Introduction aux vecteurs de Witt

Léo et Fadhel

novembre 2019

La présentation suivie est celle qui a été présentée par Offer Gabber et Lorenzo Ramero dans leur monographie : *Foundations for almost ring theory.*

Dans ce qui suit tous les anneaux sont commutatifs, p est un premier fixé, $\underline{a} = (a_n)$ désigne une suite à coefficients dans A indicée par $\mathbb{N}$.

1 Motivation

Nous allons définir $W(A)$ l'anneau des vecteurs de Witt sur A. L'anneau des vecteurs de Witt est défini sur l'ensemble sous jacent $A^{\mathbb{N}}$, des suites à coefficients dans A. Les lois d'anneaux sur $W(A)$ ne sont pas les lois "composantes par composantes" mais des lois qui font intervenir un nombre premier p fixé au préalable. Pour donner une première idée voici la 1-ième composante de la somme d'éléments $\underline{X}$, $\underline{Y}$

$$S_1 = X_1 + Y_1 - \sum_{k=1}^{p-1} \frac{1}{p}\binom{p}{k} X_0^k Y_0^{p-k}$$

Le but de cette section est de motiver cette loi étrange *via* l'exemple de $\mathbb{Z}_p$. On suppose une connaissance préalable de l'anneau $\mathbb{Z}_p$ des entiers p-adiques.

L'idée sous-jacente à garder en tête pour comprendre la direction de cette partie est $\mathbb{Z}_p = W(\mathbb{F}_p)$.

On rappelle que $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ où le diagramme sous-entendu de la limite est le système de projections entre les différents quotients de $\mathbb{Z}$ par les puissances de p.

Dans $\mathbb{Z}_p$ on a le résultat suivant :

Lemme 1. *Tout élément de $x \in \mathbb{Z}_p$ s'écrit de façon unique comme une série :*

$$x = \sum_{n=0}^{\infty} x_n p^n$$

avec $(x_n) \in \{0, \dots, p-1\}^{\mathbb{N}}$

Ainsi une suite d'éléments dans $\{0, \dots, p-1\}$ définit uniquement un élément de $\mathbb{Z}_p$. L'approche qu'on va essayer de développer est la suivante : faire de l'algèbre sur $\mathbb{Z}_p$ en utilisant des suites à coefficients dans $\mathbb{F}_p$ et faire les calculs d'anneaux (addition, multiplication) dans $\mathbb{F}_p$ directement sur ces suites, sans passer par la représentation en série. Par exemple pour $(x_n), (y_n) \in \{0, \dots, p-1\}^{\mathbb{N}}$ on cherche à calculer l'unique suite $(s_n) \in \{0, \dots, p-1\}^{\mathbb{N}}$ telle que :

$$\sum x_n p^n + \sum y_n p^n = \sum s_n p^n$$

L'objectif est d'exprimer s_n en fonction de $x_0, \ldots, x_n, y_0, \ldots, y_n$ en une formule polynomiale close dans $\mathbb{F}_p$.

Avec de tels coefficients on n'arrive pas à cet objectif. En effet le calcul de (s_n) est ici l'addition en base p, simplement itérée à l'infini, avec retenue. Par exemple :

$$s_1 \equiv \epsilon + x_1 + y_1 \mod p\mathbb{Z}_p$$

Où ϵ vaut 0 ou 1 en fonction de si on a dû effectuer une retenue à l'étape précédente ou non. Cette prise en compte de la retenue est un obstacle pour exprimer les s_n comme voulu.

On va maintenant exprimer les éléments de $\mathbb{Z}_p$ en série "à coefficients dans $\mathbb{F}_p$" d'une autre manière, et on verra que ce nouveau contexte se prette beaucoup mieux au problème qu'on vient d'exprimer. On va utiliser le lemme suivant :

Lemme 2. *Si $x \equiv y \mod p^n\mathbb{Z}_p$ alors $x^{p^r} \equiv y^{p^r} \mod p^{n+r}\mathbb{Z}_p$*

Ce lemme se démontre en travaillant quelque peu avec les coefficients binomiaux ; nous reportons sa démonstration à plus tard car il va être traité dans une plus grande généralité.

Comme $x^p \equiv x \mod p\mathbb{Z}_p$ on en déduit que pour $\alpha \in \{0, \ldots, p-1\}$ on a $(\alpha^{p^n} | n \in \mathbb{N}) \in \mathbb{Z}_p$

On peut alors poser :

Définition. On pose $\tau : \mathbb{F}_p \to \mathbb{Z}_p$ qu'on appelle *l'application de Teichmüller* définie par

$$\tau(\alpha) = (\alpha, \alpha^p, \alpha^{p^2} \ldots) = (\alpha^{p^n} | n \in \mathbb{N})$$

Où l'on a pris implicitement un représentant de α dans $\mathbb{Z}$ qu'on a projetté adéquatement sur chaque composante. On appelle $\tau(\alpha)$ le *représentant de Teichmüller de α*.

On exhibe quelques propriétés de cette application :

Lemme 3. *τ est une section de la réduction modulo p*

1. *$\tau(\alpha)^p = \tau(\alpha)$*
2. *Tout élément de $x \in \mathbb{Z}_p$ s'écrit de manière unique :*

$$x = \sum_{n=0}^{\infty} \tau(x_n) p^n$$

avec $(x_n) \in \mathbb{F}_p^{\mathbb{N}}$

Démonstration. Comme la réduction modulo p dans $\mathbb{Z}_p$ se lit dans la première variable de la suite, le 1) est clair.

Pour le 2) : si $\alpha = 0$ on est bon. Sinon on a β avec $\alpha\beta \equiv 1 \mod p\mathbb{Z}_p$, et donc en utilisant un lemme qui précède : $\alpha^{p^n}\beta^{p^n} \equiv 1 \mod p^{n+1}$. Alors $\alpha^{p^n} \in (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$. Comme ce dernier groupe est de cardinal $p^n(p-1)$ on obtient le résultat.

Pour le 3) on construit la suite (x_n) par récurrence sur $n \in \mathbb{N}$: on veut montrer que pour tout $i \in \mathbb{N}$, il existe $x_i \in \mathbb{F}_p$ tel que : $p^{n+1} \mid x - \sum_{i=0}^{n} \tau(x_i)p^i$ pour tout $n \in \mathbb{N}$. On sait que $x = \sum_{n=0}^{\infty} b_n p^n$, pour $(b_n) \in \{0, \ldots p-1\}^{\mathbb{N}}$. On pose alors $x_0 = b_0$, où l'on a projeté b_0 dans $\mathbb{F}_p$. Puis pour l'étape d'induction on prend $n \geq 1$ et on suppose le résultat vrai pour $0, \ldots, n-1$. On a l'existence de $(c_n) \in \{0, \ldots, p-1\}^{\mathbb{N}}$ telle que : $x - \sum_{i=0}^{n-1} \tau(x_i)p^i = \sum_{k=n}^{\infty} c_k p^k$ comme $p^n \mid x - \sum_{i=0}^{n-1} \tau(x_i)p^i$ par hypothèse de récurrence. On pose alors $x_n = c_n$ avec projection implicite. L'unicité vient de l'unicité du développement "standard" qui intervient à chaque étape de la récurrence.

□

Revenons à notre problème énoncé plus haut ; cette fois on va essayer étant donnée deux suites $(x_n), (y_n) \in \mathbb{F}_p^{\mathbb{N}}$ de trouver la suite (s_n) telle que :

$$\sum \tau(x_n)p^n + \sum \tau(y_n)p^n = \sum \tau(s_n)p^n$$

on veut donc exprimer les s_n en fonction des $x_0, .., x_n, y_0, \ldots, y_n$ par une formule polynomiale dans $\mathbb{F}_p$.

On obtient en réduisant le système modulo les puissance successives de p :

$$\begin{aligned} \tau(x_0) + \tau(y_0) &\equiv \tau(s_0) \mod p\mathbb{Z}_p \\ \tau(x_0) + \tau(x_1)p + \tau(y_0) + \tau(y_1)p &\equiv \tau(s_0) + \tau(s_1)p \mod p^2\mathbb{Z}_p \\ &\vdots \end{aligned}$$

La première ligne est équivalente à $s_0 = x_0 + y_0$ en vertu du point 1) du lemme qu'on vient de démontrer. Pour résoudre la deuxième équation (et la n-ième plus généralement), la stratégie est de mettre en évidence p (plus gén. p^{n-1}) pour se ramener modulo p et ainsi pouvoir passer des coefficients de Teichmüller à $\mathbb{F}_p$. Pour le faire on applique l'idée suivante pour transformer ces équations : on utilise la propriété $\tau(\alpha)^p = \tau(\alpha)$ pour les coefficients de Teichmüller pour ré-écrire :

$$\tau(x_0)^p + \tau(x_1)p + \tau(y_0)^p + \tau(y_1)p \equiv \tau(s_0)^p + \tau(s_1)p \mod p^2\mathbb{Z}_p$$

Maintenant comme :

$$\tau(x_0) + \tau(y_0) \equiv \tau(s_0) \mod p\mathbb{Z}_p$$

On a par un lemme énoncé plus haut :

$$\tau(s_0)^p \equiv (\tau(x_0) + \tau(y_0))^p = \tau(x_0)^p + \tau(y_0)^p + p\sum_{k=1}^{p-1} \frac{1}{p}\binom{p}{k}\tau(x_0)^k\tau(y_0)^{p-k} \mod p^2\mathbb{Z}_p$$

Ainsi en injectant cette expression pour $\tau(s_0)^p$ dans l'équation plus haut, en simplifiant les termes qui apparaissent des deux côtés de l'équation et en se ramenant modulo p, puis à $\mathbb{F}_p$ on obtient :

$$s_1 = x_1 + y_1 - \sum_{k=1}^{p-1} \frac{1}{p}\binom{p}{k} x_0^k y_0^{p-k}$$

On a donc obtenu une formule polynomiale pour s_1 en fonction de $x_0, \ldots, x_n, y_0, \ldots, y_n$. La même idée de transformation des équations va fonctionner pour trouver les s_n pour n quelconque ; c'est à dire transformer les équations en :

$$\sum_{i=0}^{n} \tau(s_i)^{p^{n-i}} p^i \equiv \sum_{i=0}^{n} \tau(x_i)^{p^{n-i}} p^i + \sum_{i=0}^{n} \tau(y_i)^{p^{n-i}} p^i \mod p^{n+1}\mathbb{Z}_p$$

En fait, après avoir rajouté ces puissances aux coefficients de Teichmüller, les manipulations qu'on a effectué pour trouver s_1 sont surprenamment indépendantes du fait qu'on travaillait

dans $\mathbb{Z}_p$ et on aurait pu résoudre ce système avec des variables et des inconnues. On montre cela dans ce qui suit : on prend des variables $(X_n), (Y_n)$ et on affirme qu'on peut répondre à notre problème en résolvant le système suivant d'inconnues (S_n) :

$$\begin{aligned} S_0 &= X_0 + Y_0 \\ S_0^p + S_1 p &= X_0^p + X_1 p + Y_0^p + Y_1 p \\ &\vdots \end{aligned}$$

Pour écrire ce système on note désormais $\omega_n(X_0, \ldots, X_n) = \sum_{i=0}^n X_i^{p^{n-i}} p^i$; on ré-écrit donc pour $n \in \mathbb{N}$:

$$\omega_n(S_0, \ldots, S_n) = \omega_n(X_0, \ldots, X_n) + \omega_n(Y_0, \ldots, Y_n) \tag{1}$$

Un calcul immédiat donne que les S_0,S_1 correspondent bien aux , s_0, s_1 trouvés plus haut dans $\mathbb{F}_p$ à une évaluation près.

Introduire les vecteurs de Witt permet de résoudre le système général pour n quelconque.

La somme du n-ième terme sur les vecteurs de Witt entre deux éléments $(a_n), (b_n)$ sera donnée par $S_n(a_0, \ldots, a_n, b_0, \ldots, b_n)$. Un produit sera construit de manière analogue, qu'on aurait pu découvrir également en partant de la multiplication de séries dans $\mathbb{Z}_p$.

Clôturons notre problème d'introduction ; si on suppose l'existence des S_n qui résolvent (1), alors on trouve une formule close pour les s_n : $s_n = S_n(x_0, \ldots, x_n, y_0, \ldots, y_n)$. En effet si on pose cela on trouve :

$$\tau(s_i) \equiv S_i(\tau(x_0), \ldots, \tau(y_i)) \mod p\mathbb{Z}_p$$

Donc en utilisant encore une fois le lemme cité plus haut :

$$\tau(s_i)^{p^{n-i}} \equiv S_i(\tau(x_0), \ldots, \tau(y_i))^{p^{n-i}} \mod p^{n+1-i}\mathbb{Z}_p$$

Donc :

$$\tau(s_i)^{p^{n-i}} p^i \equiv S_i(\tau(x_0), \ldots, \tau(y_i))^{p^{n-i}} p^i \mod p^{n+1}\mathbb{Z}_p$$

Et donc on a bien en utilisant (1) :

$$\sum_{i=0}^n \tau(s_i)^{p^{n-i}} p^i \equiv \sum_{i=0}^n S_i(\tau(x_0), \ldots, \tau(y_i))^{p^{n-i}} p^i = \sum_{i=0}^n \tau(x_i)^{p^{n-i}} p^i + \sum_{i=0}^n \tau(y_i)^{p^{n-i}} p^i \mod p^{n+1}\mathbb{Z}_p$$

Ce qui montre qu'on aurait la bonne formule pour les s_n. Une fois les vecteurs de Witt construits on aura alors atteint notre objectif de faire de l'algèbre sur $\mathbb{Z}_p$ en faisant les calculs directement sur les suites à coefficients dans $\mathbb{F}_p$ qui représentent les éléments de $\mathbb{Z}_p$. La somme et le produit des vecteurs de Witt sont les opérations à mettre sur les suites à coefficient dans F_p pour que cet anneau corresponde à $\mathbb{Z}_p$ via l'identification d'une suite à la série en les coefficients de Teichmüller. On aura alors $W(\mathbb{F}_p) = \mathbb{Z}_p$ par :

$$\begin{aligned} W(\mathbb{F}_p) &\rightleftarrows \mathbb{Z}_p \\ (x_0, x_1, \ldots) &\rightleftarrows \sum \tau(x_n) p^n \end{aligned}$$

Remarque. On voit que le système (1) a des solutions uniques dans $\mathbb{Q}[X_i, Y_i]$. Witt a montré que ces polynômes sont en réalité dans $\mathbb{Z}[X_i, Y_i]$. Nous allons le faire également dans ce qui suit par une méthode qui évite des calculs fastidieux.

2 Construction de $W(A)$

2.1 Polynômes de Witt et lemme de Dwork

La discussion ci dessus nous mène à la définition suivante des polynômes de Witt :

Définition. Le n-ième polynôme de Witt noté ω_n est donné par

$$\omega_n(X_0, \dots, X_n) = \sum_{i=0}^{n} p^i X_i^{p^{n-i}} \in \mathbb{Z}[X_0, \dots X_n]$$

il sera utile d'observer les relations de récurrence suivantes

$$\omega_{n+1}(X_0, \dots, X_{n+1}) = \omega_n(X_0^p, \dots, X_n^p) + p^{n+1} X_{n+1} = X_0^{p^{n+1}} + p\omega_n(X_1, \dots, X_{n+1})$$

À l'aide des ω_n, on définit la n-ième *composante fantôme* de $\underline{a} := (a_n \mid n \in \mathbb{N}) \in A^{\mathbb{N}}$

$$\omega_n(\underline{a}) := \omega_n(a_0, \dots, a_n)$$

et *l'application fantôme* $\omega_A : A^{\mathbb{N}} \to A^{\mathbb{N}}$

$$\omega_A(\underline{a}) := (\omega_n(\underline{a}) \mid n \in \mathbb{N}) \in A^{\mathbb{N}}$$

Le but dans la suite est de définir une structure d'anneau $(A^{\mathbb{N}}, \hat{+}, \hat{\cdot})$ telle que :

$$\omega_A(\underline{a} \hat{+} \underline{b}) = \omega_A(\underline{a}) + \omega_A(\underline{b})$$
$$\omega_A(\underline{a} \hat{\cdot} \underline{b}) = \omega_A(\underline{a})\omega_A(\underline{b})$$

C'est pour cela qu'on appelle ces composantes "fantômes". Le "vrai" anneau qui va compter pour nous est $(\hat{+}, \hat{\cdot})$. L'application ω_A nous permet uniquement comprendre ce qui s'y passe et $\omega_A(\underline{a})$ ne vit pas dans la structure qui va nous intéresser mais en est seulement une ombre.

Il est bon de remarquer que pour trouver de tels $(\hat{+}, \hat{\cdot})$, si ω_A est injective, d'image un sous-anneau de $A^{\mathbb{N}}$, on a ce qu'on veut par simple transport de structure.

Le lemme suivant est un lemme technique qui permet de montrer le lemme principal de cette section : le lemme de Dwork.

Lemme 4. *(Lemme technique)*
Soit $J_n, n \in \mathbb{N}$ une suite d'idéaux d'un anneau A et vérifiant

$$pJ_n + J_n^p \subset J_{n+1} \subset J_n$$

alors

1. *si $x \equiv y : \mod J_0$ alors on a pour tout $n \in \mathbb{N} : x^{p^n} \equiv y^{p^n} \mod J_n$*
2. *si pour $m \in \mathbb{N}$ on a $a_i \equiv b_i \mod J_m$ pour tout $i \in \{0, \dots, n\}$, alors pour tout $j \in \{0, \dots, n\}$ on a $\omega_j(\underline{a}) \equiv \omega_j(\underline{b}) \mod J_{m+j}$*

Démonstration. 1. La première assertion découle d'un raisonnement par récurrence sur m. Pour cela il suffit de montrer que si $x \equiv y \mod J_m$ alors $x^p \equiv y^p \mod J_{m+1}$ ce qui s'obtient de la façon suivante :

$$\begin{aligned} x^p - y^p &= (x-y)^p - \sum_{k=1}^{p-1} \binom{p}{k} x^k (-y)^{p-k} \\ &= (x-y)^p - \sum_{\substack{1 \le k \le l \le p-1 \\ k+l=p}} \binom{p}{k} x^k (-y)^l + \binom{p}{l} x^l (-y)^k \end{aligned}$$

où on a rassemblé ensembles les termes d'indices symétriques par rapport à $\frac{p}{2}$.
Maintenant on remarque que p divise $\binom{p}{k} = \binom{p}{l}$ et que $x^k(-y)^l - x^l(-y)^k$ se factorise par $x - y$ (pourvu que $p \neq 2$)). Moyennant l'hypothèse de récurrence on obtient que $\binom{p}{k}x^k(-y)^l + \binom{p}{l}x^l(-y)^k \in pJ_m$ et $(x-y)^p \in J_m^p$ ce qui nous permet de conclure vu la propriété d'inclusion $pJ_m + J_m^p \subset J_{m+1}$
Le cas $p = 2$ se traite par une inspection directe.

2. Comme $a_i \equiv b_i \mod J_m$ il s'en suit par 1. que $a_i^{p^{j-i}} \equiv b_i^{p^{j-i}} \mod J_{m+j-i}$ puis que $p^i a_i^{p^{j-i}} \equiv p^i b_i^{p^{j-i}} \mod J_{m+j}$. En prenant la somme pour $i \in \{0...j\}$ on obtient le résultat

□

Lemme 5. *(Dwork)*

1. *Si dans A, p n'est pas un diviseur de zéro (resp. inversible) alors ω_A est injective (resp. bijective).*
2. *si A admet un endomorphisme d'anneau ϕ tel que pour tout $x \in A$, $\phi(x) \equiv x^p \mod pA$ (et on dit dans ce cas que ϕ est un relèvement du Frobenius) alors $Ima\omega_A$ est donné par*

$$\operatorname{Im}\omega_A = \{\underline{b} \in A^{\mathbb{N}} \mid b_{n+1} \equiv \phi(b_n) \mod p^{n+1} \text{ pour tout } n \in \mathbb{N}\}$$

en particulier $\operatorname{Im}\omega_A$ est un sous anneau de $A^{\mathbb{N}}$ (muni des opérations du produit direct)

Démonstration. 1. On prouve l'injectivité sous l'hypothèse que p n'est pas diviseur de 0.
Supposons que $\omega_A(\underline{a}) = \omega_A(\underline{b})$. Par récurrence, on montre que $\underline{a} = \underline{b}$.
$\omega_0(a_0) = \omega_0(b_0)$ donne $a_0 = b_0$. supposons que $\forall i \in \{0 \dots n-1\}, a_i = b_i$, l'égalité de la composante fantôme d'indice n donne : $p^n a_n = p^n b_n$. par la régularité de p on conclut. (le cas p inversible se traite de façon similaire.)

2. On montre la double inclusion :
   — On montre que $\omega_{n+1}(x_0, \dots, x_{n+1}) \equiv \phi(\omega_n(x_0, \dots, x_n)) \mod p^{n+1}$. D'abord, comme ϕ est un morphisme, on a $\phi(\omega_n(x_0, \dots, x_n)) = \omega_n(\phi(x_0), \dots, \phi(x_n))$, maintenant on a que pour tout $i \in \{0 \dots n\}$ $\phi(x_i) \equiv x_i^p \mod p$, d'où par le point 2. du lemme précédent $\omega_n(\phi(x_0), \dots, \phi(x_n)) \equiv \omega_n(x_0^p, \dots, x_n^p) \mod p^{n+1}$. D'autre part la relation de récurrence pour ω_n donne : $\omega_{n+1}(x_0, \dots, x_{n+1}) = \omega_n(x_0^p, \dots, x_n^p) + p^{n+1}x_{n+1} \equiv \omega_n(x_0^p, \dots, x_n^p) \mod p^{n+1}$ ce qui conclut ce point.
   — Supposons que $\underline{b} \in A^{\mathbb{N}}$ vérifie $b_{n+1} \equiv \phi(b_n) \mod p^{n+1}$ pour tout $n \in \mathbb{N}$ nous allons construire par récurrence une suite $(x_n \mid n \in \mathbb{N}) \in A^{\mathbb{N}}$ telle que $\omega_A(\underline{x}) = \underline{b}$. On prend $x_0 = b_0$ et supposons qu'on a construit $x_0, \dots, x_n$ tels que $\omega_i(x_0, \dots, x_i) = b_i$ pour tout $i \in \{0, \dots, n\}$. Maintenant, x_{n+1} est donné par $p^{n+1}x_{n+1} = b_{n+1} - \omega_n(x_0^p, \dots, x_n^p)$ or $b_{n+1} \equiv \phi(b_n) = \phi(\omega(x_0, \dots, x_n)) \equiv \phi(x_0^p, \dots, x_n^p) \mod p^{n+1}$.(ceci s'obtient par l'application du lemme précédent) D'où $b_{n+1} \equiv \omega_n(x_0^p, \dots, x_n^p) \mod p^{n+1}$ et donc $x_{n+1} = \frac{b_{n+1} - \omega_n(x_0^p, \dots, x_n^p)}{p^{n+1}}$ existe.

□

2.2 Vecteurs de Witt

On prend $A = \mathbb{Z}[X_n, Y_n \mid n \in \mathbb{N}]$. Cet anneau satisfait les hypothèses du lemme de Dwork : il admet un relèvement du Frobenius (c'est l'unique morphisme d'anneau ϕ tel que $\phi(X) = X^p$ pour $X \in \{X_n, Y_n \mid n \in \mathbb{N}\}$), et p n'est pas diviseur de zéro dans cet anneau.

Ainsi $\omega_A : A^{\mathbb{N}} \to \operatorname{Im}\omega_A$ est une bijection. Comme $\operatorname{Im}\omega_A$ est un anneau (sous-anneau de l'anneau produit par Dwork) par transport de structure on a une structure d'anneau sur $A^{\mathbb{N}}$ héritée par ω_A. On dénote désormais par $(W(A), \hat{+}, \hat{\cdot})$ cet anneau.

Le but est de généraliser cette construction à un anneau à quelconque. On note $\underline{X} := (X_0, X_1, \ldots)$ et $\underline{Y} := (Y_0, Y_1, \ldots)$ des éléments de $W(A)$. On note $\underline{S}$, $\underline{P}$ et $\underline{I}$ les éléments tels que :

$$\underline{S} = \underline{X} \hat{+} \underline{Y}$$
$$\underline{P} = \underline{X} \hat{\cdot} \underline{Y}$$
$$\underline{I} = -\underline{X}$$

Par construction de cet anneau on a :

$$\omega_n(S_0, \ldots, S_n) = \omega_n(X_0, \ldots, X_n) + \omega_n(Y_0, \ldots, Y_n) \tag{2}$$
$$\omega_n(P_0, \ldots, P_n) = \omega_n(X_0, \ldots, X_n)\omega_n(Y_0, \ldots, Y_n) \tag{3}$$
$$\omega_n(I_0, \ldots, I_n) = -\omega_n(X_0, \ldots, X_n) \tag{4}$$

Ainsi $I_n \in \mathbb{Z}[X_0, \ldots X_n]$ et $P_n, S_n \in \mathbb{Z}[X_0, \ldots, X_n, Y_0 \ldots, Y_n]$.

Remarque. Si on pose :

$$S_A : A^{\mathbb{N}} \times A^{\mathbb{N}} \to A^{\mathbb{N}}$$
$$S_A(\underline{a}, \underline{b}) = (S_n(a_0, \ldots, a_n, b_0, \ldots, b_n) \mid n \in \mathbb{N})$$

et

$$P_A : A^{\mathbb{N}} \times A^{\mathbb{N}} \to A^{\mathbb{N}}$$
$$P_A(\underline{a}, \underline{b}) = (P_n(a_0, \ldots, a_n, b_0, \ldots, b_n) \mid n \in \mathbb{N})$$

ainsi que :

$$I_A : A^{\mathbb{N}} \to A^{\mathbb{N}}$$
$$I_A(\underline{a}) = (I_n(a_0, \ldots, a_n) \mid n \in \mathbb{N})$$

alors si $\psi : A \to B$ est un morphisme d'anneau on a :

$$\psi^{\mathbb{N}}(S_A) = S_B(\psi^{\mathbb{N}}, \psi^{\mathbb{N}}) \quad \psi^{\mathbb{N}}(P_A) = P_B(\psi^{\mathbb{N}}, \psi^{\mathbb{N}}) \quad \psi^{\mathbb{N}}(I_A) = I_B(\psi^{\mathbb{N}})$$

Théorème 1. *Soit A un anneau. Les applications S_A,I_A et P_A définissent une structure d'anneau sur $A^{\mathbb{N}}$, avec S_A la somme, I_A l'inverse additif, et P_A le produit. L'élement neutre additif est $\hat{0} = (0, 0, \ldots)$ est l'élément neutre multiplicatif est $\hat{1} = (1, 0, 0, \ldots)$. De plus on a :*

$$\omega_A(S_A(\underline{a}, \underline{b})) = \omega_A(\underline{a}) + \omega_A(\underline{b})$$
$$\omega_A(P_A(\underline{a}, \underline{b})) = \omega_A(\underline{a})\omega_A(\underline{b})$$
$$\omega_A(I_A(\underline{a}) = -\omega_A(\underline{a})$$

Démonstration. Le dernier point suit de des équations (2) et (3) ci-dessus après évaluations des polynômes dans chaque composante.

On montre la distributivité ; les autres propriétés d'anneaux se montrent similairement. L'idée est de montrer dans le cas "universel" $A = \mathbb{Z}[X_i, Y_i, Z_i]$ où ω_A est injective car c'est un anneau sans p-torsion (p régulier), pour les éléments $\underline{X} := (X_0, X_1, \ldots)$, $\underline{Y} := (Y_0, Y_1, \ldots)$ et $\underline{Z} := (Z_0, Z_1, \ldots)$. En utilisant le dernier point du théorème déjà démontré et en utilisant la structure d'anneau présente dans $A^{\mathbb{N}}$ une fois qu'on appliqué ω_A on obtient :

$$\omega_A(P_A(\underline{Z}, S_A(\underline{X}, \underline{Y}))) = \omega_A(\underline{Z})(\omega_A(\underline{X}) + \omega_A(\underline{Y}))$$
$$= \omega_A(\underline{Z})\omega_A(\underline{X}) + \omega_A(\underline{Z})\omega_A(\underline{Y}) = \omega_A(P_A(\underline{Z}, \underline{X})) + \omega_A(P_A(\underline{Z}, \underline{Y}))$$
$$= \omega_A S_A[P_A(\underline{Z}, \underline{X}), P_A(\underline{Z}, \underline{Y})]$$

C'est à dire en utilisant l'injectivité de ω_A :

$$S_A[P_A(\underline{Z},\underline{X}),P_A(\underline{Z},\underline{Y})] = P_A(\underline{Z},S_A(\underline{X},\underline{Y}))$$

Pour avoir l'assertion dans un anneau quelconque B et des éléments $\underline{a},\underline{b},\underline{c}$ on pose $\psi : A \to B$, définie par $X_i \mapsto a_i$, $Y_i \mapsto b_i$, $Z_i \mapsto c_i$, et en utilisant le dernier point de la remarque précédente on obtient l'associativité dans un anneau quelconque. $\square$

Définition. Soit A un anneau. Alors la structure d'anneau $(A^{\mathbb{N}},\hat{+},\hat{\cdot})$ donnée par :

$$\underline{a}\hat{+}\underline{b} := S_A(\underline{a},\underline{b}) = (S_n(a_0,\ldots,a_n,b_0,\ldots,b_n) \mid n \in \mathbb{N})$$
$$\underline{a}\hat{\cdot}\underline{b} := P_A(\underline{a},\underline{b}) = (P_n(a_0,\ldots,a_n,b_0,\ldots,b_n) \mid n \in \mathbb{N})$$

est appelée *Anneau des vecteurs de Witt de A* et est notée $W(A)$. On appelle un élément $\underline{a} \in W(A)$ un vecteur de Witt. $(0,0\ldots)$ et $(1,0,\ldots)$ sont neutres pour l'addition et la multiplication respectivement.

Remarques.

1. L'application fantôme ω_A est donc un morphisme d'anneau de $W(A)$ vers $A^{\mathbb{N}}$.
2. La construction des vecteurs de Witt est fonctorielle :

$$W : \mathbf{Ann} \to \mathbf{Ann}$$
$$A \mapsto W(A)$$
$$\phi : A \to B \mapsto W(\phi : \underline{a} \mapsto (\phi(a_n) \mid n \in \mathbb{N})$$

3. Si $\phi : A \to B$ est un morphisme d'anneau alors si on note $\phi^{\mathbb{N}}$ l'application associée au foncteur produit dénombrable sur les anneaux on obtient :

$$\phi^{\mathbb{N}}\omega_A = \omega_B W(\phi)$$

   Ainsi ω est une transformation naturelle du foncteur W vers le foncteur produit dénombrable sur les anneaux.
4. La première définition des vecteurs pour le cas $A = \mathbb{Z}[X_,Y_n \mid n \in \mathbb{N}]$ qu'on a faite en début de paragraphe coïncide avec celle qui précède.

3 Les applications Frobenius et Verschiebung, l'application de Teichmüller et le cas de $\mathbb{F}_p$-algèbres

3.1 Frobenius et Verschiebung

Sur $W(A)$ On définit applications F_A et V_A qui vérifient certaines propriétés intéressantes. Notamment F_A est un relèvement de l'application de mise à la puissance p sur $W(A)/pW(A)$.

Dans $A = \mathbb{Z}[X_i]$ en utilisant le lemme de Dwork on remarque que : $(\omega_{n+1}(X_0,\ldots,X_{n+1}) \mid n \in \mathbb{N}) \in \operatorname{Im}\omega_A$. Alors on a l'existence de $F_n \in \mathbb{Z}[X_0,\ldots,X_{n+1}]$ tel que :

$$\omega_n(F_0,\ldots,F_n) = \omega_{n+1}(X_0,\ldots,X_{n+1})$$

Définition. F_A, V_A
On définit $F_A : W(A) \to W(A)$ l'application suivante

$$F_A(\underline{a}) = (F_n(a_0,\ldots,a_{n+1}) \mid n \in \mathbb{N})$$

et $V_A : W(A) \to W(A)$

$$V_A(\underline{a}) = (0, a_0, a_1, a_2, \ldots)$$

On appelle F_A *l'application de Frobenius sur* $W(A)$ et V_A *l'application de Verschiebung ou de décalage sur* $W(A)$.

On définit également ce qu'on va appeler les analogues fantômes de F et de V qu'on va noter f et v. Ces applications vont nous permettre de montrer les propriétés de F et de V car comme on va le voir, les démonstrations des propriétés élémentaires se démontrent toute de la même façon : en passant aux composantes fantômes dans le cas de $A = \mathbb{Z}[X_i, Y_i]$ où ω_A est injectif puis en évaluant.

Définition. Analogues fantômes des applications F et V
On pose $f_A : A^{\mathbb{N}} \to A^{\mathbb{N}}$ le morphisme d'anneau suivant :

$$f_A(\underline{a}) = (a_1, a_2, a_3, \ldots)$$

qu'on appelle *analogue fantôme de* F_A. On définit aussi le morphisme de groupe additif $v_A : A^{\mathbb{N}} \to A^{\mathbb{N}}$:

$$v_A(\underline{a}) = (0, pa_0, pa_1, pa_2, \ldots)$$

qu'on appelle *l'analogue fantôme de* V_A.

On montre maintenant que ces appelations sont justifiées.

Lemme 6. *1.* $\omega_A F_A = f_A \omega_A$

2. $\omega_A V_A = v_A \omega_A$

Démonstration. Ce sont des vérifications directes. Le 1) se montre en utilisant la propriété des polynômes F_n en passant aux composantes fantômes :

$$\omega_A F_A(\underline{a}) = (\omega_n(F_0(a_0, a_1), \ldots, F_n(a_0, \ldots, a_{n+1})) \mid n \in \mathbb{N}) = (\omega_{n+1}(a_0, \ldots, a_{n+1}) \mid n \in \mathbb{N}) = f_A \omega_A(\underline{a})$$

Le 2) utilise une des relations de récurrence mise en évidence sur les ω_n :

$$\omega_A V_A(\underline{a}) = (0, \omega_n(0, a_0, \ldots, a_{n-1}) \mid n \geq 1) = (0, p\omega_{n-1}(a_0, \ldots, a_{n-1}) \mid n \geq 1) = v_A \omega_A(\underline{a})$$

□

Remarque. Pour tous anneaux A, B et morphisme d'anneaux $\psi : A \to B$ on a :

$$W(\psi) F_A = F_B W(\psi)$$
$$W(\psi) V_A = V_B W(\psi)$$

Cela se montre par vérification directe car les morphismes d'anneaux commute aux polynômes.

Lemme 7. *1. L'application* F_A *est un morphisme d'anneau et l'application* V_A *est un morphisme de groupe additif.*

2. On a les identités suivantes :

$$F_A V_A = p \hat{\cdot} \mathrm{Id}_{W(A)}$$
$$V_A(\underline{a} \hat{\cdot} F_A(\underline{b})) = V_A(\underline{a}) \hat{\cdot} \underline{b}$$

pour tous $\underline{a}, \underline{b} \in W(A)$

Démonstration. Pour le 1) on utilise le lemme précédent et on travaille d'abord dans $A = \mathbb{Z}[X_i, Y_i]$ où l'application fantôme est injective. On montre seulement que V_A est un morphisme additif ; toutes les autres propriétés se démontrent de façon similaire. On note $\underline{X} = (X_0, X_1, \ldots) \in W(A)$ et $\underline{Y} = (Y_0, Y_1, \ldots) \in W(A)$. Alors :

$$\begin{aligned}\omega_A(V_A(\underline{X}\hat{+}\underline{Y})) &= v_A\omega_A(\underline{X}\hat{+}\underline{Y}) = v_A(\omega_A(\underline{X}) + \omega_A(\underline{Y})) \\ &= v_A(\omega_A(\underline{X})) + v_A(\omega_A(\underline{Y}) = \omega_A V_A(\underline{X}) + \omega_A V_A(\underline{Y}) = \omega_A(V_A(\underline{X})\hat{+}V_A(\underline{Y}))\end{aligned}$$

où l'on a utilisé que ω_A et v_A sont des morphismes additifs. Par injectivité de ω_A dans le cas particulier $A = \mathbb{Z}[X_i, Y_i]$ on a : $V_A(\underline{X}\hat{+}\underline{Y}) = V_A(\underline{X})\hat{+}V_A(\underline{Y})$. Maintenant si A est un anneau quelconque et $\underline{a}, \underline{b} \in A$ alors on utilise l'évaluation $\psi : \mathbb{Z}[X_i, Y_i] \to A$ $X_i \mapsto a_i$ et $Y_i \mapsto b_i$; $W(\psi)$ appliquée à l'égalité ci-dessus. Avec ce la on a bien : $V_A(\underline{a}\hat{+}\underline{b}) = V_A(\underline{a})\hat{+}V_A(\underline{b})$ car $W(\psi)$ commute avec V_A et la somme. On ainsi montré que V_A est un morphisme additif.
Pour montrer le 2) on montre désormais uniquement pour $\underline{X}, \underline{Y}$ dans $A = \mathbb{Z}[X_i, Y_i]$. En évaluant on peut ensuite montrer la propriété dans n'importe quel anneau. La première partie du 2 suit de :

$$\omega_A(F_A V_A(\underline{X})) = f_A v_A \omega_A(\underline{X}) = (p\omega_n(X_0, \ldots, X_n) \mid n \in \mathbb{N}) = p\omega_A(\underline{X}) = \omega_A(p\hat{\cdot}\underline{X})$$

Ensuite pour la deuxième partie :

$$\omega_A(V_A(\underline{X}\hat{\cdot}F_A(\underline{Y}))) = v_A[\omega_A(\underline{X}) f_A \omega_A(\underline{Y})] = (0, p\omega_n(X_0, \ldots, X_n)\omega_{n+1}(Y_0, \ldots, Y_{n+1}) \mid n \in \mathbb{N})$$

Tout comme :

$$\omega_A(V_A(\underline{X})\hat{\cdot}\underline{Y}) = v_A\omega_A(\underline{X})\omega_A(\underline{Y}) = (0, p\omega_n(X_0, \ldots, X_N)\omega_{n+1}(Y_0, \ldots, Y_{n+1}) \mid n \in \mathbb{N})$$

□

Remarque. On peut maintenant interpréter F et V grâce à ce résultat et à la remarque précédente comme des transformations naturelles de W vers W pour F et de OW vers OW pour V(où OW désigne le foncteur qui oublie la structure multiplicative). Cela est simplement l'énoncé formalisé du fait suivant : F et V sont des applications définies de "manière uniforme" (compatible avec la structure) sur les vecteurs de Witt sans dépendre de l'anneau A.

On définit les vecteurs de Witt tronqués.

Définition. On pose $V_n(A) = \operatorname{Im} V_A^n$ un idéal de $W(A)$ (par le point 2) du lemme plus haut) pour tout $n \in \mathbb{N}$. On pose ensuite *les n-vecteurs de Witt tronqués* $W_n(A)$ comme étant le quotient :

$$W_n(A) = W(A)/V_n(A)$$

Remarque. On a $W_1(A) = W(A)/V_1(A) = A$

Définition. Projections et troncations
On notera α_n pour $n \in \mathbb{N}$ la projection de $W(A$ sur $W_n(A)$. Si $m \geq n$ alors α_m se factorise par α_n. On note t_{mn} l'application $W_m(A) \to W_n(A)$ résultante et on appelle ces morphismes les *applications de troncation.*

Remarque. On se représente $W_n(A)$ comme des $n+1$ uplets $(a_0, .., a_n)$ de A où on prend les lois d'anneaux de $W(A)$ mais où l'on s'occupe uniquement des premières composantes. Ainsi les applications de troncation définissent bien une "troncation".

Lemme 8. *On a :*

$$W(A) = \varprojlim W_n(A)$$

où le diagramme sous-jacent et celui donné par le applications de troncations.

Démonstration. On utilise la description suivante de $\varprojlim W_n(A)$:

$$\varprojlim W_n(A) = \{\underline{x} \in \prod_{n=1}^{\infty} \mid t_{mn}(x_m) = x_n\}$$

La collection de morphismes $\alpha_n : W(A) \to W_n(A)$ induit une application vers la limite, car par définition des t_{mn} les α_n sont compatibles. Alors on a $\alpha : W(A) \to \varprojlim W_n(A)$. L'injectivité est obtenue car un élément du noyau est dans : $\cap_{n=1}^{\infty} V_n(A) = \{0\}$. La surjectivité est obtenue car un élément $\underline{x} \in \varprojlim W_n(A)$ définit une suite dans A par la compatibilité donnée par les applications de troncation. □

On montre maintenant une propriété importante de F_A qui explique son nom et qui va fortement intervenir dans la section suivante qui traite la propriété universelle des vecteurs de Witt dans un cas particulier.

Théorème 2. *F_A est un relèvement du Frobenius sur $W(A)/pW(A)$ c'est à dire :*

$$F_A(\underline{a}) \equiv \underline{a}^p \mod pW(A)$$

pour tout $\underline{a} \in W(A)$

Démonstration. Soit $\underline{X} = (X_0, X_1, \ldots) \in W(\mathbb{Z}[X_i, Y_i])$. On pose $A = \mathbb{Z}[X_i \mid i \in \mathbb{N}]$. On montre que $\underline{a} = \omega_A(F_A(\underline{X})\hat{-}\underline{X}^p) \in p \operatorname{Im} \omega_A$.

Par souci de clarté explicitons les composantes de $\underline{a}$:

$$a_n = \omega_{n+1}(X_0, \ldots, X_{n+1}) - (\omega_n(X_0, \ldots, X_n))^p$$

On remarque en premier lieu que comme :

$$\begin{aligned}(\omega_n(X_0, \ldots, X_n))^p &= \left(\sum_{i=0}^{n} p^i {X_i}^{p^{n-i}}\right)^p \equiv \sum_{i=0}^{n} (p^i {X_i}^{p^{n-i}})^p \equiv X_0^{p^{n+1}} \\ &\equiv \omega_{n+1}(X_0, \ldots, X_{n+1}) \mod p\mathbb{Z}[X_0, \ldots X_{n+1}]\end{aligned}$$

on a un $\underline{b} \in A^{\mathbb{N}}$ tel que $\underline{a} = p\underline{b}$. On cherche donc à montrer : $\underline{b} \in \operatorname{Im} \omega_A$. Comme le lemme de Dwork avec le relèvement de Frobenius $\phi : \mathbb{Z}[X_i \mid i \in \mathbb{N}] \to \mathbb{Z}[X_i \mid i \in \mathbb{N}]$ donné par $X_i \mapsto X_i^p$ explicite l'image de ω_A de la façon suivante :

$$\operatorname{Im} \omega_A = \{\underline{c} \in A^{\mathbb{N}} \mid c_{n+1} \equiv \phi(c_n) \mod p^{n+1} \text{ pour tout } n \in \mathbb{N}\}$$

on est ramené à montrer : $b_{n+1} \equiv \phi(b_n) \mod p^{n+1}$. Mais pour cela, comme $\underline{a} = p\underline{b}$, il suffit de montrer : $\phi(a_n) \equiv a_{n+1} \mod p^{n+2}$.

Pour cela on traite les deux termes de la différence $a_n = \omega_{n+1}(X_0, \ldots, X_{n+1}) - (\omega_n(X_0, \ldots, X_n))^p$ séparément

En utilisant les relations de récurrence sur les ω_n on obtient d'une part :

$$\phi(\omega_{n+1}(X_0, \ldots, X_{n+1})) = \omega_{n+1}(X_0^p, \ldots, X_{n+1}^p) = \omega_{n+2}(X_0, \ldots, X_{n+2}) - p^{n+2} X_{n+2}$$

et d'autre part :

$$\phi(\omega_n(X_0,\dots,X_n))^p) = (\omega_n(X_0^p,\dots,X_n^p))^p = (\omega_{n+1}(X_0,\dots,X_{n+1}) - p^{n+1}X_{n+1})^p$$
$$\equiv (\omega_{n+1}(X_0,\dots,X_{n+1}))^p \mod p^{n+2}$$

Ces deux relations misent ensemble donnent bien : $\phi(a_n) \equiv a_{n+1} \mod p^{n+2}$.

Maintenant qu'on a montré $\underline{a} = \omega_A(F_A(\underline{X})\hat{-}\underline{X}^p) \in p\,\mathrm{Im}\,\omega_A$, par injectivité de ω_A on obtient :

$$F_A(\underline{X}) \equiv \underline{X}^p \mod pW(A)$$

Pour passer à $\underline{x} \in W(B)$ pour un anneau arbitraire B, on "évalue" $\underline{X}$ en $\underline{x}$. □

3.2 Quelques résultats dans le cas des $\mathbb{F}_p$-algèbres

Dans la suite A est de caractéristique p, c'est à dire une $\mathbb{F}_p$-algèbre. On va montrer quelques propriétés de $W(A)$ dans ce cas.

Lemme 9. *On a la congruence suivante :* $F_n(X_0,\dots,X_{n+1}) \equiv X_n^p \mod p\mathbb{Z}[X_0,\dots,X_{n+1}]$

Démonstration. On montre le résultat par récurrence sur n. Comme $F_0 = X_0^p + pX_1$ le résultat est clair pour 0. Soit maintenant $n \in \mathbb{N}$ et supposons le résultat vrai pour tout les naturels $< n$. On montre le résultat pour n ; en travaillant modulo p^{n+1} on a :

$$\omega_n(F_0,\dots,F_n) = \omega_{n+1}(X_0,\dots,X_{n+1}) = \omega_n(X_0^p,\dots,X_n) + p^{n+1}X_{n+1} \equiv \omega_n(X_0^p,\dots,X_n)$$
$$= \omega_{n-1}(X_0^{p^2},\dots,X_{n-1}^{p^2}) + p^nX_n^p \mod p^{n+1}\mathbb{Z}[X_0,\dots,X_{n+1}]$$

Comme par hypothèse de récurrence $F_i \equiv X_i^p \mod p$ pour tout $i \in \{0,...,n-1\}$ on a en utilisant le lemme technique démontré dans la partie 2.1 pour la suite d'idéaux $J_n = (p^n)$: $F_i^p \equiv X_i^{p^2} \mod p^2$ pour tout $i \in \{0,...,n-1\}$. En utilisant le deuxième point de ce même lemme on a alors :

$$\omega_{n-1}(F_0^p,...,F_{n-1}^p) \equiv \omega_{n-1}(X_0^{p^2},\dots,X_{n-1}^{p^2}) \mod p^{n+1}$$

Alors :

$$\omega_n(F_0,\dots,F_n) = \omega_{n-1}(F_0^p,\dots,F_{n-1}^p) + p^nF_n \equiv \omega_{n-1}(X_0^{p^2},\dots,X_{n-1}^{p^2}) + p^nF_n \mod p^{n+1}$$

On peut alors conclure que $p^nF_n \equiv p^nX_n^p \mod p^{n+1}$ et donc $F_n \equiv X_n^p \mod p$ □

En utilisant le lemme précédent dans le cas où A est une $\mathbb{F}_p$-algèbre on a pour tout $\underline{a} \in W(A)$: $F_A(\underline{a}) = (a_n^p \mid n \in \mathbb{N})$

Lemme 10. *Pour tout* $\underline{a} \in W(A)$ *on a :* $p\hat{\cdot}\underline{a} = V_AF_A(\underline{a}) = F_AV_A(\underline{a}) = (0, a_0^p, a_1^p, a_2^p, \dots)$. *De plus* $p^nW(A) \subset V_n(A)$

Démonstration. En utilisant ce que vaut F_A dans une $\mathbb{F}_p$-Algèbre et que : $p\hat{\cdot}\underline{a} = F_AV_A(\underline{a})$ on a le résultat. □

Corrolaire 1. *Si A est une $\mathbb{F}_p$-algèbre réduite alors $W(A)$ est sans p-torsion.*

Démonstration. Si $p\hat{\cdot}\underline{a} = 0$, c'est que $a_n^p = 0$ pour tout $n \in \mathbb{N}$ par le lemme précédent ; comme A est réduit on a forcément $a_n = 0$ pour tout $n \in \mathbb{N}$. □

On suppose maintenant que A est parfait, c'est à dire que $\Phi_A : A \to A$ le morphisme de Frobenius est un automorphisme. En utilisant cette hypothèse supplémentaire on obtient les conséquences suivantes :

Lemme 11. *1. F_A est un automorphisme de $W(A)$*

2. $p^n W(A) = V_n(A)$

3. $W(A)/pW(A) = A$

Démonstration. On note a^{-p} l'inverse de a par le Frobenius. Comme si $(0, \ldots, 0, a_0, a_1, \ldots) \in V_n(A)$ on a $p^n(a_0^{p^{-n}}, a_1^{p^{-n}}, \ldots) = (0, \ldots, a_0, a_1, \ldots)$ 2) suit. 3) suit immédiatement. □

3.3 L'application de Teichmüller

On a déjà vu l'application de Teichmüller dans le cas de $\mathbb{Z}_p$. On généralise maintenant cette construction à l'anneau des vecteurs de Witt.

Définition. On note $\tau_A : A \to W(A)$ l'application suivante :

$$\tau_A(a) = (a, 0, 0, 0, \ldots)$$

On l'appelle *l'application de Teichmüller* et $\tau_A(a)$ *le représentant de Teichmüller de A*

Lemme 12. *1. τ_A est une application multiplicative, c'est à dire pour tout $a, b \in A$ $\tau_A(ab) = \tau_A(a)\tau_A(b)$*

2. τ est une section de $\alpha_1 : W(A) \to A$

3. Pour tout $\underline{b} \in W(A)$ et $a \in A$ on a : $\tau_A(a)\underline{b} = (a^{p^n} b_n \mid n \in \mathbb{N})$

Démonstration. 2) suit de la lecture de l'énoncé. On montre le 3). On commence par travailler dans $W(A)$ pour $A = \mathbb{Z}[X_i, Y_i]$ où l'application fantôme est injective. En utilisant la définition des n-ièmes polynômes de Witt on obtient :

$$\begin{aligned}\omega_n(S_n(X_0, 0, \ldots, 0, Y_0, \ldots, Y_n)) = \omega_n(X_0, 0, \ldots, 0)\omega_n(Y_0, \ldots, Y_n) &= X_0^{p^n}\omega_n(Y_0, \ldots, Y_n) \\ &= \omega_n(X_0Y_0, X_0^pY_1, X_0^{p^2}, \ldots, X_0^{p^n}Y_n)\end{aligned}$$

Comme cela tient pour tout n, par injectivité dans le cas des polynômes et en évaluant pour passer dans un anneau quelconque on montré l'assertion. On a ainsi montré 3). 1) en est une conséquence directe.

□

Remarque. Attention : $\tau(a + b) \neq \tau(a) + \tau(b)$

Remarque. Une vérification directe montre que si $\psi : A \to B$ est un morphisme d'anneau alors :

$$\tau_B\psi = W(\psi)\tau_A$$

Cette commutativité peut être capturée de manière catégorique de la manière suivante : si A désigne le foncteur d'oubli des anneaux vers la structure multiplicative et $\mathrm{Id}_{\mathbf{Ann}}$ le foncteur identité des anneaux alors τ est une transformation naturelle du foncteur $A(\mathrm{Id}_{\mathbf{Ann}})$ vers AW.

4 Propriété universelle des vecteurs de Witt pour les anneaux sans p-torsion

Dans cette section les anneaux sont sans p-torsion. On note $p\mathbf{Ring}$ la catégorie des anneaux sans p-torsion. Pour A un anneau on notera par la lettre ϕ une application qui est un relèvement du Frobenius sur A/pA, c'est à dire :

$$\phi(x) \equiv x^p \mod pA$$

On va montrer que le foncteur de Witt est adjoint à droite au foncteur d'oubli de la catégorie des *Anneaux sans p-torsion muni d'un relèvement du Frobenius* vers les anneaux sans p-torsion.

Pour énoncer les propriétés catégoriques qu'on veut démontrer il nous faut la définition suivante :

Définition. On note $p\mathbf{Ring}\Phi$ la catégorie des anneaux sans p-torsion munis d'un relèvement du Frobenius. Un morphisme dans cette catégorie est un morphisme d'anneau $g : A \to B$ tel que, si ϕ_A, ϕ_B désignent respectivement les relèvements du Frobenius de A et de B alors :

$$g\phi_A = \phi_B g$$

Les vecteurs de Witt $W(A)$ dans cette catégorie seront toujours munis de leur application F_A comme relèvement du Frobenius dans ce qui suit ; on a donc un foncteur : $W : p\mathbf{Ring} \to p\mathbf{Ring}\Phi$. Comme dans ce contexte $W(A)$ est un sous-anneau de $A^{\mathbb{N}}$ on a bien que $W(A)$ est sans p-torsion. On rappelle qu'on note pour A un anneau $\alpha_{1A} : W(A) \to A$ la projection par quotient par l'idéal $V_1(A)$.

Une facette de l'adjonction annoncée s'énonce de la façon suivante. Si B est un anneau muni d'un relèvement du Frobenius ϕ et $h : B \to A$ un morphisme d'anneau vers un anneau A qui n'est pas muni d'une structure de relèvement du Frobenius alors les vecteurs de Witt $W(A)$ permettent de remonter, prolonger h en un morphisme entre des structures munies d'un relèvement du Frobenius de manière unique, naturelle :

$$\begin{tikzcd} B \arrow[r, "h"] \arrow[dr, dashed, "\bar{h}"'] & A \\ & W(A) \arrow[u, "\alpha_{1A}"'] \end{tikzcd}$$

Avant de déterminer $\bar{h}$ pour un h quelconque prenons un cas très particulier : $h = \mathrm{Id}_B : B \to B$. On veut donc trouver un "prolongement de l'identité" (on verra par la magie des catégories que relever l'identité permettra de tout relever) comme suit :

$$\begin{tikzcd} B \arrow[r, "\mathrm{Id}_B"] \arrow[dr, dashed, "\bar{\mathrm{Id}}_B = \Delta_B"'] & B \\ & W(B) \arrow[u, "\alpha_{1A}"'] \end{tikzcd}$$

où Δ_B est la notation qu'on utilisera pour ce "prolongement de l'identité". On veut donc que Δ_B soit un morphisme de $p\mathbf{Ring}\Phi$ c'est à dire :

$$\Delta_B \phi = F_B \Delta_B$$

Notons $\Delta_B = (\delta_0, \delta_1, ...)$. La commutativité du diagramme donne $\delta_0 = \mathrm{Id}_B$. Pour obtenir des informations pour δ_n on passe aux composantes fantômes l'égalité ci-dessus. Commençons par la composante fantôme d'indice 0 :

$$\omega_0(\delta_0\phi) = \phi = \omega_1(\delta_0, \delta_1)$$

Puis pour la composante d'indice 1 :

$$\omega_1(\delta_0\phi, \delta_1\phi) = \phi^2 = \omega_2(\delta_0, \delta_1, \delta_2)$$

Où l'on a utilisé notre connaissance de $\omega_1(\delta_0, \delta_1)$. On voit donc que par récurrence on devrait avoir pour ce prolongement de l'identité Δ_B :

$$\omega_n(\delta_0, \ldots, \delta_n) = \phi^n$$

La question est donc, dans un premier temps, la suivante : est-ce que ce Δ_B existe ? La réponse est affirmative pour $B \in p\mathbf{Ring}\Phi$ comme on va le voir maintenant.

Soit donc B un anneau sans p-torsion muni d'un relèvement du Frobenius ϕ. Le lemme de Dwork assure que $(\phi^n(b)) \in \operatorname{Im} \omega_B$.
ω_B étant injective par l'absence de p-torsion, il existe un unique élément $\Delta_B(b) = (\delta_n(b) \mid n \in \mathbb{N}) \in W(B)$ tel que $\omega_n(\delta_0(b), \ldots, \delta_n(b)) = \phi^n(b)$. On montre dans ce qui suit que $\Delta_B : B \to W(B)$ est un morphisme d'anneau. Ce Δ se révèlera être l'unité de l'adjonction annoncée.

Définition. Soit $B \in p\mathbf{Ring}\Phi$ avec ϕ son relèvement du Frobenius. $\Delta_B : B \to W(B)$ comme ci-dessus est appelé *vecteurs des δ-opérations relativement à ϕ* et on note $\Delta_B = (\delta_n)$. $\delta_n : B \to B$ est appelé la *n-ième δ-opération sur B relativement à ϕ.*

Lemme 13. *La fonction Δ_B comme ci-dessus est un morphisme d'anneau qui vérifie :*

$$\begin{tikzcd} B \arrow[r, "\Delta_B"] \arrow[rr, bend right, "\phi^n"'] & W(B) \arrow[r, "\omega_n"] & B \end{tikzcd}$$

Démonstration. Le diagramme est vérifié par construction. Pour montrer que c'est un morphisme d'anneaux on passe aux composantes fantômes et on utilise l'injectivité. (Qui est donnée on le rappelle par la première partie du lemme de Dwork comme B est sans p-torsion) On montre l'aspect additif ; les autres aspects sont similaires. Soient $a, b \in B$. Alors quelque soit $n \in \mathbb{N}$

$$\omega_n(\delta_0(a+b), \ldots, \delta_n(a+b)) = \phi^n(a+b) = \phi^n(a)+\phi^n(b) = \omega_n(\delta_0(a), \ldots, \delta_n(a))+\omega_n(\delta_0(b), \ldots, \delta_n(b))$$

Où l'on a utilisé la définition de Δ_B ainsi que le fait que ϕ soit un morphisme. Alors :

$$\omega_B(\Delta_B(a+b)) = \omega_B(\Delta_B(a) \hat{+} \Delta_B(b))$$

L'injectivité conclut. □

Par exemple on a $\delta_0(a) = a$. C'est à dire $\delta_0 = \mathrm{Id}_B$. Pour δ_1 on a :

$$\delta_1(a) = \frac{\phi(a) - a^p}{p}$$

Pas de panique : comme ϕ est un relèvement du Frobenius, le numérateur est bien divisible par p.

Lemme 14. *Soit $B \in p\mathbf{Ring}\Phi$ et $A \in p\mathbf{Ring}$. Un morphisme de $g = (g_n) : B \to W(A)$ de $p\mathbf{Ring}\Phi$ satisfait pour tout $n \in \mathbb{N}$*

$$\omega_n(g_0, \ldots, g_n) = g_0 \phi_B^n$$

Démonstration. On a déjà fait la preuve pour l'identité plus haut : on montre le résultat par récurrence sur les naturels. En 0 le résultat est donné : $\omega_0(g_0) = g_0$. On suppose maintenant le résultat vrai pour tout les naturels $\leq n$ et on montre le résultat pour $n+1$. Par hypothèse : $g\phi_B = F_A g$. En passant aux composantes fantômes cette égalité on obtient :

$$(\omega_n(g_0\phi_B, \ldots, g_n\phi_B)) = (\omega_{n+1}(g_0, \ldots, g_{n+1}))$$

Alors en utilisant l'hypothèse de récurrence : $\omega_n(g_0\phi_B, \ldots, g_n\phi_B) = (g_0\phi_B)\phi_B^n$, on a démontré l'assertion.

□

On montre maintenant la propriété universelle annoncée.

Théorème 3. *Propriété universelle des vecteurs de Witt ; cas sans p-torsion.*

Soit A un anneau sans p-torsion. Soit B un anneau sans p-torsion muni d'un relèvement ϕ_B du Frobenius. Alors pour tout morphisme d'anneau $h : B \to A$, il existe un unique morphisme $\bar{h} : B \to W(A)$ tel que $\bar{h}\phi_B = F_A\bar{h}$ et :

$$\begin{tikzcd} B \arrow[r, "h"] \arrow[dr, dashed, "\bar{h}"'] & A \\ & W(A) \arrow[u, "\alpha_{1A}"'] \end{tikzcd}$$

Plus précisément, si on note $U : p\mathbf{Ring}\Phi \to p\mathbf{Ring}$ le foncteur d'oubli, alors U est adjoint à gauche de W. Pour $A \in p\mathbf{Ring}$ et $B \in p\mathbf{Ring}\Phi$ l'adjonction est donnée par :

$$\begin{aligned} p\mathbf{Ring}(U(B), A) &\xrightarrow{\sim} p\mathbf{Ring}\Phi(B, W(A)) \\ h &\to \bar{h} \overset{def.}{=} W(h)\Delta_B \\ \bar{g} \overset{def.}{=} \alpha_{1A}U(g) = g_0 &\leftarrow g = (g_n) \end{aligned}$$

En conséquence pour tout $A \in p\mathbf{Ring}$ le foncteur contravariant $p\mathbf{Ring}(U(-), A) : p\mathbf{Ring}\Phi \to \mathbf{Set}$ est représenté par $W(A)$ avec l'adjonction comme choix d'isomorphisme naturel.

Démonstration. On commence par montrer que l'adjonction annoncée est bien définie et bijective. On montrera ensuite la naturalité en A et B.

Il faut montrer que si $h \in p\mathbf{Ring}(U(B), A)$ alors $W(h)\Delta_B$ est bien un morphisme de $p\mathbf{Ring}\Phi$, c'est à dire de montrer que : $W(h)\Delta_B\phi_B = F_AW(h)\Delta_B$. Pour cela on passe aux composantes fantômes ; d'une part :

$$\omega_A(W(h)\Delta_B\phi_B) = W(h)\omega_B\Delta_B\phi_B = (h\phi^{n+1})$$

Où l'on a utilisé la propriété de Δ_B en passant aux composantes fantômes. Comme d'autre part :

$$\omega_A(F_AW(h)\Delta_B) = f_AW(h)\omega_B\Delta_B = (h\phi^{n+1})$$

On a bien montré que $\bar{h}$ est bien définie.

Montrons maintenant que l'application est bijective. Premièrement étudions $\bar{\bar{h}}$:

$$h \to W(h)\Delta_B \to (W(h)\Delta_B)_0 = h\delta_0$$

Comme $\delta_0 = \mathrm{Id}_B$ on a bien $\bar{\bar{h}} = h$. Ensuite étudions $\bar{\bar{g}}$:

$$g \to g_0 \to W(g_0)\Delta_B$$

Passons aux composantes fantômes. Comme $\omega_n(g_0, \ldots, g_n) = g_0\phi_B^n$ et que $\omega_A(W(g_0)\Delta_B) = W(g_0)\omega_B(\Delta_B) = W(g_0)(\phi_B^n) = (g_0\phi_B^n) = \omega_A(g)$ on a bien en utilisant l'injectivité de ω_A : $\bar{\bar{g}} = g$.

Montrons maintenant la naturalité de cette bijection. Il faut vérifier que :

1. $\overline{U(B) \xrightarrow{h} A \xrightarrow{p} A'} = B \xrightarrow{\bar{h}} W(A) \xrightarrow{W(p)} W(A')$
2. $\overline{B \xrightarrow{q} B' \xrightarrow{g} W(A)} = U(B) \xrightarrow{U(q)} U(B') \xrightarrow{\bar{g}} A$

Pour 1) : $\overline{ph} = W(ph)\Delta_B = W(p)W(h)\Delta_B = W(p)\bar{h}$; en utilisant le caractère fonctoriel de W. Le 2) se montre de façon similaire en utilisant le caractère fonctoriel de U.

Pour se ramener au premier énoncé : montrons qu'il y a une unique flèche p qui fait commuter le diagramme suivant :

$$\begin{tikzcd} U(B) \arrow[r, "h"] \arrow[dr, "U(p)"'] & A \\ & U(W(A)) \arrow[u, "\alpha_{1A}"'] \end{tikzcd}$$

Une telle flèche vérifie $U(p)\alpha_{1A} = h$. Alors $\overline{U(p)\alpha_{1A}} = \bar{h}$. Comme : $\overline{\mathrm{Id}_{W(A)}} = \alpha_{1A}$, on a : $\overline{\alpha_{1A}} = \mathrm{Id}_{W(A)}$. Alors en utilisant la naturalité qu'on vient de démontrer : $\overline{U(p)\alpha_{1A}} = p\overline{\alpha_{1A}} = p = \bar{h}$. Ainsi p est forcément $\bar{h}$. $\square$

Remarque. On voit donc que l'anneau des vecteurs de Witt permet de relever de manière universelle des applications vers des anneaux A qui ne possèdent pas forcément de relèvement du Frobenius, vers un anneau qui en possède un : $W(A)$.

On a vu dans la section précédente que des propriétés intéressantes apparaissaient dans le cas de $\mathbb{F}_p$- algèbres, donc des anneaux avec de la p-torsion. Pour capturer une propriété universelle des vecteurs de Witt dans le cas d'un anneau quelconque, en particulier dans le cas où A est une $\mathbb{F}_p$-algèbre, on sera poussé à prendre au sérieux les δ-opérations rencontrées en chemin. Plus abstraitement on peut définir une notion de δ-anneaux, une catégorie d'anneaux munis de δ-opérations δ_n analogues aux δ_n rencontrées ici. Ces opérations devront vérifier des axiomes qui feront des anneaux qui en sont munis des généralisations des anneaux sans p-torsion munis d'un relèvement du Frobenius.