An essay on Witt Vectors

Let $p \in \mathbf{Z}$ be a prime number. In a first course in algebraic number theory one usually encounters, when studying unramified extensions of the field $\mathbf{Q}_p$, the following equivalence of categories

$$\begin{aligned} \phi : \{\text{Finite unramified extensions } K/\mathbf{Q}_p\} &\longrightarrow \{\text{Finite field extensions } k/\mathbf{F}_p\} \\ K &\longmapsto \mathcal{O}_K/p \end{aligned}$$

where, importantly, $p \in K$ is a uniformiser by hypothesis of $K/\mathbf{Q}_p$ being unramified. Conceptually, both fully faithfulness and essential surjectivity are consequences of Hensel's lemma: the generator (cfr. the primitive element theorem) of an extension $K/\mathbf{Q}_p$ can of course chosen to be integral and then, as a morphism of fields $K_1 \to K_2$ over $\mathbf{Q}_p$ restricts to a map on rings of integers $\mathcal{O}_{K_1} \to \mathcal{O}_{K_2}$ and is determined by where it sends such a generator, it's no loss of data to consider the corresponding mod p map $k_1 \to k_2$ since Hensel's lemma states existence and uniqueness of lifts - the reduction mod p of the minimal polynomials of the generators of K_1 and K_2 over $\mathbf{Q}_p$ must be irreducible as $K_1, K_2/\mathbf{Q}_p$ are unramified.

Essential surjectivity, on the other hand, is argued by taking $\zeta_n \in \mathbf{F}_{p^n}$ a primitive $p^n - 1$-th root of unity and lifting it via Hensel's lemma to $\widetilde{\zeta_n} \in \overline{\mathbf{Z}}_p$. The Galois extension $\widetilde{\zeta_n} \in \overline{\mathbf{Q}}_p$ generates over $\mathbf{Q}_p$ must then be unramified and have $\mathbf{Z}_p[\widetilde{\zeta_n}]$ as its ring of integers: indeed, $\mathbf{Q}_p(\widetilde{\zeta_n})$ is the splitting field of a polynomial whose reduction modulo p is irreducible, $\mathcal{O}_{\mathbf{Q}_p(\widetilde{\zeta_n})}$ certainly contains $\mathbf{Z}_p[\widetilde{\zeta_n}]$ as a subring and

$$\deg q_{\widetilde{\zeta_n}} = [\mathbf{Q}_p(\widetilde{\zeta_n}) : \mathbf{Q}_p] = \deg \overline{q}_{\widetilde{\zeta_n}} = \deg q_{\zeta_n} = [\mathbf{F}_{p^n} : \mathbf{F}_p] = n$$

where $q_{\widetilde{\zeta_n}}$ and q_{ζ_n} are the monic minimal polynomials in $\mathbf{Z}_p[T]$ and $\mathbf{F}_p[T]$ of $\widetilde{\zeta_n}$ and ζ_n respectively, the latter being the mod p reduction of the former. Since $\mathbf{Z}_p[\widetilde{\zeta_n}]/(p) \cong \mathbf{F}_{p^n}$ by construction, we get that $\mathbf{Z}_p[\widetilde{\zeta_n}]$ is indeed the ring of integers and thus $\phi(\mathbf{Q}_p(\widetilde{\zeta_n})) \cong \mathbf{F}_{p^n}$.

An important consequence is that finite unramified extensions of local fields are all Galois and cyclic, by the above fully faithfulness result, and all finite cyclic groups appear as the Galois group of a unique unramified extension $K/\mathbf{Q}_p$.

The reliance on the $p^n - 1$-th roots of unity in the above construction for fully faithfulness is suggestive: it uses roots of unity in the unramified extensions of $\mathbf{Q}_p$ as representatives for the mod p equivalence classes of elements in their residue fields; for example, this constrasts the common usage of the elements $0, 1, \ldots, p-1 \in \mathbf{Z}_p$ in the power series expansions

$$a = \sum_{i=0}^{\infty} a_i p^n, \;\; a_i \in \{0, 1, \ldots, p-1\}$$

of arbitrary p-adic integers $a \in \mathbf{Z}_p$ - if one were to trace through the construction of the trivial unramified extension corresponding to $\mathbf{F}_p/\mathbf{F}_p$ (which of course is just $\mathbf{Q}_p/\mathbf{Q}_p$) then it would be in line to consider p-adic integers a in $\mathbf{Z}_p$ expressed as power series of the form

$$a = \sum_{i=0}^{\infty} \widetilde{\zeta_1}^{\alpha_i} p^i.$$

The rather beautiful consequence of this replacement for the usual representatives of elements in $\mathbf{Z}_p/p$ is that it provides a description (albeit a somewhat inexplicit one) of the multiplication and addition in $\mathbf{Z}_p$ in terms of the above power-series expressions; this boils down essentially to the fact that the elements $1, \widetilde{\zeta_1}, \ldots, \widetilde{\zeta_1}^{p-1}$ are the images under a *group homomorphism*

$$\begin{aligned}[-] : \mathbf{F}_p^\times &\to \mathbf{Z}_p^\times \\ \zeta_1 &\mapsto \widetilde{\zeta_1}\end{aligned}$$

which is a section of the projection $\mathbf{Z}_p^\times \to \mathbf{F}_p^\times$, as opposed to the elements $1, 2, \ldots, p-1 \in \mathbf{Z}_p$. The same discussion can of course be made for any unramified extension of $\mathbf{Q}_p$.

We can try to figure out via brute-force how to add such power series: fix $n \geq 1$ and elements

$$\begin{aligned}a &= \sum_{i=0}^{\infty} \widetilde{\zeta_n}^{\alpha_i} p^i = \sum_{i=0}^{\infty} [a_n] p^n, \\ b &= \sum_{i=0}^{\infty} \widetilde{\zeta_n}^{\beta_i} p^i = \sum_{i=0}^{\infty} [b_i] p^n \in \mathbf{Z}_p[\widetilde{\zeta_n}]\end{aligned}$$

(where we set $\zeta_n^{\alpha_i} = a_i$ and $\zeta_n^{\beta_i} = b_i$) in the ring of integers of the unique unramified $\mathbf{Z}/n$-extension of $\mathbf{Q}_p$ and express their sum in terms of a power series

$$a + b = \sum_{i=0}^{\infty} [(a+b)_i] p^i$$

as well. Reducing mod p we see that $a_0 + b_0 = (a+b)_0$, but things get a little trickier for higher powers: modulo p^2 we see that

$$[a_0] + [b_0] + ([a_1] + [b_1])p \equiv [a_0 + b_0] + [(a+b)_1]p \mod p^2$$

whence

$$[(a+b)_1]p \equiv ([a_1] + [b_1])p + ([a_0] + [b_0] - [a_0 + b_0]) \mod p^2$$

so to get an expression for $(a+b)_1 \in \mathbf{F}_{p^n}$ in terms of a_0, a_1, b_0, b_1 it would be great if the difference $[a_0] + [b_0] - [a_0 + b_0]$ were a multiple of p, or at the very least modulo p^2 (in order to 'divide' both sides by p and get an equality modulo p, i.e. in $\mathcal{O}_{\mathbf{Q}_p(\widetilde{\zeta_n})}/p \cong \mathbf{F}_{p^n}$).

But $\mathbf{F}_{p^n}$ is a perfect field and $[-]$ is a group homomorphism! So we can express

$$a_0 = (a_0^{1/p})^p, \;\; b_0 = (b_0^{1/p})^p$$

and then

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

Finally, $([a_0^{1/p}] + [b_0^{1/p}])^p - [a_0^{1/p} + b_0^{1/p}]^p$ is a multiple of p^2 since $[a_0^{1/p}] + [b_0^{1/p}] \equiv [a_0^{1/p} + b_0^{1/p}]$ modulo p. Since the binomial coefficient $\binom{p}{i}$ is a multiple of p for every i between 1 and $p-1$, we get the expression

$$(a+b)_1 = a_1 + b_1 - \sum_{i=1}^{p-1} \frac{1}{p} \binom{p}{i} a_0^{i/p} b_0^{1-i/p}.$$

Generally speaking, the terms $(a+b)_m, (a\cdot b)_m \in \mathbf{F}_{p^n}$ are given as polynomial expressions with integral coefficients in the terms $a_m, b_m, a_{m-1}^{1/p}, b_{m-1}^{1/p}, \ldots, a_0^{1/p^m}, b_0^{1/p^m}$. For example, simple pattern recognition shows that the parts of these polynomials depending on a_m, b_m are $a_m + b_m$ and $a_m \cdot b_m$ respectively.

An intriguing and somewhat enlightening observation is that these computations really depend on few properties $\mathbf{F}_{p^n}$ enjoys. We first make a sketchy digression on how to proceed, and then discuss a these ideas more meticulously: given an arbitrary *perfect* $\mathbf{F}_p$-algebra A, we can run through the same construction to produce an algebra $W^{\text{naïve}}(A)$ over $\mathbf{Z}_p$ whose mod-p reduction is A by setting

$$W^{\text{naïve}}(A) = \left\{ \sum_{i=0}^{\infty} [a_i] p^i \mid a_i \in A \right\}$$

(here the elements $[a_i] \in W^{\text{naïve}}(A)$ for $a_i \in A$ are just formal elements and p^i is just a placeholder; concretely, on underlying sets we have $|W^{\text{naïve}}(A)| = A^{\mathbf{N}}$) and define addition and multiplication on $W^{\text{naïve}}(A)$ as

$$\left(\sum_{i=0}^{\infty} [a_i] p^i \right) + \left(\sum_{i=0}^{\infty} [b_i] p^i \right) := \left(\sum_{i=0}^{\infty} \left[S_i \left(a_0^{1/p^n}, \ldots, a_n, b_0^{1/p^n}, \ldots, b_n \right) \right] p^i \right)$$
$$\left(\sum_{i=0}^{\infty} [a_i] p^i \right) \cdot \left(\sum_{i=0}^{\infty} [b_i] p^i \right) := \left(\sum_{i=0}^{\infty} \left[P_i \left(a_0^{1/p^n}, \ldots, a_n, b_0^{1/p^n}, \ldots, b_n \right) \right] p^i \right)$$

where S_i and $P_i \in \mathbf{Z}[A_0, \ldots, A_n, B_0, \ldots, B_n]$ are the aforementioned polynomials. We thus recover the ring of integers $\mathcal{O}_{\mathbf{Q}_p(\widetilde{\zeta_n})}$ from above as $W^{\text{naïve}}(\mathbf{F}_{p^n})$ purely by construction.

The issue with this strategy is that it doesn't generalise to algebras over $\mathbf{Z}_p$ in which p isn't equal to zero, let alone the non-perfect $\mathbf{F}_p$-algebras; this would be a desirable feature since then W would turn out to define a functor on the whole category of $\mathbf{Z}_p$-algebras and a ring-scheme over $\mathbf{Z}_p$ (this will actually turn out to be crucial even to define W for perfect $\mathbf{F}_p$ algebras, even though this might be unclear as of now).

To solve this issue, we *approximate*: instead of constructing $W^{\text{naïve}}(A)$ directly, we can define the ring of truncated Witt vectors $W_n(A)$ by setting

$$W_n(A) = \left\{ \sum_{i=0}^{n} [a_i] p^i \mid a_i \in A \right\}$$

and defining addition and multiplication by

$$\left(\sum_{i=0}^{n} [a_i] p^i \right) + \left(\sum_{i=0}^{n} [b_i] p^i \right) := \left(\sum_{i=0}^{n} \left[S_i \left(a_0, \ldots, a_n, b_0, \ldots, b_n \right) \right] p^i \right)$$
$$\left(\sum_{i=0}^{n} [a_i] p^i \right) \cdot \left(\sum_{i=0}^{n} [b_i] p^i \right) := \left(\sum_{i=0}^{n} \left[P_i \left(a_0, \ldots, a_n, b_0, \ldots, b_n \right) \right] p^i \right)$$

so that then if A is a perfect $\mathbf{F}_p$-algebra we get an isomorphism

$$W_n(A) \longrightarrow W^{\text{naïve}}(A)/p^{n+1}$$
$$[a_0] + [a_1]p + \ldots + [a_n]p^n \longmapsto [a_0^{1/p^n}] + [a_1^{1/p^{n-1}}]p + \ldots + [a_n]p^n$$

where $W^{\text{naïve}}(A)$ is as in our above definition. Finally, since $W^{\text{naïve}}(A) \cong \varprojlim_n W^{\text{naïve}}(A)/p^{n+1}$ essentially by construction, it's then justified to set

$$W(A) := \varprojlim_n W_n(A)$$

for an *arbitrary* $\mathbf{Z}_p$-algebra A! This way $W(A) \cong W^{\text{naïve}}(A)$ whenever A is perfect over $\mathbf{F}_p$ - note that here a key property we used is that multiplication by p on $W^{\text{naïve}}(A)$ *'shifts'* all coefficients upwards by one; this will not generally be the case if A isn't an algebra over $\mathbf{F}_p$.

Proposition 1. *Let $K/\mathbf{Q}_p$ be a finite field extension with ring of integers $\mathcal{O}_K$ and uniformiser $\pi \in \mathfrak{m}_K$; set $q = p^n$ where $\mathcal{O}_K/\pi \cong \mathbf{F}_q$. Define the polynomials*

$$w_n(X_0, \ldots, X_n) := X_0^{q^n} + \pi \cdot X_1^{q^{n-1}} + \ldots + \pi^n \cdot X_n \in \mathcal{O}_K[X_0, \ldots, X_n]$$

for $n \geq 0$. There exist unique polynomials $(S_n, P_n)_{n \geq 0}$ in $\mathcal{O}_K[X_0, \ldots, X_n, Y_0, \ldots, Y_0]$ such that

$$w_n(X_0, \ldots, X_n) + w_n(Y_0, \ldots, Y_n) = w_n(S_0(X_0, Y_0)\,,\, \ldots\,,\, S_n(X_0, \ldots, X_n, Y_0, \ldots, Y_n))$$
$$w_n(X_0, \ldots, X_n) \cdot w_n(Y_0, \ldots, Y_n) = w_n(P_0(X_0, Y_0)\,,\, \ldots\,,\, P_n(X_0, \ldots, X_n, Y_0, \ldots, Y_n)).$$

Proof. The construction follows the same lines as the computation we described above for $(a+b)_1$: we have $S_0(X_0, Y_0) = X_0 + Y_0$ and if we suppose S_n exists, we construct S_{n+1} as follows: since

$$w_{n+1}(X_0, \ldots, X_{n+1}) = w_n(X_0^q, \ldots, X_n^q) + \pi^{n+1} X_{n+1}$$

we're forced to have

$$\pi^{n+1} S_{n+1}(X_0, \ldots, X_{n+1}, Y_0, \ldots, Y_{n+1}) = w_{n+1}(X_0, \ldots, X_{n+1}) + w_{n+1}(Y_0, \ldots, Y_{n+1}) \\ - w_n(S_0(X_0, Y_0)^q, \ldots, S_n(X_0, \ldots, X_n, Y_0, \ldots, Y_n)^q).$$

Now we can conclude by noting that the left hand side

$$w_{n+1}(X_0, \ldots, X_{n+1}) + w_{n+1}(Y_0, \ldots, Y_{n+1}) - w_n(S_0(X_0, Y_0)^q, \ldots, S_n(X_0, \ldots, X_n, Y_0, \ldots, Y_n)^q) = \\ \pi^{n+1}(X_{n+1} + Y_{n+1}) + (w_n(X_0^q, \ldots, X_n^q) + w_n(X_0^q, \ldots, X_n^q) - w_n(S_0(X_0, Y_0)^q, \ldots, S_n(X_0, \ldots, X_n, Y_0, \ldots, Y_n)^q))$$

is a multiple of π^{n+1} since for each $i = 0, \ldots, n$

$$\begin{aligned} & S_i(X_0, \ldots, X_n, Y_0, \ldots, Y_n)^q \equiv S_i(X_0^q, \ldots, X_n^q, Y_0^q, \ldots, Y_n^q) \mod \pi \\ \implies & (S_i(X_0, \ldots, X_n, Y_0, \ldots, Y_n)^q)^{q^{n-i}} \equiv S_i(X_0^q, \ldots, X_n^q, Y_0^q, \ldots, Y_n^q)^{q^{n-i}} \mod \pi^{n-i+1} \\ \implies & \pi^i \cdot (S_i(X_0, \ldots, X_n, Y_0, \ldots, Y_n)^q)^{q^{n-i}} \equiv \pi^i \cdot S_i(X_0^q, \ldots, X_n^q, Y_0^q, \ldots, Y_n^q)^{q^{n-i}} \mod \pi^{n+1} \end{aligned}$$

and adding these congruences altogether yields

$$w_n(S_0(X_0, Y_0)^q, \ldots, S_n(X_0, \ldots, X_n, Y_0, \ldots, Y_n)^q) \equiv \underbrace{w_n(S_0(X_0^q, Y_0^q), \ldots, S_n(X_0^q, \ldots, X_n^q, Y_0^q, \ldots, Y_n^q))}_{= w_n(X_0^q, \ldots, X_n^q) + w_n(Y_0^q, \ldots, Y_n^q)} \mod \pi^{n+1}.$$

The uniqueness assertion follows directly since we were forced to define $S_n(X_0, \ldots, X_n, Y_0, \ldots, Y_n)$ as

$$\frac{1}{\pi^n} \cdot (w_n(X_0, \ldots, X_n) + w_n(Y_0, \ldots, Y_n) - w_n(S_0(X_0, Y_0)^q, \ldots, S_{n-1}(X_0, \ldots, X_{n-1}, Y_0, \ldots, Y_{n-1})^q)) \quad (1)$$

now that we've checked that this indeed defines a polynomial in $\mathcal{O}_K[X_0, \ldots, X_n, Y_0, \ldots, Y_n]$. The construction of the polynomials $(P_i)_{i \geq 0}$ follows the same steps and we omit the details. ∎

To continue, the aim would be to define a ring structure on $W_{\mathcal{O}_K}(A) := \left\{ \sum_{i=0}^{\infty} [a_i]\pi^i \mid a_i \in A \right\}$ for an arbitrary $\mathcal{O}_K$-algebra A by setting

$$\left(\sum_{n=0}^{\infty} [a_n]\pi^n \right) + \left(\sum_{n=0}^{\infty} [b_n]\pi^n \right) = \sum_{n=0}^{\infty} [S_n(a_0, \ldots, a_n, b_0, \ldots, b_n)]\pi^n, \text{ and}$$
$$\left(\sum_{n=0}^{\infty} [a_n]\pi^n \right) \cdot \left(\sum_{n=0}^{\infty} [b_n]\pi^n \right) = \sum_{n=0}^{\infty} [P_n(a_0, \ldots, a_n, b_0, \ldots, b_n)]\pi^n,$$

mimicking our above discussion, but it's unclear why this should define a ring structure on $W_{\mathcal{O}_K}(A)$. To this end, define the sequence of maps

$$\begin{aligned} w_n : W_{\mathcal{O}_E}(A) &\longrightarrow A \\ \sum_{n=0}^{\infty} [a_i]\pi^i &\longmapsto w_n(a_0, \ldots, a_n) \end{aligned}$$

which induce

$$w : W_{\mathcal{O}_E}(A) \xrightarrow{(w_n)_n} \prod_{n=0}^{\infty} A$$

where $\prod_{n\geq 0} A$ enjoys the product ring structure. If the above formulas defined a ring structure on $W_{\mathcal{O}_K}(A)$, then $(w_n)_{n\geq 0}$ would be a ring homomorphism by the functional equations the polynomials S_i, P_i satisfy; thus, in case $(w_n)_{n\geq 0} : W_{\mathcal{O}_K}(A) \to \prod_n A$ is injective, $W_{\mathcal{O}_K}(A)$ is indeed a well-defined ring and a sub-$\mathcal{O}_K$-algebra of $\prod_n A$.

If $\pi \in A^\times$, then $(w_n)_{n\geq 0}$ is a bijection as can be seen by noting that the term in w_n depending on X_n is a unit multiple of X_n. Then $W_{\mathcal{O}_K}(A)$ is indeed an $\mathcal{O}_K$-algebra and $(w_n)_{n\geq 0}$ is an isomorphism of rings. Now note that if A is π-torsion free, then $W_{\mathcal{O}_K}(A)$ injects into $W_{\mathcal{O}_K}(A[\pi^{-1}])$ and this realises $W_{\mathcal{O}_K}(A)$ as a subring of $W_{\mathcal{O}_K}(A[\pi^{-1}])$. Lastly, if A is π-torsion free and $I \subset A$ is any ideal, then the surjectivity of $W_{\mathcal{O}_K}(A) \twoheadrightarrow W_{\mathcal{O}_K}(A/I)$ once again implies the ring structure on $W_{\mathcal{O}_K}(A/I)$ is well-defined. We can thus conclude that $W_{\mathcal{O}_K}(A)$ is a well defined $\mathcal{O}_K$-algebra for any $\mathcal{O}_K$-algebra A, since any such ring is a quotient of a polynomial ring of the form $\mathcal{O}_K[T_i \mid i \in I]$ which is π-torsion free.

Note that since $W_{\mathcal{O}_K}$ is a functor, we have a Frobenius map $\Phi_{W_{\mathcal{O}_K}(A)} : W_{\mathcal{O}_K}(A) \to W_{\mathcal{O}_K}(A)$ whenever A is a perfect algebra over $\mathbf{F}_q$.

Proposition 2.

1. *The map*
$$[-] : A \to W_{\mathcal{O}_K}(A)$$
defined by $[a] \mapsto [a] + [0]\pi + \ldots \in W_{\mathcal{O}_K}(A)$ *is a multiplicative map, natural in* A.

2. *There exists a natural transformation* $\Phi : W_{\mathcal{O}_K} \to W_{\mathcal{O}_K}$ *which agrees with the Frobenius map* $\Phi_{W_{\mathcal{O}_K}(A)} : W_{\mathcal{O}_K}(A) \to W_{\mathcal{O}_K}(A)$ *from above on* $\mathbf{F}_q$*-algebras* A.

3. *The map*
$$\begin{aligned} V : W_{\mathcal{O}_K}(A) &\longrightarrow W_{\mathcal{O}_K}(A) \\ \sum_{n=0}^{\infty} [a_n]\pi^n &\longmapsto \sum_{n=1}^{\infty} [a_{n-1}]\pi^n \end{aligned}$$
defines a natural morphism of $\mathcal{O}_K$*-modules* $W_{\mathcal{O}_K}(A) \to W_{\mathcal{O}_K}(A)$.

Proof. 1. If $\pi \in A$ is invertible then $W_{\mathcal{O}_K}(A) \xrightarrow[\cong]{w} \prod_n A$ as discussed and $[-] : A \to W_{\mathcal{O}_K}(A)$ identifies with the map

$$\begin{aligned} A &\longrightarrow \prod_n A \\ a &\longmapsto (a, a^q, a^{q^2}, \ldots) \end{aligned}$$

which is indeed multiplicative - for general A the same argument from our discussion above holds.

3. Since
$$\pi \cdot w_n(a_0, \ldots, a_n) = w_{n+1}(0, a_0, \ldots, a_n)$$
we see that by considering the $\mathcal{O}_K$-linear map
$$\begin{aligned} v : \prod_{n\geq 0} A &\longrightarrow \prod_{n\geq 0} A \\ (x_0, x_1, x_2, \ldots) &\longmapsto (0, \pi \cdot x_0, \pi \cdot x_1, \ldots) \end{aligned}$$
for $\mathcal{O}_K$-algebras A in which π is invertible, we have a commutative diagram
$$\begin{array}{ccc} W_{\mathcal{O}_K}(A) & \xrightarrow[\cong]{w} & \prod_n A \\ \downarrow{\scriptstyle V} & & \downarrow{\scriptstyle v} \\ W_{\mathcal{O}_K}(A) & \xrightarrow[\cong]{w} & \prod_n A \end{array}$$
and thus V indeed is $\mathcal{O}_K$-linear - once again, the same strategy applies to conclude V is $\mathcal{O}_K$-linear for all algebras A.

2. We refrain from discussing the details for the sake of brevity, but the gist is just as above: by induction on n one can prove the existence of polynomials $F_n \in \mathcal{O}_E[X_0, \ldots, X_{n+1}]$ such that $F_n \equiv X_n^q$ for every n and
$$w_n(F_0, \ldots, F_n) = w_{n+1}(X_0, \ldots, X_{n+1}).$$
Then the map defined by $\Phi_A : \sum\limits_{n\geq 0} [a_n]\pi^n \mapsto \sum\limits_{n\geq 0} [F_n(a_0, \ldots, a_{n+1})]\pi^n$ defines a natural transformation $W_{\mathcal{O}_E} \to W_{\mathcal{O}_E}$ by the same argument as above, since the diagram
$$\begin{array}{ccc} W_{\mathcal{O}_E}(A) & \xrightarrow{w} & A^{\mathbf{N}} \\ \downarrow{\scriptstyle \Phi} & & \downarrow{\scriptstyle \text{shift}} \\ W_{\mathcal{O}_E}(A) & \xrightarrow{w} & A^{\mathbf{N}} \end{array}$$
where $\text{shift}(a_0, a_1, \ldots) = (a_1, a_2, \ldots)$, is commutative by construction.

■

Example 3. We now mention some properties the morphisms V and F satisfy, which aren't hard to show although we omit their discussion since the proofs shed light on no new ideas and really just follow the same strategy outlined in Proposition 2: the idea is to always check '*functorially*' formulas on the counterparts of V and F as natural transformations $A^{\mathbf{N}} \to A^{\mathbf{N}}$. We have relations

1. $F(V(x)) = \pi \cdot x$,
2. $V(F(x)y) = xV(y)$,
3. $\pi \cdot F(x) \cdot y = F(x \cdot V(y))$.

In particular, we see that the image of V^n, given by elements of the form $\left\{\sum_{i\geq n} [a_i]\pi^i\right\} \subset W_{\mathcal{O}_E}(A)$, is an ideal; moreover, as one might expect, $W_{\mathcal{O}_E}(A)$ is complete with respect to the cofiltered system of ideals defined by the images of V^n, i.e.
$$W_{\mathcal{O}_E}(A) \cong \varprojlim_{n\geq 0} W_{\mathcal{O}_E}(A)/V^n(W_{\mathcal{O}_E}(A)).$$

This follows from the fact that, as sets, $A^{\mathbf{N}}$ is the projective limit $\varprojlim_n A^n$ and each quotient $W_{\mathcal{O}_E}(A)/V^n(W_{\mathcal{O}_E}(A))$ is identified with A^{n+1}. This implies any element $x \in W_{\mathcal{O}_E}(A)$ can be expressed as a power series of the form

$$\sum_{n=0}^{\infty} V^n([x_n])$$

for elements $x_i \in A$; note that the x_i's don't necessarily agree with the components of the expression $x = \sum_n [a_i]\pi^i$, but there is a relation between them if A is a perfect $\mathbf{F}_q$-algebra: we have

$$\sum_{i=0}^{\infty} V^n([x_i]) = \sum_{i=0}^{\infty} \left[x_i^{1/q^i}\right] \pi^i$$

as can be checked by first showing that $V \circ F$ is also given by multiplication by π in this particular case. Thus, if A is a perfect $\mathbf{F}_q$-algebra, $W_{\mathcal{O}_E}(A)$ is π-adically complete.

From now on, we fix a non-archimedean algebraically closed field F over $\mathbf{F}_q$, and a finite extension E of $\mathbf{Q}_p$ with residue field $\mathbf{F}_q$.

Definition 4. We define the ring $\mathbf{A}_{\text{inf}} = \mathbf{A}_{\text{inf},E,F}$ as the $\mathcal{O}_E$-algebra of Witt vectors

$$\mathbf{A}_{\text{inf}} = W_{\mathcal{O}_E}(\mathcal{O}_F).$$

The importance of $\mathbf{A}_{\text{inf}}$ is in its relevance with the following notion.

Definition 5. Let A be a π-complete $\mathcal{O}_E$ algebra. Define the *tilt* of A as

$$A^\flat := \varprojlim_{x \mapsto x^q} A/\pi$$

which is a perfect $\mathbf{F}_q$-algebra.

More details on tilts are discussed in the notes from this semester's course, lecture 7.

Proposition 6. *The pair of functors*

$$W_{\mathcal{O}_E}(-) \dashv (-)^\flat$$

form an adjoint pair between the categories of π-complete $\mathcal{O}_E$-algebras and perfect $\mathbf{F}_q$-algebras. The counit

$$\theta : W_{\mathcal{O}_E}((-)^\flat) \to (-)$$

is called Fontaine's map.

Proof. We start by constructing θ. The map

$$\begin{aligned} w_n : W_{\mathcal{O}_E}(A) &\to A \\ \sum_{n=0}^{\infty} [a_n]\pi^n &\mapsto w_n(a_0, \ldots, a_n) \end{aligned}$$

is a ring homomorphism since it's the composition of w as constructed above and the projection $A^{\mathbf{N}} \to A$ onto the n-th factor; it induces

$$W_{\mathcal{O}_E,n}(A) := W_{\mathcal{O}_E}(A)/V^{n+1}(W_{\mathcal{O}_E}(A)) \to A/\pi^{n+1}.$$

Since

$$a_i \equiv 0 \text{ for } i = 0, \ldots, n \mod \pi \implies w_n(a_0, \ldots, a_n) \equiv 0 \mod \pi^{n+1}$$

we get that the above map factors as

$$\begin{array}{ccc} W_{\mathcal{O}_E,n}(A) & \longrightarrow & A/\pi^{n+1} \\ & \searrow \quad \nearrow_{\theta_n} & \\ & W_{\mathcal{O}_E,n}(A/\pi) & \end{array}$$

and the collection of ring homomorphisms $(\theta_n)_n$ are compatible with the Frobenius Φ in the sense that the diagram

$$\begin{array}{ccc} W_{\mathcal{O}_E,n}(A/\pi) & \xrightarrow{\theta_{n+1}} & A/\pi^{n+1} \\ \downarrow{\scriptstyle \Phi} & & \downarrow \\ W_{\mathcal{O}_E,n-1}(A/\pi) & \xrightarrow{\theta_n} & A/\pi^n \end{array}$$

is commutative - this follows from the equality

$$w_{n+1}(X_0,\dots,X_{n+1}) = w_n(X_0^q,\dots,X_n^q) + \pi^{n+1}X_{n+1}$$

since $\Phi : W_{\mathcal{O}_E}(A/\pi) \to W_{\mathcal{O}_E}(A/\pi)$ is induced by the Frobenius on A/π by Proposition 2. Taking the inverse limit along this compatible system and using that A is π-adically compelte we get the desired Fontaine map

$$\theta : W_{\mathcal{O}_E}(A^\flat) \cong \varprojlim_n W_{\mathcal{O}_E,n}(A/\pi) \to A = \varprojlim_n A/\pi^n$$

where the first isomorphism follows by taking the diagonal along the indexing category of the following limit

$$W_{\mathcal{O}_E}(A^\flat) \cong \varprojlim_\Phi \varprojlim_n W_{\mathcal{O}_E,n}(A/\pi).$$

We have another description of θ, which follows from Corollary 7.6 in the notes mentioned above: recall the existence of the Teichmüller map

$$\begin{aligned} A^\flat = \varprojlim_{x\mapsto x^q} A/\pi &\longrightarrow A \\ a = (a_i)_i &\longmapsto a^\# := \lim_{n\to\infty} \widetilde{a}_i^{q^i} \end{aligned}$$

where $\widetilde{a}_i \in A$ is an arbitrary lift of $a_i \in A/\pi$. Then θ from above can also be described as

$$\begin{aligned} \theta : W_{\mathcal{O}_E}(A^\flat) &\longrightarrow A \\ \sum_{n=0}^{\infty} [a_n]\pi^n &\longmapsto \sum_{n=0}^{\infty} a_n^\# \pi^n; \end{aligned}$$

indeed, if we call θ' the map given above (which as of now is just a map of sets), then the composition

$$W_{\mathcal{O}_E}(A^\flat) \xrightarrow{\theta'} A \to A/\pi^{n+1}$$

is, by construction, constant on the cosets of the ideal $V^{n+1}(W_{\mathcal{O}_E}(A^\flat))$ and thus induces a map

$$\theta'_n : W_{\mathcal{O}_E,n}(A^\flat) \to A/\pi^{n+1}.$$

If $W_{\mathcal{O}_E,n}(p_n) : W_{\mathcal{O}_E,n}(A^\flat) \to W_{\mathcal{O}_E,n}(A/\pi)$ denotes the map on n-truncated Witt vectors induced by the projection $p_n : A^\flat = \varprojlim A/\pi \to A/\pi$ onto the n-th component of the projective limit, then we have a factorisation of θ'_n as

$$W_{\mathcal{O}_E,n}(A^\flat) \xrightarrow{W_{\mathcal{O}_E}(p_n)} W_{\mathcal{O}_E,n}(A/\pi) \xrightarrow{\theta_n} A/\pi^{n+1}$$

where the rightmost map is the *ring homomorphism* (!) θ_n from above

$$\sum_{i=0}^{n}[a_i]\pi^i \mapsto w_n(a_0,\dots,a_n) = a_0^{q^n} + \pi a_1^{q^{n-1}} + \dots + \pi^n a_n \in A/\pi^{n+1};$$

indeed, we have that

$$\theta'_n\left(\sum_{i=0}^{n}[a_i]\pi^i\right) := a_0^{\#} + a_1^{\#}\pi + \dots + a_n^{\#}\pi^n \in A/\pi^{n+1}$$

and since[1] $a^{\#} \equiv p_i(a)^{q^i}$ modulo π^{i+1} for any $a \in A^\flat$, this last expression equals

$$\sum_{i=0}^{n} p_n(a_i)^{q^{n-i}}\pi^i = w_n(a_0,\dots,a_n)$$

as desired. Since θ' is the projective limit of the maps θ_n along precisely the same projective system as θ, these two maps agree.

On the other hand, the unit is quite easy: given a perfect $\mathbf{F}_q$-algebra R, the $\mathcal{O}_E$-algebra $W_{\mathcal{O}_E}(R)$ satisfies $W_{\mathcal{O}_E}(R)/\pi \cong W_{\mathcal{O}_E,0}(R) \cong R$ so $W_{\mathcal{O}_E}(R)^\flat \cong \varprojlim R \cong R$ and thus it's natural to just take the identity functor as our unit[2]. Now it's a simple verification, which we omit, to draw the corresponding triangle diagrams and check that the natural transformations

$$\eta = \theta : W_{\mathcal{O}_E}((-)^\flat) \longrightarrow \mathrm{id},$$
$$\epsilon = 1 : \mathrm{id} \longrightarrow W_{\mathcal{O}_E}(-)^\flat$$

induce the desired adjunction. ■

At this point we have all the necessary tools to discuss the tilting equivalence[3]. Suppose R is a perfectoid $\mathbf{F}_p$-algebra, $R^+ \subset R$ a subring of integral elements and let $(R^\#, R^{\#+})$ be an untilt of the Huber pair (R, R^+), i.e. a perfectoid Huber pair equipped with an isomorphism of Huber pairs

$$\iota : (R^{\#\flat}, R^{\#+\flat}) \xrightarrow{\cong} (R, R^+),$$

which thus induces an isomorphism of p-typical Witt vectors $W(R^{\#+\flat}) \cong W(R^+)$ (the notation we use is $W(-) = W_{\mathbf{Z}_p}(-)$). Recall that $R^\#$ admits a pseudo-uniformiser $\varpi^\# \in R^{\#+}$ such that $\varpi^{\#p} \mid p$ and $\varpi^\#$ has a compatible system of p^n-th roots of unity $(\varpi^{\#1/p^i})_{i\geq 0}$ in $R^{\#+}$ thus defining an element $\varpi \in (R^{\#+})^\flat \cong R^+$ which is again a pseudo-uniformiser - this notation is consistent in the sense that by construction $(\varpi)^\# = \varpi^\#$ where $(-)^\# : (R^{\#+})^\flat \cong R \to R^{\#+}$ is the multiplicative map described in the proof of Proposition 6.

We study the Fontaine map θ for $R^{\#+}$, which in this situation identifies via ι with a ring homomorphism

$$W(R^+) \longrightarrow R^{\#+}.$$

Note that modulo $[\varpi] \in W(R^+)$, θ gives rise to the map

$$\sum_{n=0}^{\infty}[a_n]p^n \longmapsto a_0^{\#} \in R^{\#+}/\varpi^\#$$

[1] Explicitly put, for any $x = (x_i)_i \in \varprojlim A/\pi$ with lifts $\widetilde{x}_i \in A$ of x_i for each i, the sequence $\widetilde{x}_0, \widetilde{x}_1^q, \dots \in A$ stabilises modulo π^{i+1} at the term $x_i^{q^i}$, by the Key Lemma for Everything which we've implicitly been using throughout these notes:P

[2] Since the unit is an isomorphism, this implies in particular that the left adjoint $W_{\mathcal{O}_E}(-)$ is fully faithful.

[3] We now require some notions developed in the de Rham comparison course.

since $\varpi^\# \mid \varpi^{\#p} \mid p$. By Corollary 7.6 in [deRham] we have an isomorphism

$$R^+ \xrightarrow{\cong} \varprojlim R^{\#+}/p \xrightarrow{\cong} \varprojlim R^{\#+}/\varpi^\#$$

and since R is perfectoid it follows that $(-)^\# : R^+ \to R^{\#+}/\varpi^\#$ is surjective $\implies$ θ is surjective modulo $[\varpi]$. Since $W(R^+)$ is $[\varpi]$-adically complete and $R^{\#+}$ is $\varpi^\#$-adically complete, we can conclude by approximation that θ is also surjective, and thus the (arbitrary!) untilt $R^{\#+}$ is a quotient of the ring of Witt vectors $W(R^+)$.

The ideal $\ker\theta$ is of course subject to strong constraints (for a start, $W(R^+)/\ker\theta$ has to be perfectoid). We claim there exists an element $\xi \in W(R^+)$ of the form

$$\xi = p + [\varpi]\alpha \in W(R^+)$$

for some $\alpha \in W(R^+)$ such that $\theta(\xi) = 0$. For this, it'll be sufficient to construct $f \in R^+$ such that $\varpi \mid f$ and $f^\# \equiv p$ modulo $p\varpi^\#$: indeed, given f we can then express $p - f^\# \in R^{\#+}$ as

$$p - f^\# = p\varpi^\# \cdot x$$

for some $x \in R^{\#+}$, and since θ is surjective we can express $x = \theta(\alpha')$ allowing us to conclude that the element $p - ([f] - [\varpi]\cdot\alpha')$ is of the desired form and lies in $\ker\theta$.
To see that such an f exists, we have that $p/\varpi^\# \in R^{\#+}$ and because $(-)^\# : R^+ \to R^{\#+}/p$ is surjective - once again using that R is perfectoid - we can write

$$p/\varpi^\# \equiv \beta^\# \mod p$$

for some $\beta \in R^+ \implies f := \varpi\beta$ does the trick. To conclude our discussion, observe that this forces $\ker\theta$ to be generated by ξ as an ideal, since the induced surjective map

$$W(R^+)/\xi \twoheadrightarrow R^{\#+}$$

is an isomorphism modulo $[\varpi]$ - because

$$W(R^+)/(\xi, [\varpi]) = W(R^+)/(p, [\varpi]) \cong R^+/\varpi \cong R^{\#+}/\varpi^\#$$

(by Lemma 7.8 in [deRham]) - and thus $W(R^+)/\xi \to R^{\#+}$ must also be an isomorphism, once again by approximation.

Lastly, note that the whole construction goes through backwards as well: $W(R^+)/\xi$ is an untilt of R^+ regardless of the element ξ we choose, so long as it satisfies $(\xi) = (p + [\varpi]\alpha)$ for some α.

This motivates the following notion.

Definition 7. A *perfect prism* over $\mathcal{O}_E$ is a pair $(W_{\mathcal{O}_E}(R^+), I)$ where R^+ is a perfect $\mathbf{F}_q$-algebra, $I \subseteq W_{\mathcal{O}_E}(R^+)$ is a principal ideal generated by an element $d \in W_{\mathcal{O}_E}(R^+)$ satisfying

$$\frac{F(d) - d^q}{\varpi} \in W_{\mathcal{O}_E}(R^+)^\times.$$

Corollary 8 (The Tilting Equivalence)**.** *1. There's an equivalence of categories*

$$\{\textit{Perfectoid Huber pairs } (S, S^+)\} \xrightarrow{\cong} \{\textit{Perfect prisms over } \mathbf{Z}_p\}$$
$$(S, S^+) \mapsto (W(S^{+\flat}), \ker\theta).$$

2. Let R be a perfectoid ring. We have an equivalence of categories

$$\{\textit{Perfectoid Huber pairs over } (R, R^+)\} \xrightarrow{\cong} \left\{\textit{Perfectoid Huber pairs over } (R^\flat, R^{+\flat})\textit{-algebras}\right\}$$
$$S \mapsto S^\flat$$

with quasi-inverse given by $(B, B^+) \mapsto (B^\sharp[\pi^{-1}], B^\sharp := W(B) \otimes_{W(A^\flat)} A)$.

Proof. Part 1 follows directly from the premising discussion and the fact that $S = \mathrm{Frac}(S^+)$. As for part 2, we have that the category of perfectoid R-algebras S identifies with the category of perfect prisms $(W(B), I)$ over the perfect prism $(W(R), \ker \theta_R)$; the corresponding ring homomorphism

$$W(R) \to W(B)$$

is induced by a ring homomorphism $f : R \to B$ by W's fully faithfulness. If $I = (p + [\varpi]\alpha), \ker \theta_R = (p + [\varpi]\beta)$ (where we fix a pseudo-uniformiser $\varpi \in R$ and the corresponding pseudo-uniformiser image in B) then

$$p + [\varpi]\beta \mid f(p + [\varpi]\alpha) = p + [\varpi]f(\alpha).$$

If we express

$$p + [\varpi]f(\alpha) = (p + [\varpi]\beta) \cdot \left(\sum_{n \geq 0} [u_n] p^n \right) = \left(\sum_{n \geq 0} [u_n^p] p^{n+1} \right) + [\varpi]\beta \cdot \left(\sum_{n \geq 0} [u_i] p^i \right)$$

then modulo $[\varpi]$ we see that $u_0^p \equiv 1 \mod \varpi \implies u_0 \in B^\times$ since $\varpi \in B$ is topologically nilpotent $\implies \sum_n [u_n] p^n \in W(B)^\times$ and thus the extended ideal of $f(\ker \theta_R)$ in $W(B)$ agrees with I.

Essential surjectivity now follows from Proposition 6, and for fully faithfulness we see that a morphism of perfectoid R-algebras $S \to S'$ is identified with a ring homomorphism

$$W(S^\flat)/I \to W(S'^\flat)/I'$$

for perfect prisms $(W(S^\flat), I), (W(S'^\flat), I')$ which corresponds to a ring homomorphism $W(S^\flat) \to W(S'^\flat)$ so that I is mapped to a subset of I'; however, since I and I' are the extensions of ideals $\ker \theta_B$, this forces the extension of I in $W(S'^\flat)$ to equal I', and thus morphisms $S \to S'$ over R are in bijection with $S^\flat \to S'^\flat$ over $R^\flat$. ■

Remark 9. In a genuinely great post on Math Overflow motivating perfectoid spaces, it's discussed how almost mathematics can be used to show that the equivalence in Corollary 8 can be restristed to an equivalence of finite étale algebras, so that then if R and, consequently $R^\flat$ are fields in mixed/respectively equal characteristic, their absolute Galois groups are isomorphic. For instance, this yields an isomorphism of absolute Galois groups

$$G_{\mathbf{Q}_p(p^{1/p^\infty})^\wedge} \cong G_{\mathbf{F}_p(\!(t^{1/p^\infty})\!)}.$$

References

[Se] Jean Pierre Serre - *Corps Locaux.*

[Fa] Laurent Fargues, Jean-Marc Fontaine - *Courbes et fibrés vectoriels en théorie de Hodge p-adique.*

[Sch] Peter Scholze, Jared Weinstein - *Berkeley lectures on p-adic geometry.*

[deRham] Lecture notes from a course on the de Rham comparison taught by Johannes Anschütz.

[Ja] Lecture notes from a course on the Fargues Fontaine Curve taught by Johannes Anschütz.