Witt Vectors

Rızacan Çiloğlu

Whenever we deal with the p-adic topology, it will be assumed to be seperated.

1 Motivating observation

We will begin by defining the *Teichmüller representatives* which are a functorial set of representatives of mod p residues of a p-adically complete ring. They are the image of a certain section of the canonical projection defined below.

Proposition 1. *Let A be a p-adically complete ring with A/pA perfect. Then there exist a unique multiplicative map $f : A/pA \to A$ which sections the projection.*

Proof. We begin by making some observations

Lemma 2. *For $a, b \in A$, if $a = b$ mod p then we have $a^p = b^p$ mod p^2.*

To see this notice that as $b = a + px$ for some x, the binomial theorem implies $b^p = (a + px)^p = a^p + p(px)a^{p-1} + \cdots + p^p x^p$. Looking at this equality mod p^2 proves the claim.

More generally, the same argument shows if for $a = b \bmod p^n$ then we will have $a^p = b^p \bmod p^{n+1}$ and that $a^{p^n} = b^{p^n} \mod p^{n+1}$.

Lemma 3. *Each residue class in A/pA has a unique representative which has p^n-th roots for all n.*

Since A/pA is perfect, for each residue class $[a]$ mod p, there exist a unique residue class mod p $[b_n] := [a]^{p^{-n}}$. This means elements in $[a]$ admitting a p^n-th root are all congruent modulo p. By previous lemma this means they are even congruent modulo p^{n+1}. Therefore elements admitting p^n-th roots for all n must be congruent modulo p^n for all n therefore equal to each other. We can construct one such element by the following procedure:

For $n \geq 0$, let b_n be a random representative of the unique residue class $[a]^{p^{-n}}$. Consider the sequence $(b_n^{p^n})$. Note that as $b_{n+1}^p = b_n \bmod p$, we have $b_{n+1}^{p^{n+1}} = b_n^{p^n} \bmod p^{n+1}$. As A is p-adically complete this represents an element. Moreover, this element has a p^n-th root for all n since one can simply consider the sequence $y_k := b_{n+k}$. To see why $(y_k)^p = (b_n)$ notice that by the first lemma as

$$b_{n+k}^{p^k} = b_n \mod p \Rightarrow b_{n+k}^{p^{n+k}} = b_n^{p^n} \mod p^{n+1}$$

Showing $(y_k)^{p^n}$ and (b_n) represent the same element. □

This finally leads us to the proof of our initial proposition as we can define the unique multiplicative homomorphism as the one which takes each residue class to its unique representative admitting p^n-th roots for all n.

The upshot is, this section is functorial. For instance, if p is not a zero divisor in A then its elements can be represented uniquely as a as power series $\sum_{i=0}^{\infty} a_i p^i$ where a_i are a set of representatives of A/pA. However if one chooses the representatives of the residue classes mod p naively, it will not be functorial, meaning if we have a map to another p-adically complete ring it does not immediately give a map between the power series representation. Using the image of f constructed in Proposition 1 as the representatives would give rise to such a map thanks to their functoriality. Moreover, using the image of f representatives,

if we figure out how to carry out the multiplication and addition it would give rise to a method to recover a p-adically complete ring A (where p is not a zero-divisor) from the knowledge of its residues A/pA. This hopefully will motivate the following discussion

2 Witt Scheme

Let $\mathbb{A}^\infty$ denote the scheme representing the functor $R \mapsto R^\infty$ with the product ring structure. Equivalently, it is $\operatorname{Spec} \mathbb{Z}[w_0, \cdots]$ given ring scheme structure by the following maps

$$\begin{aligned} a(w_s) :=& w_s \otimes 1 + 1 \otimes w_s \\ m(w_s) :=& w_s \otimes w_s \end{aligned}$$

Let $W := \operatorname{Spec} \mathbb{Z}[x_0, \cdots]$. Fix a prime number p and define a map $w :\to A^\infty$ by

$$\begin{aligned} w_0 &\mapsto x_0 \\ w_1 &\mapsto x_0^p + px_1 \\ &\vdots \\ w_n &\mapsto x_0^{p^n} + px_1^{p^{n-1}} + \cdots + p^n x_n \end{aligned}$$

Theorem 4. *The ring scheme structure of $\mathbb{A}^\infty$ induces a ring scheme structure on W, which is the unique ring structure making w into a morphism of ring schemes.*

Proof. After base change to $\mathbb{Z}[1/p]$, w becomes an isomorphism because we can find polynomials (with $\mathbb{Z}[1/p]$ coefficients) which express w_i in terms of x_j for $j \leq i$ thus allowing us to define an inverse map. Thus, throught the isomorphism $W \times \mathbb{Z}[1/p]$ inherits a ring structure. Naturally, the maps which correspond to the ring operations can be described using polynomials with coefficients in $\mathbb{Z}[1/p]$. We will show that these polynomials actually turn out to have coefficients in $\mathbb{Z}$ which will allow us to extend the maps defining the ring structure from $W \times \operatorname{Spec} \mathbb{Z}[1/p]$ to whole W as it is separated (it is affine) and $W \times \mathbb{Z}[1/p]$ is a dense open subset. Therefore the maps satisfying the ring axioms in the dense open subset will imply they satisfy it globally (To see why, notice that the locus of agreement of two scheme maps $f, g : X \to Y$ is closed given X is separated).

By a slight abuse of notation, we will denote by $w_n(x)$ the polynomial that takes $x_0, \cdots, x_n$ to w_n as defined above. Given a polynomial in two variables Φ with integral coefficients, as discussed above, we can find polynomials $\varphi_n(x_0, \cdots, x_n; x_0' \cdots x_n')$ with coefficents in $\mathbb{Z}[1/p]$ such that for every n

$$\Phi(w_n(x), w_n(x')) = w_n(\varphi_0(x, x'), \cdots, \varphi_n(x, x')) \tag{1}$$

Proposition 5. *The coefficients of φ_n are integral*

Proof. We need a small lemma

Lemma 6. *Let R be a ring. If $r_i \equiv s_i \mod pR$, then $w_n(r) \equiv w_n(s) \mod p^{n+1}R$.*

This follows immediately from the observation made about the Frobenius in the previous section and the definition of w_n. □

Now armed with the lemma, we proceed by strong induction. The proposition is true for $n = 0$ trivially. Assume that the proposition is true for $i < n$.

$w_n(x) = w_{n-1}(x^p) + p^n x_n$ (please excuse the abuse of notation, should be clear what is meant by x^p.). By solving for $\varphi_n(x, x')$ from 1 we get

$$\varphi_n(x, x') = \frac{\Phi(w_n(x), w_n(x')) - w_{n-1}(\varphi_{n-1}(X, X')^p)}{p^n}$$

(Note that this is actually the recursive formula with which φ's are defined.). If we show $\Phi(w_n(x), w_n(x')) \equiv w_{n-1}(\varphi(x,x')^p \mod p^n$ then we will be done. In the left hand side, we will substitue $w_n(x) = w_{n-1}(x^p) + p^n x_n$ as before. However this time we can discard $p^n X_n$ as we are interested in it mod p^n. Then

$$\Phi(w_n(x), w_n(x')) \equiv \Phi(w_{n-1}(x^p), w_{n-1}(x'^p)) \mod p^n$$

Using 1 once again we see that

$$\Phi(w_n(x), w_n(x')) \equiv w_{n-1}(\varphi(x^p, x'^p)) \mod p^n$$

As $\varphi_i(x^p, x'^p) \equiv \varphi_i(x,x')^p \mod p$ by the Frobenius, our lemma finishes the proof. □

Given a ring R we will define the ring of Witt vectors (with respect to p) over R as $\mathrm{Hom}_{Sch}(\mathrm{Spec}\, R, W)$

3 Recovering A from A/pA

Consider again a p-adically complete ring A with A/pA perfect. With notation as in the last section we have

Theorem 7. *For all pair of sequences (x_i) and (x'_i) with $x_i, x'_i \in A/pA$ we have*

$$\Phi\left((\sum_i f({x_i}^{p^{-i}})p^i), (\sum_i f({x'_i}^{p^{-i}})p^i)\right) = f(\varphi_0(x_0, x'_0)) + \cdots + p^i f(\varphi_i(x,x')^{p^{-i}}) + \cdots$$

Proof. It suffices to show the equality hold mod p^{n+1} for every $n \in \mathbb{N}$. Fix some n. Substitute $y_i := {x_i}^{p^{-n}}$, $y'_i := {x'_i}^{p^{-n}}$. What we want to prove is

$$\Phi\left((\sum_i^n f({y_i}^{p^{n-i}})p^i), (\sum_i^n f({y'_i}^{p^{n-i}})p^i)\right) \equiv f(\varphi_0(y_0, y'_0)^{p^n}) + pf(\varphi_0(y,y')^{p^{n-1}}) \cdots + p^n f(\varphi_n(y,y')^{p^{-n}}) \mod p^{n+1}$$

However notice that right hand side can then be rewritten as $w_n(f(\varphi(y,y')))$ and left hand side can be rewritten as $\Phi(w_n(f(y)), w_n(f(y')))) = w_n(\varphi(f(y), f(y')))$. As per our lemma from the last section, to show the equivalence mod p^{n+1} it will suffice to show the equivalence $f(\varphi_i(y,y')) \equiv \varphi(f(y), f(y')) \mod p$. But this is immediate since by construction f respects the congruence class mod p. □

This whole discussion shows that $A \cong \mathrm{Hom}_{Sch}(\mathrm{Spec}\, A/pA, W)$ by an isomorphism. Explicitly, it is the map

$$\Theta : (x_0, x_1, \cdots) \mapsto \sum_i f(x_i)^{p^{-i}} p^i$$

Above theorem shows that it is actually a ring map. The inverse map is given by mapping a sum to the sequence composed of the coefficients. From the explicit description of W, arguing along the same lines, one can show that given a perfect $\mathbb{F}_p$ algebra R, the ring of Witt vectors over it is a complete ring where p is not a zero-divisior and its residues mod p is precisely R. Furthermore the functors $\mathrm{Hom}_{Sch}(\bullet, W)$ and $\bullet/\bullet p$ turn out to be quasi-inverses considered between the category of perfect $\mathbb{F}_p$ algebras and the category of p-adically complete rings with perfect residues mod p, flat over $\mathbb{Z}_p$.

4 Some endomorphisms

There is an endomorphism (as a scheme) of W given by $X_n \mapsto X_{n-1}$ where for $n = 0$ X_0 is just sent to 0. In the level of A valued points this is just the map $(a_0, a_1, \cdots) \mapsto (0, a_1, a_2, \cdots)$. Now, when working over $\mathrm{Spec}\, \mathbb{Z}[1/p]$, after passing through the isomorphism to $\mathbb{A}^\infty$ transforms the map is transformed to $w_n \mapsto p w_{n-1}$ which clearly is additive, thus by repeating the previous arguments it must be additive for W as well. For evident reasons, it is called Verschiebung (shift) map and denoted V.

Over $\mathbb{F}_p$ the Frobenius induces by functoriality an endomorphism (as a ring scheme this time) of W. This will be denoted F. Equivalently it is the map given by $x_n \mapsto x_n^p$.

Proposition 8. $VF = p = FV$

Proof. Notice we can always write an $\mathbb{F}_p$ algebra as a quotient of a polynomial ring, which embeds into a perfect ring (for example, its own perfection). Therefore it will suffice to prove it only for perfect $\mathbb{F}_p$ algebras. But in that case we know there is an isomorphism between the power series Θ.

$$\Theta(FV(x)) = \sum_{i=0}^{\infty} f(x_i^{p^{-i}})p^{i+1} = p\Theta((x)) = \Theta(p(x))$$

.

□

5 Truncations

The n-Truncated Witt vectors are the points of $\text{coker}(V^n : W \to W)$. They are denoted by W_n. Equivalently, they are the ring schemes obtained by repeating this story but only for a finite amount of variables. The canonical maps $W_n \to W_{n-1}$ are given by the inclusion $\mathbb{Z}[x_0, \cdots, x_{n-1}] \to \mathbb{Z}[x_0, \cdots, x_n]$. This naturally forms a direct system and we have

$$\text{colim}_n W_n = W$$

.

6 Bonus definition for perfect $\mathbb{F}_p$ algebras

Given an $\mathbb{F}_p$ algebra R, turns out the Frobenius induces the 0 endomorphism on the cotangent complex $L_{R/\mathbb{F}_p}$. This is essentially because Frobenius induces the zero map on $\Omega^1_{R/\mathbb{F}_p}$. If R is perfect, then as Frobenius is an isomorphism, so is the induced map 0 meaning $L_{R/\mathbb{F}_p} = 0$. This then tells us, there is a unique flat lift of R over $\mathbb{Z}_p$. The Witt vectors turn out to be one such lift (They are torsion free and $\mathbb{Z}_p$ is a PID). Therefore, this can be taken as an equivalent definition of the Witt vectors, at least in the case of a perfect $\mathbb{F}_p$ algebra.

7 Witt Vector Affine Grassmannian

Let me conclude with statement of the theorem we are trying to understand.

Theorem 9. *For $G = \text{GL}_n$ the functor $\text{Gr}^{W\,aff,[a,b]}$ on perfect rings R is the set of $W(R)$ lattices $\Lambda \subset (W(R)[1/p])^n$ such that*

$$p^b W(R)^n \subset \Lambda \subset p^a W(R)^n$$

This functor is representable by perfection of a projective variety over $\mathbb{F}_p$. Consequently $\text{Gr}^{W\,aff}$ the set of lattices without any bounds is representable by an inductive limit of perfections of projective varieties.