COMPOSITIO MATHEMATICA

SAUL LUBKIN

# Generalization of $p$-adic cohomology ; bounded Witt vectors. A canonical lifting of a variety in characteristic $p \neq 0$ back to characteristic zero

*Compositio Mathematica*, tome 34, nº 3 (1977), p. 225-277

<http://www.numdam.org/item?id=CM_1977__34_3_225_0>

COMPOSITIO MATHEMATICA, Vol. 34, Fasc. 3, 1977, pag. 225–277
Noordhoff International Publishing
Printed in the Netherlands

# GENERALIZATION OF $p$-ADIC COHOMOLOGY; BOUNDED WITT VECTORS

# A CANONICAL LIFTING OF A VARIETY IN CHARACTERISTIC $p \neq 0$ BACK TO CHARACTERISTIC ZERO

Saul Lubkin

*Note*: The reader who is only interested in learning about the canonical lifting back to characteristic zero should skip the Introduction. The Introduction is a brief summary of two earlier papers. The body of the paper starts with Section I.

## Introduction

1. In "A $p$-Adic proof of Weil's Conjectures" ([1], last chapter), I introduce a cohomology with the following domain. Let $\mathcal{O}$ be a complete discrete valuation ring with quotient field $K$ of characteristic zero and with residue class field $k$. Then let $\mathscr{C}$ be the category of all complete, absolutely non-singular algebraic varieties over the field $k$. Then on the category $\mathscr{C}$, I construct a contravariant functor, $X \rightsquigarrow H^h(X, K)$, $0 \leq h \leq 2n$, $n =$ dimension $X$, which I call *$K$-adic cohomology*, from the category $\mathscr{C}$ into the category of skew-commutative, associative graded $K$-algebras. This is a "good" cohomology theory. I.e.,

a) The coefficient group is a field of characteristic zero.

b) The cohomology has cup products and obeys Poincaré duality and

c) The cohomology obeys the Kunneth relations.

d) There is a good theory of canonical classes.

(d) is possibly the most important property.) In the paper [1], I use this cohomology theory to prove the first two Weil conjectures (Lefschetz theorem and functional equation). And I also prove the finite generation of the group of numerical equivalence classes of cycles, another old problem.

2. In a seminar at Harvard University entitled "Zeta Matrices of an Algebraic Family" that I gave in 1969–70, this cohomology theory is generalized. (I also spoke in various colloquia in 1968, in which I presented summaries of that material.) The generalization is as follows:

Let $\mathcal{O}$, $K$, $k$ be as in 1. above. Let $A$ be any $k$-algebra and let $\underset{\sim}{A}$ be an $\mathcal{O}$-algebra such that $(\underset{\sim}{A} \otimes_{\mathcal{O}} k)/(\text{nilpotent elements}) \approx A$. Then let $\mathscr{C}A$, $\underset{\sim}{A}$ be the category having for objects the schemes $X$ simple and proper over $A$ and that are liftable over $\underset{\sim}{A}$ (i.e., such that there exists $\underset{\sim}{X}$ over $\underset{\sim}{A}$ simple and proper such that $X \approx \underset{\sim}{X} \times_{\underset{\sim}{A}} A$.). The *maps* in $\mathscr{C}A$, $\underset{\sim}{A}$ are all maps of schemes over $A$ (whether or not they can be lifted.). Then I construct a contravariant factor, the $(\underset{\sim}{A}\dagger \otimes_{\mathcal{O}} K)$*-adic cohomology*, from the category $\mathscr{C}A$, $\underset{\sim}{A}$ into the category of skew-commutative, graded, locally free $(\underset{\sim}{A}\dagger \otimes_{\mathcal{O}} K)$-modules: $X \rightsquigarrow H^h(X, \underset{\sim}{A}\dagger \otimes_{\mathcal{O}} K)$, $0 \le h \le 2n$, where $n$ is the largest dimension of $X \times_A \mathbb{K}(\mathfrak{p})$ (= the fiber of $X$ at the point $\mathfrak{p}$), all prime ideals $\mathfrak{p} \subset A$. These groups obey Poincaré duality and the Kunneth relations and have a good theory of canonical classes. Also, they are functorial with respect to "semi-linear maps". That is, if $B$ is another $k$-algebra and $\underset{\sim}{B}$ is an $\mathcal{O}$-algebra such that $(\underset{\sim}{B} \otimes_{\mathcal{O}} K)/(\text{nilpotent elements}) \approx B$, then if $X \in \mathscr{C}_{A,\underset{\sim}{A}}$ and $Y \in \mathscr{C}_{B,\underset{\sim}{B}}$, if $f\colon B \to A$ and $F\colon \underset{\sim}{B} \to \underset{\sim}{A}$ are a $k$-homomorphism and an $\mathcal{O}$-homomorphism of rings, such that the diagram:

$$\begin{array}{ccc} \underset{\sim}{B} & \xrightarrow{F} & \underset{\sim}{A} \\ \downarrow & & \downarrow \\ B & \longrightarrow & A \end{array}$$

is commutative, and if $\varphi\colon X \to Y$ is a map of schemes such that the diagram

$$\begin{array}{ccc} X & \xrightarrow{\varphi} & Y \\ \downarrow & & \downarrow \\ \operatorname{Spec}(A) & \xrightarrow{\operatorname{Spec}(f)} & \operatorname{Spec}(B) \end{array}$$

is commutative, then there is induced a homomorphism from the $\underset{\sim}{B}\dagger \otimes_{\mathcal{O}} K$-module into the $\underset{\sim}{A}\dagger \otimes_{\mathcal{O}} K$-module:

$$H^h(Y, \underset{\sim}{B}\dagger \underset{\mathcal{O}}{\otimes} K) \xrightarrow{H^h(F,\varphi)} H^h(X, \underset{\sim}{A}\dagger \underset{\mathcal{O}}{\otimes} K), \quad h \ge 0,$$

that is semi-linear with respect to the ring homomorphism:

$$F\dagger \otimes_{\mathcal{O}} K\colon \underline{B}\dagger \otimes_{\mathcal{O}} K \to \underline{A}\dagger \otimes_{\mathcal{O}} K.$$

In my Harvard seminar, "Zeta Matrices of an Algebraic Family," I then applied this cohomology theory to define what I call the *zeta matrices of an algebraic family*. The definition of these matrices is purely cohomological, and uses this general $p$-adic cohomology theory for its definition. (They are purely *$p$-adic* invariants. In practice they are not difficult to compute, as I show by an example.) These zeta matrices

(1) Generalize the zeta function by replacing it by a somewhat stronger invariant. In fact, these *zeta matrices* were defined in the seminar for any complete, non-singular liftable algebraic variety over any field of characteristic $p \neq 0$. (The zeta function is only defined over finite fields. In this case, the zeta matrices determine the zeta function by a simple explicit formula whenever the latter is defined.)

(2) The zeta matrices, as indicated above, are defined even for *algebraic families*. (The zeta matrices of an algebraic family typically has $p$-adic convergent power series for its entries.) The zeta matrices of an algebraic family can be used to determine by a simple formula the zeta matrices, and therefore functions, of all algebraic varieties in the family (by letting the $p$-adic convergent power series take special values, depending on each variety of the family). As an example, I compute explicitly the zeta function of every elliptic curve $Y^2 = 4X^3 - g_2X - g_3$, $p \neq 0, 2, 3$, as a function of $g_2$ and $g_3$ only. (Of course, results apply to any algebraic family of complete non-singular varieties such that the family is liftable, this being only a typical example of an explicit computation).

3. The problem which we answer in this paper is, how do we generalize these $p$-adic cohomology theories to, say, the non-liftable case? (*Note*: In a later paper, I'll give a different generalization which also gives information about the zeta functions (and matrices) of singular varieties. This alternative generalization applies to any algebraic variety over, say, a finite field, whether or not it is liftable, singular, affine, complete or whatnot. The Lefschetz theorem is generalized and proved for such arbitrary varieties. A "homology with compact supports" – both $q$-adic and $p$-adic – are used and defined for this very general Lefschetz theorem. (The functional equation fails in this generality. Counterexamples will be given. But a generalization of the "Riemann hypothesis" conjecture holds at this level of generality as a consequence of Weil's "Riemann hypothesis",

proved by P. Deligne. I will state this generalization of the last Weil conjecture and prove it equivalent to the latter under suitable conditions in that Followup paper.)

In this paper I give a generalization that removes the assumption of liftability – (But see the parenthetical paragraph above. The methods of that Followup paper also apply to our bounded Witt theory defined in this paper.) – and also that has the right $p$-torsion.

*Notes*: 1. I presented this paper in a few talks at the Nordic Summer School on Algebraic Geometry held at the University of Oslo at Blindernveinen in Oslo, Norway, in the summer of 1970. A manuscript (virtually identical to this one) was prepared to be published along with the other papers presented at that Conference. It was not published with the other papers of that Conference due to a series of misunderstandings.

2. The research for this paper was completed at the University of California at Berkeley during the academic year September, 1967 – September, 1968, and was first written down as notes at that time. I am indebted to Mr. Barry Moyer for translating the paper [3] of Witt, which of course was necessary for this material.

3. Since completing the research for this paper, in early 1971, I discovered another generalization (a more direct generalization, but one which does not yield "a canonical lifting back to characteristic zero", and which is less "canonical") of the cohomology theory described in [1]. This will appear soon in print ([2]).

So we start over.

I start by defining a canonical lifting of every ring, algebraic variety, prescheme and proscheme over $\mathbb{Z}/p\mathbb{Z}$, $p$ a rational prime, back to characteristic zero, by making a modification of the Witt vector construction. Let us start with ordinary Witt vectors.

Since presenting this manuscript in 1970, I discovered that André Weil discovered, in essence, "bounded Witt vectors", at least in the case of curves, ca. 25 years ago in unpublished notes.

## I. Ordinary Witt vectors

I recall the original definition by Witt of Witt vectors [3].

Definition a): Let $A$ be a ring containing $\mathbb{Z}/p\mathbb{Z}$ where $p$ is a rational prime. Then define

(1) $W(A) = A^{\omega} = \{(a_i)_{i\geq 0}: a_i \in A, \text{ all non-negative integers } i\}.$

The elements of $W(A)$ are the *Witt vectors* of the $\mathbb{Z}/p\mathbb{Z}$ algebra $A$.

The *sum* and *product* of two elements of $W(A)$ are defined as follows. For each integer $h \geq 0$ there are explicit polynomials $S_h$, $Q_h$ with integer coefficients, each of total degree $p^h$, in $2h+2$ variables $A_0, A_1, \ldots, A_h, B_0, B_1, \ldots, B_h$. These polynomials depend on the prime $p$ and, if $A_i$ and $B_i$ are regarded as being weighted of degree $p^i$, $0 \leq i \leq h$, then $S_h$ and $Q_h$ are both homogeneous of degree $p^h$, all integers $h \geq 0$. The polynomials $S_h$ and $Q_h$ are determined by certain simple explicit recursions in the paper of Witt [3]. (I won't recall these here. Instead I'll write down enough information to determine them, as the explicit recursions are lengthy and less informative than our alternative description.) The sum and product in $W(A)$ are then defined as follows:

(2)
$$(a_i)_{i\geq 0} + (b_i)_{i\geq 0} = (S_i(a_0, \ldots, a_i, b_0, \ldots, b_i))_{i\geq 0}$$
$$(a_i)_{i\geq 0} \cdot (b_i)_{i\geq 0} = (Q_i(a_0, \ldots, a_i, b_0, \ldots, b_i))_{i\geq 0},$$

all $(a_i)_{i\geq 0}, (b_i)_{i\geq 0} \in W(A)$. (Witt [3]). As we shall see, there are also more elegant ways to define the sum and product of Witt vectors.

b): *Topology on* $W(A)$. Regard $W(A) = A^{\omega}$ as being a topological space with the direct product topology, where each copy of $\underset{\sim}{A}$ is given the discrete topology. We call this topology on $W(A)$ the *V-topology*. (The terminology will be motivated shortly.) Then, since $S_h$ and $Q_h$, $h \geq 0$, are polynomials, it follows that $W(A)$ is a topological ring for the $V$-topology. $W(A)$ is a complete topological ring for the $V$-topology.

c): *Standard operations in* $W(A)$. For every Witt vector $a = (a_i)_{i\geq 0} \in W(A)$, define

(3) $$V(a_0, a_1, a_2, a_3, \ldots, a_i, \ldots) = (0, a_0, a_1, a_2, \ldots, a_i, \ldots)$$

and

(4) $$F(a_0, a_1, a_2, a_3, \ldots, a_i, \ldots) = (a_0^p, a_1^p, a_2^p, \ldots, a_i^p, \ldots).$$

Then $V$ and $F$ are both continuous functions from $W(A)$ into itself. $V$ is additive, that is

(5) $$V(a+b) = V(a) + V(b),$$

all $a, b \in W(A)$. (To prove this one uses the explicit form of $S_h$ and $Q_h$. Alternatively, property (5) can be used as part of a determination of $S_h$, $h \geq 0$.) Also, $F$ is a ring endomorphism of $W(A)$. That is,

$$(6) \qquad F(a \cdot b) = F(a) \cdot F(b), F(1) = 1, F(a+b) = F(a) + F(b).$$

(Property (6) follows from the facts that $S_h$ and $Q_h$ are polynomials, $h \geq 0$, from equation (4) and the fact that the ring $A$ is a $\mathbb{Z}/p\mathbb{Z}$ algebra.)

$$(7) \qquad V \circ F = F \circ V = \text{multiplication by } p.$$

$$(8) \qquad V(a \cdot F(b)) = V(a) \cdot b$$

(Note that, if the ring $A$ has no nilpotent elements, then $F$ is injective. Equation (8) thrown through $F$ becomes an identity if we use equations (6) and (7). Thus, in the case that $A$ has no nilpotent elements, equation (8) is a consequence of equations (6) and (7).)

d): *Functorality*. If $f: A \to B$ is a homomorphism of $\mathbb{Z}/p\mathbb{Z}$-algebras then define $W(f)$: $W(A) \to W(B)$ by requiring that, for every $a = (a_i)_{i \geq 0} \in W(A)$, we have

$$(9) \qquad (W(f))(a_i)_{i \geq 0} = (f(a_i))_{i \geq 0}.$$

Then $W$ is a functor from the category of commutative $(\mathbb{Z}/p\mathbb{Z})$-algebras with identity into the category of commutative rings with identity.

*Note*: The operator $F$ (defined in equation (4)) on $W(A)$ can be characterized as being $F = W(p'^{\text{th}}$ power map), the image under the functor $W$ of the $p'^{\text{th}}$ power endomorphism: $x \to x^p$ of the ring $A$, all commutative $\mathbb{Z}/p\mathbb{Z}$-algebras with identity $A$, all rational primes $p$.

e): *Multiplicative representatives*. For every $a \in A$, define

$$(10) \qquad a' = (a, 0, 0, 0, \ldots, 0, \ldots).$$

Then the assignment: $a \to a'$ is multiplicative. That is,

$$(11) \qquad a, b \in A \text{ implies } (a \cdot b)' = a' \cdot b'.$$

Also,

(12) The function: $W(A) \to A$ that maps $(a_i)_{i \geq 0} \in W(A)$ into $a_0$, all

$(a_i)_{i\geq 0} \in W(A)$, is a ring homomorphism. (We call this ring homomorphism the *canonical epimorphism from* $W(A)$ *into* $A$.)

I note that, if $W(A)$ is defined by equation (1), all commutative $(\mathbb{Z}/p\mathbb{Z})$-algebras with identity $A$, and if $W(f)$ is defined by equation (9), all commutative $\mathbb{Z}/p\mathbb{Z}$-algebras with identity $A$, $B$ and all homomorphisms of rings with identity $f: A \to B$, and if $V$, $F$ and the operation $a \to a'$ are defined by equations (3), (4) and (10), and the topology on $W(A)$ is the $V$-topology as defined in property b) above, then the requirements that $W$ be a functor into the category of rings, that properties (5), (6), (7) and (12) above hold, that $(x')^p = (x^p)'$, all $x \in A$, and that property f(2) below holds, determine completely the ring structure (i.e., the sum and product operations) on $W(A)$, all commutative $(\mathbb{Z}/p\mathbb{Z})$algebras with identity $A$.

(This is not too difficult to prove, if we use property g) below, and the proof of this property as in g) and [3].)

I give here an alternative, in some ways simpler, characterization of the sum and product in $W(A)$.

f): *Another characterization.* Another characterization of the sum and product in $W(A)$ is as follows:

(1) Both sum and product are continuous for the $V$-topology on $W(A)$ (as defined in b) above), and $W(A)$ is a ring with this sum and product.

(2) For every Witt vector $a = (a_i)_{i\geq 0} \in W(A)$ we have

$$a = \sum_{i\geq 0} V^i(a_i'),$$

where the infinite sum is taken with respect to the $V$-topology as defined in b) above, and where the operators $V$ and $b \to b'$ are defined by equations (3) and (10) above.

(3) If $F$ is defined by equation (4) above, then properties (5), (6), (7), (8), (11) and (12) above hold.

(4) For every $a$, $b \in A$, we have

$$a' + b' = (P_i(a, b))_{i\geq 0},$$

where $P_i \in \mathbb{Z}[X, Y]$ is a polynomial with integer coefficients in two variables $X$ and $Y$, homogeneous of degree $p^i$, determined by the explicit recursions:

$$P_0(X, Y) = X + Y,$$
$$X^{p^i} + Y^{p^i} = (X+Y)^{p^i} + pP_1(X^{p^{i-1}}, Y^{p^{i-1}}) + \cdots + p^{i-1}P_{i-1}(X^p, Y^p) + p^iP_i(X, Y),$$

all integers $i \geq 1$.

(This characterization is especially convenient. It is both explicit and easy to use. Of course, the polynomials $S_h$ and $Q_h$, $h \geq 0$, described in (a) above can very easily be determined from the polynomials $P_h$, $h \geq 0$, in (4) above and by properties (2), (3) and (4). As noted above, functorality can be used as an axiom in place of (4) and equation (8), allowing also a weakening of (11).)

g) REMARK: In a certain special case, the Witt vectors on $A$ can be characterized especially easily.

PROPOSITION: *Let $p$ be a rational prime and let $A$ be a commutative $(\mathbb{Z}/p\mathbb{Z})$-algebra with identity. Suppose that the $p^{th}$ power endomorphism $x \to x^p$ of the $(\mathbb{Z}/p\mathbb{Z})$-algebra $A$ is an automorphism of $A$ (i.e., is one-to-one and onto). Then the ring $W(A)$ and the natural homomorphism $\varphi$: $W(A) \to A$ that sends $(a_i)_{i\geq 0}$ into $a_0$, all $(a_i)_{i\geq 0} \in W(A)$ are determined uniquely up to canonical isomorphism by the following properties.*

(1) *$W(A)$ is a commutative ring with identity, complete for the $p$-adic topology.*

(2) *The ring homomorphism $\varphi$: $W(A) \to A$ induces an isomorphism:*

$$W(A)/pW(A) \underset{\rightarrow}{\approx} A$$

*by passing to the quotient.*

(3) *$x \in W(A)$, $px = 0$ implies $x = 0$.*

*Under the assumptions of the proposition, the $V$-topology on $W(A)$ coincides with the $p$-adic topology. Also, in this case, for every $x \in A$, the element $x' \in W(A)$ is determined by the following properties:*

(1) *The image of $x' \in W(A)$ in $A$ under the natural homomorphism: $W(A) \to A$ is $x$.*

(2) *For every integer $i \geq 1$, there exists an element $y \in W(A)$ such that $y^{p^i} = x'$.*

The proof of the above Proposition is entirely similar to the proof in the case in which $A$ is a perfect field $k$. This latter is proved in Witt's paper [3]. In short, Witt's proof for perfect fields generalizes to yield the above Proposition without significant change.

h) *The $V$-topology is given by ideals.* Let $A$ be an arbitrary commutative $(\mathbb{Z}/p\mathbb{Z})$-algebra with identity, where $p$ is a rational prime. Then the $V$-topology on $W(A)$ can be characterized as the one given by the ideals: $\{V^i(W(A)): i \geq 0\}$. This explains the terminology "$V$-topology" that I have chosen previously.

i) *Other properties of Witt vectors.* (Some of the properties below were established by Witt in [3].)

Let $p$ be a rational prime and let $A$ be a commutative $(\mathbb{Z}/p\mathbb{Z})$-algebra with identity. Then

i(1) $A$ is an integral domain *if and only if* $W(A)$ is an integral domain.

i(2) $A$ has no non-zero nilpotent elements *iff* $W(A)$ has no non-zero $p$-torsion elements *iff* $W(A)$ has no non-zero nilpotent elements.

i(3) (This is property g) above.) If the $p'^{\text{th}}$ power map: $x \to x^p$ of $A$ is an automorphism, then $W(A)$ is a complete $\hat{\mathbb{Z}}_p$-algebra without non-zero $p$-torsion elements and we have that

$$W(A) \otimes_{\hat{\mathbb{Z}}_p} (\mathbb{Z}/p\mathbb{Z}) \approx A.$$

These properties characterize $W(A)$ up to canonical isomorphisms in the case that the $p'^{\text{th}}$ power endomorphism: $x \to x^p$ of the ring $A$ is an automorphism.

i(4) The endomorphism: $x \to x^p$ of the $\mathbb{Z}/p\mathbb{Z}$-algebra $A$ is an automorphism *iff* the endomorphism $F$: $W(A) \to W(A)$ is an automorphism *iff* $W(A)/pW(A)$ has no non-zero nilpotent elements.

i(5) The natural homomorphism: $W(A) \to A$ (that carries $(a_i)_{i \geq 0}$ into $a_0$, all $(a_i)_{i \geq 0} \in W(A)$) always induces a natural epimorphism of $(\mathbb{Z}/p\mathbb{Z})$-algebras

$$W(A)/pW(A) \to A.$$

The kernel of this epimorphism is an ideal $I$ such that $I^2 = \{0\}$.

i(6) There is a natural isomorphism:

$$(W(A)/pW(A))/(\text{nilpotent elements}) \approx A/(\text{nilpotent elements}).$$

i(7) Later, in chapter VI, I will describe explicitly

$W((\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_n])$ This is a useful concrete example.

i(8) (Witt). If $k$ is a perfect field of characteristic $p$ with $W(k)$ is (the unique) complete discrete valuation ring $\mathcal{O}$ of mixed characteristic such that we have an isomorphism: $\mathcal{O}/p\mathcal{O} \approx k$.

i(9) (Witt). $W(\mathbb{Z}/p\mathbb{Z}) = \hat{\mathbb{Z}}_p$, the $p$-adic integers.

*Perfect rings*

*Perfection.* (I don't believe this extremely elementary concept has been studied before, as it yields non-Noëtherian objects. However, it is natural in studying Witt vectors and related constructions, and also in $p$-adic (and even $q$-adic) cohomology.)

Let $A$ be a commutative ring with identity and $p$ be a rational prime. Suppose that $p \cdot 1 = 0$ in $A$ – it is equivalent to say that $A$ is a $(\mathbb{Z}/p\mathbb{Z})$-algebra. Then the function: $x \to x^p$ from $A$ into itself is a ring endomorphism, which we call the *$p'^{th}$ power map.*

DEFINITION: The commutative $\mathbb{Z}/p\mathbb{Z}$-algebra with identity $A$, $p$ a rational prime, is *perfect* if and only if the $p'^{\text{th}}$ power map: $x \to x^p$ is an automorphism of $A$. Equivalently, $A$ is *perfect* if and only if $A$ has no non-zero nilpotent elements, and $a \in A$ implies there exists $b \in A$ such that $b^p = a$.

DEFINITION: Let $A$ be a commutative ring with identity and let $p$ be a rational prime such that $p \cdot 1 = 0$ in $A$ (i.e., such that $A$ is a $(\mathbb{Z}/p\mathbb{Z})$-algebra). Then by the *perfection $A^{p^{-\infty}}$ of the ring $A$ in characteristic $p$* we mean

(1) A commutative ring with identity $A^{p^{-\infty}}$ that is a perfect $(\mathbb{Z}/p\mathbb{Z})$-algebra.

(2) A homomorphism of rings with identity $i\colon A \to A^{p^{-\infty}}$ such that

(3) Given any other such pair $B$, $j$, there exists a unique homomorphism of rings $k\colon A^{p^{-\infty}} \to B$ such that $k \circ i = j$.

PROPOSITION: *Let $A$ be an arbitrary commutative $(\mathbb{Z}/p\mathbb{Z})$-algebra with identity. Then there exists a perfection $A^{p^{-\infty}}$ of $A$. The perfection of $A$ is unique up to canonical isomorphisms.*

PROOF: Uniqueness is obvious. Proof of existence: In fact, define $A^{p^{-\infty}}$ to be the direct limit of the sequence of rings and homomorphisms:

$$A \xrightarrow{x \to x^p} A \xrightarrow{x \to x^p} A \xrightarrow{x \to x^p} A \xrightarrow{x \to x^p} \cdots$$

Then $A^{p^{-\infty}}$ has the indicated properties.

EXAMPLE: If $A$ is a field $k$, of characteristic $p \neq 0$, then the above definition of "perfect" becomes the usual definition of "perfect field". If $A$ is a field $k$ of characteristic $p \neq 0$, then the perfection $A^{p^{-\infty}}$ of the ring $A$ as defined above is simply and purely inseparable algebraic closure $k^{p^{-\infty}}$ of the field $k$.

*Perfect proschemes*

Let $X$ be a prescheme or proscheme over $\mathbb{Z}/p\mathbb{Z}$ where $p$ is a rational prime. Then by the *$p'^{th}$ power map*: $X \to X$ we mean the morphism of preschemes or proschemes that is the set-theoretic identity function, and is such that, for every $x \in X$, the induced ring endomorphism of the $(\mathbb{Z}/p\mathbb{Z})$-algebra $\mathcal{O}_{X,x}$ (the stalk at $x$) is the $p'^{\text{th}}$ power endomorphism of this $(\mathbb{Z}/p\mathbb{Z})$-algebra.

DEFINITION: A prescheme or proscheme $X$ over $\mathbb{Z}/p\mathbb{Z}$, $p$ a rational prime, is *perfect* if and only if for every $x \in X$ the local ring $\mathcal{O}_{X,x}$ is perfect. An equivalent definition: $X$ is *perfect* if and only if the $p'^{\text{th}}$ power map: $X \to X$ is an automorphism.

DEFINITION: Let $X$ be a prescheme or a proscheme over $(\mathbb{Z}/p\mathbb{Z})$. Then by a *perfection* of $X$ we mean

(1) A prescheme or proscheme $X^{p^{-\infty}}$ that is perfect together with

(2) A morphism of preschemes or of proschemes $i: X^{p^{-\infty}} \to X$ such that

(3) Given any other such pair $Y$, $j$ there exists a unique morphism of preschemes or of proschemes $k: Y \to X^{p^{-\infty}}$ such that $i \circ k = j$.

PROPOSITION: *Let $p$ be an arbitrary rational prime and let $X$ be an arbitrary prescheme or proscheme over $\mathbb{Z}/p\mathbb{Z}$. Then there exists a perfection $X^{p^{-\infty}}$ of $X$. Any two perfections of $X$ are canonically isomorphic.*

PROOF: Uniqueness is obvious. To prove existence. Define $\mathcal{O}_{X^{p^{-\infty}}}$ to be the direct limit in the category of sheaves of rings on the topological space $X$ of the sequence:

$$\mathcal{O}_X \xrightarrow{x \to x^p} \mathcal{O}_X \xrightarrow{x \to x^p} \mathcal{O}_X \xrightarrow{x \to x^p} \cdots$$

where "$x \to x^p$" denotes the $p'^{\text{th}}$ power map of the sheaf $\mathcal{O}_X$ into itself (i.e., the endomorphism of the sheaf $\mathcal{O}_X$ of rings on the topological space $X$ that induces the $p'^{\text{th}}$ power map of each stalk $\mathcal{O}_{X,x}$, all $x \in X$). Then the pair consisting of the underlying topological space of $X$ together with the sheaf $\mathcal{O}_{X^{p^{-\infty}}}$ just defined is a prescheme or proscheme $X^{p^{-\infty}}$ and obeys the hypotheses of the Proposition.

(Note that $X$ and $X^{p^{-\infty}}$ always have the same, or more precisely canonically homeomorphic, underlying topological spaces. And that if $X$ is a prescheme (respectively: separated prescheme, affine scheme) then so is $X^{p^{-\infty}}$.)

Note also that the above definitions generalize the ones that we gave earlier for rings. That is, if $A$ is any commutative $(\mathbb{Z}/p\mathbb{Z})$-algebra with identity and if $X = \operatorname{Spec}(A)$, then $A$ is perfect if and only if $X$ is perfect; and if $A^{p^{-\infty}}$ denotes the perfection of the ring $A$ then $X^{p^{-\infty}} = \mathrm{Spec}(A^{p^{-\infty}})$ is the perfection of the proscheme $X$.

EXAMPLE: The perfection of a commutative $(\mathbb{Z}/p\mathbb{Z})$-algebra with identity (that is neither a field nor the zero ring) is generally not Nöetherian. E.g., the perfection of the polynomial ring $(\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_n]$ is the ring: $(\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_n, \quad T_1^{1/p}, \ldots, T_n^{1/p}, T_1^{1/p^2}, \ldots, T_n^{1/p^2}, \ldots, T_1^{1/p^i}, \ldots, T_n^{1/p^i}, \ldots]$, i.e., the ring formed by adjoining arbitrary $p^{i\text{th}}$ roots of each of the indeterminates $T_1, \ldots, T_n$, all integers $i \geq 0$. This ring is of course not Noëtherian (consider the ideal generated by $T_1, \ldots, T_n, T_1^{1/p}, \ldots, T_n^{1/p}, \ldots, T_1^{1/p^i}, \ldots, T_n^{1/p^i}, \ldots$) if $n \geq 1$.

*Note*: We have already considered certain special properties of perfect rings, e.g., property g) above.

## II. Definition of the Bounded Witt Vectors

(The *bounded Witt vectors*, which I describe below, were an invention of mine. In generalizing $p$-adic cohomology, I initially started working with a more complicated subring of $W(A)$, about three or four years before. I figured out the canonical lifting, described in Section III, $W^-(X)$ of a variety, prescheme or proscheme $X$ in Spring, 1968. The rest was done shortly afterward. (Although I defined $F$-differentials earlier for the more complicated subring of $W(A)$ alluded to above.))

If $A$ is any $(\mathbb{Z}/p\mathbb{Z})$-algebra, $p$ a rational prime, then in this section I define a certain subring of the ring $W(A)$. We denote this subring as $W^-(A)$ and call it the *bounded Witt vectors* on $A$. In Section III below, this definition is generalized from $(\mathbb{Z}/p\mathbb{Z})$-algebras with identity to algebraic varieties, preschemes and proschemes over $\mathbb{Z}/p\mathbb{Z}$. The ordinary Witt vectors do not generalize similarly, which is one of the reasons why we make the construction. (The construction gives a canonical lifting of varieties, preschemes and proschemes back to characteristic zero.) We give the definition in steps.

*Case A.* $A = (\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_n]$, a polynomial ring in finitely many variables over the prime field of characteristic $p$, $\mathbb{Z}/p\mathbb{Z}$. Then for every element $a \in W(A)$ we define the *degree of a with respect to the indeterminates* $T_1, \ldots, T_n$, which we denote $\deg_{T_1, \ldots, T_n}(a)$, or more briefly $\deg(a)$, as follows.

If $a = (a_i)_{i \geq 0} \in W(A)$ then

$$\deg(a) = \sup_{i \geq 0} \left( \frac{1}{p^i} \deg(a_i) \right), \tag{1}$$

where $\deg(a_i)$ denotes the total degree of the polynomial $a_i \in (\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_n]$. Thus, if $a \neq 0$, $\deg(a)$ is either a non-negative real number or else $+\infty$. (If $n \geq 1$ then every real number $\geq 0$, and $+\infty$, are degrees of certain Witt vectors $a \in W(A)$.) If we wish, we define $\deg(0) = -1$. Define

$$W^{-}(A) = \{a \in W(A) \colon \deg(a) < +\infty\}. \tag{2}$$

Then $W^{-}(A)$ is a subset of $A$. Also, it is easy to see that $W^{-}(A)$ is a subring of $W(A)$.

*Note*: The function $\deg_{T_1, \ldots, T_n}$ of course depends on the choice of a set of parameters $T_1, \ldots, T_n$ in $A$. Thus, it is not obvious at this point that the subset $W^{-}(A)$ of $W(A)$ depends only on the ring structure of $A$ (i.e., that an element $a \in W(A)$ is of degree $< +\infty$ with respect to one set of $n$ ring generators $T_1, \ldots, T_n$ *iff* it is of finite degree with respect to another.) This, however, is easy to verify directly. A more elegant derivation is the one we are following.

LEMMA: *Let $r$, $n$ be integers $\geq 0$ and let $\varphi\colon (\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_r] \to (\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_n]$ be a homomorphism of $(\mathbb{Z}/p\mathbb{Z})$-algebras. Then $W(\varphi)$ maps $W^{-}((\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_r])$ into $W^{-}((\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_n])$.*

The proof is very elementary (and similar to the direct proof that the subset $W^{-}((\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_n])$ of $W((\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_n])$ is independent of the choice of a set of parameters $T_1, \ldots, T_n$ in the polynomial ring). (*Note*: The proof of the Lemma makes use of the fact that the polynomials $P_h(X, Y)$ described in property f), subproperty (4), of section I, are of degree $\leq p^h$, all integers $h \geq 0$.)

*Case B.* $A$ is an arbitrary finitely generated $(\mathbb{Z}/p\mathbb{Z})$-algebra with identity. Then pick an integer $n \geq 0$ and an epimorphism of rings with identity

$$(\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_n] \to A.$$

Define $W^{-}(A) =$ image of $W^{-}((\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_n])$ under the map: $W((\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_n]) \to W(A)$.

I must show that this definition of $W^{-}(A)$ is independent of the integer $n$ and the epimorphism of rings with identity

$$(\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_n] \to A$$

chosen.

PROPOSITION: *The above definition of $W^-(A)$, a certain subset of $W(A)$, $A$ a finitely generated $(\mathbb{Z}/p\mathbb{Z})$-algebra, is independent of the non-negative integer $n$ and the epimorphism of rings with identity: $\psi$: $(\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_n] \to A$ chosen.*

PROOF: Let $m \geq 0$ and $\rho: (\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_m] \to A$ be another epimorphism of rings with identity. We must show that the subsets

$$(W(\psi))(W^-((\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_n])) \subset W(A)$$

and

$$(W(\rho))(W^-((\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_m])) \subset W(A)$$

coincide.

In fact, since $\psi$ is an epimorphism, there exist elements $a_1, \ldots, a_m \in (\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_n]$ such that $\psi(a_i) = \rho(T_i)$, $1 \leq i \leq m$. Let $\alpha: (\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_m] \to (\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_n]$ be the unique homomorphism of rings with identity such that $\alpha(T_i) = a_i$, $1 \leq i \leq m$. Then the diagram

$$\begin{tikzcd}
(\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_n] \arrow[dr, "\psi"] & \\
& A \\
(\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_m] \arrow[uu, "\alpha"] \arrow[ur, "\rho"'] &
\end{tikzcd}$$

is commutative. By the Lemma in Case A, we have that

$$W(\alpha)(W^-((\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_m])) \subset W^-((\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_n]).$$

Taking the image of this inclusion under $W(\psi)$, and using the fact that from the above commutative diagram that $W(\psi) \circ W(\alpha) = W(\psi \circ \alpha) = W(\rho)$, we obtain that

$$W(\rho)(W^-((\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_m])) \subset W(\psi)(W^-((\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_n])).$$

By symmetry, we also have the reverse inclusion. Therefore

$$W(\rho)(W^-((\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_m])) = W(\psi)(W^-((\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_n])).$$

This completes the proof.

Thus if $A$ is any finitely generated, commutative $(\mathbb{Z}/p\mathbb{Z})$-algebra with identity, then we have defined $W^-(A)$, a subring of $W(A)$ independent of any choices.

*Case C.* General case. $A$ an arbitrary commutative $(\mathbb{Z}/p\mathbb{Z})$-algebra with identity. Then define

$$W^-(A) = \varinjlim_{A_i} W^-(A_i),$$

where $A_i$ runs through the set of all subalgebras of $A$ with identity that are finitely generated as $(\mathbb{Z}/p\mathbb{Z})$-algebras.

Then $W^-$ is a functor from the category of commutative $\mathbb{Z}/p\mathbb{Z}$-algebras with identity into the category of $\hat{\mathbb{Z}}_p$-algebras. ($W^-$ maps into the category of $\hat{\mathbb{Z}}_p$-algebras, since $W^-(\mathbb{Z}/p\mathbb{Z}) = W(\mathbb{Z}/p\mathbb{Z}) = \hat{\mathbb{Z}}_p$). $W^-$ is a subfunctor of $W$.

REMARK: $W^-$ can be characterized as being the smallest subfunctor of the functor $W$ such that, for every integer $n \geq 0$, we have that the subset $W^-((\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_n])$ of $W((\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_n])$ is as described in Case A. above.

Some basic properties of $W^-(A)$, $A$ an arbitrary commutative $(\mathbb{Z}/p\mathbb{Z})$-algebra with identity:

The operators $V$ and $F$ map the subring $W^-(A)$ of $W(A)$ into itself. If $f \in A$ is any element of $A$, then the element $f' = (f, 0, \ldots, 0, \ldots) \in W(A)$ is an element of the subring $W^-(A)$ of $W(A)$. Hence, equations (2), (3), (4), (5), (6), (7), (8), equation (9) with $W^-(f)$ replacing $W(f)$, (10), (11), (12) and f(4) of Section I hold equally well in $W^-(A)$. Note also that, as in $W(A)$, $1' = 1$, $0' = 0$ and the assignment: $f \to f'$, though multiplicative, is not additive unless $A$ is the zero ring.

*Note*: The following alternative explicit description of $W^-(A)$ may be useful for comprehension. Let $A$ be any commutative ring with identity such that $p \cdot 1 = 0$ in $A$, where $p$ is a rational prime. Then $W^-(A) = \{(a_i)_{i \geq 0} \in A^\omega$: there exist integers $m \geq 1$, $d \geq 1$, a sequence of $m$ elements $b_1, \ldots, b_m \in A$ and an infinite sequence of polynomials $f_0, f_1, f_2, \ldots, f_i, \ldots, \ldots \in (\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_m]$ in $m$ indeterminates with coefficients in $(\mathbb{Z}/p\mathbb{Z})$ (or in $\mathbb{Z}$), such that the total degree of $f_i$ is $\leq p^i \cdot d$, and such that $a_i = f_i(b_1, \ldots, b_m)$, all integers $i \geq 0\}$. (The reader who understands the definition using Cases A, B and C above but finds it difficult to understand this note can skip the note.)

We study some of the properties of $W^-(A)$, $A$ a commutative $\mathbb{Z}/p\mathbb{Z}$-algebra with identity, in Section III below. Let us note only one fact here: Namely, that $W^-(A)$ is dense in $W(A)$ for the $V$-topology.

(Proof: In fact, if $n$ is any integer $\geq 1$, and if $a_0, \ldots, a_n \in A$ are any $n+1$ elements of $A$, then the Witt vector $(a_0, \ldots, a_n, 0, 0, \ldots, 0, \ldots) \in W(A)$ is bounded (since it is the image of the bounded Witt vector $(T_0, \ldots, T_n, 0, 0, \ldots, 0, \ldots) \in W^-((\mathbb{Z}/p\mathbb{Z})[T_0, \ldots, T_n])$ under $W(\psi)$, where $\psi: (\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_n] \to A$ is the homomorphism of rings with identity that sends $T_i$ into $a_i$, $0 \leq i \leq n$). And the set of elements of the form $(a_0, \ldots, a_n, 0, \ldots, 0, \ldots) \in W(A)$ such that $n \geq 0$, $a_0, \ldots, a_n \in A$ is obviously dense in $W(A)$ $(= A^\omega)$ for the $V$-topology (= the product topology)). Let us define the *$V$-topology* on $W^-(A)$ to be the topology induced on the subset $W^-(A)$ of the topological ring $W(A)$. An equivalent description is: The $V$-topology on $W^-(A)$ is the one given by the set of ideals $\{V^i W^-(A): i \geq 0\}$. Then

$$W^-(A)^{\wedge V} = W(A),$$

where "$\wedge V$" denotes the completion of the topological ring $W^-(A)$ with respect to the $V$-topology.

Equivalently,

$$\lim_{\substack{\leftarrow \\ i \geq 0}} (W^-(A)/V^i W^-(A)) \approx W(A).$$

Thus, $W^-(A)$ together with its $V$-topology is a finer invariant than $W(A)$ in the sense that $W^-(A)$ determines $W(A)$. Moreover, the $V$-topology on the ring $W^-(A)$ is determined by the operator $V$. (Namely, a base for the neighborhood system at zero for this topology is $\{V^i W^-(A): i > 0\}$.)

(Note that statements f(1) and f(2) of section I remain valid if we replace $W(A)$ by $W^-(A)$.)

*Note*: We will define another topology on $W^-(A)$ later, in the case that $A$ is finitely generated, which is finer than the $V$-topology, and with respect to which $W^-(A)$ is complete. This second topology we will call the *bounded topology* on $W^-(A)$. It does not have a denumerable neighborhood base unless $A$ is finite (as a set).

Note that $W^-(A)$, like $W(A)$, is rarely Noëtherian.

We will see later that an analogy can be drawn as follows between bounded Witt vectors and polynomials. Let $B$ be any ring. Then we have the polynomial ring $B[T]$ and the formal power series ring $B\langle T\rangle$. $B[T]$ is a subring of $B\langle T\rangle$. We can define the (usual, naïve) *degree* of any element of $B\langle T\rangle$, which may be $+\infty$. $B[T]$ can be characterized as being the set of all elements in $B\langle T\rangle$ of degree $< +\infty$. There is a topology on $B[T]$, namely, the $T$-adic topology, such that $B\langle T\rangle$ is the completion of $B[T]$ relative to this topology. The analogy is: $W^{-}(A)$, for $A$ a commutative $(\mathbb{Z}/p\mathbb{Z})$-algebra with identity, $p$ a rational prime, corresponds to $B[T]$, $B$ any commutative ring with identity. Under this analogy, $W(A)$ corresponds to $B\langle T\rangle$, the formal power series ring. The operator $V$ on $W^{-}(A)$ corresponds to the operation "multiplication by $T$" in $B[T]$. We will see later that this analogy holds good for several other important properties. Thus, the bounded Witt vectors are like polynomials, (of finite degree), while the full Witt vectors are like formal power series. (Several other properties of bounded Witt vectors analogous to polynomials: They "paste together well" to lift algebraic varieties, preschemes or proschemes, unlike formal power series or full Witt vectors. We will also see that bounded Witt vectors have better cohomological properties than full Witt vectors – an analogy with polynomials and power series that holds good if $B$ is not of constant characteristic zero.) Other analogous operations: $f \to f'$ from $A$ into $W^{-}(A)$ or $W(A)$ corresponds to the inclusion, $B \subset B[T]$ or $B\langle T\rangle$ (although $f \to f'$ is merely multiplicative, while the inclusion from $B$ is a ring homomorphism). The natural epimorphism $W^{-}(A) \to A$ or $W(A) \to A$ that carries $(a_0, a_1, a_2, \ldots, a_i, \ldots, \ldots)$ into $a_0$ corresponds to the natural epimorphism of $B$-algebras $B[T] \to B$, or $B\langle T\rangle \to B$, that sends $T$ into zero, and every power series or polynomial into its constant term. Another analogy of $W^{-}(A)$ to polynomials will appear when we describe $W^{-}((\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_n])$ explicitly later. In fact, we will be tempted to use the phrase "bounded Witt polynomial in $n$ variables" for an element of this ring. (However, in this case, the analogy is possibly closer between $W^{-}((\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_n])$ and the polynomial ring $\mathcal{O}[T_1, \ldots, T_n]$ where $\mathcal{O}$ is a complete discrete discrete valuation ring. Then the full Witt vectors $W((\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_n])$ corresponds to the $\mathcal{O}$-adic completion of $\mathcal{O}[T_1, \ldots, T_n]$). The most important analogy between $W^{-}(A)$ and polynomials is the one given by the first two theorems of Section III below, and the cohomological properties.

## III. Properties of bounded Witt vectors. The bounded Witt lifting

THEOREM 1: *Let $p$ be a rational prime and let $A$ be a commutative $(\mathbb{Z}/p\mathbb{Z})$-algebra with identity. Then*

*A. For every element $f \in A$, the canonical homomorphism is an isomorphism*

$$W^{-}(A)_{f'} \xrightarrow{\approx} W^{-}(A_f). \tag{1}$$

*B. Let n be a non-negative integer and let $f_1, \ldots, f_n$ be elements of A. Then $f_1, \ldots, f_n$ generate the unit ideal in A if and only if $f'_1, \ldots, f'_n$ generate the unit ideal in $W^-(A)$.*

*Notes*: The analogue of Theorem 1 for $W(A)$ is not entirely true. Part B holds for $W(A)$ as well as $W^-(A)$, but the analogue of Part A fails in general for $W(A)$. Instead, under the hypotheses of Theorem 1, Part A, it is not difficult to show that the natural homomorphism induces an isomorphism:

$$W(A)_{f'}^{\wedge V} \xrightarrow{\approx} W(A_f),$$

where "$\wedge V$" denotes the completion with respect to the $V$-topology on $W(A_{f'})$, i.e. the topology having for open neighborhood base at the origin the set of ideals $\{V^i(W(A)_{f'}): i \geq 0\}$. (The operators $F$ and $V$ on the ring $W(A)$ extend uniquely to $W(A)_{f'}$ in such a way as to preserve the formulae: $F(xy) = F(x) \cdot F(y)$, $V(x \cdot F(y)) = V(x) \cdot y$. Also $V^i(W(A)_{f'}) = (V^i(W(A)))_{f'}$, the localization of the $W(A)$-module $V^i(W(A))$ at the element $f' \in W(A)$, all integers $i \geq 0$).

The proof of property $A$ of $W^-(A)$ is extremely simple; it follows almost immediately from the definitions. (The corresponding property for $W(A)$ alluded to above is a consequence of property $A$ for $W^-(A)$ and the fact that $W^-(A_f)^{\wedge V} \approx W(A_f)$.) The proof of the analogue of property $B$ for $W(A)$ is almost as easy. However, the proof of property $B$ for $W^-(A)$ is a bit more interesting. In the proof, it is necessary to use the facts that the polynomials $P_h$, $h \geq 0$, of two variables, defined recursively in property f(4) of section I, are each homogeneous of degree exactly $p^h$, each integer $h \geq 0$. (Homogeneity of these polynomials is definitely used in the proof.)

THEOREM 2: *Let X be either an algebraic variety over a field of characteristic $p \neq 0$, a prescheme over $\mathbb{Z}/p\mathbb{Z}$, or a proscheme over $\mathbb{Z}/p\mathbb{Z}$. Then there is induced, respectively, a prescheme, prescheme or proscheme over $\hat{\mathbb{Z}}_p$, call it $W^-(X)$, and a map of preschemes, preschemes or proschemes over $\mathbb{Z}/p\mathbb{Z}$:*

$$X \to W^-(X) \underset{\hat{\mathbb{Z}}_p}{\times} (\mathbb{Z}/p\mathbb{Z}) \tag{2}$$

*that is a homeomorphism of topological spaces and a closed immersion of preschemes, preschemes or proschemes. The sheaf of ideals I on the structure sheaf of $W^-(X) \times_{\hat{\mathbb{Z}}_p} (\mathbb{Z}/p\mathbb{Z})$ that defines the closed sub-object X is therefore contained in the subsheaf of nilpotent elements of*

$\mathcal{O}_{W^-(X)\times_{\hat{\mathbb{Z}}_p}(\mathbb{Z}/p\mathbb{Z})}$. *In fact*

$$I^2 = 0, \tag{3}$$

*i.e., $I$ is a sheaf of ideals of square zero.*

The assignment: $X \rightsquigarrow W^-(X)$ is a covariant functor from the category of all algebraic varieties over a field of characteristic $p$, or the category of all preschemes over $\mathbb{Z}/p\mathbb{Z}$ or the category of all proschemes over $\mathbb{Z}/p\mathbb{Z}$ into, respectively, the category of all preschemes, preschemes or proschemes over $\hat{\mathbb{Z}}_p$.

The maps (2) define a homomorphism of functors.

If $A$ is any commutative $(\mathbb{Z}/p\mathbb{Z})$-algebra with identity, then there is induced a canonical isomorphism

$$W^-(\operatorname{Spec}(A)) \approx \operatorname{Spec}(W^-(A)). \tag{4}$$

The isomorphism (4) is an isomorphism of functors.

If $U$ is an open subset of an algebraic variety, prescheme or proscheme $X$, then $W^-(U)$ is an open subprescheme, subprescheme or subproscheme, respectively, of $W^-(X)$. Also, the functor $W^-$ preserves arbitrary unions and all finite intersections of open subsets of $X$, all algebraic varieties, preschemes or proschemes $X$.

*Note* 1. The functor $W^-$, considered as a functor on the category of all algebraic varieties over a given field of characteristic $p \neq 0$, or else considered as a functor on the category of all preschemes over $\mathbb{Z}/p\mathbb{Z}$, is characterized uniquely up to canonical isomorphism of functors by the properties given in the above Theorem. A few additional axioms are needed to characterize the functor $W^-$ on the category of all proschemes over $\mathbb{Z}/p\mathbb{Z}$: namely that $W^-$ preserves arbitrary unions of subsets closed under generalization of $X$, all proschemes $X$ over $\mathbb{Z}/p\mathbb{Z}$, and that the topology on $W^-(X)$ is the coarsest possible topology such that all of the above axioms hold. (More explicitly, a base for the open subsets of $W^-(X)$ is $\{W^-(U)_f$: $U$ is an open subset of $X$, $f \in W^-(\Gamma(U, O_X))\}$, where $W^-(U)_f = \{x \in W^-(U)$: the image of $f$ in the residue class field at the prime ideal in $W^-(\Gamma(U, O_U))$ determined by $x$ is not zero$\}$.

*Sketch of proof*: The algebraic variety case is a special case of the prescheme case. If $X$ is any prescheme over $\mathbb{Z}/p\mathbb{Z}$, then parts A and B of Theorem 1 above are exactly the conditions needed for the topological spaces $\{W^-(U)$: $U$ is an affine open subset of $X\}$ to "paste together", including with their structure sheaves, to form a prescheme $W^-(X)$. Equations (2) and (3) reduce to the case in which $X = \operatorname{Spec}(A)$, $A$ a commutative $(\mathbb{Z}/p\mathbb{Z})$-algebra with identity. Then the proof of equations (2) and (3) is similar to the proof of the corresponding equations in i(5) of section I for $W(A)$, $A$ a commutative $(\mathbb{Z}/p\mathbb{Z})$-algebra with identity. The rest of the theorem then follows easily.

Proof of Theorem 2 *in the case in which $X$ is a proscheme over* $\mathbb{Z}/p\mathbb{Z}$: Define the underlying set of $W^-(X)$ to be a quotient set of the disjoint union of $\{\operatorname{Spec}(W^-(\mathcal{O}_{X,x})): x \in X\}$ following a certain equivalence relation. Namely, if $x, y \in X$ and $\mathfrak{p} \in \operatorname{Spec}(W(\mathcal{O}_{X,x}))$ and $\mathfrak{q} \in \operatorname{Spec}(W^-(\mathcal{O}_{X,y}))$, then $\mathfrak{p}$ is equivalent to $\mathfrak{q}$ if and only if there exists a point $z \in X$ and an element $\mathfrak{r} \in \operatorname{Spec}(W^-(\mathcal{O}^q_{X,z}))$ such that $x$ and $y$ are both specializations of $z$ in $X$ and such that the image of $\mathfrak{r}$ in $\operatorname{Spec}(W^-(\mathcal{O}_{X,x}))$ and in $\operatorname{Spec}(W^-(\mathcal{O}_{X,y}))$ is $\mathfrak{p}$ and $\mathfrak{q}$ respectively. Then $W^-(X)$ is a set, and the assignment: $X \rightsquigarrow W^-(X)$ is a covariant functor from the category of proschemes over $(\mathbb{Z}/p\mathbb{Z})$ into the category of sets. Define a topology in $W^-(X)$ by taking for open base $\{W^-(U)_f: U$ is an open subset of $X$, $f \in W^-(\Gamma(U, \mathcal{O}_U))\}$, where $W^-(U)_f$ is defined as in the Note above, all open subsets $U$ of $X$ and all elements $f \in W^-(\Gamma(U, \mathcal{O}_U))$. Then there is induced a natural structure of sheaf on the topological space $W^-(X)$ together with which $W^-(X)$ becomes a proscheme.

*Note* 2. Roughly speaking, Theorem 1, plus the most elementary topological argument, implies Theorem 2.

I call $W^-$ the *bounded Witt functor*. For every algebraic variety over a field of characteristic $p \neq 0$, prescheme over $\mathbb{Z}/p\mathbb{Z}$ or proscheme over $\mathbb{Z}/p\mathbb{Z}$ where $p$ is a rational prime I call $W^-(X)$ the *bounded Witt lifting* of $X$. Thus, every algebraic variety $X$ over a field of characteristic $p \neq 0$, or prescheme $X$ or proscheme $X$ over $\mathbb{Z}/p\mathbb{Z}$ where $p$ is a rational prime, admits a canonical "lifting" back to characteristic 0, namely $W^-(X)$. (Of course, $W^-(X)$ is not a "perfect lifting" except under unusual conditions, vide infra. However, always $W^-(X)$ is a "perfect lifting" of $X$ together with a few additional nilpotent (in fact, two-potent) elements. Equations (2) and (3) above say this more precisely.)

Some properties of the bounded Witt lifting that follow immediately from properties described in Theorem 2 and Note 1 are the following:

$W^-$ carries a prescheme or proscheme such that the intersection of any two affine open subsets is affine into a prescheme or proscheme such that the intersection of any two affine open subsets is affine. A little bit more subtle is the following. Call a scheme *infinitely projective* if it is isomorphic to the Proj of a commutative non-negatively graded ring with identity. Then $W^-$ carries infinitely projective schemes into infinitely projective schemes. Moreover, if $X$ is an infinitely projective scheme coming from a non-negatively graded commutative ring with identity such that the ideal of elements of positive degree is generated by $n$ elements, then $W^-(X)$ is also infinitely projective and comes from a graded ring with similar properties (and the same integer $n$). Hence, a projective algebraic variety $X$ over a field $k$ of characteristic $p$ (or even a projective scheme over a commutative $(\mathbb{Z}/p\mathbb{Z})$-algebra with identity $A$) is such that $W^-(X)$ is infinitely projective, but comes from a non-negatively graded, commutative ring with identity such that the ideal of positive elements is generated by finitely many elements of degree $+1$ (in fact, by $N$ elements of degree $+1$ if $X \subset \mathbb{P}^N(k)$ or in $\mathbb{P}^N(A)$ as a closed subvariety or closed subscheme). However, if $X$ is, e.g. a projective algebraic variety over a field $k$ of characteristic $p$, say even the prime field of characteristic $p$, $\mathbb{Z}/p\mathbb{Z}$, then unless $X$ is of dimension 0, $W^-(X)$ is by no means an algebraic variety over $\hat{\mathbb{Z}}_p$; although $W^-(X)$ is an infinitely projective scheme over $W^-(k)$, or $\hat{\mathbb{Z}}(k)$, or over $\hat{\mathbb{Z}}_p$, in this case the rings of $W^-(X)$ are not even Noëtherian. (Of course, in this case, $W^-(X)$ is covered by $N$ affines if $X \subset \mathbb{P}^N(k)$ or in $\mathbb{P}^N(\mathbb{Z}/p\mathbb{Z})$). An interesting example is $W^-(\mathbb{P}^N(\mathbb{Z}/p\mathbb{Z}))$, which admits a morphism into $\mathbb{P}^N(\hat{\mathbb{Z}}_p)$, but is "very much bigger" then $\mathbb{P}^N(\hat{\mathbb{Z}}_p)$. (A peculiar fact is that the morphism from $W^-(\mathbb{P}^N(\mathbb{Z}/p\mathbb{Z}))$ into $\mathbb{P}^N(\hat{\mathbb{Z}}_p)$ is an affine map.)

Thus, even if we start with algebraic varieties, the functor $W^-$ maps us into very infinite, non-Noëtherian schemes.

*Note* 3. The reader who does not like preschemes and proschemes can nevertheless "escape". Let $X$ be an arbitrary algebraic variety over a field of characteristic $p \neq 0$ (or, if one wishes, a prescheme or proscheme over $\mathbb{Z}/p\mathbb{Z}$, $p$ a rational prime). Then, from Theorem 1 above, it follows that the assignment: $U \rightsquigarrow W^-(\Gamma(U, \mathcal{O}_X))$ is a sheaf on the open base for the topological space $X$ consisting of the affine open subsets. (If $X$ is a proscheme, then one must say: "The assignment $U \rightsquigarrow W^-(\Gamma(U, \mathcal{O}_X))$, $U$ an open subset of $X$, is a presheaf on the topological space $X$. Consider the associated sheaf.") Therefore, this assignment extends uniquely, up to canonical isomorphisms, to a sheaf, call it $\mathcal{W}^-(X)$, on the topological space $X$. The pair $(X, \mathcal{W}^-(X))$ is a ringed space (i.e., a topological space together with a sheaf of commutative rings with identity) – although not a local ringed space unless $X$ is either empty or a disjoint union of zero dimensional algebraic varieties over $\mathbb{Z}/p\mathbb{Z}$. Moreover, this pair is a finer invariant than the prescheme or proscheme $W^-(X)$ constructed in Theorem 2 above, in the sense that the prescheme or proscheme $W^-(X)$ can easily be constructed from the ringed space $(X, \mathcal{W}^-(X))$, but not conversely (except in the degenerate case that $X$ is either empty or a disjoint union of zero dimensional algebraic varieties over $\mathbb{Z}/p\mathbb{Z}$). Thus the sheaf of $\hat{\mathbb{Z}}_p$-algebras $\mathcal{W}^-(X)$ on $X$ is, in fact, a stronger invariant than the "infinite prescheme" or "infinite proscheme" $W^-(X)$. $W^-(X)$ can be regarded as being in some sense a "logic prescheme or proscheme," since it is normally very infinite and non-Noëtherian – and since it can, if we wish, be replaced by the sheaf $\mathcal{W}^-(X)$ on $X$. In all applications of $W^-(X)$ (except for the heuristic application that $W^-(X)$ is, after all, a kind of canonical lifting of $X$ back to characteristic zero), including all homological, cohomological, and a few other applications, one can work equally well with the sheaf $\mathcal{W}^-(X)$ on the topological space $X$ as with the infinite prescheme or proscheme $W^-(X)$. In fact, in certain ways $\mathcal{W}^-(X)$ might be considered better by some people (it is a somewhat stronger invariant). That is basically a matter of taste.

*Note* 4. Theorem 1 above is the really important properties of the bounded Witt vectors not shared by the Witt vectors which makes them very useful in certain applications, including $p$-adic cohomology. First, the bounded Witt vectors fit together well to lift algebraic varieties, preschemes or proschemes. (This is analogous to the functor, $B \rightsquigarrow B[T]$, which also obeys the analogous properties of Theorem 1, and therefore generalizes to $X \rightsquigarrow X[T]$, $X$ an algebraic variety, prescheme or proscheme.) The properties of Theorem 1 are also important for the $p$-adic cohomology. Because $A \rightsquigarrow W^-(A)$ "behaves like polynomials," it turns out that the corresponding $p$-adic cohomology "behaves like the $p$-adic cohomology of polynomials." (In fact, we will see later, after defining the concept, that the $p$-adic cohomology of $(\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_n]$, using bounded Witt vectors, is canonically isomorphic to the $p$-adic hypercohomology of the polynomial ring $\hat{\mathbb{Z}}_p[T_1, \ldots, T_n]$. The corresponding $p$-adic cohomology defined using full Witt vectors is canonically isomorphic to the $p$-adic hypercohomology of the formal power series ring $\hat{\mathbb{Z}}_p\langle T_1, \ldots, T_n\rangle$. The latter is undesirable if $n \geq 1$, as that cohomology group has topological $p$-torsion elements that are not $p$-torsion elements, (see [1] for a detailed computation). (Of course, $p$-adic cohomology using the bounded Witt vectors can be defined using the sheaf $\mathcal{W}^-(X)$ instead of the "lifting" $W^-(X)$ if desired. Thus, for the $p$-adic cohomology, Theorem 1 is more significant than Theorem 2.)

*Note* 5. At the other pole from the reader who likes algebraic varieties but prefers to avoid preschemes, there are those who will want to know more about proschemes. These are an abstraction useful in proving both $q$-adic and $p$-adic cohomology theorems that I introduced and described in [1] and earlier in the paper, "On a Conjecture of André Weil", American J. of Mathematics. They are more general even than preschemes, and I think they are a really "better" and "more natural" category. (They are no harder to work with than preschemes, and often are easier because of their greater generality. E.g., a subset closed under generalizations of an algebraic variety is not always a prescheme, but is always a proscheme. Also the category of proschemes, unlike preschemes and algebraic varieties, is closed under arbitrary inverse limits indexed by arbitrary set-theoretically legitimate categories.) This is a matter of heuristics; everyone to his own taste.

*Some other properties of the bounded Witt lifting $W^-(X)$ of an algebraic variety, prescheme or proscheme in characteristic $p \neq 0$:*

Let $X$ be an arbitrary prescheme or proscheme over $\mathbb{Z}/p\mathbb{Z}$. Then

1. $W^-(X)$ is integral (i.e., the local rings, or stalks, $\mathcal{O}_{W^-(X),x}$ of the structure sheaf, all $x \in W^-(X)$, are all integral domains) *if and only if* $X$ is integral.

2. $W^-(X)$ is reduced (i.e., each of the local rings $\mathcal{O}_{W^-(X),x}$ has no non-zero nilpotent elements, all $x \in W^-(X)$) *if and only if* $W^-(X)$ is flat over $\hat{\mathbb{Z}}_p$ (i.e., each of the local rings $\mathcal{O}_{W^-(X),x}$ has no non-zero $p$-torsion elements, all $x \in W^-(X)$) *if and only if* $X$ is reduced.

2a. Always, the natural morphism is an isomorphism:

$$W^-(X)_{\mathrm{red}} \xrightarrow{\approx} W^-(X_{\mathrm{red}}).$$

3. $W^-(X)$ is irreducible *if and only if* $X$ is irreducible.

4. The natural morphism:

$$X \to W^-(X) \underset{\hat{\mathbb{Z}}_p}{\times} (\mathbb{Z}/p\mathbb{Z})$$

(see equation (2) of Theorem 2 above) is an isomorphism *if and only if* $W^-(X) \times_{\hat{\mathbb{Z}}_p} (\mathbb{Z}/p\mathbb{Z})$ is reduced *if and only if* $X$ is perfect (see the last part of section I).

4a. For every prescheme or proscheme $X$ over $\mathbb{Z}/p\mathbb{Z}$, if $X^{p^{-\infty}}$ denotes the perfection of $X$, then there is a natural isomorphism of preschemes or proschemes:

$$W^-(X^{p^{-\infty}}) \xrightarrow{\approx} \varprojlim (\cdots \xrightarrow{F} W^-(X) \xrightarrow{F} W^-(X) \xrightarrow{F} W^-(X)).$$

(Here the inverse limit is the category of preschemes or proschemes respectively. E.g., if $X$ is a prescheme, then the inverse limit is a prescheme. If $X = \operatorname{Spec}(A)$, then this inverse limit corresponds to the direct limit of rings:

$$W^-(A) \xrightarrow{F} W^-(A) \xrightarrow{F} W^-(A) \xrightarrow{F} \cdots.$$

The operator $F$ is, of course, defined as $F = W^-(p^{\prime\text{th}}$ power map).)

Of course $W^-(X)$, like $W^-(A)$ and $W(A)$, is rarely Noëtherian. Also $W^-$(perfect field), unlike $W$(perfect field) is *not* usually a valuation ring, unless $k$ is a finite field. However, for any commutative, finitely generated $(\mathbb{Z}/p\mathbb{Z})$ algebra with identity $A$ that is set-theoretically finite (e.g., a finite field), we have $W^-(A) = W(A)$. In particular, $W^-$(a finite field) $= W$(the finite field) is a discrete valuation ring, and $W^-(\mathbb{Z}/p\mathbb{Z}) = W(\mathbb{Z}/p\mathbb{Z}) \approx \hat{\mathbb{Z}}_p$.

REMARK: A statement analogous to 2a. for the full Witt vectors on a ring would be false. The corresponding true statement for full Witt vectors of a commutative $(\mathbb{Z}/p\mathbb{Z})$-algebra with identity $A$ is that we have a canonical isomorphism:

$$W(A)/(\text{closure for the } V\text{-topology of the set of nilpotent elements}) \xrightarrow{\approx} W(A/(\text{nilpotent elements})).$$

Also, the analogue of condition 4a. to the full Witt vectors on a commutative $\mathbb{Z}/p\mathbb{Z}$ algebra with identity $A$ is also false. The corresponding true statement for full Witt vectors is:

$$[\varinjlim (W(A) \xrightarrow{F} W(A) \xrightarrow{F} W(A) \xrightarrow{F} \cdots)]^{\wedge V} \xrightarrow{\approx} W(A^{p^{-\infty}}).$$

Here the "$\wedge V$" denotes completion with respect to the topology on the direct limit ring $R$ having for neighborhood base at 0, $\{V^iR: i \geq 0\}$.

Thus, equations 2a. and 4a., like the very important property $A$ of Theorem 1, and Theorem 2, are properties enjoyed by bounded Witt vectors that are not enjoyed by full Witt vectors. The analogy with polynomials – $B[T]$ or $X[T]$ – and formal power series – $B\langle T\rangle$ – holds good in these examples. (Bounded Witt vectors and the bounded Witt lifting resemble polynomials, while the full Witt vectors resemble formal power series.) Note also, that the fact that $W^-(k)$ is not always a discrete valuation ring, even if $k$ is a perfect field, is also true for polynomials: $k[T]$ is in fact never a field or discrete valuation ring. While if $k$ is a perfect field, then $W(k)$ is a discrete valuation ring. (And if $k$ is any field, then $k\langle T\rangle$ is a discrete valuation ring.)

*The bounded topology on* $W^-(A)$: Let $A$ be an arbitrary commutative $(\mathbb{Z}/p\mathbb{Z})$-algebra with identity. Then, as we have observed earlier, we have a topology on $W^-(A)$, namely the *$V$-topology*, such that $W^-(A)$ together with this topology is a topological ring. We defined the $V$-topology to be the topology induced from the $V$-topology on $W(A)$ – or, equivalently, the one for which a neighborhood base at 0 is the set of ideals $\{V^iW^-(A): i \geq 0\}$. Then $W^-(A)$, together with its $V$-topology, is a topological ring such that the completion of this topological ring is the full Witt vectors $W(A)$ with its $V$-topology.

In the case that $A$ is a *finitely generated* commutative $(\mathbb{Z}/p\mathbb{Z})$-algebra with identity, $p$ a rational prime, then I define a second, finer topology on $W^-(A)$, which I call the *bounded topology*.

In fact, given a finitely generated, commutative $(\mathbb{Z}/p\mathbb{Z})$-algebra with identity $A$, pick an integer $m \geq 1$ and an epimorphism $\psi: (\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_m] \to A$ of rings with identity. Then define $W_n(A) = \{f \in W(A)$: there exists $g \in W((\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_m])$ such that $g$ is of degree (see section II, equation (1)) $\leq n$ and such that $f = W(\psi)(g)]\}$. Then $W_n(A)$ is a subset of $W(A)$, compact for the $V$-topology, and contained in $W^-(A)$, all integers $n \geq 0$. And in fact

$$W^-(A) = \bigcup_{n \geq 0} W_n(A).$$

Define a topology, which we call the *bounded topology*, on $W^-(A)$ as follows. A subset $U$ of $W^-(A)$ is open for the bounded topology *if and only if* $U \cap W_n(A)$ is open in $W_n(A)$ (for the compact topology induced from the $V$-topology on $W(A)$), all integers $n \geq 0$. It is easy to see that the bounded topology on $W^-(A)$, so defined, is independent of the choice of an integer $m \geq 0$ and of an epimorphism of rings with identity $\psi$: $(\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_m] \to A$. Then the sum and product: $W^-(A) \times W^-(A) \to W^-(A)$ are continuous for the bounded topology, so that $W^-(A)$ together with the bounded topology is a topological ring. Similarly the operators $V$ and $F$ are continuous for the bounded topology.

If $A$ is any finitely generated, commutative, $(\mathbb{Z}/p\mathbb{Z})$-algebra with identity, then the topological ring $W^{-}(A)$ is complete for the bounded topology. (The reason for this is that, if we choose $m$ and $\psi$ as above, then $W_n(A)$ is a compact abelian subgroup of $W^{-}(A)$, and $W^{-}(A)$ is the direct limit of compact topological abelian groups and monomorphisms:

$$W^{-}(A) = \varinjlim_{n \geq 0} W_n(A)$$

in the category of topological abelian groups. A general topology theorem, which I will publish later, therefore implies that $W^{-}(A)$ is complete for the bounded topology).

Note that if $A$ is a finitely generated commutative $(\mathbb{Z}/p\mathbb{Z})$-algebra with identity that is not a finite set, then the topological abelian group $W^{-}(A)$ does *not* have a denumerable neighbourhood base at zero. However, note that the topology on $W^{-}(A)$ is always given by open subgroups. (I.e., there exists a fundamental system of open neighborhoods of zero such that each neighborhood is an additive subgroup.)

REMARK: Intuitively speaking, the bounded topology on $W^{-}(A)$ is "just enough additional structure" to know when a subset of $W^{-}(A)$ is bounded in the sense that it does not contain elements of arbitrarily high degree. In fact, one can define a subset $S$ of $W^{-}(A)$ to be *of bounded degree* (or, more briefly, *bounded*) if and only if its closure for the bounded topology is compact. (A corresponding definition using the $V$-topology would not produce the intuitive idea of "bounded degree," e.g. in the case $A$ is a polynomial ring.) In fact, it is possible to reconstruct the bounded topology on $W^{-}(A)$ from the operator $V$ and knowledge of which sets are bounded in the above sense. (Namely, first note that the operator $V$ determines the $V$-topology on $W^{-}(A)$. Then note that a subset $U$ of $W^{-}(A)$ is open for the bounded topology on $W^{-}(A)$ if and only if, for every bounded subset $S$ of $W^{-}(A)$, the intersection of $U$ and $S$ is open in $S$ for the "$V$-topology on $S$" (i.e., for the topology on $S$ induced by the $V$-topology on $W^{-}(A)$)). (Note that, if $S$ is any subset of $W^{-}(A)$, then $S$ is of bounded degree as just defined *iff* there exists a subset $S_0$ of $W^{-}((\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_n])$ and an integer $N$ such that every element of $S_0$ is of degree $\leq N$, and such that $W^{-}(\psi)(S_0) = S$. Note that this property of a subset $S$ of $W^{-}(A)$ is independent of the choice of an integer $n$ or of an epimorphism $\psi$: $(\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_n] \to A$. (Since by definition a subset $S$ of $W^-(A)$ is bounded if and only if the closure of $S$ for the bounded topology on $W^-(A)$ is compact.))

*Note.* Let $A$ be an arbitrary commutative $(\mathbb{Z}/p\mathbb{Z})$-algebra with identity. Then we can define the *bounded topology* on $W^-(A)$ by requiring that the underlying abelian group of $W^-(A)$, together with this "bounded topology," be the direct limit in the category of topological abelian groups:

$$\lim_{\substack{\rightarrow \\ A_i}} W^-(A_i)$$

where $A_i$ runs through the set of all finitely generated $(\mathbb{Z}/p\mathbb{Z})$-subalgebras with identity of $A$, and where each $W^-(A_i)$ is regarded as a topological abelian group with its bounded topology. If we pose this definition, then the assignment: $A \rightsquigarrow W^-(A)$ from the category of rings with identity into the category of topological abelian groups (where each $W^-(A)$ is given its bounded topology) preserves direct limits indexed by arbitrary directed sets. (Note that the assignment $A \rightsquigarrow W(A)$, the full Witt vectors with the $V$-topology, preserves arbitrary inverse limits indexed by arbitrary directed sets or even indexed by arbitrary set-theoretically legitimate categories.)

If $A$ is any commutative $(\mathbb{Z}/p\mathbb{Z})$-algebra with identity that is of *denumerable* cardinality as a set, then I can show that $W^-(A)$ is complete for the bounded topology as just defined, and is a topological ring. (E.g., $A = B^{p^{-\infty}}$, where $B$ is any finitely (or denumerably) generated $(\mathbb{Z}/p\mathbb{Z})$-algebra, is denumerable as a set).

## IV. *F*-differentials on $W^-(A)$. *F*-null elements

In this section I define *F-differentials* over the bounded Witt vectors. It turns out that the familiar Kahler differentials do not have the desired properties, but a certain quotient, which I define and call the *F-differentials*, and denote $\Gamma^*_{W^-(A)}(W^-(B))$, have the desired properties.

a) Recall the familiar definition of the ordinary, or *Kahler differentials* of a commutative algebra with identity over a commutative ring with identity. Let $A$ be an arbitrary commutative ring with identity and let $B$ be an arbitrary commutative $A$-algebra with identity. Then we define a sequence

$\mathrm{Kah}^q_A(B)$, all integers $q \geq 0$. The definition is: $\mathrm{Kah}^*_A(B)$ is a differential, graded, associative, skew-commutative) $A$-algebra (i.e.,

$\mathrm{Kah}_A^*(B)$ is a non-negatively indexed cochain complex of $A$-modules, and is also a non-negatively indexed graded, associative skew-commutative $A$-algebra), such that if $u \in \mathrm{Kah}_A^h(B)$ and $v \in \mathrm{Kah}_A^q(B)$ then

$$d^{h+q}(u \cup v) = d^h(u) \cup v + (-1)^h(u \cup d^q(v)),$$

together with a homomorphism of $A$-algebras

$$B \to \mathrm{Kah}_A^0(B), \text{ such that the}$$

differential graded $A$-algebra $\mathrm{Kah}_A^*(B)$ and the homomorphism of $A$-algebras $B \to \mathrm{Kah}_A^0(B)$ are universal with these properties. One proves that such an object $\mathrm{Kah}_A^*(B)$ exists and is unique up to canonical isomorphisms. And one shows that

$$\mathrm{Kah}_A^0(B) = B, \mathrm{Kah}_A^q(B) = \bigwedge_B^q \mathrm{Kah}_A^1(B),$$

the $q$-th exterior power over $B$ of $\mathrm{Kah}_A^1(B)$. (Each $\mathrm{Kah}_A^q(B)$ is a $B$-module, since it is a $\mathrm{Kah}_A^0(B)$-module, and $\mathrm{Kah}_A^0(B) = B$.) Thus, the Kahler differential $q$-forms $\mathrm{Kah}_A^q(B)$ of $B$ over $A$, for $q \geq 1$, are determined by the Kahler 1-differentials, $\mathrm{Kah}_A^1(B)$.

b) Let $A$ be a commutative ring with identity and let $B$ be an arbitrary commutative $A$-algebra with identity. Suppose that we have a *topology* on the underlying set of $B$ such that $B$, together with its additive abelian group structure and together with this topology, is a topological abelian group. Suppose further that this topology on $B$ is such that a fundamental system of neighborhoods of 0 consists of open subgroups. Then there is induced a corresponding topology on $\mathrm{Kah}_A^q(B)$, such that $\mathrm{Kah}_A^q(B)$ becomes a topological abelian group such that the topology is given by open subgroups, all integers $q \geq 0$. The definition of a topology on $\mathrm{Kah}_A^q(B)$ is as follows. For each sequence $U_0, \ldots, U_q$ of open subgroups of $B$, let $N_{U_0,\ldots,U_q}$ be the image of $U_0 \otimes_Z U_1 \otimes_Z \cdots \otimes_Z U_q$ under the abelian group homomorphism that sends $x_0 \otimes_Z \cdots \otimes_Z x_p$ into $x_0 \cdot (dx_1) \wedge \cdots \wedge (dx_p) \in \mathrm{Kah}_A^q(B)$. Then we define the topology on $\mathrm{Kah}_A^q(B)$ to be one given by the open subgroups $\{N_{U_0,\ldots,U_q}: U_0, \ldots, U_q$ are open additive subgroups of $B\}$, each integer $q \geq 0$.

Example 1: Let $A$ be an arbitrary finitely generated commutative $(\mathbb{Z}/p\mathbb{Z})$-algebra with identity and let $B$ be an arbitrary finitely generated commutative $A$-algebra with identity. Then $W^-(B)$ is a commutative $W^{-}(A)$-algebra with identity, so we have the $W^{-}(B)$-modules

$$\mathrm{Kah}^{q}_{W^{-}(A)}(W^{-}(B)),$$

each integer $q \geq 0$. We also have defined the bounded topology on $W^{-}(B)$. We have observed that with the bounded topology and its additive abelian group structure, $W^{-}(B)$ is a topological abelian group such that the topology is given by open subgroups (even though there is usually no denumerable neighborhood base at 0). Then by the above construction, there is induced a topology on $\mathrm{Kah}^{q}_{W^{-}(A)}W^{-}(B)$ such that the topology is given by open subgroups, all integers $q \geq 0$. We call this topology the *bounded topology* on $\mathrm{Kah}^{q}_{W^{-}(A)}W^{-}(B)$, each integer $q \geq 0$. (As on $W^{-}(B) = \mathrm{Kah}^{0}_{W^{-}(A)}W^{-}(B)$, this topology almost never possesses a denumerable neighborhood base at zero.)

EXAMPLE 2: Let $A$ be an arbitrary commutative $(\mathbb{Z}/p\mathbb{Z})$-algebra with identity and let $B$ be an arbitrary $A$-algebra. Then the full Witt vectors $W(B)$ is a commutative $W(A)$-algebra with identity. We have the $V$-topology on $W(B)$, which is given by the open subgroups $V^{i}W(B)$, $i \geq 0$. Then by the above procedure there is induced a topology on $\mathrm{Kah}^{q}_{W(A)}W(B)$ that is given by open subgroups, all integers $q \geq 0$, which we call the *$V$-topology*. Since the $V$-topology on $W(B)$ admits a denumerable neighborhood base at 0, it follows that the $V$-topology on $\mathrm{Kah}^{q}_{W(A)}(W(B))$ admits a denumerable neighborhood base at 0.

Under the assumptions of this example, we can also define similarly the *$V$-topology* on $\mathrm{Kah}^{q}_{W^{-}(A)}W^{-}(B)$, all integers $q \geq 0$. This is a topology given by open subgroups and admitting a denumerable neighborhood base at 0. (If $A$ and $B$ are finitely generated $(\mathbb{Z}/p\mathbb{Z})$-algebras then we have both the bounded topology and the $V$-topology on $\mathrm{Kah}^{q}_{W^{-}(A)}W^{-}(B)$, all integers $q \geq 0$. The former is finer than the latter, and is the more important topology on this group, $q \geq 0$.)

c) *$F$-null elements. $F$-differentials.* Let $A$ be an arbitrary commutative $(\mathbb{Z}/p\mathbb{Z})$-algebra with identity and let $B$ be an arbitrary $A$-algebra. Then I define a subgroup of $\mathrm{Kahler}^{q}_{W^{-}(A)}(W^{-}(B))$, $q \geq 0$, which I call the *$F$-null elements.* I then define the *$F$-differential $q$-forms* to be the quotient group, $\Gamma^{q}_{W^{-}(A)}(W^{-}(B)) = \mathrm{Kahler}^{q}_{W^{-}(A)}(W^{-}(B))/(F\text{-null elements})$.

*Case I. $A$ and $B$ are both finitely generated $(\mathbb{Z}/p\mathbb{Z})$-algebras.*

*Subcase IA.* $A \approx (\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_r]$, $B \approx (\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_s]$, there exist integers $r, s \geq 0$ such that $s \geq r$, where the ring homomorphism

$A \to B$ corresponds to the inclusion: $(\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_r] \hookrightarrow (\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_s]$.

Then we have a commutative diagram of ring homomorphisms:

$$\begin{tikzcd} W^-(B) \arrow[r, "F"] & W^-(B) \\ W^-(A) \arrow[r, "F"] \arrow[u] & W^-(A) \arrow[u] \end{tikzcd}$$

This induces an endomorphism, call it $F^q$, of $\mathrm{Kahler}^q_{W^-(A)}(W^-(B))$, all integers $q \geq 0$.

Definition: An element $u \in \mathrm{Kahler}^q_{W^-(A)} W^-(B)$ is an *$F$-torsion element* if and only if there exists an integer $i \geq 0$ such that $(F^q)^i(u) = 0$. (Here $(F^q)^i$ denotes the composite of $F^q$ with itself $i$ times.) The *$F$-null elements* in $\mathrm{Kahler}^q_{W^-(A)}(W^-(B))$ are the closure, for the bounded topology, of the $F$-torsion elements. Then, as we have indicated above, we define the *$F$-differential $q$-forms of $W^-(B)$ over $W^-(A)$* to be

$$\Gamma^q_{W^-(A)}(W^-(B)) = \mathrm{Kahler}^q_{W^-(A)}(W^-(B))/(F\text{-null elements}).$$

I define a topology on $\Gamma^q_{W^-(A)}(W^-(B))$, namely the quotient topology from the bounded topology on $\mathrm{Kahler}^q_{W^-(A)}(W^-(B))$. I call this topology the *bounded topology* on $\Gamma^q_{W^-(A)}(W^-(B))$, all integers $q \geq 0$. Then we obtain the following theorem.

Theorem: *If $A$ and $B$ are as in Subcase IA, then $\Gamma^q_{W^-(A)} W^-(B)$ is complete for the bounded topology, all integers $q \geq 0$.*

*Subcase IB.* $A$ an arbitrary finitely generated commutative $(\mathbb{Z}/p\mathbb{Z})$-algebra with identity, $B$ an arbitrary commutative finitely generated $A$-algebra with identity.

Then picking integers $r$ and $s$ such that $s \geq r \geq 0$ and pick epimorphisms of rings with identity $\varphi: (\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_r] \to A$ and $\psi: (\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_s] \to B$ such that the diagram

$$\begin{tikzcd} (\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_s] \arrow[r, "\psi"] & B \\ (\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_r] \arrow[r, "\varphi"] \arrow[u, hook] & A, \arrow[u] \end{tikzcd}$$

is commutative, where the vertical homomorphisms are the inclusion and the given homomorphism $A \to B$ respectively. Then define the *$F$-null elements* in $\text{Kahler}^q_{W^-(A)}(W^-(B))$ to be the closure for the bounded topology in $\text{Kahler}^q_{W^-(A)}(W^-(B))$ of the image under the induced homomorphism of abelian groups:

$$\text{Kahler}^q_{W^-((\mathbb{Z}/p\mathbb{Z})[T_1,\ldots,T_r])} W^-((\mathbb{Z}/p\mathbb{Z})[T_1,\ldots,T_s]) \to \text{Kahler}^q_{W^-(A)} W^-(B)$$

of the $F$-torsion elements (as defined in Subcase IA above) in $\text{Kahler}^q_{W^-((\mathbb{Z}/p\mathbb{Z})[T_1,\ldots,T_r])} W^-((\mathbb{Z}/p\mathbb{Z})[T_1,\ldots,T_s])$. It is easy to see that this definition of the $F$-null elements in $\text{Kahler}^q_{W^-(A)} W^-(B)$ is independent of the choice of integers $r$, $s \geq 0$ and of epimorphisms $\varphi$, $\psi$ having the above properties.

Then define

$$\Gamma^q_{W^-(A)} W^-(B) = \text{Kahler}^q_{W^-(A)}(W^-(B))/(F\text{-null elements}).$$

We regard $\Gamma^q_{W^-(A)} W^-(B)$ as being a topological abelian group with the quotient topology from the bounded topology on $\text{Kah}^q_{W^-(A)}(W^-(B))$. We call this topology on $\Gamma^q_{W^-(A)} W^-(B)$ the *bounded topology*. Then, once again,

THEOREM: *Under the hypotheses of Subcase IB, we have that $\Gamma^q_{W^-(A)} W^-(B)$ is complete for the bounded topology, all integers $q \geq 0$.*

*Case II.* General Case: $A$ is an arbitrary commutative $(\mathbb{Z}/p\mathbb{Z})$-algebra with identity, $p$ a rational prime, and $B$ is an arbitrary commutative $A$-algebra with identity.

Then define the *$F$-differential $q$-forms of $W^-(B)$ over $W^-(A)$* to be

$$\Gamma^q_{W^-(A)} W^-(B) = \varinjlim_{(A',B')} \Gamma^q_{W^-(A')} W^-(B'),$$

where the direct limit is taken in the category of abelian groups, each integer $q \geq 0$, and where the indexing directed set is the set of all pairs $(A', B')$ where $A'$ is a finitely generated subring of $A$ and $B'$ is a finitely generated sub-$A'$-algebra of $B$ (pairs being ordered in the obvious way).

REMARK 1: In the situation of Case II, we can define the *bounded topology* on $\Gamma^q_{W^-(A)} W^-(B)$ to be the topology such that $\Gamma^q_{W^-(A)}(W^-(B))$ becomes the direct limit of the indicated direct system in the category of all topological spaces. Then if the ring $B$ is of denumerable cardinality as a set, I can show that the abelian group $\Gamma^q_{W^-(A)}(W^-(B))$ together with the bounded topology so defined, is a topological abelian group, and is also *complete* for the bounded topology, all integers $q \geq 0$. (This applies, e.g., to $\Gamma^q_{W^-(A)}(W^-(B^{p^{-\infty}}))$ and to $\Gamma^q_{W^-(A)}(W^-(B))$ whenever $B$ is an $A$-algebra, $A$ is any ring in characteristic $p$, and $B$ is denumerably generated as a ring.)

Thus, in all cases, if $B$ is an arbitrary commutative $A$-algebra with identity where $A$ is an arbitrary commutative $(\mathbb{Z}/p\mathbb{Z})$-algebra with identity, $p$ a rational prime, we have constructed a certain quotient abelian group of the Kahler differential $q$-forms $\mathrm{Kah}^q_{W^-(A)}W^-(B)$, which we denote as $\Gamma^q_{W^-(A)}(W^-(B))$, and call the *F-differential q-forms of $W^-(B)$ over $W^-(A)$*, all integers $q \geq 0$. If $B$ is denumerable as a set, then we have defined a topology on $\Gamma^q_{W^-(A)}(W^-(B))$, which we call the *bounded topology*, such that the additive abelian group of $\Gamma^q_{W^-(A)}(W^-(B))$ is a complete topological abelian group with the bounded topology, all integers $q \geq 0$. It is easy to see that $\Gamma^*_{W^-(A)}(W^-(B))$ is always a *differential graded $W^-(A)$-algebra* – i.e., that the structure of differential graded $W^-(A)$-algebra (that is, the coboundary operators and the cup product) defines, by passing to the quotient, the structure of non-negatively graded differential graded $W^-(A)$-algebra on the non-negatively graded $W^-(A)$-module $\Gamma^*_{W^-(A)}(W^-(B))$, all pairs $A$, $B$ where $A$ is an arbitrary commutative $(\mathbb{Z}/p\mathbb{Z})$-algebra with identity and where $B$ is an arbitrary commutative $A$-algebra with identity. (Thus, for every such $A$ and $B$, if $\Gamma^q_{W^-(A)}(W^-(B))$ is the $F$-differential $q$-forms, then we have $d^q\colon \Gamma^q_{W^-(A)}(W^-(B)) \to \Gamma^{q+1}_{W^-(A)}(W^-(B))$, a homomorphism of $W^-(A)$-modules, all integers $q \geq 0$, and that for every pair of integers $h$, $q \geq 0$, if $f \in \Gamma^h_{W^-(A)}(W^-(B))$ and $g \in \Gamma^q_{W^-(A)}(W^-(B))$ then we have the cup product $f \cup g \in \Gamma^{h+q}_{W^-(A)}(W^-(B))$. And the operators $d^q$, $q \geq 0$, and cup products, obey the usual familiar identities.) Also, the natural homomorphism $W^-(B) \to \Gamma^0_{W^-(A)}(W^-(B))$ is a isomorphism, all commutative $(\mathbb{Z}/p\mathbb{Z})$-algebras with identity $A$, all commutative $A$-algebras with identity $B$, and all rational primes $p$.

REMARK 2: Let $A$, $B$ be as above. Then we can also define the *$V$-topology* on $\Gamma^q_{W^-(A)}W^-(B)$, all integers $q \geq 0$. $\Gamma^q_{W^-(A)}W^-(B)$ is not in general complete for the $V$-topology. We use the symbol $\Gamma^q_{W(A)}W(B)$ for the completion of $\Gamma^q_{W^-(A)}W^-(B)$ with respect to the $V$-topology, all commutative $(\mathbb{Z}/p\mathbb{Z})$-algebras with identity $A$, all commutative $A$-algebras with identity $B$, all rational primes $p$. Then $\Gamma^*_{W(A)}(W(B))$ is a differential non-negatively graded $W(A)$-algebra, and the natural ring homomorphism $W(B) \to \Gamma^0_{W(A)}(W(B))$ is an isomorphism, all pairs $(A, B)$ obeying the above hypotheses. We call $\Gamma^*_{W(A)}(W(B))$ the *F-differentials of $W(B)$ over $W(A)$*. These $F$-differentials of $W(B)$ over $W(A)$ play an analogous role with respect to full Witt vectors that the $F$-differentials $\Gamma^*_{W^-(A)}(W^-(B))$ of $W^-(B)$ over $W^-(A)$ play with respect to bounded Witt vectors.

*Sheaves of F-differentials over a proscheme*

THEOREM 1: *Let $A$ be an arbitrary commutative $(\mathbb{Z}/p\mathbb{Z})$-algebra with identity where $p$ is a rational prime. Let $X$ be an arbitrary prescheme over the ring $A$. Then $W^-(X)$ is a prescheme over the ring $W^-(A)$. Then for each integer $q \geqq 0$ there exists, up to canonical isomorphisms, a unique sheaf of $\mathcal{O}_{W^-(X)}$-modules over $W^-(X)$, call it $\Gamma^q_{W^-(A)}(X)$, such that*

(1) *For every affine open subset $U_0$ of $X$, if $B = B_{U_0} = \Gamma(U_0, \mathcal{O}_X)$, and $U = W^-(U_0)$, then we have a fixed isomorphism between $\Gamma^q_{W^-(A)}(X)|U$ and the quasicoherent sheaf of $\mathcal{O}_U$-modules over $U \approx$ Spec $(W^-(B))$ corresponding to the $W^-(B_{U_0})$-module, $\Gamma^q_{W^-(A)}(W^-(B_{U_0}))$, and*

(2) *If $U_0 \subset V_0$ are affine open subsets of $X$, then the restriction homomorphism $(\Gamma^q_{W^-(A)}(X))(V) \to (\Gamma^q_{W^-(A)}(X))(U)$ corresponds, under the fixed isomorphisms* (1), *to the restriction homomorphism*

$$\Gamma^q_{W^-(A)}(W^-(B_{V_0})) \to \Gamma^q_{W^-(A)}(W^-(B_{U_0}))$$

*induced by the ring homomorphism*: $B_{V_0} \to B_{U_0}$, where $B_{U_0} = \Gamma(U_0, \mathcal{O}_X)$, $B_{V_0} = \Gamma(V_0, \mathcal{O}_X)$, *and $U = W^-(U_0)$ and $V = W^-(V_0)$.*

The proof of Theorem 1 is obvious.

THEOREM 2: *Let $A$ be an arbitrary commutative $(\mathbb{Z}/p\mathbb{Z})$-algebra with identity where $p$ is an arbitrary rational prime. Let $X$ be an arbitrary proscheme over $A$. Then $W^-(X)$ is a proscheme over $W^-(A)$. Then for each integer $q \geq 0$, there is induced a sheaf $\Gamma^q_{W^-(A)}(X)$ of $\mathcal{O}_{W^-(X)}$-modules over $W^-(X)$, such that,*

(1) *For every subset $U$ closed under generalization of $X$, if $U$ is affine, then there is induced a fixed isomorphism between $\Gamma^q_{W^-(A)}(X)|W^-(U)$ and the sheaf of $\mathcal{O}_{W^-(U)}$-modules over $W^-(U) \approx$ Spec $(W^-(B_U))$ (where $B_U = \Gamma(U, \mathcal{O}_U)$) that corresponds to the $W^-(B_U)$-module $\Gamma^q_{W^-(A)}(W^-(B_U))$.*

(2) *Let $U$, $V$ be open subsets of $X$ such that $u \subset V$. Then the*

*diagram*:

$$\begin{array}{ccc}(\Gamma^q_{W^-(A)}(X))(W^-(V)) & \to & \Gamma^q_{W^-(A)}(X)(W^-(U)) \\ \uparrow & & \uparrow \\ \Gamma^q_{W^-(A)}(W^-(\Gamma(V, \mathcal{O}_X))) & \to & \Gamma^q_{W^-(A)}(W^-(\Gamma(U, \mathcal{O}_X)))\end{array}$$

*is commutative, where the vertical homomorphisms are the natural maps, and where the horizontal homomorphisms are the restriction and the homomorphism induced by the $A$-algebra homomorphism:*

$$\Gamma(V, \mathcal{O}_X) \to \Gamma(U, \mathcal{O}_X).$$

Theorems 1 and 2 are quite easy to prove. Notice that in the situation of Theorem 1, each of the sheaves $\Gamma^q_{W^-(A)}(X)$ is quasi-coherent, while we do not know this in the situation of Theorem 2. (However, in the situation of Theorem 2, for every subset closed under generalization $U$ of $X$ that is a prescheme, we can show that $\Gamma^q_{W^-(A)}(X)|W^-(U)$ is canonically isomorphic to $\Gamma^q_{W^-(A)}(U)$ as defined in Theorem 1, and therefore is a quasi-coherent sheaf of $\mathcal{O}_{W^-(U)}$-modules over $W^-(U)$. At any rate, under the hypotheses of either Theorem 1 or 2, the sheaves $\Gamma^q_{W^-(A)}(X)$, $q \geq 0$, form in a natural way a (non-negatively graded) sheaf of associative, anti-commutative differential graded $W^-(A)$-algebras, call if $\Gamma^*_{W^-(A)}(X)$, over $W^-(X)$ (i.e., we have the expected coboundaries and cup products, and these obey the expected identities).

Remark 3: The sheaves $\Gamma^q_{W^-(A)}(X)$, $q \geq 0$, and the cochain complex of sheaves $\Gamma^*_{W^-(A)}(X)$, over $W^-(X) q \geq 0$, can be interpreted as coming from sheaves $\boldsymbol{\Gamma}^q_{W^-(A)}(X)$ of $\mathcal{W}^-(X)$-modules over $X$, and cochain complexes of sheaves $\boldsymbol{\Gamma}^*_{W^-(A)}(X)$ of $\mathcal{W}^-(A)$-modules over $X$, respectively, where $\mathcal{W}^-(X)$ is the sheaf on $X$ described in section III, Note 3. This enables one to escape working with $W^-(X)$ in the $p$-adic cohomological applications if desired. Another slight advantage to this point of view: The operators $V$ and $F$ on $W^-(A)$, $A$ a commutative $(\mathbb{Z}/p\mathbb{Z})$-algebra with identity, both generalize to operators, call them $V$ and $F$, on the sheaf $\mathcal{W}^-(X)$, where $X$ is any prescheme or proscheme over $(\mathbb{Z}/p\mathbb{Z})$. (More precisely, the generalized $V$ and $F$ are additive endomorphisms of the sheaf $\mathcal{W}^-(X)$ over the topological space $X$. $F$ is also multiplicative, and is an endomorphism of the sheaf of rings $\mathcal{W}^-(X)$.) This is an advantage to taking the $W^-(X)$ point of view. For, although the operator $F$ makes sense on $W^-(X)$ (we define it to be $W^-(p'^{\text{th}}$ power map)), there is no reasonable way to make sense of $V$ on $W^-(X)$ for a general $X$ (even in the case $X$ is Euclidean space, $X = \operatorname{Spec}((\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_n])$, if $n \geq 1$). The difficulty is that there is no natural *continuous* such operator $V$ on the underlying topological space of $W^-(X)$ such that, together with some homomorphism of sheaves of abelian groups on $W^-(X)$: $\mathcal{O}_{W^-(X)} \to V_*(\mathcal{O}_{W^-(X)})$, the resulting operator $V$ is compatible with our previously defined $V$ on the global sections of $W^-(U)$, all open subsets $U$ of $X$. If $X$ is *perfect*, then such a $V$ can be defined. In the general case (even in the case $X$ = Euclidean space over $(\mathbb{Z}/p\mathbb{Z})$ of dimension $\geq 1$), it is impossible to define such an operator $V$ such that the induced function $W^-(X) \to W^-(X)$ is *continuous*. (It is, however, possible to define a discontinuous $V$). However, if we take the *sheaf* point of view $\mathcal{W}^-(X)$ instead of the *canonical lifting* point of view $W^-(X)$, then such a $V$ is easy to define, as indicated above.

Remark 4: The definition of sheaves of $F$-differentials given in Theorems 1 and 2 above can be generalized. Let $p$ be any rational prime and let $Y$ be a prescheme (or proscheme) over $\mathbb{Z}/p\mathbb{Z}$. Let $X$ be a prescheme (or proscheme) over $Y$. Then we can define the *$F$-differentials* $\Gamma^*_{W^-(Y)}(X)$, a sheaf of differential graded $\mathcal{O}_{W^-(Y)}$-algebras over $W^-(X)$ such that $\Gamma^0_{W^-(Y)} = \mathcal{O}_{W^-(X)}$. If $X$ and $Y$ are preschemes, then each $\Gamma^q_{W^-(Y)}(X)$ is a quasi-coherent sheaf of $\mathcal{O}_{W^-(X)}$-modules over $W^-(X)$, $q \geq 0$. (In general, $\Gamma^q_{W^-(Y)}(X)$ and $\Gamma^*_{W^-(Y)}(X)$ can be regarded as coming from $\boldsymbol{\Gamma}^q_{W^-(Y)}(X)$ and $\boldsymbol{\Gamma}^*_{W^-(Y)}(X)$, sheaves and differential graded sheaves of $W^-(A)$-algebras, respectively, over $X$, all integers $q \geq 0$, as in Remark 3 of section III and as in Remark 3 above.)

## V. Definition of $p$-Adic Cohomology using the Bounded Witt Vectors

Definition: Let $p$ be an arbitrary rational prime and let $A$ be an arbitrary commutative ring with identity. Let $X$ be an arbitrary prescheme, or proscheme, over $A$. Let $U$ be any open subset of $X$. Then we define the *$p$-adic cohomology groups of $X$ modulo $U$ with coefficients in $W^-(A)$*:

$$H^i(X, U, W^-(A)), \quad i \geq 0,$$

a sequence of $W^-(A)$-modules that form an associative, anti-commutative graded $W^-(A)$-algebra with respect to an operation called the *cup product.*

First recall that we have $W(A)$, the (ordinary) Witt vectors on $A$ (section I). We have defined the bounded Witt vectors $W^{-}(A)$ on $A$, a subring of $W(A)$ (section II). We have defined $W^{-}(X)$, a prescheme or proscheme over $W^{-}(A)$ (that is a "canonical lifting" of $X$ back to characteristic zero) (section III). We have defined the $F$-differentials on $W^{-}(X)$ over $W^{-}(A)$, $\Gamma^{*}_{W^{-}(A)}(X)$, a quotient sheaf of differential graded algebras of the usual Kahler differentials $\mathrm{Kah}^{*}_{W^{-}(A)}(W^{-}(X))$ by a subsheaf of ideals which we called the *F-null elements* (section IV). Finally, we define

$$H^{h}(X, U, W^{-}(A)) = H^{h}(W^{-}(X), W^{-}(U), \Gamma^{*}_{W^{-}(A)}(X)), \tag{1}$$

all integers $h \geq 0$. The cohomology groups on the right side of equation (1) are the hypercohomology groups of the topological space $W^{-}(X)$ modulo the open subset $W^{-}(U)$ with coefficients in the cochain complex of sheaves of $W^{-}(A)$-algebras $\Gamma^{*}_{W^{-}(A)}(X)$, as defined in [1] and [2].

REMARK 1: The definition of the cohomology of $X$ modulo $U$ with coefficients in $W^{-}(A)$ can be given without using the canonical lifting $W^{-}(X)$. Namely, consider the sheaf $\mathcal{W}^{-}(X)$ of $\hat{\mathbb{Z}}_{p}$-algebras on the topological space $X$ defined in Remark 3 of section III. And consider the cochain complex of sheaves of $W^{-}(A)$-modules (in fact, sheaf of differential non-negatively graded $W^{-}(A)$-algebras) over the topological space $X$, $\boldsymbol{\Gamma}^{*}_{W^{-}(A)}(X)$, defined in Remark 3 of section IV. Then define alternatively

$$H^{h}(X, U, W^{-}(A)) = H^{h}(X, U, \boldsymbol{\Gamma}^{*}_{W^{-}(A)}(X)), \tag{1'}$$

all integers $h \geq 0$, the hypercohomology of the topological space $X$ modulo the open subset $U$ with coefficients in the cochain complex of sheaves of $W^{-}(A)$-modules $\boldsymbol{\Gamma}^{*}_{W^{-}(A)}(X)$ described in Remark 3 of section IV. Then I can show that definitions (1) and (1′) are equivalent in the sense that they yield canonically isomorphic $W^{-}(A)$-modules $H^{h}(X, U, W^{-}(A))$, $h \geq 0$. (The natural map is from the right side of equation (1′) into the right side of equation (1). A few spectral sequences show that this map is always an isomorphism. The proof is especially simple in the case that $X$ is a prescheme.) Notice also that the definition of the sheaf $\mathcal{W}^{-}(X)$ makes sense if $X$ is merely a commutative ringed space (with identity) over $\mathbb{Z}/p\mathbb{Z}$, $p$ a rational prime, and the sheaves $\boldsymbol{\Gamma}^{*}_{W^{-}(A)}(X)$ can be defined in this case if merely $X$ is a topological space together with a sheaf $\mathcal{O}_X$ of commutative

$A$-algebras with identity over the topological space $X$, where $A$ is any commutative $(\mathbb{Z}/p\mathbb{Z})$-algebra with identity and $p$ is any rational prime. Therefore, even at this level of generality, if we use the definition (1′) instead of (1), ((1) and (1′) are equivalent whenever (1) makes sense), then we obtain a definition of the non-negatively graded, associative, anti-commutative $W^{-}(A)$-algebra $H^h(X, U, W^{-}(A))$, $h \geq 0$, all open subsets $U$ of $X$.

REMARK 2: Let $p$ be a rational prime, let $Y$ be a prescheme or proscheme over $(\mathbb{Z}/p\mathbb{Z})$ and let $X$ be a prescheme or proscheme over $Y$. Let $U$ be any open subset of $X$. Then we can define a graded $W^{-}(\Gamma(Y, O_Y))$-algebra

$$(2) \qquad H^h(X, U, W^{-}(Y)) = H^h(W^{-}(X), W^{-}(U), \Gamma^*_{W^{-}(Y)}(X)),$$

all integers $h \geq 0$. An alternative equivalent definition, (2′), analogous to definition (1′) in Remark 1 above, in which sheaves on $X$ replace the sheaves on $W^{-}(X)$ to give hypercohomology groups on $X$ modulo $U$ instead of on $W^{-}(X)$ modulo $W^{-}(U)$, can also be given. Again, this latter definition can be generalized even beyond the proscheme case; which can be interpreted as an advantage.

Note that the $p$-adic cohomology we have defined above *does not require tensoring over* $\hat{\mathbb{Z}}_p$ *with* $\hat{\mathbb{Q}}_p$. This is an advantage over the theory that I defined in [1] and [2].[1]

Does the $p$-adic hypercohomology, which is a functor of $X$ and $U$, depend only on the perfections $X^{p^{-\infty}}$ and $U^{p^{-\infty}}$ of $X$ and $U$? The following theorem, and the Remark following, answer this.

THEOREM: *Let $p$ be a rational prime, let $A$ be a commutative $(\mathbb{Z}/p\mathbb{Z})$-algebra with identity and let $X$ be a proscheme over $A$ that is cover finite. (E.g., if $X$ is a prescheme, then $X$ is cover finite iff $X$ is quasicompact, and the intersection of any two affine open subsets of $X$ is quasicompact.) Let $U$ be a quasicompact open subset of $X$. Then the natural homomorphism is an isomorphism*:

$$(2) \qquad H^h(X, U, W^{-}(A)) \underset{\hat{\mathbb{Z}}_p}{\otimes} \hat{\mathbb{Q}}_p \approx \xrightarrow{\approx} H^h(X^{p^{-\infty}}, U^{p^{-\infty}}, W^{-}(A)) \underset{\hat{\mathbb{Z}}_p}{\otimes} \hat{\mathbb{Q}}_p,$$

*all integers $h \geq 0$.*

[1] However, the alternative generalization of our $p$-adic cohomology, in our forthcoming paper [2], which generalizes directly the theory in our paper [1], (See Note 3 in the footnote following the Introduction), shares this advantage.

*Note.* We also always have that $W^{-}(A^{p^{-\infty}}) \otimes_{\hat{\mathbb{Z}}_p} \hat{\mathbb{Q}}_p \approx W^{-}(A) \otimes_{\hat{\mathbb{Z}}_p} \hat{\mathbb{Q}}_p$. Since $X$ is cover-finite and $U$ is quasicompact, the operation of "$\otimes_{\hat{\mathbb{Z}}_p} \hat{\mathbb{Q}}_p$" commutes with taking cohomology of sheaves over $X$ modulo $U$. Therefore in equation (2), we can replace the coefficient group $W^{-}(A)$ on the right side of the equation with $W^{-}(A^{p^{-\infty}})$, if we wish, and this still leaves a correct formula.

*Sketch of proof*: Recall that $X$ and $X^{p^{-\infty}}$ have the same underlying topological space. Using property 4a. following Note 5 of section III, it is easy to see that the natural homomorphism of cochain complexes of sheaves of $W^{-}(A)$-modules over $W^{-}(X)$:

$$\Gamma^{*}_{W^{-}(A)}(X) \underset{\hat{\mathbb{Z}}_p}{\otimes} \hat{\mathbb{Q}}_p \to \Gamma^{*}_{W^{-}(A)}(X^{p^{-\infty}}) \underset{\hat{\mathbb{Z}}_p}{\otimes} \hat{\mathbb{Q}}_p$$

is an isomorphism. Since the topological space $X$ is cover finite and since $U$ is a quasicompact open subset of $X$, we have that

$$H^{h}(X, U, F^{*} \underset{\hat{\mathbb{Z}}_p}{\otimes} \hat{\mathbb{Q}}_p) \approx H^{h}(X, U, F^{*}) \underset{\hat{\mathbb{Z}}_p}{\otimes} \hat{\mathbb{Q}}_p,$$

all cochain complexes of sheaves $F^{*}$ of $W^{-}(A)$-modules over the topological space $X$. Applying this last isomorphism to the two cochain complexes $\Gamma^{*}_{W^{-}(A)}(X)$ and $\Gamma^{*}_{W^{-}(A)}(X^{p^{-\infty}})$, and using the isomorphism

$$\Gamma^{*}_{W^{-}(A)}(X) \underset{\hat{\mathbb{Z}}_p}{\otimes} \hat{\mathbb{Q}}_p \approx \Gamma^{*}_{W^{-}(A)} X^{p^{-\infty}} \underset{\hat{\mathbb{Z}}_p}{\otimes} \hat{\mathbb{Q}}_p$$

yields the theorem. The proof of the observation in the Note is similar.

Remark: The preceding theorem implies that, for "reasonable" (more precisely, cover finite) $X$ and $U$, the $p$-adic hypercohomology groups (1), *after tensoring over* $\hat{\mathbb{Z}}_p$ *with* $\hat{\mathbb{Q}}_p$, depend only on the perfections $X^{p^{-\infty}}$ and $U^{p^{-\infty}}$ of $X$ and $U$. In particular, $H^{h}(X, U, W^{-}(A)) \otimes_{\hat{\mathbb{Z}}_p} \hat{\mathbb{Q}}_p$ does not depend on the nilpotent elements on $X$:

Corollary: *Let $p$ be a rational prime, let $A$ be a commutative $(\mathbb{Z}/p\mathbb{Z})$-algebra with identity, let $X$ be a proscheme over $A$ that is cover finite, and let $U$ be an open subset of $X$ that is quasicompact. Then the* *natural homomorphisms are isomorphisms*:

$$(3)\quad H^h(X, U, W^-(A)) \underset{\hat{\mathbb{Z}}_p}{\otimes} \hat{\mathbb{Q}}_p \approx H^h(X_{\text{red}}, U_{\text{red}}, W^-(A)) \underset{\hat{\mathbb{Z}}_p}{\otimes} \hat{\mathbb{Q}}_p$$
$$\approx H^h(X^{p^{-\infty}}, U^{p^{-\infty}}, W^-(A^{p^{-\infty}})) \underset{\hat{\mathbb{Z}}_p}{\otimes} \hat{\mathbb{Q}}_p$$

*all integers* $h \geq 0$.

PROOF: $X$ and $X_{\text{red}}$ have the same perfection. Therefore the Corollary follows from the Theorem and the Note.

REMARK 1: One might wonder whether either the above theorem or corollary remain true if we do not tensor over $\hat{\mathbb{Z}}_p$ with $\hat{\mathbb{Q}}_p$. The answer is "no," counterexamples to both statements are easy to construct. Thus, the hypercohomology groups [1] tensored over $\hat{\mathbb{Z}}_p$ with $\hat{\mathbb{Q}}_p$ are independent of nilpotent elements and, in fact, depend only on the perfections if $X$ and $U$ obey a very mild condition ("cover finite." All algebraic varieties are cover finite). However, if we do *not* tensor over $\hat{\mathbb{Z}}_p$ with $\hat{\mathbb{Q}}_p$, then this is no longer the case. Roughly speaking, the $p$-torsion in the group [1] is sensitive to nilpotent elements on $X$. (But once we tensor over $\hat{\mathbb{Z}}_p$ with $\hat{\mathbb{Q}}_p$, then if $X$ and $U$ are cover finite, the resulting groups are independent of nilpotent elements on $X$ and, in fact, depend only on the perfections $X^{p^{-\infty}}$ and $U^{p^{-\infty}}$ of $X$ and $U$.)

REMARK 2: Considering the definition (1), we have the two spectral sequences of relative hypercohomology (see [1]), both of which abut at the groups (1). The first of these is as follows:

$$E_1^{p,q} = H^q(W^-(X), W^-(U), \Gamma^p_{W^-(A)}(X)) \Rightarrow H^n(X, U, W^-(A)).$$

This spectral sequence induces a filtration on the abutment, i.e. on the groups (1), which in [1] I have called the *Hodge filtration*. One is tempted to define the associated graded (i.e., ${}^I E_\infty^{p,q}(W^-(X), W^-(U), \Gamma^*_{W^-(A)}(X))$, the $E_\infty^{p,q}$-term for the first spectral sequence of relative hypercohomology) to be the "Hodge decomposition." Of course, such "Hodge pieces"

$$H^{p,q}(X, U, W^-(A)) = {}^I E_\infty^{p,q}(W^-(X), W^-(U), \Gamma^*_{W^-(A)}(X))$$

are functors of the pair $(X, U)$ (and even of the triple $(X, U, W^-(A))$.

A few examples show, however, that such a definition does not always have all the properties that we would normally expect of a "Hodge decomposition."

EXAMPLE: Let $A = k$ be a finite field of characteristic $p$, where $p$ is any rational prime. Let $\mathcal{O} = W(k) = W^{-}(k)$, the unique complete discrete valuation ring with maximal ideal generated by $p$ such that $k$ is the residue class field of $\mathcal{O}$. Let $X$ be an elliptic curve over $A$. Assume for simplicity of statement that $X$ is absolutely connected over $k = A$. Then, if one takes the above definition of "$H^{0,1}(X, W^{-}(A))$" and "$H^{1,0}(X, W^{-}(A))$," then it turns out that

*Case* 1. If $X$ is not supersingular, then $H^{0,1}(X, \mathcal{O})$ and $H^{1,0}(X, \mathcal{O})$ are both free $\mathcal{O}$-modules of rank 1. But

*Case* 2. If $X$ is supersingular, then $H^{0,1}(X, \mathcal{O})$ is a free $\mathcal{O}$-module of rank 2 while $H^{1,0}(X, \mathcal{O}) = \{0\}$.

Thus, in the case of an elliptic curve over a finite field, the definition in the above Remark of a "Hodge decomposition" (which, of course, by the above definition, is always functorial in $X$), has the desired properties if and only if the elliptic curve $X$ is not supersingular. Thus, the would-be "Hodge decomposition" described in the above Remark does not in general have all familiar properties that one would want of a Hodge decomposition. (Even the formula $\beta^{p,q} = \beta^{q,p}$ fails if $p = 1$, $q = 0$ and $X$ is a supersingular elliptic curve over a finite field.)

## VI. A concrete example: Euclidean space

We compute the bounded Witt vectors $W^{-}((\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_n])$ (and the full Witt vectors) of a polynomial ring. This is illustrative. Then we compute the differentials, $\Gamma^{q}_{W^{-}(\mathbb{Z}/p\mathbb{Z})}(W^{-}((\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_n])$ over Euclidean space. The latter motivates and explains why we divide out the elements which I have called *F-null*. I also note what the $p$-adic cohomology of Euclidean space is, which explains in what cohomological sense the bounded Witt vectors resemble ordinary polynomials over $\hat{\mathbb{Z}}_p$.

a) *Full Witt vectors on a polynomial ring*

A direct computation (using f) of Section I) shows that

(1) $W((\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_n]) =$

$$\Bigg\{ \sum_{\substack{i_1, \ldots, i_n \in p^{-1}\mathbb{Z} \\ i_1, \ldots, i_n \geq 0}} \alpha_{i_1, \ldots, i_n} T_1^{i_1} \ldots T_n^{i_n} : \alpha_{i_1, \ldots, i_n} \in \hat{\mathbb{Z}}_p :$$

$\alpha_{i_1, \ldots, i_n} \to 0$ in $\hat{\mathbb{Z}}_p$, and such that denominator $(i_1, \ldots, i_n)$ divides $\alpha_{i_1, \ldots, i_n}$ in $\hat{\mathbb{Z}}_p$, all $i_1, \ldots, i_n \in p^{-1}\mathbb{Z}$, $i_1, \ldots, i_n \leq 0\}$, $n \geq 0$, $p$ a prime.

In equation (1) above, the symbol "$p^{-1}\mathbb{Z}$" denotes all rational numbers such that the denominator is a power of the fixed prime $p$. Thus the range of the summation indices $i_1, \ldots, i_n$ is the set of all non-negative rational numbers such that the denominator is a power of $p$. Also, in equation (1), the symbol "denominator $(i_1, \ldots, i_n)$" denotes the least common denominator of the rational numbers $i_1, \ldots, i_n$. Thus denominator $(i_1, \ldots, i_n)$ is a power of the fixed prime $p$, all $i_1, \ldots, i_n \in p^{-1}\mathbb{Z}$, $i_1, \ldots, i_n \geq 0$. (The condition $\alpha_{i_1, \ldots, i_n} \to 0$ in $\hat{\mathbb{Z}}_p$ means, of course, that for each integer $j \geq 0$, there are only finitely many sequences of indices $(i_1, \ldots, i_n)$ s.t. $i_1, \ldots, i_n \in p^{-1}\mathbb{Z}$, $i_1, \ldots, i_n \geq 0$, and such that $p^j$ does not divide $\alpha_{i_1, \ldots, i_n}$ in $\hat{\mathbb{Z}}_p$.)

EXAMPLES: (1) $T + pT^{1/p} + p^2 T^{p^2+1/p^2} + T^{p^2} + \Sigma_{n \geq 3}\, p^n T^{1/p^n}$ is an element of $W((\mathbb{Z}/p\mathbb{Z})[T])$, all rational primes $p$. So is $\Sigma_{n \geq 0}\, (p^n/r) T^{p^n}$, $r$ any integer prime to $p$.

(2) $p^2 X^{1/p^2} Y + \Sigma_{i \geq 2}\, p^i X^{1/p^2} Y^{1/p^i}$ is an element of $W((\mathbb{Z}/p\mathbb{Z})[X, Y])$.

b) *The degree of an element of* $W((\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_n])$

In Section II, equation (1), we have defined the *degree* of an element $a \in W((\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_n])$. This was a real number $\geq -1$ or $+\infty$, and we denoted it as $\deg_{T_1, \ldots, T_n}(a)$, or as $\deg(a)$. An explicit computation using equation (1) of Section II and equation (1) above show that

PROPOSITION: *Let*

(2) $$a = \sum_{\substack{i_1, \ldots, i_n \in p^{-1}\mathbb{Z}, \\ i_1, \ldots, i_n \geq 0}} \alpha_{i_1, \ldots, i_n} \cdot T_1^{i_1} \ldots T_n^{i_n} \in W((\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_n])$$
be non-zero.

*Then the degree* $\deg(a)$ *of* $a$ *as defined in equation* (1) *of Section II is*

(3) $$\deg(a) = \sup\{i_1 + \cdots + i_n : \alpha_{i_1, \ldots, i_n} \neq 0, \text{ all } i_1, \ldots, i_n \in p^{-1}\mathbb{Z}, i_1, \ldots, i_n \geq 0\}.$$

Thus, the degree, as defined earlier in equation (1) of Section II, of the expression on the right side of equation (2) above is exactly what we would naively call the "total degree" or "degree" of the expression. (This explains the terminology "degree" defined in Section II, equation (1).) And indeed, if $n > 1$ then this number "$\deg(a)$" can be an arbitrary non-negative real number or $+\infty$ if $a \neq 0$, as we have noted previously in Section II.

c) *Explicit expression for the bounded Witt vectors of a polynomial ring*

Considering the definition of bounded Witt vectors (see Section II, equation (2)), which started by defining the object in the case of a polynomial ring, and equations (1), (2) and (3) above, we see that

$$(4)\qquad W^{-}((\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_n]) = \Bigg\{ \sum_{\substack{i_1, \ldots, i_n \in p^{-1}\mathbb{Z} \\ i_1, \ldots, i_n \geq 0}} \alpha_{i_1, \ldots, i_n} T_1^{i_1} \ldots T_n^{i_n}:$$

$\alpha_{i_1,\ldots,i_n} \in \hat{\mathbb{Z}}_p$, $\alpha_{i_1,\ldots,i_n} \to 0$ in $\hat{\mathbb{Z}}_p$, denominator $(i_1, \ldots, i_n) | \alpha_{i_1,\ldots,i_n}$, all $i_1, \ldots, i_n \in p^{-1}\mathbb{Z}$, $i_1, \ldots, i_n \geq 0$, and there exists a real number $N$ such that $i_1, \ldots, i_n \in p^{-1}\mathbb{Z}$, $i_1, \ldots, i_n \geq 0$, and $i_1 + \cdots + i_n > N$ implies that $\alpha_{i_1,\ldots,i_n} = 0\Bigg\}$.

Of course, the degree of the typical non-zero element written out on the right side of equation (4) can be described as being the smallest real number $N$ (always a non-negative real number since the Witt vector in question is bounded, and by definition of bounded Witt vectors) such that the indicated property in the bracelets holds.

Examples: $T + pT^{1/p} + p^2T^{1/p^2} + \cdots + \cdots$ is a bounded Witt vector on $(\mathbb{Z}/p\mathbb{Z})[T]$, i.e., is an element of $W^{-}((\mathbb{Z}/p\mathbb{Z})[T])$. The degree is 1. But $T + pT^p + pT^{p^2} + \cdots + \cdots \in W((\mathbb{Z}/p\mathbb{Z})[T])$ is a Witt vector on $(\mathbb{Z}/p\mathbb{Z})[T]$, but is *not* bounded, i.e., is not an element of $W^{-}((\mathbb{Z}/p\mathbb{Z})[T])$, since its degree is $+\infty$. (Notice that of the two Witt vectors written out in the Example (1) above, the first is bounded of degree $p^2 + 1/p^2$ while the second such vector is not bounded as the degree is $+\infty$.)

The Witt vector in (2) of the last Example is bounded and is of degree $1 + 1/p^2$.)

d) *F-differentials on the bounded Witt vectors on polynomial rings over $W^{-}(\mathbb{Z}/p\mathbb{Z})$*

First, consider the polynomial ring in one variable, $(\mathbb{Z}/p\mathbb{Z})[T]$. Then the $F$-differentials of dimension zero of $W^{-}((\mathbb{Z}/p\mathbb{Z})[T])$ over $W^{-}(\mathbb{Z}/p\mathbb{Z})$ are just $W^{-}((\mathbb{Z}/p\mathbb{Z})[T])$ itself, explicated in equation (4). The $F$-differential $q$-forms are zero for $q \geq 2$, and

(5) $$\Gamma^1_{W^-(\mathbb{Z}/p\mathbb{Z})}(W^-((\mathbb{Z}/p\mathbb{Z})[T])) \subset \Bigg\{ \sum_{\substack{i>-1 \\ i\in p^{-1}\mathbb{Z}}} \alpha_i T^i dT : \alpha_i \in \hat{\mathbb{Z}}_p,$$

$i \in p^{-1}\mathbb{Z}$, $i > -1$, $\mathrm{den}(i) \cdot \alpha_i \to 0$ in $\hat{\mathbb{Z}}_p$, and there exists $N$ a real number such that $\alpha_i = 0$ whenever $i > N\Big\}$.

The last condition (the one involving $N$) is, of course, a boundedness condition: it says that what we would intuitively call the degree is $< +\infty$. Notice that the convergence condition on the $\alpha_i$ is different from the one in the bounded Witt vectors: on the $F$-differentials of degree 1, the condition is "$(\mathrm{den}\, i) \cdot \alpha_i \to 0$", a weaker condition, and also that the condition "$\mathrm{den}(i)|\alpha_i$" has vanished. Also notice that negative exponents of $T$ are allowed; the condition now on the index $i$ is "$i > -1$, $i \in p^{-1}\mathbb{Z}$". Possibly two examples will show why negative powers $> -1$ occur in the $F$-differentials of dimension 1, and why the convergence condition becomes less restrictive.

EXAMPLES: (1) $d(pT^{1/p}) = T^{-1+1/p}dT \in \Gamma^1_{W^-(\mathbb{Z}/p\mathbb{Z})}(W^-(\mathbb{Z}/p\mathbb{Z})[T])$

(Notice that $T$ has a negative exponent, namely $-1 + 1/p$. Notice also that $\mathrm{den}(i) = p$ does not divide $\alpha_i = 1$).

(2) $$d\left(\sum_{i\geq 0} p^i T^{1/p^i}\right) = \sum_{i \geq 0} T^{-1+1/p^i} dT.$$

(Notice that the coefficients $\alpha_i$, which are all $+1$, all integers $i$, do not converge to 0 $p$-adically. But denominator $(i) \cdot \alpha_i = p^i \cdot 1$ does converge to zero $p$-adically. Notice also that the exponents of $T$ in this $F$-differential 1-form, which are all elements of $p^{-1}\mathbb{Z}$, approach arbitrarily close to $-1$, but always remain, as they must, strictly greater than $-1$.)

Notice that in equation (5) we do not have an equality but merely an inclusion. In fact this inclusion is strict. For example, one can show that the element $T^{p^{-1}}dT$ of the right side of equation (5) is not the image of an element of the left side of equation (5). (It is difficult, but not impossible, to write down very explicitly which elements of the right side of equation (5) are or are not in the image of the left side of equation (5). An easy, but not "explicit", answer to this question is: An element of the right side of equation (5) is in the image of an element of the left side of equation (5) if and only if it can be written in the form $f_1 dg_1 + \cdots + f_m dg_m$, there exist an integer $m \geq 1$ and elements $f_1, g_1, \ldots, f_m, g_m \in W^{-}((\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_n])$. Here the operator "$d$", from the right side of equation (4) into the right side of equation (5), is the naïve differential operator (using the obvious interpretation of the expressions on the right side of (4) as "power series with rational exponents").)

*Note*: In equations (1), (2), (4) and (5), if one is thoroughly rigorous, symbols like "$T$", "$T_1$", ..., "$T_n$" actually should be replaced by the Witt vectors $T' = (T, 0, 0, 0, \ldots)$, $T'_j = (T_j, 0, 0, \ldots)$, etc. In all cases two elements as on the right side of the equation coincide if and only if the formal expressions coincide. Similarly for some of the equations below. Thus, $V(T) = pT^{1/p}$ (or, more rigorously, $V(T') = p(T')^{1/p}$, which can be deduced from equations in Section II, since $T' = (T, 0, 0, \ldots)$, $F(T, 0, 0, \ldots) = (T^p, 0, 0, \ldots) = (T')^p$, and $V \circ F =$ multiplication by $p$.) In equations (1) and (3), the operator $F$ is the $\hat{\mathbb{Z}}_p$-endomorphism that sends $T$ into $T^p$, and $T_1, \ldots, T_n$ into $T_1^p, \ldots, T_n^p$. $V$ sends $T_1^{i_1} \ldots T_n^{i_n}$ into $pT_1^{i_n/p} \ldots T_n^{i_n/p}$. $V$ or $F$ send any one of the "infinite sums" (which are convergent for both the $V$-topology and also the bounded topology in the case of equation (3)) into the corresponding infinite sum of the image of each monomial under $V$ or $F$.

As for the $F$-differential $q$-forms on the bounded Witt vectors of a polynomial ring in $n$ variables we have

$$(6) \qquad \Gamma^q_{W^{-}(\mathbb{Z}/p\mathbb{Z})}(W^{-}((\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_n])) \subset \Bigg\{ \sum_{1 \leq j_1 < \cdots < j_q \leq n} \sum_{\substack{i_1, \ldots, i_n \in p^{-1}\mathbb{Z}, \\ i_{j_1}, \ldots, i_{j_q} > -1, \\ i \in \{i_1, \ldots, i_n\} \sim \{i_{j_1}, \ldots, i_{j_q}\} \\ \text{implies } i \geq 0.}}$$

$\alpha_{i_1, \ldots, i_n, j_1, \ldots, j_q} T_1^{i_1} \ldots T_n^{i_n} (dT_{j_1}) \wedge \cdots \wedge (dT_{j_q})$: $\alpha_{i_1, \ldots, i_n, j_1, \ldots, j_q} \in \hat{\mathbb{Z}}_p$, all $j_1, \ldots, j_q$ such that $1 \leq j_1 < \cdots < j_q \leq n$, all $i_1, \ldots, i_n \in p^{-1}\mathbb{Z}$ such that $i_{j_1}, \ldots, i_{j_q} > -1$, and every $i \in \{i_1, \ldots, i_n\} - \{i_{j_1}, \ldots, i_{j_q}\}$ is $\geq 0$; denominator $(j_1 \ldots j_q) \cdot \alpha_{i_1, \ldots, i_n, j_1, \ldots, j_q} \to 0$ in $\hat{\mathbb{Z}}_p$; and there exists a real number $N$ such that if $i_1 + \cdots + i_n > N$, $i_1, \ldots, i_n \in p^{-1}\mathbb{Z}$, $1 \leq j_1 < \cdots < j_q \leq n$, $i_{j_1}, \ldots, i_{j_q} > -1$, $i \in \{i_1, \ldots, i_n\}$, $i \neq i_{j_1}, \ldots, i_{j_q}$ implies $i \geq 0$, then $\alpha_{i_1, \ldots, i_n, j_1, \ldots, j_q} = 0\}$.

EXAMPLES:

(1) $T_3 T_1^{-1+1/p} T_2^{-1+1/p} (dT_1) \wedge (dT_2) \wedge (dT_3) = T_3 \cdot (d(pT_2^{1/p})) \cdot (d(pT_3^{1/p}))$.

Therefore

$$(T_3 \cdot T_1^{-1+1/p} \cdot T_2^{-1+1/p}(dT_1) \wedge (dT_2) \wedge (dT_3)$$
$$\in \Gamma^3_{W^-(\mathbb{Z}/p\mathbb{Z})}(W^-(\mathbb{Z}/p\mathbb{Z})(T_1, T_2, T_3]).$$

(2) $$\sum_{i\geq 1} T_1^{-1+1/p^i} dT_1 + \sum_{i\geq 0} T_2 \cdot T_3^{-1+1/p^i} \cdot dT_3$$
$$= d\sum_{i\geq 1} d(p^i T_1^{1/p^i}) + T_2 \cdot \sum_{i\geq 0} d(p^i T_3^{1/p^i}).$$

Therefore

$$\sum_{i\geq 1} T_1^{-1+1/p^i} \cdot dT_1 + \sum_{i\geq 0} T_2 \cdot T_3^{-1+1/p^i} \cdot dT_3 \in \Gamma^1_{W^-(\mathbb{Z}/p\mathbb{Z})} W^-((\mathbb{Z}/p\mathbb{Z})[T_1, T_2, T_3]).$$

(3) Although $T_1^{p-1}dT_1$ is an element of the right side of equation (6) in the case $q = n = 3$, nevertheless it is not an element of $\Gamma^1_{W^-(\mathbb{Z}/p\mathbb{Z})}(W^-((\mathbb{Z}/p\mathbb{Z})[T_1, T_2, T_3]))$.

*Note*: If I did not divide the Kähler differentials by the $F$-null elements, then equations (5) and (6) would become false. Intuitively speaking, the $F$-null elements are the smallest group that one can divide out by so that the obvious formal rules of taking differentials should work, "allowing $p^{\prime th}$ roots". The following examples of $F$-torsion and $F$-null elements may make this clear.

EXAMPLES: (1) The element $V(T') \cdot dT' - pT' \cdot dV(T')$ is an $F$-torsion element in $\mathrm{Kah}^1_{W^-(\mathbb{Z}/p\mathbb{Z})}(W^-(\mathbb{Z}/p\mathbb{Z})[T])$. (In fact, $F^1(V(T')dT' - pT'd(V(T'))) = (FV)(T')dF(T') - pF(T') \cdot d(F(V(T'))) = pT' \cdot d(T')^p - p(T')^p \cdot d(pT') = pT' \cdot (p(T')^{p-1}) \cdot dT' - p(T')^p \cdot pdT' = p(T')^p dT' - p(T')^p dT' = 0$). (The image of this element on the right side of equation (5) is $(pT^{1/p}) \cdot dT - pT \cdot d(pT^{1/p}) = pT^{1/p} \cdot dT - pT \cdot T^{(1/p)-1} \cdot dT = pT^{1/p}dT - pT^{1/p}dT = 0$. This last computation might show why we want to divide out by this element.)

(2) $\Sigma_{i\geq 0}(V^i(T') \cdot dT' - p^iT' \cdot dV^i(T'))$ is an $F$-null element in $\mathrm{Kah}^1_{W^-(\mathbb{Z}/p\mathbb{Z})}(W^-((\mathbb{Z}/p\mathbb{Z})[T])$. In fact, the element $f_i = V^i(T') \cdot dT' - p^iT' \cdot dV^i(T')$ is an $F$-torsion element, since an explicit computation similar to the Example (1) above shows that $(F^1)^i$ (the composite of the endomorphism $F^1$ of $\mathrm{Kah}^1_{W^-(\mathbb{Z}/p\mathbb{Z})}(W^-((\mathbb{Z}/p\mathbb{Z})[T])$ with itself $i$ times) maps the element $f_i$ into zero. But the infinite sum $\Sigma_{i\geq 0} f_i$ is a Cauchy sum for the bounded topology (and also for the $V$-topology) on $\mathrm{Kah}^1_{W^-(\mathbb{Z}/p\mathbb{Z})}(W^-((\mathbb{Z}/p\mathbb{Z})[T]))$. Therefore $\Sigma_{i\geq 0} f_i = \Sigma_{i\geq 0}(V^i(T') \cdot dT' - pT' \cdot d(V^i(T')))$ is an $F$-null element in $\mathrm{Kah}^1_{W^-(\mathbb{Z}/p\mathbb{Z})}(W^-((\mathbb{Z}/p\mathbb{Z})[T]))$. It can be shown that this $F$-null element

is not an $F$-torsion element. (Of course, if we write $V^i(T') = p^i T'^{1/p^i}$, and require that the usual rules of differentiation, including with fractional exponents, hold, then we would have to have that this element is zero. That is an intuitive reason why we divide out by $F$-null elements.)

The $F$-null elements in $\mathrm{Kah}^q_{W^-(\mathbb{Z}/p\mathbb{Z})}(W^-(\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_n])$, $q, n \geq 0$, $q$, $n \in \mathbb{Z}$, $p$ a rational prime, can be characterized as follows. Using the universal definition of Kahler differentials that I quoted in section IV, part a), we easily obtain a natural homomorphism of differential graded $\hat{\mathbb{Z}}_p$-algebras from $\mathrm{Kah}^q_{W^-(\mathbb{Z}/p\mathbb{Z})}(W^-(\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_n])$, $q \geq 0$, into the right side of equation (6). The $F$-null elements in $\mathrm{Kah}^q_{W^-(\mathbb{Z}/p\mathbb{Z})}(W^-(\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_n])$ are simply the kernel of this natural homomorphism. Thus, to get decent differentials (i.e., differentials that in the case of the polynomial ring are subgroups of equation (6), i.e., that have a reasonable rigid expression, it is exactly necessary to pass to the quotient by the $F$-null elements. This quotient is the $F$-differentials that we have defined in Section IV, Case IA, when $r = 0$. A formula similar to (6) (and a similar heuristic explanation) applies to

$$\Gamma^q_{W^-((\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_r])}(W^-((\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_s])),$$

all integers $q \geq 0$, all integers $r$, $s$ with $s \geq r \geq 0$.

In addition to the argument that we want the "differentials" to have a nice rigid formula, I once worked out an example to show that Kahler differentials do *not* have some (probably, not any except VII a)) of the cohomological properties noted in the next section, while $F$-differentials do have these nice properties (as well as being nicely computable, in a rigid form, e.g., see equations (5) and (6) above.)

e) *p-Adic Cohomology of Euclidean Space*

The following theorem gives an illustration of how nicely the $p$-adic cohomology that we defined in Section V above behaves, if we use bounded Witt vectors, $F$-differentials, and relative hypercohomology.

THEOREM: *Let n be any integer* $\geq 0$ *and let p be a rational prime. Then there is a canonical isomorphism*

$$\text{(7)} \qquad H^h(\mathrm{Spec}((\mathbb{Z}/p\mathbb{Z})[T_1, \ldots, T_n]), W^-(\mathbb{Z}/p\mathbb{Z})) \approx H^h(\mathrm{Kahler}^*_{\hat{\mathbb{Z}}_p}(\hat{\mathbb{Z}}_p[T_1, \ldots, T_n]),$$

all integers $h \geq 0$.

In the above equation, the $p$-adic cohomology group on the left side of the equation is that defined in equation (1) of Section V. Note that the Theorem tells us that the $p$-adic cohomology of Euclidean space is *exactly* isomorphic to the $p$-adic hypercohomology of the polynomial ring $\hat{\mathbb{Z}}_p[T_1, \ldots, T_n]$ over $\hat{\mathbb{Z}}_p$. This is, of course, a best possible result.

REMARK 1: Notice that we do not have to "$\otimes_{\mathcal{O}} K$" in the above theorem, unlike the situation in our $p$-Adic Proof [1], where this was necessary for functorality. Notice also that the torsion is *exactly* right.[1]

REMARK 2: The proof of the above theorem, as well as that of the final theorem of the next section, is similar to the proof of the corresponding assertion in [1]. (But note that there is no tensoring over $\sigma$ with $K$ in this case, so the theorem is stronger.)

## VII. Some properties of the $p$-adic hypercohomology that we have defined in Section V using bounded Witt vectors and $F$-differentials

Roughly speaking, all of the cohomology theorems which we proved in [1] go over to the bounded Witt hypercohomology theory which we have just defined in Section V above. The methods of proof are also very similar. I simply state a list of theorems and note how they are used; proofs will appear later.

a) Excision, the cohomology sequence of a triple of open sets and the Meyer–Vietoris sequence follow immediately from Chapter 1 of [1], since the definition of cohomology in $V$ is as relative hypercohomology.

b) There is a "universal coefficients" theorem relating the cohomology of equation (1) of $V$ to the ordinary $\operatorname{mod} p$ hypercohomology of $X$ modulo $U$:

THEOREM: *$A$, $X$ and $U$ as in equation* (1) *of Section V, suppose that $X$ is a quasicompact prescheme such that the intersection of any two affine open subsets is quasicompact, and that $U$ is a quasicom-*

[1] It is not difficult to establish the analogous statement for our other generalization of our $p$-adic cohomology, see the Note at the end of the Introduction, and reference [2]. (This would fail completely, of course, if one worked with the full Witt vectors $W(A)$, or the full completion, even if one $\otimes_{\hat{\mathbb{Z}}_p} \hat{\mathbb{Q}}_p$, see [1]).

*pact open subset of X. Suppose that the set of simple points of X over A contains the complement of U. Then there is induced a second quadrant spectral sequence*

$$E_2^{p,q} = \mathrm{Tor}_{-p}^{W^-(A)}(H^q(X, U, W^-(A)), A) \Rightarrow H^n(X, U, \Gamma_A^*),$$

*where* $\Gamma_A^* = \Gamma_A^*(X)$ *is the ordinary sheaves of Kahler differentials of X over A.*

EXAMPLES: If $A = \mathbb{Z}/p\mathbb{Z}$, then another way of phrasing the above theorem is to assert that we have a long exact sequence

$$(1) \qquad \ldots \xrightarrow{\partial^{n-1}} H^n(X, U, \hat{\mathbb{Z}}_p) \xrightarrow{p} H^n(X, U, \hat{\mathbb{Z}}_p) \longrightarrow$$

$$H^n(X, U, \mathbb{Z}/p\mathbb{Z}) \xrightarrow{\partial^n} H^{n+1}(X, U, \hat{\mathbb{Z}}_p) \xrightarrow{p} \cdots$$

where we define $H^n(X, U, \mathbb{Z}/p\mathbb{Z}) = H^n(X, U, \Gamma_{\mathbb{Z}/p\mathbb{Z}}^*(X))$, where $\Gamma_{\mathbb{Z}/p\mathbb{Z}}^*(X) = \mathrm{Kahler}_{\mathbb{Z}/p\mathbb{Z}}^*(X)$.

c) $X$ and $U$ as in equation (1) of section V, then

THEOREM: *Let* $C^*(X, U, W^-(A)) = C^*(W^-(X), W^-(U), \Gamma_{W^-(A)}^*(X))$, *where* $C^*$ *is, say, the Godement cochain functor* ([1]). *Then there is induced a canonical ismorphism*:

$$H^h(C^*(W^-(X), W^-(U), W^-(A)) \underset{\mathbb{Z}}{\otimes} \Gamma_{\mathbb{Z}}^*(\mathbb{Z}[T]))$$
$$\xrightarrow{\approx} H^h(W^-(X[T]), W^-(U[T]), W^-(A)),$$

*all integers* $h \geq 0$, *where* $\Gamma_{\mathbb{Z}}^*(\mathbb{Z}[T]) = \mathrm{Kahler}_{\mathbb{Z}}^*(\mathbb{Z}[T])$.

d) *Canonical classes*

THEOREM: *X and A as in equation* (1) *of Section V, suppose that X is simple over A. Let Y be a closed subproscheme of X that is "generically simple" over A – i.e., that is such that* $y \in \{$*generic points of fibers of Y over* Spec($A$)$\}$ *implies that the local ring* $\mathcal{O}_{Y,y}$ *is simple over A.* (*This latter condition is automatic if A is a field, if Y is simple over A, or if X is the product of two separated proschemes simple over* Spec($A$) *and if Y is the graph of a map.*) (*More general conditions can be stated*). *Then*

$$H^h(X, X - Y, W^-(A)) \underset{\hat{\mathbb{Z}}_p}{\otimes} \hat{\mathbb{Q}}_p = \{0\}$$

*whenever $h < 2d$, $d =$ codimension of $Y$ in $X$; and there is induced a canonical element*

$$u_{X,Y} \in H^{2d}(X, X - Y, W^{-}(A)) \bigotimes_{\hat{\mathbb{Z}}_p} \hat{\mathbb{Q}}_p.$$

*Note*: For this theorem, it is necessary to tensor over $\hat{\mathbb{Z}}_p$ with $\hat{\mathbb{Q}}_p$, as can be shown by counterexamples (similar to those in [1]). Under the assumptions of this last theorem, if $Y$ is also simple over $A$, then the stronger "Lefschetz duality" theorem holds: Assume that every irreducible component of $Y$ is of the same codimension $d$ on $X$. Then there is induced a canonical isomorphism

$$H^h(X, X - Y, W^{-}(A)) \bigotimes_{\hat{\mathbb{Z}}_p} \hat{\mathbb{Q}}_p \approx H^{h-2d}(Y, W^{-}(A)) \bigotimes_{\hat{\mathbb{Z}}_p} \hat{\mathbb{Q}}_p,$$

all integers $h \geq 0$.

e) THEOREM: (*Poincaré duality*) *$X$ and $A$ as in equation* (1) *of Section V, suppose that $X$ is simple and proper over $A$. Suppose that all the fibers of $X$ over $A$ are of the same dimension $n$. Then $H^*(X, W^{-}(A))$ obeys "Poincaré duality". That is*

$$H^h(X, W^{-}(A)) \bigotimes_{\hat{\mathbb{Z}}_p} \hat{\mathbb{Q}}_p = 0, \text{all integers } h > 2n;$$

*If $A^0 = H^0(X, W^{-}(A))$, then $A^0$ is an étale covering of $W^{-}(A)$; ($A^0 \approx W^{-}(A)$ as étale covering, if and only if the fibers of $X$ over $A$ are all absolutely connected), and*

$$H^{2n}(X, W^{-}(A)) \approx A^0 \text{ canonically as } A^0\text{-modules};$$

*and the cup product induces a (canonical) isomorphism of $A^0$-modules*

$$H^i(X, W^{-}(A)) \bigotimes_{\hat{\mathbb{Z}}_p} \hat{\mathbb{Q}}_p \approx \mathrm{Hom}_{A^0}(H^{2n-i}(X, W^{-}(A)), A^0) \bigotimes_{\hat{\mathbb{Z}}_p} \hat{\mathbb{Q}}_p,$$

*all integers $i \geq 0$.*

f) THEOREM: (*Kunneth relations*) *$X$ and $Y$ over $A$ as in e) implies*

$$H^h(X \times_A Y, W^{-}(A)) \bigotimes_{\hat{\mathbb{Z}}_p} \hat{\mathbb{Q}}_p \approx \bigoplus_{i+j=h} (H^i(X, W^{-}(A)) \bigotimes_{W^{-}(A)} H^j(Y, W^{-}(A)) \bigotimes_{\hat{\mathbb{Z}}_p} \hat{\mathbb{Q}}_p),$$

*all integers $h \geq 0$.*

g) Using the above properties, I obtain, as in [1], a $p$-adic proof of the Weil conjectures using this bounded Witt hypercohomology. The method applies to all complete non-singular algebraic varieties over finite fields, liftable or not. (Also, the method shows that on any complete, absolutely non-singular algebraic variety over any field, that the group of numerical equivalence classes of cycles is finitely generated.) For these theorems, I have already given two different proofs, one $q$-adic ("On a Conjecture of Andre Weil", American Journal of Mathematics), and one $p$-adic ("A $p$-adic proof of Weil's Conjectures" [1]). The $q$-adic proof did not require liftability, while the proof in [1] did require liftability.[1]

An advantage of this $p$-adic hypercohomology theory using bounded Witt vectors is not only that no liftability is needed, but also that the cohomology groups have coefficients in a complete discrete valuation ring $\mathcal{O}$ of mixed characteristic, rather than in the quotient field $K$ of such a valuation ring.

h) Also, let $X$ be simple and proper over a ring $A$ where $A$ is a commutative $(\mathbb{Z}/p\mathbb{Z})$-algebra with identity. Then I obtain zeta matrices of $X$ with coefficients in $W^-(A)$. (The formalism is similar to that of my Harvard seminar on "Zeta Matrices" where the matrices had coefficients in $A\dagger \otimes_{\mathcal{O}} K$). As in the zeta matrices in that seminar, these matrices have coefficients that are typically "a kind of power series". Instead of $p$-adic convergent power series in several variables as in the seminar, in this case they can be interpreted as being a kind of "bounded Witt polynomial in several variables" – more precisely, elements of the right side of equation (4) of Section VI for some integer $n$. To find the zeta matrices of any algebraic variety in the family we let the parameters take special values as in the Harvard seminar. (In this case, the "special values" are the multiplicative representatives $(a_1', \ldots, a_n')$ of the coordinates $(a_1, \ldots, a_n)$ in the parameter variety). (Note that a "bounded Witt polynomial" is like a $p$-adic convergent power series of bounded degree in several variables and all their $p^{i\text{'th}}$ roots, all integers $i \geq 0$, with certain constraints.) Of course, the algebraic family does not have to be liftable to get these zeta matrices. (In particular every complete absolutely non-singular variety over a field $k$ of characteristic $p \neq 0$ has zeta matrices with coefficients in $W^-(k)$; however, as I noted in the footnote following the Introduction, in [2] the assumption of liftability is removed by another method. An advantage of the

[1] (See Note 3 in the footnote following the Introduction, and reference [2]). Since giving this talk, I have produced a direct generalization of all the results of [1] that, among other things, completely removes liftability assumptions and "$\otimes_{\mathcal{O}} K$".

bounded Witt method (and of the method in [2]) over that used in my Harvard seminar is that the matrices then have coefficients in a discrete valuation ring $\mathcal{O}$ rather than in the quotient field $K$ of such a valuation ring $\mathcal{O}$.)[1] But in cases where both kinds of zeta matrices are defined (E.g., the case of the zeta matrix that determines the zeta functions of all elliptic curves

$$Y^2 = 4X^3 - g_2X - g_3$$

in characteristic $\neq 0, 2, 3$, where $27g_2^3 - 8g_3^2 \neq 0$), the matrices seem to sometimes look more elegant when done with bounded Witt vectors than by the method of paper [2].

EXAMPLE: Suppose that $X$ is simple and proper over $A = (\mathbb{Z}/p\mathbb{Z})[X, Y]$ (or a quotient ring of this polynomial ring). Then the zeta matrices of $X$ have coefficients in $W^{-}(A)$. Therefore each entry in each of the zeta matrices of $X$ over $A$ is an expression of the form

$$\sum_{\substack{i,j \in p^{-1}\mathbb{Z} \\ 0 \leq i,\, j \leq N}} \alpha_{ij} X^i Y^j,$$

where $N$ is some positive real, and where denominator $(i, j) | \alpha_{ij}$, all $i, j \in p^{-1}\mathbb{Z}$, $0 \leq i$, $j \leq N$. E.g., an expression like:

$$X^2 + Y^3 + XY + pX^{1/p} + p^2X^{1+1/p^2} \cdot Y^{1/p^2} + p^2X^{2+1/p} + \sum_{i \geq 0} p^i X^{1/p^i}$$

is such a "bounded Witt polynomial" of degree 3 in $X$ and $Y$.

Therefore, zeta matrices using bounded Witt vectors are sometimes somewhat different and yield different sets of formulas for zeta functions for a given algebraic family as in h). In practice, I think that the bounded Witt zeta matrices are somewhat easier to compute. The reason is that the kind of recursions that occur appear to be more elegant. They turn out to be related to the recursions for the Witt $S_h$, $Q_h$, $h \geq 0$, (see Section I), at least in the case of elliptic curves.

i) *The coefficient group*

Let $A$ be a $\mathbb{Z}/p\mathbb{Z}$-algebra, let $\underline{A}$ be a $\hat{\mathbb{Z}}_p$-algebra such that $(\underline{A} \otimes_{\mathcal{O}} K)/(\text{nilpotent elements}) \approx A$, where $\mathcal{O} = \hat{\mathbb{Z}}_p$ and $K = \hat{\mathbb{Q}}_p$, and let

[1] It should note that the theorems of paper [1], and their generalizations to algebraic families presented in the Harvard seminar on "Zeta Matrices", are made use of in the proofs of [2].

$X$ be an object in the category $\mathscr{C}_{A,\underset{\sim}{A}}$ described in [2] (of proschemes simple over $A$ obeying a mild condition, and all maps of such proschemes over $A$, liftable or not). Then we have the $p$-adic cohomology groups as defined in [2], with coefficients in a certain $\underset{\sim}{A}$-algebra. But we also have the groups defined in this paper, Section V, equation (1),

$$H^h(X, W^-(A)), \quad h \geq 0.$$

Both are "good" cohomology theories. How are they related? (They cannot be isomorphic, since they have different coefficient groups. In general neither coefficient group contains the other.) It is probably possible to prove that if we choose a certain commutative ring $\underset{\sim}{A}'$ with identity containing both coefficient groups then after tensoring with the larger coefficient ring, that the theories then become isomorphic. That is, there is undoubtedly some functorial common *larger* coefficient group. (E.g., if there exists an endomorphism $F: \underset{\sim}{A} \to \underset{\sim}{A}$ lifting the $p$'th power map, then both coefficient groups are contained in $W(A^{p^{-\infty}})$, the full Witt vectors on the perfections of $A$, see Chapter I.[1]

However, it is in general almost certainly not possible to get a common functorial coefficient group that is contained in the coefficient groups of both theories.

(This is no surprise. In fact we cannot find a common functorial coefficient group, not even a larger one, between $p$-adic cohomology and $q$-adic cohomology for all but finitely many primes $q$ (not even if we leave out $p$), as can be shown by a counterexample).

j) Another, much simpler aesthetic application of $W^-(X)$, is as follows. Let $X$ be an arbitrary algebraic variety, or even proscheme, entirely in characteristic $p \neq 0$. Then we have the *canonical lifting* $W^-(X)$, defined in Section III, functorial in $X$, of any such $X$ back to characteristic zero. $W^-(X)$ is flat over $\hat{\mathbb{Z}}_p$ *iff* $X$ is reduced. In all cases,

$$R = W^-(X) \underset{\hat{\mathbb{Z}}_p}{\times} (\mathbb{Z}/p\mathbb{Z})$$

[1] In fact, if $\underset{\sim}{A}$ is a commutative ring with identity having no non-zero $p$-torsion such that $(\underset{\sim}{A}/p\underset{\sim}{A})/(\text{nilpotents}) \approx A/(\text{nilpotents})$, and if $F: \underset{\sim}{A} \to \underset{\sim}{A}$ is an endomorphism of the ring $\underset{\sim}{A}$ such that $F \otimes_{\mathbb{Z}} (\mathbb{Z}/p\mathbb{Z})$ is the $p$'th power endomorphism: $x \to x^p$ of $A/pA$, then there exists a unique homomorphism of rings with identity $i: \underset{\sim}{A} \to W(A^{p^{-\infty}})$, such that $i \circ F = F \circ i$ (where $F: W(A^{p^{-\infty}}) \to W(A^{p^{-\infty}})$ is the usual Witt $F$ for Witt vectors) and such that $i$ induces the natural map: $\underset{\sim}{A}/p\underset{\sim}{A}(\text{nilpotents}) \to A^{p^{-\infty}}$. (*Proof*: Consider $\underset{\sim}{A}_0 = \varinjlim (\underset{\sim}{A} \to_F A \to_F A \to_F \cdots)$. Then by the first Proposition in Chapter I applied to the perfect $(\mathbb{Z}/p\mathbb{Z})$-algebra $A^{p^{-\infty}}$, there is a canonical isomorphism: $\underset{\sim}{A}_0^{\wedge p} \approx W(A^{p^{-\infty}})$. (Basically, this argument is similar to those in [3]).

is such that there is a canonical subsheaf I of the sheaf of ideals of nilpotent elements, such that $I$ is of square zero, and such that, after reducing the structure sheaf modulo $I$, $R$ becomes isomorphic to $X$. Possibly this aesthetic application may be of interest in itself.

## REFERENCES

[1] SAUL LUBKIN: A $p$-Adic Proof of Weil's Conjectures. *Annals of Mathematics*, *87*, Nos. 1–2, Jan–March, 1968, 105–255.

[2] SAUL LUBKIN: Generalization of $p$-adic Cohomology (to appear).

[3] ERNST WITT: Zyklische Körper und Algebren der Charackteristik $p$ von Grade $p^n$. *J. Reine angew. Math.*, *176* (1936) 126–140.

(Oblatum 3-V-1971 & 2-VII-1974)

The University of Rochester
Rochester N.Y. 14627.