(k)) = V(T^k) = pT^{k/p} = e_0(k/p)$ since $\upsilon_p(k/p) = -1$.

If $k/p \in \mathbb{Z}$, $V(e_0(k) = pT^{k/p} = pe_0(k)$.

$V(e_1(k)) = V(T^k \text{dlog} T) = pT^{k/p} \text{dlog} T = pe_1(k/p)$.

If $k \in \mathbb{Z}$, $F(e_0(k)) = F(T^k) = T^{kp} = e_0(kp)$.

If $k \notin \mathbb{Z}$, $F(e_0(k)) = F(p^{-\upsilon_p(k)} T^k) = p^{-\upsilon_p(k)} T^{kp} = pe_0(kp)$.

$F(e_1(k)) = F(T^k \text{dlog} T) = T^{kp} \text{dlog} T = e_1(kp)$.

□

Proposition 4.5.4. *Let $r \in \mathbb{N}$ and $k \in \mathbb{Z}[1/p]$. Define $s = s(k) = -\upsilon_p(k)$ and*

$$\upsilon(r,k) = \begin{cases} r - s & if\, s > 0, r \geq s \\ 0 & if\, s > 0, r < s \\ r & if\, s \leq 0 \end{cases}$$

Then

$$_k Fil^r E = p^{\upsilon(r,k)}\ _k E \tag{4.5.8}$$

Proof. First we will show that

$$p^{\upsilon(r,k)}\ _k E \subset\ _k \mathrm{Fil}^r E$$

Case 1 : $k \in \mathbb{Z}$

$$p^{\upsilon(r,k)} e_0(k) = p^r T^k = V^r(T^{kp^r}) \in\ \mathrm{Fil}^r E \cap_k E$$

Case 2 : $k \notin \mathbb{Z}$ and $r \geq s$.

$$p^{\upsilon(r,k)} e_0(k) = p^{r-s} p^s T^k = p^r T^k = V^r(T^{kp^r}) \in\ \mathrm{Fil}^r E \cap_k E$$

Case 3 : $k \notin \mathbb{Z}$ and $s > r$.

$$p^{\upsilon(r,k)} e_0(k) = p^s T^k = V^r(p^{s-r} T^{kp^r}) = V^r(e_0(kp^r)) \in\ \mathrm{Fil}^r E \cap_k E.$$

Since $-\upsilon_p(kp^r) = s - r$.

We have $p^{\upsilon(r,k)}\ _k E^0 \subset\ _k \mathrm{Fil}^r E^0$. Since $p^{\upsilon(r,k)} e_1(k) \in V^r E^1 \subseteq \mathrm{Fil}^r E$ in all cases, we obtain

$$p^{\upsilon(r,k)}\ _k E \subset\ _k \mathrm{Fil}^r E$$

Now, we need to show $p^{\upsilon(r,k)}\ _k E \subseteq\ _k \mathrm{Fil}^r E$. Since $\mathrm{Fil}^r E = \mathrm{Fil}^r E^0 \oplus \mathrm{Fil}^r E^1$, we will deal with $_k \mathrm{Fil}^r E^i = \mathrm{Fil}^r E^i \cap\ _k E$ for $i = 0, 1$.

write $n = kp^r$.

Case 1 : $n \notin \mathbb{Z}$,

$$V^r(e_0(n)) = V^r(p^{-\upsilon_p(n)} T^n) = p^{r-\upsilon_p(n)} T^{n/p^r}$$

$$V^r(e_0(n)) = p^{\upsilon_p(k)} T^k = e_0(k)$$

Case 2 : $n \in \mathbb{Z}$ and $k \notin \mathbb{Z}$,

$$V^r(e_0(n)) = V^r(T^n) = p^r T^{n/p^r} = p^{r+\upsilon_p(k)} p^{-\upsilon_p(k)} T^k = p^{\upsilon(r,k)} e_0(k)$$

Since $\upsilon_p(n) - r = \upsilon_p(k)$ and $r - s \geq 0$.

Case3 : $k \in \mathbb{Z}$

$$V^r(e_0(n)) = p^r T^{n/p^r} = p^{\upsilon(r,k)} e_0(k).$$

Cince $\upsilon_p(k) \geq 0$.

Then

$$_k\mathrm{Fil}^r E^0 \subset p^{\upsilon(r,k)} \ _kE^0.$$

By above calculations, we obtain $_kV^r(E^0) = p^{\upsilon(r,k)} E^0$ and then

$$dV^r(E^0) \cap \ _kE^1 = d(p^{\upsilon(r,k)} E^0) = p^{\upsilon(r,k)} dE^0 \subset p^{\upsilon(r,k)} \ _kE^1.$$

and since E is generated as a dga by E^0, any element of E^1 can be written as xdy for $x, y \in E^0$. $V^r(xdy) = V^r(x) dV^r(y)$ shows that

$$V^r E^1 \subset p_k^{\upsilon(r,k)} E$$

Then we have

$$p^{\upsilon(r,k)} E =_k \mathrm{Fil}^r E$$

□

Since $p^{\upsilon(r,k)+1} = p^{\upsilon(r,k)}$. We have the corollary :

Corollary 4.5.5. *Multiplication by* p *on* E *induce an injective homomorphism for all* $r \geq 0$.

$$E_r \longrightarrow E_{r+1}$$

Since $\mathrm{Fil}^{r+1} E \subset \mathrm{Fil}^r E$, we have restriction maps from $E_{r+1} \to E_r$. Then take the inverse limit and define

$$\hat{E} := \varprojlim_{r \geq 0} E_r$$

Then $\hat{E}$ has no p-torsion. Since we have the maps $E \to E_r$ for all $r \geq 0$ and $\bigcap_r \text{Fil}^r E = 0$, we have an injective map

$$E \to \hat{E}$$

Claim: $E_{.}$ is a V-complex over the ring A. We have

$$\lambda : W_r(A) \longrightarrow E_r$$

for all $r \geq 0$ and also λ is compatible with V and the restriction maps. We already know

$$V(xdy) = V(x)dV(y) \; for \; x, y \in E_r$$

$$V(x)d(\lambda([T^k])) = V(x)dT^k = V(xF(dT^k)) = V(xkT^{kp}\text{dlog}T)$$

$$= V(xT^{k(p-1)}dT^k) = V(x\lambda([T^k]^{p-1}))d\lambda(V([T^k]))$$

This proves Theorem4.4.1(i).

$$\lambda : W_r(A) \longrightarrow E_r$$

induces the map

$$\lambda : \Omega^{\cdot}_{W_r(A)} \longrightarrow E_r.$$

Let $r = 1$. We have $W_1\Omega^{\cdot}_A = \Omega^{\cdot}_{W_1(A)}$ and we are done. Assume we have map $\lambda : W_r\Omega^{\cdot}_A \longrightarrow E^{\cdot}_r$ for all $s < r$. Then we have

$$\lambda : W_r\Omega^{\cdot}_A \longrightarrow E^{\cdot}_r$$

since $V(xdy) = V(x)dV(y)$ and $V(x)d\lambda[a] = V(x\lambda[a]^{p-1}d\lambda[a])$ for all $x \in E_r$ and $a \in A$. (in fact we already have this map since the de Rham-Witt complex is the initial object in the category of V-complexes.)

Define for $k \in \mathbb{Z}[1/p]$,

$$f_0(k) = \begin{cases} [T^k] & if \; k \in \mathbb{Z} \\ p^s[T^k] & if \; k \notin \mathbb{Z} \end{cases}$$

$$f_1(k) = [T^k]\text{dlog}[T]$$

then $f_i(k) \in W\Omega_{\bar{A}}$. since $E^{\cdot}$ is generated by $e_i(k)$ as a $\mathbb{Z}_p$-dga, we can define the map

$$\psi : E^{\cdot} \longrightarrow W\Omega^{\cdot}_{\bar{A}}$$

$$e_i(k) \mapsto f_i(k)$$

Define

$$(\mathrm{Fil}')^r W\Omega^{\cdot}_{\bar{A}} = V^r W\Omega^{\cdot}_{\bar{A}} + dV^r W\Omega^{\cdot -1}_{\bar{A}}$$

Consider the projection $W_{\cdot}\Omega^{\cdot}_{\bar{A}} \overset{V^r}{\to} W_{\cdot+r}\Omega^{\cdot}_{\bar{A}} \overset{proj.}{\to} W_r\Omega^{\cdot}_{\bar{A}}$ and passing to the limit,

$$W\Omega^{\cdot}_{\bar{A}} \overset{V^r}{\to} W\Omega^{\cdot}_{\bar{A}} \to W_r\Omega^{\cdot}_{\bar{A}}$$

The map ψ we defined above sends $\mathrm{Fil}^r E$ to $(\mathrm{Fil}')^r E$ and

$$(\mathrm{Fil}')^r E \subset Ker W\Omega_{\bar{A}} \to W_r\Omega^{\cdot}_{\bar{A}}.$$

So ψ induce a map

$$\psi_{\cdot} : E_{\cdot} \longrightarrow W_{\cdot}\Omega^{\cdot}_{\bar{A}}$$

$\psi_{\cdot}$ is compatible with V and d.

$$f_0(k) = p^s[T^k] = V^s[T^{kp^s}] \in W_r(A)$$

for $k \notin \mathbb{Z}$ and

$$f_1(k) = [T]^k \mathrm{dlog}[T] = k_0^{-1} dV^s[T^{kp^s}] \in W_r\Omega^{\cdot}_A$$

where $s = -\upsilon_p(k)$. Then in fact image of ψ is p-typical de Rham-Witt complex over A, i.e.,

$$\psi : E_{\cdot} \longrightarrow W_{\cdot}\Omega^{\cdot}_A.$$

$W_r\Omega^{\cdot}_A$ is generated by $W_r(A)$ as a $\mathbb{Z}_p$-dga and any Witt vector in $W_r(A)$ is written as a sum of $V^s[T^k]$'s. So $f_i(k)$'s generates $W_r\Omega^{\cdot}_A$. This finishes the proof of the Theorem 4.4.1.

References

[1] V. Costeanu, *On the 2-typical de Rham-Witt complex*, Doc.Math. 13(2008).

[2] M. Hazewinkel, *Witt Vectors, Part1*. 2007.
http://arxiv.org/ftp/arxiv/papers/0804/0804.3888.pdf.

[3] L. Hesselholt and Ib Madsen, *The de Rham-Witt complex in mixed characteristic*. 2003.
http://www.math.nagoya-u.ac.jp/ larsh/papers/013/.

[4] L. Illusie, *Complexe de de Rham-Witt et cohomologie cristalline*. Annales scientiques de l'Ecole Normale Superieure, 12(4): 501661, 1979.

[5] E. Kunz, *Kähler differentials*. Advanced Lectures in Mathematics. Braunschweig/Wiesbaden: Friedr. Vieweg, Sohn. VII, 1986. MR0864975.

[6] S. Lang, *Algebra*, Second ed., Addison-Wesley Publishing Company Advanced Book Program, Reading,MA,1984, MR MR783636 (86j:00003).

[7] H. Matsumura, *Commutative Ring Theory*, Cambridge studies in advanced mathematics, vol. 8, Cambridge University Press.

[8] J. Rabinoff, *The Theory of Witt vectors*.
http://www.math.harvard.edu/ rabinoff/misc/witt.pdf

[9] K. Rulling, *The generalized de Rham-Witt complex over a field is a complex of zero cycles*, J. Algebraic Geometry,16(2007) 109-169.

[10] J.P. Serre, *Local Fields*, Graduate Texts in Mathematics, vol.67,Springer-Verlag,New York, 1979, Translated from the french by Marvin Jay Greenberg. MR MR554237 (82e:12016).

[11] E. Witt, *Zyklische körper und algebren der charakteristik p vom grad* p^n, *struktur diskret bewerteter perfekter körper mit volkommenem restklassenkörper der charakteristik* p, J. Reine Angew. Math.(1936), no. 176, 126-140.