Motivation

On veut donner une manière de passer de la caractéristique p à la caractéristique mixte [1] $(0, p)$. Idée du développement en base p, qui ne préserve pas du tout la structure d'anneau... (retenues).
Construire un foncteur :

$$W : \mathbf{Z}_p - \text{Alg} \longrightarrow \mathbf{Z}_p - \text{Alg}$$

(ou : sur $\mathcal{O}_L$, on parle alors de vecteurs de Witt ramifiés)
tel que $W(\mathbf{F}_{p^n}) = \mathbf{Z}_{p^n}$, l'anneau d'entiers de $\mathbf{Q}_{p^n}$, l'extension non ramifiée de corps résiduel $\mathbf{F}_{p^n}$ ($\mathbf{Z}_{p^n} = \mathbf{Z}_p[\mu_{p^n-1}]$).

1 Polynômes de Witt

Dans toute la suite : on fixe L une extension finie de $\mathbf{Q}_p$, $\mathcal{O}_L$ son anneau d'entiers, k_L son corps résiduel, et π une uniformisante de L.

Définition 1.1. Le n-ème polynôme de Witt est

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

On a les formules de récurrence :

$$\begin{aligned}\Phi_n(X_0, \ldots, X_n) &= X_0^{q^n} + \pi\Phi_{n-1}(X_1, \ldots, X_n) \\ &= \Phi_{n-1}(X_0^q, \ldots, X_{n-1}^q) + \pi^n X_n\end{aligned}$$

Soit B une $\mathcal{O}_L$-algèbre

Lemme 1.2. Si $b_0, \ldots, b_n$ et $c_0, \ldots c_n$ vérifient $b_i \equiv c_i \pmod{\pi^m B}$, alors :

$$\forall i \in [\![0, n]\!], \quad \Phi_i(b_0, \ldots, b_i) \equiv \Phi_i(c_0, \ldots, c_i) \pmod{\pi^{m+i} B}$$

De plus, la réciproque est vraie si $\pi \in B$ n'est pas un diviseur de 0.

Démonstration. Le sens direct se montre en remarquant :

$$b_i \equiv c_i \pmod{\pi^m B} \implies b_i^{q^n} \equiv c_i^{q^n} \pmod{\pi^{m+n} B}$$

et on en déduit le résultat en utilisant la deuxième formule de récurrence.
Le sens réciproque se prouve aussi en utilisant la deuxième formule de récurrence. □

Définition 1.3.

- On définit l'anneau "fantôme" $(B^{\mathbf{N}}, +, \times)$ comme l'anneau $B^{\mathbf{N}}$, où les opérations se font composantes par composante.
- Frobenius (fantôme) : $f_B(b_0, b_1, \ldots) = (b_1, b_2, \ldots)$.
- Verschiebung (=décalage) (fantôme) : $v_B(b_0, b_1, \ldots) = (0, \pi b_0, \pi b_1, \ldots)$.

On a $f_B v_B = \pi \in B^{\mathbf{N}}$.
On définit :

$$\Phi_B : \mathbf{b} = (b_0, b_1, \ldots) \in B^{\mathbf{N}} \longmapsto (\Phi_n(b_0, \ldots, b_n))_{n \in \mathbf{N}} \in B^{\mathbf{N}}$$

Exemple 1.4. Si $B = k_L$ (ou plus généralement, une k_L-algèbre), alors : $\Phi_{k_L}(\mathbf{b}) = (b_0, b_0^q, b_0^{q^2}, \ldots)$.

Lemme 1.5. Si π n'est pas un diviseur de zéro, Φ_B est injective. Si $\pi \in B^\times$, Φ_B est bijective.

1. i.e. : caractéristique 0 et caractéristique résiduelle p

Démonstration. $\Phi_B(\mathbf{b}) = \mathbf{u}$ s'écrit :

$$\begin{cases} b_0 & = & u_0 \\ \pi^n b_n + \Phi_{n-1}(b_0^q, \dots, b_{n-1}^q) & = & u_n \end{cases}$$

L'injectivité est alors une conséquence du lemme 1.2, sens réciproque.
Si π est inversible, on peut construire b_n par récurrence, et Φ_B est surjective. □

Proposition 1.6. Supposons qu'il existe $\sigma : B \to B$ un morphisme d'algèbres, avec :

$$\sigma(b) \equiv b^q \pmod{\pi B}$$

Alors :

$$B' := \mathrm{Im}(\Phi_B) = \{(u_n) \in B^{\mathbf{N}}, \quad \forall n,\, \sigma(u_{n-1}) \equiv u_n \pmod{\pi^n B}\}$$

Remarque 1.7. En particulier, B' ne dépend pas du choix de l'uniformisante π.

Démonstration. Il suffit de procéder par récurrence, et de résoudre l'équation :

$$u_n = \Phi_n(b_0, \dots, b_n) = \Phi_{n-1}(b_0^q, \dots, b_{n-1}^q) + \pi^n b_n$$

Si $u_{n-1} = \Phi_{n-1}(b_0, \dots, b_{n-1})$, cette équation a une solution $b_n \in B$ ssi :

$$u_n \equiv \Phi_{n-1}(b_0^q, \dots, b_{n-1}^q) \equiv \sigma(u_{n-1}) \pmod{\pi^n B}$$

□

Exemple 1.8. En prenant $B = \mathcal{O}_L$, et $\sigma(b) = b$ (qui vérifie l'hypothèse), on en déduit que B' s'identifie à $\mathcal{O}_L$, et on en déduit une application (qui n'est pas un morphisme) :

$$\Omega : \mathcal{O}_L \longrightarrow \mathcal{O}_L^{\mathbf{N}} \qquad \text{avec} \quad (\Phi_{\mathcal{O}_L} \circ \Omega)(\lambda) = (\lambda, \lambda, \dots)$$

On a par exemple $\Omega_0(\lambda) = \lambda$, $\Omega_1(\lambda) = \pi^{-1}(\lambda - \lambda^q)$, et des formules plus compliquées ensuite.
Si B est quelconque, en utilisant la flèche $\mathcal{O}_L \to B$, on en déduit une application $\Omega : \mathcal{O}_L \to B^{\mathbf{N}}$.

2 L'anneau des vecteurs de Witt

On veut définir un anneau $W(B)_L$ tel que $\Phi_B : W(B)_L \to B^{\mathbf{N}}$ soit un morphisme. Le problème est que Φ_B n'est pas injective, donc ce n'est pas bien défini. L'idée est de définir la loi par des 'équations universelles' (polynomiales sur $\mathcal{O}_L$ ici).

On applique donc la proposition 1.6 avec :

$$A = \mathcal{O}_L[X_0, Y_0, X_1, Y_1, \dots] \qquad \text{et} \qquad \sigma(X_i) = X_i^q,\, \sigma(Y_i) = Y_i^q$$

Corollaire 2.1. Il existe des éléments uniques $(S_n), (P_n), (I_n)$ et (F_n) de $A^{\mathbf{N}}$ tels que :

$$\Phi_A(\mathbf{S}) = \Phi_A(\mathbf{X}) + \Phi_A(\mathbf{Y})$$

$$\Phi_A(\mathbf{P}) = \Phi_A(\mathbf{X})\Phi_A(\mathbf{Y})$$

$$\Phi_A(\mathbf{I}) = -\Phi_A(\mathbf{X})$$

$$\Phi_A(\mathbf{F}) = f_A(\Phi_A(\mathbf{X}))$$

et on a de plus :

$$S_n, P_n \in \mathcal{O}_L[X_0, Y_0, \dots, X_n, Y_n]$$

$$I_n \in \mathcal{O}_L[X_0, \dots, X_n]$$

$$F_n \in \mathcal{O}_L[X_0, \dots, X_{n+1}]$$

Remarque 2.2. Si $p \neq 2$, on a en fait $I_n = -X_n$...

Exemple 2.3. S'amuser à calculer :

$$S_0 = X_0 + Y_0 \qquad ; \qquad S_1 = X_1 + Y_1 - \pi^{-1} \sum_{i=1}^{q-1} \binom{q}{i} X_0^i Y_0^{q-i}$$

$$P_0 = X_0 Y_0 \qquad ; \qquad P_1 = \pi X_1 Y_1 + X_0^q Y_1 + Y_0^q X_1$$

$$F_0 = X_0^q + \pi X_1 \qquad ; \quad F_1 = X_1^q + \pi X_2 - \sum_{i=0}^{q-1} \binom{q}{i} \pi^{q-i-1} X_0^{qi} X_1^{q-i}$$

Remarque 2.4. Si $L = \mathbf{Q}_p$, tous les polynômes sont à coefficients dans $\mathbf{Z}$.

Soit B une $\mathcal{O}_L$-algèbre.

Définition 2.5. On définit l'anneau des vecteurs de Witt $W(B)_L$, qui est l'ensemble $B^{\mathbf{N}}$, muni des opérations :

- Addition : $\mathbf{b} \boxplus \mathbf{c} = \mathbf{S}(\mathbf{b}, \mathbf{c})$
- Multiplication : $\mathbf{b} \boxdot \mathbf{c} = \mathbf{P}(\mathbf{b}, \mathbf{c})$

Proposition 2.6. (i) $(W(B)_L, \boxplus, \boxdot)$ est un anneau, de zéro $\mathbf{0} = (0, 0, \ldots)$ et de 1 l'élément $\mathbf{1} = (1, 0, 0, \ldots)$. L'inverse est donné par I.

(ii) $\Omega : \mathcal{O}_L \to W(B)_L$ est un morphisme d'anneaux, et munit ainsi $W(B)_L$ d'une structure de $\mathcal{O}_L$-algèbre.

(iii) $\Phi_B : W(B)_L \to B^{\mathbf{N}}$ est un morphisme de $\mathcal{O}_L$-algèbres ; en particulier $\Phi_{m,B} : W(B)_L \to B$ aussi.

Démonstration. (i) Vérifier que c'est un anneau n'est pas totalement évident : par exemple, on a bien :

$$\Phi_B((a \boxplus b) \boxplus c) = \Phi_B(a \boxplus (b \boxplus c))$$

mais Φ_B n'est pas toujours injective... L'idée pour palier ce problème est de poser $B_1 = \mathcal{O}_L[(X_b)_{b \in B}]$. On a alors un diagramme commutatif :

$$\begin{array}{ccc} W(B_1)^3 & \longrightarrow & W(B_1) \\ \downarrow & & \downarrow \\ W(B)^3 & \longrightarrow & W(B) \end{array}$$

la flèche en haut (et en bas) étant au choix, l'addition dans un ordre ou dans l'autre. Il suffit donc de montrer l'identité dans $W(B_1)_L$; mais celle-ci est évidente car Φ_{B_1} est injective.

C'est la seule difficulté de la preuve. □

On a fonctorialité en B :

Proposition 2.7. Soit $\rho : B_1 \to B_2$ un morphisme d'algèbres. Alors $W(\rho) = \rho^{\mathbf{N}}$ est un morphisme d'anneaux $W(B_1)_L \to W(B_2)_L$.

Démonstration. Comme ρ est un morphisme d'algèbres, il commute à l'action des polynômes de Witt, on a donc un diagramme :

$$\begin{array}{ccc} W(B_1)_L & \xrightarrow{\Phi_{B_1}} & B_1^{\mathbf{N}} \\ \downarrow{\scriptstyle W(\rho)} & & \downarrow{\scriptstyle \rho^{\mathbf{N}}} \\ W(B_2)_L & \xrightarrow{\Phi_{B_2}} & B_2^{\mathbf{N}} \end{array}$$

et on en déduit la preuve de la proposition, dans la même veine que précédemment (Φ_{B_2} n'est pas toujours injective...). □

Définition 2.8. Pour $\mathbf{b} \in W(B)_L$, on appelle $(b_0, b_1, \ldots)$ ses *vraies* composantes, et $(\Phi_0(\mathbf{b}), \Phi_1(\mathbf{b}), \ldots)$ ses composantes *fantômes*.

Attention : les composantes fantômes ne déterminent pas toujours le vecteur ! Par exemple, les composantes fantômes de $p \in W(\mathbf{F}_p)$ sont $(0, 0, \ldots)$.

3 Frobenius

On peut définir le Frobenius $F : \mathbf{b} \in W(B)_L \mapsto (F_n(\mathbf{b}))_{n\in\mathbf{N}}$ et le Verschiebung : $V : (b_0, b_1, \ldots) \in W(B)_L \mapsto (0, b_0, \ldots)$ (qui est donc le décalage des vraies composantes).

Proposition 3.1. (i) F est un endomorphisme de $\mathcal{O}_L$-algèbre.

(ii) V est un endomorphisme de $\mathcal{O}_L$-module (mais pas d'algèbre).

(iii) $FV = \pi$ (i.e. la multiplication par π élément de $W(B)_L$ (via Ω)).

(iv) $V(\mathbf{a} \boxdot F(\mathbf{b})) = V(\mathbf{a}) \boxdot \mathbf{b}$.

(v) $F(\mathbf{b}) \equiv \mathbf{b}^{\boxdot q} \pmod{\pi W(B)_L}$.

Démonstration. Il suffit de montrer qu'on a les diagrammes commutatifs suivants :

$$\begin{array}{ccc} W(B)_L & \xrightarrow{\Phi_B} & B^{\mathbf{N}} \\ \downarrow{\scriptstyle F} & & \downarrow{\scriptstyle f_B} \\ W(B)_L & \xrightarrow{\Phi_B} & B^{\mathbf{N}} \end{array} \qquad \begin{array}{ccc} W(B)_L & \xrightarrow{\Phi_B} & B^{\mathbf{N}} \\ \downarrow{\scriptstyle V} & & \downarrow{\scriptstyle v_B} \\ W(B)_L & \xrightarrow{\Phi_B} & B^{\mathbf{N}} \end{array}$$

et les preuves se font comme précédemment. □

Définition 3.2. On note $V_m(B)_L = \mathrm{Im}(V^m)$, constitué des vecteurs dont les m premières (vraies) coordonnées sont nulles [2].
On note $W_m(B)_L = W(B)_L/V_m(B)_L$, l'anneau des vecteurs de longueur m.

Définition 3.3. On appelle relèvement de Teichmüller l'application multiplicative :

$$\tau : \begin{array}{ccc} B & \longrightarrow & W(B)_L \\ b & \longmapsto & (b, 0, 0, \ldots) \end{array}$$

Lemme 3.4. $W_1(B)_L = B$ et $V_1(B)_L^m = \pi^{m-1}V_1(B)_L$.

Démonstration. Comme $S_0 = X_0 + Y_0$, l'application $B \to W_1(B)$ induite par τ est un morphisme d'anneaux, d'inverse $\Phi_0 : W_1(B) \to B$, ce qui prouve la première assertion.
On prouve la deuxième pour $m = 2$: si $\mathbf{a}, \mathbf{b} \in W(B)_L$, alors :

$$V(\mathbf{a}) \boxdot V(\mathbf{b}) = V(\mathbf{a} \boxdot F(V(\mathbf{b}))) = V(\mathbf{a} \boxdot \pi\mathbf{b}) = \pi V(\mathbf{a} \boxdot \mathbf{b})$$

□

4 Cas de la caractéristique positive

Dans les faits, on prendra B tel que $\pi 1_B = 0$, c'est à dire : B une k_L-algèbre.
B possède alors un Frobenius par la mise à la puissance q ; si c'est une bijection, on dit que B est parfaite.

Proposition 4.1. Soit B une k_L-algèbre.

2. cela implique que les m premières coordonnées fantômes sont nulles, mais la réciproque est fausse.

(i) $F(\mathbf{b}) = (b_n^q)_n$ et $FV = VF = \pi$.

(ii) $V_n \boxdot V_m \subset V_{n+m}$

(iii) $\pi^m W \subset V_1^m \subset \pi^{m-1} W$.

(iv) On a des isomorphismes d'algèbres :

$$\varprojlim W_m \leftarrow W \rightarrow \varprojlim W/V_1^m$$

Si de plus B est parfaite :

(v) $V_1^m = V_m = \pi^m W$.

(vi) π n'est pas un diviseur de 0 dans W.

(vii) Pour tout $\mathbf{b} \in W$, on a :

$$\mathbf{b} = \sum_{i=0}^{m-1} \pi^i \tau(b_i^{q^{-i}}) \pmod{\pi^m W}$$

Démonstration. Pour la (i), il faut regarder F_n modulo π. On en déduit $VF(\mathbf{b}) = V(\mathbf{1} \boxdot F(\mathbf{b})) = V(\mathbf{1}) \boxdot \mathbf{b}$.
Pour la (ii), on vérifie : $V^m(\mathbf{a}) \boxdot V^n(\mathbf{b}) = V^{n+m}(F^n(\mathbf{a}) \boxdot F^m(\mathbf{b}))$.
Pour la (iii), on a : $\pi W \subset V_1$ car $\pi = VF$.
Pour la (iv) : par définition de l'anneau $W(B)_L$, on a un isomorphisme : $W \simeq \varprojlim W_m$. On a :

$$\pi^m W = \{(0, \ldots, 0, b_m, b_{m+1}, \ldots), \quad b_n \in B^{q^m} \text{ si } n \geq m\}$$

Comme $\pi^m W \subset V_m$, pour avoir le deuxième isomorphisme, il suffit de montrer :

$$\bigcap_{j \geq m} (V_j \pmod{\pi^m W}) = \{\overline{0}\}$$

on voit que si $\mathbf{c}$ est dans l'intersection, alors en prenant $j = n+1$, $c_n \in B^{q^m}$.
Pour la (v), on a $\pi^m W = V^m F^m W = V^m W = V_m$ (on a utilisé que F était inversible à la 3e égalité).
Pour la (vi), on a $\pi = FV$ et F est inversible et V injective.
Enfin, $\pi^m = V^m(\mathbf{1})$ d'où l'on déduit l'écriture de (vii) [3]

□

Proposition 4.2. Si B est une extension de corps de k_L, alors :

(i) $W(B)_L$ est un anneau local intègre, d'idéal maximal V_1, de corps résiduel B. De plus la caractéristique de Frac(W) est nulle.

(ii) Si B est parfait, alors $W(B)_L$ est un anneau de valuation discrète complet, d'uniformisante π et pour tout $\mathbf{b} \in W$:

$$\mathbf{b} = \sum_{n=0}^{\infty} \pi^n \tau(b_n^{q^{-n}})$$

Proposition 4.3. Si $L_0/\mathbf{Q}_p$ partie non ramifiée de $L/\mathbf{Q}_p$, alors si B est parfaite :

$$\mathcal{O}_L \otimes_{\mathcal{O}_{L_0}} W(B) \simeq W(B)_L$$

et le frobenius à droite correspond à $id \otimes F^{f(L/\mathbf{Q}_p)}$ à gauche.

3. il y a ici une petite arnaque ; je renvoie au lemme 1.1.13 de Schneider pour l'astuce

5 Des calculs pour terminer

5.1 Les corps finis

On prend $L = \mathbf{Q}_p$ et $\pi = p$.
$\Omega(p)$ vu dans $W(\mathbf{F}_p)$ est égal à $(0, 1, 0, 0, \ldots)$ en vraies composantes, et à $(0, 0, 0, \ldots)$ en composante fantômes !

Proposition 5.1. $\Omega : \mathbf{Z}_p \to W(\mathbf{F}_p)$ est un isomorphisme.

Démonstration. On commence par montrer que c'est injectif : si $\Omega(\lambda) = 0$, alors $(\lambda 1_{\mathbf{F}_p}, \lambda 1_{\mathbf{F}_p}, \ldots)$ est nul dans $\mathbf{F}_p^n$ donc $\lambda \in p\mathbf{Z}_p$. On en déduit que $\lambda \in V_1$. En considérant le plus grand entier m tel que $\lambda \in V_m$, et en divisant par p^m, on a une contradiction. Donc Ω est injective, et on a même : $V_m = p^m W$.
Donc : $W(\mathbf{F}_p) = \varprojlim \mathbf{Z}/p^m\mathbf{Z} = \mathbf{Z}_p$.
On a quand même utilisé la proposition 4.1 et 4.2 (ii). □

Proposition 5.2. Si $a \in \mathbf{F}_p^\times$, $\tau(a)$ est l'unique racine de $X^{p-1} - 1$ congrue à a modulo p.

Démonstration. Comme τ est multiplicative, c'est bien une racine du polynôme. Et comme la réduction modulo p revient à prendre la première coordonnée, la congruence est vérifiée. □

En utilisant 4.2 ii), on voit que $W(\mathbf{F}_q)$ est l'extension de $\mathbf{Z}_p$ engendré par les racines de $X^{q-1} - 1$; ainsi $W(\mathbf{F}_q) = \mathbf{Z}_q$.
En passant à la limite sur q, on en déduit :

$$W(\overline{\mathbf{F}_p}) = \mathbf{Z}_p^{\mathrm{nr}}$$

où le terme de droite est l'anneau d'entiers du complété de l'extension maximale non ramifiée.

5.2 Un autre exemple

Soit k un corps parfait de caractéristique p. On prend $L = \mathbf{Q}_p$.
On a toujours une flèche :

$$\mathfrak{q} : W(k)[[T]] \longrightarrow W(k[[T]])$$

(qui envoie T sur $\tau(T)$ et $W(k)$ sur $W(k)$).
On peut construire une réciproque comme suit : étant donnée $f = \sum_n f_n T^n \in W(k)[[T]]$, on définit $Uf = \sum_n f_{np} T^n$. On pose alors :

$$\mathfrak{p} : f \longmapsto \lim_{h\to\infty} U^h (f^{p^h})^{F^{-h}}$$

(on a fait agir F sur les coefficients seulement). On montre que $\mathfrak{p}$ est bien définie, et ne dépend que de la classe de $f \pmod p$; autrement dit, $\mathfrak{p} : k[[T]] \to W(k)[[T]]$ est bien définie. On peut alors définir :

$$\mathfrak{p} : \begin{array}{ccc} W(k[[T]]) & \longrightarrow & W(k)[[T]] \\ (a_0, a_1, \ldots) & \longmapsto & \mathfrak{p}(a_0) + pU\mathfrak{p}(a_1)^{F^{-1}} + \ldots + p^n U^n \mathfrak{p}(a_n)^{F^{-n}} + \ldots \end{array}$$

Proposition 5.3. On a $\mathfrak{p} \circ \mathfrak{q} = \mathrm{id}_{W(k)[[T]]}$

Autrement dit, on peut voir les éléments de $W(k)[[T]]$ dans $W(k[[T]])$.

Question : $W(\mathbf{F}_p[T])$? $W(\mathbf{F}_p(t^{\frac{1}{p^\infty}}))$?