# Motivating Witt Vectors and Delta Rings

Casimir Kothari
1/20/23

This is a note from a talk in the absolute prismatic cohomology learning seminar. It covers some of the necessary background, namely Witt Vectors and delta rings. The main sources this material is taken from are the Wikipedia page on Witt vectors [W], the Youtube lecture by James Borger on delta rings [B], and Bhatt's columbia lecture notes on prisms and prismatic cohomology [Bh].

## 1 Witt Vectors, Classically

To motivate the definition of Witt vectors, we consider the following problem: How do we find a good way to represent $p$-adic integers? One way is to represent a given $x \in \mathbb{Z}_p$ as

$$x = \sum_{i=0}^{\infty} a_i p^i \text{ with } a_i \in [0, p-1],$$

but it's not clear what algebraic formulas for addition and multiplication of such expressions would look like, as we have to do carrying of digits. Witt, following a suggestion of Hensel, figured out a better way to do this. Namely, we can use Hensel's lemma to construct the **Teichmuller character** $\omega : \mathbb{F}_p \to \mathbb{Z}_p^\times \cup \{0\}$ which sends $a \in \mathbb{F}_p^\times$ to the unique $(p-1)$st root of unity in $\mathbb{Z}_p$ which reduces to $a$ modulo $p$, and sends 0 to 0. This isn't an additive character, but it does have the key property that $\omega(a)^p = \omega(a)$ for any $a$.

Thus, we can write a given $p$-adic integer as $x = \sum_i \omega(a_i)p^i$. How do we add and multiply two such expressions? Let's consider an equality of Teichmuller digit expansions

$$\sum_i a_i p^i + \sum_i b_i p^i = \sum_i c_i p^i.$$

Then, we have $c_0 \equiv a_0 + b_0 \pmod p$, and therefore

$$c_0^p = (a_0 + b_0)^p \pmod{p^2}.$$

Let's thus try reducing the equality mod $p^2$, where we obtain

$$c_0^p + c_1 p \equiv a_0^p + a_1 p + b_0^p + b_1 p \pmod{p^2}.$$

Here, we've already used the fact that the Teichmuller coefficients satisfy $x^p = x$. But since $c_0^p = (a_0 + b_0)^p$ mod $p^2$ and $a_0^p + b_0^p - (a_0 + b_0)^p$ is divisible by $p$, we can divide by $p$ and obtain

$$c_1 \equiv a_1 + b_1 - \frac{(a_0 + b_0)^p - a_0 - b_0}{p} \pmod p.$$

Continuing, we would write

$$c_0^{p^2} + c_1^p p + c_2 p^2 \equiv a_0^{p^2} + a_1^p p + a_2 p^2 + b_0^{p^2} + b_1^p p + b_2 p^2 \pmod{p^3}$$

and solve for $c_2$ mod $p$ as well. In all cases, we notice that there exists **polynomials $\alpha_n$ with integer coefficients** such that

$$a + b = (\alpha_0(a_0, b_0), \alpha_1(a_0, a_1, b_0, b_1), \dots).$$

We could do the same thing for multiplication and find that there are polynomials $\pi_n$ with integer coefficients such that

$$ab = (\pi_0(a_0, b_0), \pi_1(a_0, a_1, b_0, b_1), \dots).$$

This defines a ring structure on $\prod_{n\geq 0} \mathbb{F}_p$ which identifies it with $\mathbb{Z}_p$. If we define the **Witt polynomials** to be $W_n = \sum_{i=0}^n p^i X_i^{p^{n-i}}$ and view them as **ghost coordinates** $W_n : \prod \mathbb{F}_p \to \mathbb{F}_p$, then observe that our construction showed that this ring structure was essentially determined once we knew the polynomial relations

$$W_n(a + b) = W_n(a) + W_n(b) \text{ and } W_n(ab) = W_n(a)W_n(b) \text{ in } \mathbb{F}_p.$$

Motivated by this, we make the following definition:

**Definition 1.1.** Given a commutative ring $A$, we define the **ring of Witt vectors** $W(A)$ (implicitly with respect to the prime $p$) to be the set $\prod_{i\geq 0} A$ endowed with the addition and multiplication as above. It is the unique ring structure on $\prod_{i\geq 0} A$ with addition and multiplication given by integer coefficient polynomials such that the projection to the ghost coordinates are ring homomorphisms.

We define the **Witt vectors of length** $n$ $W_n(A)$ to be the ring $\prod_{i=0}^{n-1} A$ with the same ring structure.

The first few terms of multiplication look like

$$ab = (a_0b_0, a_0^p b_1 + b_0^p a_1 + pa_1b_1, \dots).$$

Examples:

1. The computation above showed that $W(\mathbb{F}_p) = \mathbb{Z}_p$.

2. More generally, $W(\mathbb{F}_q) = \mathbb{Z}_p[\zeta_{q-1}]$, the ring of integers in the unramified degree $n$ extension of $\mathbb{Q}_p$, where $q = p^n$.

3. In general if $k$ is a perfect field of characteristic $p$, then $W(k)$ is a complete DVR with residue field $k$. Here, the valuation of $(a_i)$ is given by the least $i$ with $a_i \neq 0$.

4. In general if $A$ is a perfect ring of characteristic $p$, then $W(A)$ is a $p$-torsion free $p$-adically complete ring with $W(A)/(p) = A$. The idea here is that it is easy to check $W(A)/p = A$, and then one checks that $W(A)/p^nW(A) = W_n(A)$ and takes inverse limits on both sides.

5. In general though, Witt vectors can have $p$-torsion. For example $(p, p, \dots)$ is $p$-torsion in $W(\mathbb{Z}/p^2\mathbb{Z})$.

A useful perspective on Witt vectors is to view them as a functor from Rings to Rings. Indeed, consider the map $\operatorname{Spec} \mathbb{Z}[x_0, x_1, \dots] \to \operatorname{Spec} \mathbb{Z}[W_0, W_1, \dots]$ where we send $W_i$ to the $i$-th Witt polynomial. We consider the latter as a ring scheme sending $A$ to $\prod_{n\geq 0} A$ with the usual structure, and endow $\operatorname{Spec} \mathbb{Z}[x_0, x_1, \dots]$ with the unique ring scheme structure such that the given map is a homomorphism of ring schemes. With this structure, $\operatorname{Spec} \mathbb{Z}[x_0, x_1, \dots]$ represents the Witt vector functor. This lets us view the usual coordinates and ghost coordinates as actual coordinates on the Witt vectors. In fact, we can view this functor as landing in the category of $\delta$-Rings, where it is actually adjoint to the forgetful functor. More on this later.

To motivate the introduction of $\delta$-Rings, note that there is some important additional structure on the ring of Witt vectors, namely the Verschiebung and Frobenius morphisms. Verschiebung is the additive map $W(A) \to W(A)$ defined by $(a_0, a_1, \dots) \mapsto (0, a_1, a_2, \dots)$ on usual coordinates. Its easier to define Frobenius, on ghost coordinates, where it looks like $(w_0, w_1, \dots) \mapsto (w_1, w_2, \dots)$. If $A$ has characteristic $p$, this is a ring endomorphism and we can describe the Frobenius map concretely on standard coordinates as $(a_0, a_1, \dots) \mapsto (a_0^p, a_1^p, \dots)$, from which one sees that it is a map lifting the frobenius on $A$. But more generally, Frobenius is described by $F(a_0, a_1, \dots) = (f_0, f_1, \dots)$ where $W_n(f_0, \dots, f_n) = W_{n+1}(a_0, \dots, a_{n+1})$. This leads us to a consideration of the category of Rings with a Frobenius lift.

In the presence of $p$-torsion in a ring, the category of Rings with Frobenius lift is poorly behaved. The reason for this is that the definition of a Frobenius lift $\phi : A \to A$ says that for all $x \in A$, there exists $x' \in A$ such that $\phi(x) = x^p + px'$. Thus we can try to get rid of this by "keeping track" of the $x'$, analogously to the passage from sets to groupoids. As we'll see, this is exactly what the notion of $\delta$-ring does.

## 2 $\delta$-Rings

Recall that rather than keeping track of lifts of Frobenius, it is more categorically correct to keep track of the $x'$ such that $\phi(x) = x^p + px'$. Thus let's consider an arbitrary function $\delta : A \to A$ and decide what properties we want for $\phi(x) := x^p + p\delta(x)$ to be a Frobenius lift. Thinking, we arrive at:

**Definition 2.1.** A $\delta$-ring is a pair $(A, \delta)$ where $A$ is a commutative ring and $\delta : A \to A$ is a map of sets with $\delta(0) = \delta(1) = 0$, and satisfying

$$\delta(xy) = x^p\delta(y) + y^p\delta(x) + p\delta(x)\delta(y)$$
$$\delta(x+y) = \delta(x) + \delta(y) + \frac{x^p + y^p - (x+y)^p}{p}.$$

We get a category of $\delta$-rings, where the morphisms are maps of rings which respect $\delta$. The relation to Frobenius lifts is clarified by the following:

**Lemma 2.2.** If $\delta : A \to A$ is a $\delta$-structure on $A$, then the map $\phi : A \to A$ given by $\phi(f) = f^p + p\delta(f)$ is a lift of Frobenius on $A/p$. When $A$ is $p$-torsion free, this defines a bijective correspondence between lifts of Frobenius and $\delta$-structures on $A$.

*Proof.* The proof that $\phi$ is a ring homomorphism amounts to using the corresponding formulas for $\delta(x+y)$ and $\delta(xy)$. The bijective correspondence results because the equation $\phi(f) = f^p + p\delta(f)$ uniquely determines $\delta(f) = (\phi(f) - f^p)/p$ in the $p$-torsion free case. □

We can think of $\delta$ as a $p$-derivation, something which lowers $p$-adic order of vanishing by 1. Indeed, for any $\delta$-ring $A$ and $x \in A$, we can calculate

$$\delta(p^n x) = p^{np}\delta(x) + x^p\delta(p^n) + p\delta(x)\delta(p^n) \equiv p^{n-1}x^p \pmod{p^n},$$

which makes this intuition precise. We will clarify this relation further via analogy when when we discuss the relation to Witt vectors again.

**Example 2.3.** On $\mathbb{Z}$, there is only one $\delta$-structure, because the only Frobenius lift is the identity. In fact $\mathbb{Z}$ is the initial object in the category of $\delta$ rings.

**Example 2.4.** If $k$ is a perfect field of characteristic $p$, there is a unique $\delta$-structure on $W(k)$ coming from the Frobenius lift.

**Example 2.5.** If $p$ is invertible in $A$, then any endomorphism $\phi : A \to A$ is a Frobenius lift, and these all give rise to $\delta$ structures on $A$.

**Example 2.6.** If $A$ is a $\delta$-ring for which $p^n = 0$ in $A$ for some $n \geq 0$, then $A = 0$. Indeed, $0 = \delta(0) = \delta(p^n) = p^{n-1}(1 - p^{np-n})$ hence $p^{n-1} = 0$ in $A$, and we can conclude by induction.

$\delta$-ring structures are closely related to the Witt vectors, as we hinted at before. More precisely, recall the length 2 Witt vectors $W_2(A)$ of a ring $A$, which were explicitly defined via $W_2(A) = A \times A$ with addition and multiplication given by

$$(x, y) + (z, w) = (x + z, y + w + \frac{x^p + z^p - (x+z)^p}{p})$$
$$(x, y) \cdot (z, w) = (xz, x^p w + z^p y + pyw).$$

The second coordinate formulas remind us of the $\delta$-ring axioms, and in fact to put a $\delta$-ring structure on a ring $A$ is the same as specifying a ring map $w : A \to W_2(A)$ such that $\pi_1 \circ w = \mathrm{Id}_A$, where the $\delta$ structure is then just give by the second coordinate of $w$.

It is now interesting to consider the forgetful functor from $\delta$-rings to rings. The main result here is

**Proposition 2.7.** The forgetful functor $\delta$-ring $\to$ ring has both a left and right adjoint. The left adjoint $F$ constructs the free $\delta$-ring on a set, and the right adjoint is the Witt vector functor $W$.

The proof proceeds by showing that $\delta$-ring admits all colimits and limits, and that these commute with the forgetful functor, and then using the adjoint functor theorem.

Let's begin with the (more straightforward) left adjoint to the forgetful functor, namely the functor which takes $\mathbb{Z}[x_s : s \in S]$ to the free $\delta$-ring on the set $S$. In the one-variable case, we get a concrete description of

$$\mathbb{Z}\{x\} = \mathbb{Z}[x_0, x_1, \dots] \text{ with } \delta(x_i) = x_{i+1}.$$

An important idea using this is that every $\delta$-ring can be written as the quotient of a $p$-torsion free $\delta$-ring, namely $R$ is a quotient of $\mathbb{Z}\{R\}$.

We now list some properties of $\delta$-rings, which we don't prove for sake of time. A common strategy in the proof of many of these ideas is to reduce to the case of a $p$-torsion free ring by using a surjection as described above.

1. (Quotients) If $I \subset A$ is such that $\delta(I) \subset I$, there is a unique $\delta$-ring structure on $A/I$ compatible with $A \to A/I$.

2. $\delta$-Ring has arbitrary limits and colimits (compare to Rings with Frobenius lifts).

3. (Localizations) If $S \subset A$ is a multiplicative subset with $\phi(S) \subset S$, then there is a unique $\delta$-ring structure on $S^{-1}A$ compatible with that on $A$.

4. $\phi : A \to A$ is a $\delta$-map of $\delta$-rings.

5. (Completions) If $I$ is a finitely generated ideal containing $p$, then the $I$-adic completion of $A$ has a unique $\delta$-ring structure compatible with that on $A$.

# 3 Witt Vectors, Revisited

Let's understand how Witt vectors enter the picture. I learned about this analogy from [B].

Let's consider the category of Differential Rings, namely rings $R$ with a usual derivation $d : R \to R$ (which are additive and satisfy the Liebniz rule), with its forgetful functor to rings. This functor admits a right adjoint which we already know: it's the functor $P$ which assigns to a ring $A$ the ring

$$P(A) := \{\sum_n a_n \frac{t^n}{n!} : a_n \in A\}.$$

Here we think of $t^n/n!$ as a formal symbol. Addition is given componentwise, multiplication is $t^n/n! t^m/m! = t^{m+n}/(m+n)!\binom{m+n}{n}$, and the differential is $d = d/dt$.

Note that $P(A)$ comes with the map to $A$ given by projecting to $a_0$. To check that this functor is a right adjoint amounts to showing that, given a differential ring $R$ with a map $g : R \to A$, there is a unique $\tilde{g} : R \to P(A)$ which is $d$-equivariant and commutes with the projection to $a_0$. It's clear that this is the case, where

$$\tilde{g}(r) = \sum_{n \geq 0} g(d^n(r)) \frac{t^n}{n!}.$$

However, note that there is another perspective on $P(A)$; we can think about assembling the coefficients of a power series to make an identification (as sets) of $P(A) = \prod_{n \geq 0} A$. In this optic, the differential $d/dt$ just becomes shift to the left, and

$$\tilde{g}(r) = (g(r), g(d(r)), g(d^2(r)), \dots).$$

From this point of view, the ring structure on $P(A)$ is basically forced upon us by the condition of being a right adjoint; this follows from considering $\tilde{g}(r_1 r_2) = \tilde{g}(r_1)\tilde{g}(r_2), \tilde{g}(d(r_1 r_2)) = d\tilde{g}(r_1 r_2)$, and so on.

Armed with this analogy, we consider the forgetful functor from $\delta$-rings to rings. Given a $\delta$-ring $R$ and a map of rings $g : R \to A$, we consider $W(A) := \prod_{n \geq 0} A$ with $\delta$ given by the left shift as with $d$. Also consider the map $\tilde{g} : R \to W(A), r \mapsto (g(r), g(\delta(r)), g(\delta^2(r)), \dots)$. The condition of being a right adjoint again forces the multiplication and additive ring structure on $W(A)$ upon us, and if we investigate what happens, it turns out that $W(A)$ is isomorphic to the Witt ring defined earlier.

## References


[Bh] Bhargav Bhatt. Columbia Notes on Prismatic Cohomology. http://www-personal.umich.edu/~bhattb/teaching/prismatic-columbia/.

[BS] Bhatt, Scholze. *Prisms and Prismatic Cohomology.* https://arxiv.org/abs/1905.08229.

[B] James Borger, Witt Vectors, $\delta$-Rings and Prisms. https://youtu.be/_y2Tcu-iJV4.

[W] Witt Vectors, Wikipedia. https://en.wikipedia.org/wiki/Witt_vector.