On the Construction of the Ring of Witt Vectors

Zachariah Zobair

Fall 2024

1 Introduction

In this paper we aim to understand the motivation for and the construction of Witt vectors. The ring of Witt vectors is a functor $W(-)\colon \mathbf{Alg}_{\mathbb{Z}} \to \mathbf{Alg}_{\mathbb{Z}}$. We will motivate its construction by considering the multiplicative system of representatives of the residue ring κ of a strict p-ring $\mathcal{O}$. In particular, our primary motivating example will be $\kappa = \mathbb{F}_p$ and $\mathcal{O} = \mathbb{Z}_p$. Through the construction of the Witt ring, we will see that we can recover all unramified extensions of $\mathbb{Z}_p$ and also see that this construction generalizes to arbitrary rings.

2 Motivation

Let us begin by motivating the construction of the ring of Witt vectors. Many of the concepts in this section will be defined in the following sections. Given a perfect ring κ of characteristic p it is a fact that there exists a unique (up to canonical isomorphism) strict p-ring $\mathcal{O}$ with residue ring κ. Further we always have a unique multiplicative system of representatives[1] $\tau\colon \kappa \to \mathcal{O}$ such that for any $x \in \mathcal{O}$ we can express it as

$$x = \sum_{i=0}^{\infty} \tau(a_i) p^i \tag{1}$$

with $a_i \in \kappa$. In fact, the construction of $\mathcal{O}$ will turn out to be functorial in κ. That is, given a homomorphism of perfect rings of characteristic p, $f\colon \kappa \to \kappa'$, we get an induced map $F\colon \mathcal{O} \to \mathcal{O}'$ making the following commute:

$$\begin{tikzcd}
\mathcal{O} \arrow[r, dashed, "F"] \arrow[d, "\pi"] & \mathcal{O}' \arrow[d, "\pi'"'] \\
\kappa \arrow[u, bend left, "\tau"] \arrow[r, "f"] & \kappa' \arrow[u, bend right, "\tau'"']
\end{tikzcd}$$

Of course, given the multiplicative system of κ we can immediately construct the underlying set of $\mathcal{O}$, simply the set of sums of the form (1). However, when trying to endow the set of such sums with a ring structure, we find that the arithmetic is highly nontrivial (in the case of fields of mixed characteristic). This is because the multiplicative system of representatives is *not* additive.

To understand the arithmetic on $\mathcal{O}$, given sequences (a_i) and (b_i) in κ we want to determine sequences (s_i) and (p_i) such that

$$\sum_{i=0}^{\infty} \tau(a_i)p^i + \sum_{i=0}^{\infty} \tau(b_i)p^i = \sum_{i=0}^{\infty} \tau(s_i)p^i,$$

[1] This multiplicative system is often called the *Teichmuller character*. Inspired by Kedlaya's notes [2], I will abstain from using this eponymous convention due to Teichmuller's role in the Nazi party.

and

$$\left(\sum_{i=0}^{\infty} \tau(a_i)p^i\right)\left(\sum_{i=0}^{\infty} \tau(b_i)p^i\right) = \sum_{i=0}^{\infty} \tau(p_i)p^i.$$

The goal was to be able to construct $\mathcal{O}$ for any perfect ring κ of characteristic p, so we would like for the sequences (s_i) and (p_i) not to depend on κ.

3 Preliminary Definitions

We begin by recalling some basic definitions.

Definition 1. A ring A is a *Dedekind domain* if it is integrally closed and every prime ideal is maximal.

Definition 2. A ring $\mathcal{O}$ is a *discrete valuation ring* if it is a local Dedekind domain that is not a field. That is, we have a unique maximal ideal $\mathfrak{p} \subseteq \mathcal{O}$. The field $\kappa = \mathcal{O}/\mathfrak{p}$ is called the *residue field* of $\mathcal{O}$. Let π generate $\mathfrak{p}$. We call π a *uniformizing element*, or a *uniformizer.* Then any element $x \in \mathcal{O}$ can be written $x = u\pi^n$ for some unit $u \in \mathcal{O}$ and $n \in \mathbb{N}$.

The main example we will be working with is the ring of p-adic integers $\mathbb{Z}_p$. Recall that we define $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$, where the maps in our inverse system are natural projections. One can check that this is in fact a discrete valuation ring with $\mathfrak{p} = p\mathbb{Z}_p$ and $\kappa = \mathbb{F}_p$.

Definition 3. Let π generate $\mathfrak{p}$. Then any element $x \in \mathcal{O}$ can be written $x = u\pi^n$ for some unit $u \in \mathcal{O}$ and $n \in \mathbb{N}$. We can then define an *additive valuation* v on $\mathcal{O}$ via $v(x) = v(u\pi^n) = n$ if $x \neq 0$ and $v(0) = \infty$ by convention.

If we let $K = \mathrm{Frac}(\mathcal{O})$ then we can naturally extend v to $K^\times$ since if $x = a/b$ with $a, b \in \mathcal{O}$ then $x = u\pi^n$ this time with $n \in \mathbb{Z}$. Then we let $v(x) = n$ as one would hope. One can then verify that $v\colon K^\times \to \mathbb{Z}$ is a surjective group homomorphism and that $v(x+y) \geq \min\{v(x), v(y)\}$. The second property called the *ultrametric* property, and we then say that v is a *nonarchimedean* valuation. A nonarchimedean valuation induces a topology on the field on which it is defined. Recall a field is *complete* with respect to a topology if every Cauchy sequence in the field converges with respect to that topology.

Definition 4. A field K equipped with a nonarchimedean discrete valuation v is a *nonarchimedean local field* if it has finite residue field κ and is complete with respect to the topology induced by v.

Remark 1. An *archimedean local field* is defined similarly, albeit with respect to an archimedean valuation. It is a theorem of Ostrowski that (up to isomorphism) the only archimedean local fields are $\mathbb{R}$ and $\mathbb{C}$. For the remainder of the paper we will take local field to mean nonarchimedean local field.

Proposition 1. *Let $\mathcal{O}$ be a complete discrete valuation ring, K its field of fractions and κ its residue field with uniformizer π. Let Σ be a system of representatives of κ in $\mathcal{O}$; that is, the image a section of the canonical projection $\mathcal{O} \to \kappa$. Then every $a \in \mathcal{O}$ can be uniquely written as a convergent series*

$$a = \sum_{i=0}^{\infty} \sigma_n \pi^n,$$

where $\sigma_n \in \Sigma$. Furthermore, every $k \in K$ can be written

$$k = \sum_{i=n}^{\infty} \sigma_n \pi^n,$$

for some $n \leq 0$.

Example 1. The p-adic numbers, $\mathbb{Q}_p$, form a complete local field with respect to the p-adic valuation v_p.

Example 2. Let κ be a finite field. Then the field of formal Laurent series with coefficients in κ, $\kappa((t))$, is a local field.

4 The Multiplicative System, Extensions of Local Fields

The reader will notice that only two examples of local fields given were the p-adic numbers and formal Laurent series with coefficients in a finite field. In fact, we can characterize local fields into two categories: those of *equal characteristic* and those of *unequal (or mixed) characteristic.*

A local field K is of equal characteristic if $\operatorname{char} K = \operatorname{char} \kappa$ where κ is the residue field of K. Note that this can only be the case if $\operatorname{char} K > 0$ since by definition a local field has a finite residue field. On the other hand, we say K is of mixed characteristic if $\operatorname{char} K \neq \operatorname{char} \kappa$. This can only be the case if $\operatorname{char} K = 0$. It turns out that the two examples given are sufficient: all local fields of equal characteristic are isomorphic to fields of formal Laurent series with coefficients in their residue fields and all local fields of mixed characteristic are isomorphic to extensions of $\mathbb{Q}_p$. This of course is a claim that needs proof. We will be able to see this after developing the multiplicative system of representatives, but first we remark that this shows the equal characteristic case is some how less "interesting" than the mixed characteristic case. Then, when in the mixed characteristic case, we have a notion of an *unramified extension* (to be defined). As was stated in the introduction, the associated complete discrete valuation rings of such extensions (which are in fact unique) can be recovered via the Witt ring construction.

Before getting there, we first introduce the *multiplicative system of representatives* of a complete discrete valuation ring and, as a relatively immediate corollary of its construction, will prove the claim on the structure of local fields of equal characteristic. This construction is actually more general than on just complete discrete valuation rings. We can find a unique multiplicative system of representatives for any *strict p-ring.*

Definition 5. For a prime number p, a *strict p-ring* is a ring R that is complete and Hausdorff with respect to the p-adic topology and such that p is not a zero divisor. Further we require that its residue ring (note, not necessarily a field) $\kappa = R/(p)$, is perfect, in the sense that the ring homomorphism given by $x \mapsto x^p$ is an automorphism of κ.

Observe that our complete discrete valuation rings are indeed strict p-rings. Strict p-rings enjoy many nice properties, which will be given in an upcoming theorem. However, before the excitement of stating the theorem, we first need some discussion on extensions of local fields.

Suppose K is a local field with additive valuation v_K. Then, if L/K is a finite extension of degree n, the valuation on K extends uniquely to a valuation on L, v_L, given by

$$v_L(\alpha) = \frac{1}{n} v_K(N_{L/K}(\alpha)),$$

where $N_{L/K}$ is the norm. Note that all possible values of a valuation on the multiplicative group of a local field can take form a group in their own right, called the *valuation group.*

Definition 6. Let L/K be a finite extension of local fields. Then, the *ramification index* of L over K is the natural number

$$e = (v_L(L^\times) : v_K(K^\times)).$$

If $e = 1$, then we say L is *unramified* over K.

Remark 2. A related concept, the *inertia degree*, is defined as $f = [\kappa_K : \kappa_K]$, where κ_K and κ_L are the respective residue fields of L and K. Combined with the fact (which we will take without proof) that $[L : K] = ef$, we see we can equivalently characterize L/K as being unramified if

$$[L : K] = [\kappa_L : \kappa_K].$$

This notion can be extended to talking about complete discrete valuation rings of mixed characteristic. Suppose $\mathcal{O}$ is such a ring and K its field of fractions. Then, as was mentioned before, K is an extension of $\mathbb{Q}_p$. We say $\mathcal{O}$ is unramified if K is unramified over $\mathbb{Q}_p$.

Remark 3. One can characterize ramification of a complete discrete valuation ring without discussing field extensions, c.f. Ch. II §5 of [1].

Theorem 1. *Let κ be a perfect ring of characteristic p. Then,*

1. *There is a strict p-ring $\mathcal{O}$ with residue ring κ unique up to a canonical isomorphism. In the case that κ is a field, then $\mathcal{O}$ is a complete discrete valuation ring which is unramified with residue field κ.*
2. *There exists a unique system of representatives $\tau\colon \kappa \to \mathcal{O}$ such that*

$$\tau(xy) = \tau(x)\tau(y)$$

for all $x, y \in \kappa$. This system is called the multiplicative system of representatives.

3. *The construction of $\mathcal{O}$ and τ is functorial in κ in the sense that a ring homomorphism $f\colon \kappa \to \kappa'$ of perfect rings of characteristic p induces a unique homomorphism of strict p-rings $\mathcal{O} \to \mathcal{O}'$ given by*

$$\sum_{i=0}^{\infty} \tau(x_i)p^i \mapsto \sum_{i=0}^{\infty} \tau'(f(x_i))p^i.$$

Proofs of each of results of theorem 1 can be found in Ch. II §4-5 of [1]. In the case that is κ a residue field of characteristic p of a complete discrete valuation ring $\mathcal{O}$, then the multiplicative system is a map from $\kappa^\times$ to the $(q-1)$-th roots of unity in $K = \mathrm{Frac}(\mathcal{O})$, where $q = \#\kappa$. The explicit construction is given for an $a \in \kappa$ defining a sequence (a_n) via

$$a_0 = a, \quad a_n = (a_{n-1})^{1/p}.$$

Then, denoting by $\tilde{a}_n$ a lift of a_n to $\mathcal{O}$, we let

$$\tau(a) = \lim_{n\to\infty} \tilde{a}_n^{p^n}.$$

Continuity of multiplication of elements in κ then yields the multiplicativity we desired. Observe that if $\operatorname{char} K = \operatorname{char} \kappa = p$, then we have

$$\tilde{a}_n^{p^n} + \tilde{b}_n^{p^n} = (\tilde{a}_n + \tilde{b}_n)^{p^n},$$

and so τ in fact determines a ring homomorphism $\kappa \to \mathcal{O}$. Thus we get the following.

Corollary 1. *Let K be a local field of equal characteristic with complete discrete valuation ring $\mathcal{O}$, uniformizer π, and residue field κ. Then K is isomorphic to $\kappa((t))$.*

Proof. Since $K = \mathrm{Frac}(\mathcal{O})$, its sufficient to show $\kappa[[t]] \cong \mathcal{O}$. Consider the map

$$f\colon \kappa[[t]] \to \mathcal{O}$$

given via

$$\sum_{i=0}^{\infty} a_i t^i \mapsto \sum_{i=0}^{\infty} \tau(a_i)\pi^i.$$

The map f is a homomorphism since τ is in the equal characteristic case. It is bijective by proposition 1. □

The additive nature of τ is critically only present for the equal characteristic situation. However, proposition 1 says that we should still be able to at least recover the underlying set of a complete discrete valuation ring $\mathcal{O}$ with residue field κ by considering sums of the form

$$\sum_{i=0}^{\infty} \tau(a_i)\pi^i$$

for $a_i \in \kappa$. Working with the multiplicative system is nice. The usual alternative in the p-adic case is to take the set

$$\{0, 1, \dots, p-1\}$$

as our representatives of κ. However, (as the unicity statement in the second claim of theorem 1 would imply) this system is not multiplicative: $(p-1)^2 = p^2 - 2p + 1$ reduces to 1 mod p, whereas first reducing mod p then squaring is decidedly not equal to 1. Thus, it would desirable to also be able to recover the ring structure on $\mathcal{O}$ when using the multiplicative system. This desire will lead us to the construction of the ring of Witt vectors.

5 Recovering the Ring Structure

As we stated in the motivation section, to recover the arithmetic on $\mathcal{O}$, given sequences (x_i) and (y_i) in κ we need to find sequences (s_i) and (p_i) in κ such that

$$\sum_{i=0}^{\infty} \tau(a_i)p^i + \sum_{i=0}^{\infty} \tau(b_i)p^i = \sum_{i=0}^{\infty} \tau(s_i)p^i,$$

and

$$\left(\sum_{i=0}^{\infty} \tau(a_i)p^i\right)\left(\sum_{i=0}^{\infty} \tau(b_i)p^i\right) = \sum_{i=0}^{\infty} \tau(p_i)p^i.$$

Moreover, for this construction to be particularly useful, we want the determination of (s_n) and (p_n) not to rely on the perfect ring κ in which they reside. The existence of such sequences (and, in fact, a more general result) is proven in Ch. 2 §6 of [1] in a clever way due to Lazard. That said, we will follow the construction that is provided in [3] which is more explicit.

Let us begin with the sequence for sums, (s_n). We will determine each s_n inductively. To begin, we need s_0 such that

$$\tau(x_0) + \tau(y_0) \equiv \tau(s_0) \bmod p. \tag{2}$$

However, since τ is a section of the projection $\mathcal{O} \to \kappa$, it follows that $\tau(a) \equiv a \bmod p$ for any $a \in \kappa$. Thus the congruence (2) simply yields

$$x_0 + y_0 = s_0. \tag{3}$$

To determine s_1, the natural next step would be to work mod p^2 and set

$$\tau(x_0) + p\tau(x_1) + \tau(y_0) + p\tau(y_1) \equiv \tau(s_0) + p\tau(s_1) \pmod{p^2}.$$

As we just saw, $s_0 = x_0 + y_0$ and so we may rearrange the above to

$$p\tau(s_1) \equiv (\tau(x_0) + \tau(y_0) - \tau(x_0 + y_0)) + p(\tau(x_1) + \tau(y_1)) \pmod{p^2}.$$

Unfortunately, we do not know the residue of $\tau(x_0) + \tau(y_0) - \tau(x_0 + y_0)$ modulo p^2. However, we can use the fact that κ is perfect by assumption to get around this. The condition of κ being perfect ensures each $k \in \kappa$ has a unique p-th root, $k^{1/p}$. Thus from (3) we have

$$x_0{}^{1/p} + y_0{}^{1/p} = s_0{}^{1/p}. \tag{4}$$

We have the following lemma:

Lemma 1. *Let A be a ring and $x, y \in A$ such that $x \equiv y \pmod{pA}$. Then for all $i \geq 0$, $x^{p^i} \equiv y^{p^i} \pmod{p^{i+1}A}$.*

Combining this lemma with (4) and the fact that τ is multiplicative we can write

$$\tau(s_0) = \tau(s_0{}^{1/p})^p = \tau(x_0{}^{1/p} + y_0{}^{1/p})^p \equiv (\tau(x_0{}^{1/p}) + \tau(y_0{}^{1/p}))^p \pmod{p^2}.$$

From this we arrive at

$$p\tau(s_1) \equiv \tau(x_0{}^{1/p})^p + \tau(y_0{}^{1/p})^p - (\tau(x_0{}^{1/p}) + \tau(y_0{}^{1/p}))^p + p(\tau(x_1) + \tau(y_1)) \pmod{p^2}.$$

Dividing by p and expanding out yields

$$\tau(s_1) \equiv \tau(x_1) + \tau(y_1) - \frac{1}{p}\sum_{n=1}^{p-1} \binom{p}{n} \tau(x_0)^{n/p}\tau(y_0)^{(p-n)/p} \pmod{p},$$

and so once again using the fact that τ is a section of the projection, we see

$$s_1 = x_1 + y_1 - \frac{1}{p}\sum_{n=1}^{p-1} x_0{}^{n/p} y_0{}^{(p-n)/p}.$$

One can continue this process inductively to find $s_2, s_3, \ldots$ taking higher powers of p-th roots each time. However, at this point we pause to make a key observation. If we let $w_0(X_0) \in \mathbb{Z}[X_0]$ and $w_1(X_0, X_1) \in \mathbb{Z}[X_0, X_1]$ be

$$\begin{aligned} w_0(X_0) &= X_0, \\ w_1(X_0, X_1) &= X_0{}^p + pX_1, \end{aligned}$$

and solve the equations

$$w_0(S_0) = S_0 = w_0(X_0) + w_0(Y_0)$$

and

$$w_1(S_0, S_1) = S_0{}^p + pS_1 = w_1(X_0, X_1) + w_1(Y_0, Y_1)$$

for polynomials $S_0 \in \mathbb{Z}[X_0; Y_0]$, $S_1 \in \mathbb{Z}[X_0, X_1; Y_0, Y_1]$ then we arrive at

$$\begin{aligned} S_0 &= X_0 + Y_0, \\ S_1 &= X_1 + Y_1 - \frac{1}{p}\sum_{n=1}^{p-1} X_0{}^n Y_0{}^{p-n}. \end{aligned}$$

Indeed we have that $s_0 = S_0(x_0, y_0)$ and $s_1 = S_1(x_0{}^{1/p}, x_1, y_0{}^{1/p}, y_1)$. What this shows in particular is that the manipulations we did to determine s_0 and s_1 were not dependent on κ and so by considering these polynomials instead we can come to a general result.

We let $w_n(X_0, \ldots, X_n) \in \mathbb{Z}[X_0, \ldots, X_n]$ be the polynomial

$$w_n(X_0, \ldots, X_n) = \sum_{i=0}^{n} p^i {X_i}^{p^{n-i}}.$$

Then, in the same way as was done to find S_0 and S_1, we iteratively solve for polynomials $S_0, S_1, \ldots, S_n$ (where $S_i \in \mathbb{Z}[X_0, \ldots, X_i; Y_0, \ldots, Y_i]$) satisfying

$$w_n(S_0, \ldots, S_n) = w_n(X_0, \ldots, X_n) + w_n(Y_0, \ldots, Y_n).$$

One can see from how w_n is defined, the term with an S_n in $w_n(S_0, \ldots, S_n)$ is $p^n S_n$. Thus, assuming we have found the first $S_0, \ldots, S_{n-1}$, we can certainly solve this for S_n and at least have rational coefficients. One can show further that these S_i have integral coefficients (c.f. Ch. II, Theorem 6 in [1]). A completely analogous process can then be performed to arrive at polynomials $P_i \in \mathbb{Z}[X_0, \ldots, X_i; Y_0, \ldots, Y_i]$ for $0 \leq i \leq n$ such that

$$w_n(P_0, \ldots, P_n) = w_n(X_0, \ldots, X_n) w_n(Y_0, \ldots, Y_n).$$

In this way we recover the ring structure on $\mathcal{O}$:

Theorem 2. *Let $\mathcal{O}$ be a strict p-ring with perfect residue ring κ and $\tau \colon \kappa \to \mathcal{O}$ its multiplicative system of representatives. Suppose that*

$$\sum_{i=0}^{\infty} \tau(a_i)p^i + \sum_{i=0}^{\infty} \tau(b_i)p^i = \sum_{i=0}^{\infty} \tau(s_i)p^i,$$

and

$$\left(\sum_{i=0}^{\infty} \tau(a_i)p^i\right) \left(\sum_{i=0}^{\infty} \tau(b_i)p^i\right) = \sum_{i=0}^{\infty} \tau(p_i)p^i.$$

Then,

$$s_i = S_i({x_0}^{1/p^i}, {x_1}^{1/p^{i-1}}, \ldots, x_i; {y_0}^{1/p^i}, {y_1}^{1/p^{i-1}}, \ldots, y_i)$$

and

$$p_i = P_i({x_0}^{1/p^i}, {x_1}^{1/p^{i-1}}, \ldots, x_i; {y_0}^{1/p^i}, {y_1}^{1/p^{i-1}}, \ldots, y_i),$$

with the S_i and P_i as described above.

We actually have just constructed the *ring of p-typical Witt vectors with coefficients in κ*, which we will denote by $W_p(\kappa)$. A more precise definition will be given in the next section. Something to remark before that is that this construction can generalize in two ways: First, we can perform it on any ring A. Secondly, the coefficients of the polynomials w_n being powers of a prime p can also be generalized to being from a "divisor stable set". We will see these both in the next section, as well as prove that if A *is* a perfect ring of characteristic p, then $W_p(A)$ is the strict p-ring with residue ring A.

6 The Ring of Witt Vectors

In order to define the general ring of Witt vectors we first need some definitions.

Definition 7. A *divisor stable set* is a subset $P \subseteq \mathbb{N}$ such that for any $n \in P$, all proper divisors of n are contained in P. We denote by $\wp(P)$ the set of primes contained in P.

Example 3. $\mathbb{N}$ itself is a divisor stable set.

Example 4. For any prime p, the set $\{1, p, p^2, p^3, \ldots\}$ is a divisor stable set.

We then have the following:

Definition 8. For every $n \in \mathbb{N}$, we define the *n-th Witt polynomial* to be

$$w_n = \sum_{d|n} d{X_d}^{n/d}.$$

For any divisor stable set P, we define the set

$$W_P(A) = \prod_{n \in P} A.$$

We write $x \in W_P(A)$ as $x = (x_n)_{n \in P}$. Then, for each $n \in P$ the Witt polynomials define set-theoretic maps $w_n \colon W_P(A) \to A$ and we define the *ghost map* as

$$w_* \colon W_P(A) \to \prod_{n \in P} A$$

via $w_*(x) = (w_n(x))_{n \in P}$. The components $w_n(x)$ are called the *ghost components* (spooky!).

Remark 4. If A is P-torsion free (in the sense that no elements of P are zero-divisors in A), then w_* is an injection. If all elements of P have inverses in A, then w_* is a bijection.

The main theorem of this paper is as follows.

Theorem 3. *Let P be a divisor stable set. Then, there exists a unique covariant functor*

$$W_P(-) \colon \mathbf{Alg}_{\mathbb{Z}} \to \mathbf{Alg}_{\mathbb{Z}}$$

such that for any ring A,

1. *$W_P(A) = \prod_{n \in P} A$ as sets. For a ring homomorphism $f \colon A \to B$,*

$$W_P(f)((a_n)_{n \in P}) = (f(a_n))_{n \in P}.$$

2. *The maps $w_n \colon W_P(A) \to A$ are ring homomorphisms for all $n \in P$.*

3. *The additive identity in $W_P(A)$ is $(0, 0, 0, \ldots)$ and the multiplicative identity is $(1, 0, 0, \ldots)$.*

The proof will follow closely that provided in [3], which in turn follows an exercise from Serge Lang's *Algebra*, which Lang remarks came from Witt himself. In order to accomplish the proof we need some preliminaries.

Definition 9. For a ring A, we define $\Lambda(A)$ to be the multiplicative abelian group

$$\Lambda(A) = 1 + tA[[t]].$$

Lemma 2. *Let A be a ring. Then every $f = 1 + \sum_{n=1}^{\infty} x_n t^n \in \Lambda(A)$ can be written as*

$$f = \prod_{n=1}^{\infty} (1 - y_n t^n)$$

for uniquely determined $y_n \in A$. Further, there exist $Y_n \in \mathbb{Z}[X_1, \ldots, X_n]$ and $X_n \in \mathbb{Z}[Y_1, \ldots, Y_n]$ such that

$$y_n = Y_n(x_1, \ldots, x_n)$$

and

$$x_n = X_n(y_1, \ldots, y_n).$$

Proof. We will show the first claim here, and direct the reader to §3 of [3] for the second claim. To prove the first claim, we will induct on n showing that there exist unique $y_1, \ldots, y_n$ such that

$$\frac{f}{\prod_{i=1}^{n}(1-y_i t^i)} = 1 + O(t^{n+1}),$$

where $O(t^{n+1})$ simply denotes higher ordered terms. For the base case we take $n = 0$. The claim holds here clearly. Now assume the result for $n-1$ and write

$$\frac{f}{\prod_{i=1}^{n-1}(1-y_i t^i)} = 1 + zt^n + O(t^{n+1})$$

for some $z \in A$. Then, we have

$$(1-y_n t^n)^{-1}(1+zt^n + O(t^{n+1}) = 1 + (z-y_n)t^n + O(t^{n+1}).$$

This shows we can take $y_n = z$ and also shows $y_n = z$ is the only possibility. □

From this we get an immediate corollary.

Corollary 2. *For any ring A, the map $W_{\mathbb{N}}(A) \to \Lambda(A)$ given by*

$$x = (x_1, x_2, \ldots) \mapsto f_x(t) = \prod_{n=1}^{\infty}(1 - x_n t^n)$$

is a bijection.

Proof. Any vector $x \in W_{\mathbb{N}}(A)$ uniquely determines an element of $\Lambda(A)$. □

Lemma 3. *For A a $\mathbb{Q}$-algebra, define $D\colon \Lambda(A) \xrightarrow{\sim} tA[[t]]$ as*

$$D = -t\frac{d}{dt}\log,$$

where $\frac{d}{dt}\log$ for a power series f is f'/f, where the derivative is taken formally. Then, with $f_x(t)$ as defined in corollary 2,

$$D(f_x(t)) = \sum_{n=1}^{\infty} w_n(x)t^n.$$

Proof. The standard logarithm rule of

$$\log(xy) = \log(x) + \log(y)$$

is a purely formal one, and so we have

$$\log\left(\prod_{n=1}^{\infty}(1-x_n t^n)\right) = \sum_{n=1}^{\infty}\log(1-x_n t^n).$$

Thus it follows that

$$-t\frac{d}{dt}\log(f_x(t)) = \sum_{n=1}^{\infty}\frac{nx_n t^n}{1-x_n t^n} = \sum_{n=1}^{\infty}(nx_n t^n + nx_n{}^2 t^{2n} + nx_n{}^3 t^{3n} + \cdots).$$

Therefore the t^n term is precisely $w_n(x)$. □

Lemma 4. *Let A be a $\mathbb{Q}$-algebra and let $x, y \in W_{\mathbb{N}}(A)$. Set*

$$f(t) = \prod_{d,e \in \mathbb{N}} (1 - {x_d}^{m/d} {y_e}^{m/e} t^m)^{de/m},$$

where $m = \operatorname{lcm}(d, e)$. Then,

$$D(f(t)) = \sum_{n=1}^{\infty} w_n(x) w_n(y) t^n.$$

We omit the proof due to its similarity to that of lemma 3 and the fact that understanding these formal manipulations is not imperative to understanding Witt vectors. With this lemma we are ready to prove theorem 3. The proof will use a technique called "reduction to the universal case". The idea is this: We saw in section 5 that to recover the ring laws, we were able to do so by instead considering certain polynomials. Indeed, the ring laws on $W_P(A)$ can be determined in $W_P(R)$ where $R = \mathbb{Z}[\{X_n; Y_n \mid n \in P\}]$. Since R is torsion-free as a $\mathbb{Z}$-module, we can then use the injection

$$w_* \colon W_P(R) \hookrightarrow \prod_{n \in P} R$$

as described in remark 4 to derive information about $W_P(A)$.

Proof of Theorem 3. We will prove theorem 3 in the case $P = \mathbb{N}$. The existence proof for an arbitrary divisor stable set P is similar. First note that if A is a $\mathbb{Q}$-algebra, then every $n \in \mathbb{N}$ is invertible in A and so by remark 4 combined with the requirement that each $w_n \colon W_{\mathbb{N}}(A) \to A$ is a ring homomorphism, there is a unique ring structure on $W_{\mathbb{N}}(A)$ such that

$$w_* \colon W_{\mathbb{N}}(A) \to A^{\mathbb{N}}$$

is a ring homomorphism where the codomain has the product ring structure. Then observe that

$$w_*(0, 0, \ldots) = (0, 0, \ldots)$$

and

$$w_*(1, 0, \ldots) = (1, 1, \ldots).$$

Thus we see that $(0, 0, \ldots)$ is the additive identity in $W_{\mathbb{N}}(A)$ and $(1, 0, \ldots)$ is the multiplicative identity. Thus the functor $W_{\mathbb{N}}(-)$ exists and is unique in the category of $\mathbb{Q}$-algebras. We now want to show that it holds in the larger category of $\mathbb{Z}$-algebras.

To this end let $R = \mathbb{Q}[X_1, X_2, \ldots; Y_1, Y_2, \ldots]$ and let $X = (X_1, X_2, \ldots)$, $Y = (Y_1, Y_2, \ldots) \in W_{\mathbb{N}}(R)$. Let $S = (S_1, S_2, \ldots) \in W(R)$ be such that

$$\prod_{n=1}^{\infty} (1 - X_n t^n) \prod_{n=1}^{\infty} (1 - Y_n t^n) = \prod_{n=1}^{\infty} (1 - S_n t^n).$$

Using the notation of corollary 2, this is saying $f_X(t) f_Y(t) = f_S(t)$. Our lemma 2 ensures that each $S_n \in \mathbb{Z}[X_1, X_2, \ldots; Y_1, Y_2, \ldots]$ and by lemma 3 we have

$$\sum_{n=1}^{\infty} w_n(S) t^n = D(f_S(t)) = D(f_X(t) f_Y(t)) = D(f_X(t)) + D(f_Y(t)) = \sum_{n=1}^{\infty} (w_n(X) + w_n(Y)) t^n.$$

This then shows that $w_*(S) = w_*(X) + w_*(Y)$. Since R is a $\mathbb{Q}$-algebra, by the earlier comments w_* is a ring isomorphism and so $S = X + Y$. For products, we let $P = (P_1, P_2, \ldots) \in W(R)$ be such that

$$f_P(t) = \prod_{d,e\in\mathbb{N}}^{\infty} (1 - {X_d}^{m/d}{Y_e}^{m/e}t^m)^{de/m},$$

where $m = \operatorname{lcm}(d, e)$. Once again lemma 2 gives that $P_n \in \mathbb{Z}[X_1, X_2, \ldots ; Y_1, Y_2, \ldots]$ and we can invoke lemma 4 to yield

$$\sum_{n=1}^{\infty} w_n(P)t^n = D(f_P(t)) = \sum_{n=1}^{\infty} w_n(X)w_n(Y)t^n.$$

By the same reasoning as before, we then have $P = XY$.

Now take A to be an arbitrary ring and let $x, y \in W_{\mathbb{N}}(A)$. By defining $s = x+y$ by $s_n = S_n(x, y)$ and $p = xy$ by $p_n = P_n(x, y)$ we obtain well defined addition and multiplication operations on $W_{\mathbb{N}}(A)$ which are also functorial in A. Again, if A is a $\mathbb{Q}$-algebra, then we are done. However, if not, we treat it in two cases. First, suppose that A embeds in a $\mathbb{Q}$-algebra A'. Then the inclusion $W_{\mathbb{N}}(A) \hookrightarrow W_{\mathbb{N}}(A')$ respects addition and multiplication and so $W(A)$ is a subring of $W_{\mathbb{N}}(A')$ (which is a ring since A' a $\mathbb{Q}$-algebra).

Suppose B is a ring who need not embed into a $\mathbb{Q}$-algebra. Let $\{x_i\}_{i\in I}$ be generators for B as a $\mathbb{Z}$-algebra and let $A = \mathbb{Z}[\{X_i\}_{i\in I}]$. Then we have a surjective ring homomorphism

$$\varphi \colon A \to B$$

given by $\varphi(X_i) = x_i$. The induced map $W_{\mathbb{N}}(\varphi) \colon W_{\mathbb{N}}(A) \to W_{\mathbb{N}}(B)$ then also is surjective respecting addition and multiplication and we see $W_{\mathbb{N}}(B)$ is a quotient of $W_{\mathbb{N}}(A)$. Since A is a torsion-free $\mathbb{Z}$-module, A embeds into a $\mathbb{Q}$-algebra and so $W_{\mathbb{N}}(A)$ is a ring. Therefore $W_{\mathbb{N}}(B)$ is a quotient ring and hence a ring. Thus the $W_{\mathbb{N}}(-)$ functor is defined on $\mathbf{Alg}_{\mathbb{Z}}$. □

With the existence of the functor proved, we can now define the ring of Witt vectors.

Definition 10. Let A be a ring and P a divisor stable set. We call the ring $W_P(A)$ the *ring of P-Witt vectors with coefficients in A*. In the case that $P = \mathbb{N}$, we write $W(A)$ and call it the *big Witt ring with coefficients in A*. When $P = \{1, p, p^2, \ldots\}$ for a prime p, we write $W_p(A)$ and call it the *p-typical Witt ring with coefficients in A*. In cases where there is no ambiguity on P, some authors will just write $W(A)$ and call it *the* Witt ring with coefficients in A.

We now will see how this construction relates back to our discussion on recovering the ring structure on a strict p-ring from its multiplicative system of representatives.

Theorem 4. *Let κ be a perfect ring of characteristic p. Let $\mathcal{O}$ be the strict p-ring with residue ring κ and $\tau \colon \kappa \to \mathcal{O}$ its multiplicative system of representatives. Then the map $f \colon W_p(\kappa) \to \mathcal{O}$ given by*

$$f(x_0, x_1, x_2, \ldots) = \sum_{n=0}^{\infty} \tau({x_n}^{1/p^n})p^n$$

is an isomorphism of rings.

Proof. By proposition 1, this map is a well defined bijection. Then, $f(\mathbb{1}_{W_p(\kappa)}) = f(1, 0, 0, \ldots) = \tau(1) = 1$. Also we have $f(0, 0, 0, \ldots) = 0$. Thus we just have to show $f(x + y) = f(x) + f(y)$ and $f(xy) = f(x)f(y)$. The first of these is done in [3] §2, so here we will prove the multiplication is respected under f. Let $x, y \in W_p(\kappa)$ and let $\varpi = xy$. As we saw in the proof of theorem 3, we then have polynomials with integer coefficients P_i such that

$$\varpi_i = P_i(x_0, \ldots, x_i, y_0, \ldots, y_i).$$

Since $P_i \in \mathbb{Z}[X_0, \dots, X_i; Y_0, \dots, Y_i]$, we have

$$\varpi_i{}^{1/p^i} = P_i(x_0{}^{1/p^i}, \dots, x_i{}^{1/p^i}, y_0{}^{1/p^i}, \dots, y_i{}^{1/p^i}).$$

Now let $\tilde{x}_j = x_j{}^{1/p^j}$, and give similar definitions for $\tilde{y}_j$ and $\tilde{\varpi}_j$. Substituting into the above equation we get

$$\tilde{\varpi}_i = P_i(\tilde{x}_0^{1/p^i}, \tilde{x}_1^{1/p^{i-1}}, \dots, \tilde{x}_i, \tilde{y}_0^{1/p^i}, \tilde{y}_1^{1/p^{i-1}}, \dots, \tilde{y}_i).$$

So by theorem 2 we have

$$\left(\sum_{i=0}^{n} \tau(x_i{}^{1/p^i})p^i\right)\left(\sum_{i=0}^{n} \tau(y_i{}^{1/p^i})p^i\right) \equiv \left(\sum_{i=0}^{n} \tau(\varpi_i{}^{1/p^i})p^i\right) \pmod{p^{n+1}}$$

holding for all n. It then follows that $f(x)f(y) = f(\varpi) = f(xy)$. □

Corollary 3. *$W_p(\mathbb{F}_p) \cong \mathbb{Z}_p$. Furthermore, for any $q = p^n$, $W_p(\mathbb{F}_q)$ is isomorphic to the unramified extension of $\mathbb{Z}_p$ of degree n.*

References

[1] M.J. Greenberg and J.P. Serre. *Local Fields.* Graduate Texts in Mathematics. Springer New York, 2013.

[2] Kiran Kedlaya. Notes on prismatic cohomology, 2024.

[3] Joseph Rabinoff. The theory of witt vectors, 2014.