Vecteurs de Witt

1 Définitions

Pour p un premier et A un anneau commutatif unitaire déf

$$w_n(X_0, \ldots, X_n) := X_0^{p^n} + pX_1^{p^{n-1}} + \ldots + p^n X_n$$

dans $R = \mathbb{Z}[X_0, \ldots, X_n, \ldots]$.

On peut prouver que pour tout $F(X, Y) \in \mathbb{Z}[X, Y]$ il existe

$$(f_i(\bar{X}, \bar{Y}))_{i \in \mathbb{N}} \in (R \times R)^{\mathbb{N}}$$

tel que

$$w_n(f_0(\bar{X}, \bar{Y}), \ldots, f_n(\bar{X}, \bar{Y})) = F(w_n(\bar{X}), w_n(\bar{Y}))$$

en particulier pour $F(X, Y) = X + Y$ ou $X.Y$. Je note $\Phi(F) = (f_i)_{i \in \mathbb{N}}$ les polynômes associés à F. Les p, n-vecteurs de Witt maintenant c'est

$$W_n(A) := A^n$$

muni de l'addition

$$x +_{W(A)} y := (\Phi(X + Y)_i(x, y))_{i \in n}$$

et

$$x ._{W(A)} y := (\Phi(X.Y)_i(x, y))_{i \in n}$$

. Puis les p-vecteurs de Witt c'est $W(A) := W_\omega(A)$.

2 Calcul

En pratique pour le passage à la caractéristique p faut calculer d'abord dans $\mathbb{Z}$ les h_n puis réduire modulo p.

En fait c'est plus compliqué je l'explique dans 5.

2.1 Preuve de l'identité : congruences

L'unicité et la construction de $\Phi(F(X,Y))$ est directe par récurrence. A priori

$$\Phi(F(X,Y)) \in \mathbb{Z}[p^{-1}][\overline{X}]^{\mathbb{N}}$$

et on veut

$$\Phi(F(X,Y)) \in \mathbb{Z}[\overline{X}]^{\mathbb{N}}$$

et pour ça faut montrer par récurrence que pour tout $n \geq 0$

$$F(w_n(\bar{X}), w_n(\bar{Y})) = w_n(\Phi(F(X,Y))) \mod p^n$$

L'idée c'est déjà que

$$w_{n-1} \circ \varphi(x) = w_n(x) \mod p^n \tag{1}$$

puis que pour $f \in (X_0, \dots, X_n)$ on a

$$f^{p^m} \equiv f^{p^{m-1}} \circ \varphi \mod p^m \tag{2}$$

d'où si

$$F(w_{n-1}(\bar{X}), w_{n-1}(\bar{Y})) = w_{n-1}(\Phi(F(X,Y))) \tag{3}$$

on obtient

$$\begin{aligned} F(w_n(\bar{X}), w_n(\bar{Y})) &= F(w_{n-1} \circ \varphi(\bar{X}), w_{n-1} \circ \varphi(\bar{Y})) \mod p^n \\ &= w_{n-1}(h_0 \circ \varphi, \dots, h_{n-1} \circ \varphi) \mod p^n \\ &= w_{n-1}(h_0^p, h_1^p, \dots, h_{n-1}^p) \mod p^n \\ &= w_n(h_0, \dots, h_n) \mod p^n \end{aligned}$$

où la première égalité est dûe à (3) la deuxième à (1) et la troisième à (2). La dernière c'est à nouveau (1)

2.2 Preuve de (2)

L'équation (2) est obtenue simplement parce que si $A = B \mod p$ alors

$$A^{p^m} - B^{p^m} = (A^{p^{m-1}} - B^{p^{m-1}}) \left(\sum_{i=0}^{p-1} A^{p^{m-1}i} B^{p^{m-1}(p-1-i)} \right)$$

sauf que par récurrence le premier terme est divisible par p^{m-1} et le deuxième vaut 0 modulo p via la congruence $A = B \mod p$ d'où le résultat.

3 A parfait de caractéristique $p > 0$

Dans ces conditions $W(A)$ est muni de la topologie p-adique et $p^n.x = V^n\varphi^n(x)$. Ça se voit au moment du calcul si $x \in V^n(W(A))$ au moment du calcul de x^2 par exemple on voit que $\Phi(X.Y)_n(x,x) = p^n x_n^2$ qui se réduit en $0 \mod p$. Et la suite aussi.

3.1 Pré-calcul

En fait si $h_0 = h \mod p$ alors

$$p^i h_0^{p^{n-i}} = p^i h^{p^{n-i}} \mod p^{n+1}$$

en particulier, une fois qu'on a calculé $\Phi(F)_i$ on peut prendre le lift qu'on veut mod p et ça changera rien pour $\Phi(F)_j \mod p$, $j > i$. C'est pratique mais ça arrange pas non plus tout.

3.2 Topologie

Ducoup on peut munir $W(A)$ de la topologie p-adique via les $p^n W(A) =: I_n(A) = \ker(W(A) \to W_n(A))$.

3.3 Lift de Teichmüller

Le lift de Teichmüller est donné par

$$[\_] \colon a \mapsto (a, 0, \ldots)$$

et c'est clairement multiplicatif.

3.4 Verschiebung et Frobenius

L'opérateur Verschiebung (shift) de dual le Frobenius vérifie $V\varphi = \varphi V = p$ et on a

$$p.x = (0, x_0^p, x_1^p, \ldots)$$

via l'identité

$$w_n(\Phi(p.X)) = p w_n(X)$$

et une récurrence.

3.5 Écriture canonique et propriété universelle

De $p = \varphi.V$ on obtient la caractéristique 0 et l'écriture canonique

$$x = \sum_{i \in \mathbb{N}} p^n [x_n^{p^{-n}}]$$

qui montre la p-complétude et la caractéristique 0. Pour la propriété universelle, l'idée c'est que un anneau p-adiquement complet R avec $R/p = A$ comme anneau résiduel vérifie que tout élément $x \in R$ s'écrit comme $x = \sum p^i a_i$ avec a_i un représentant. Puis $W(A) \to R$ est défini terme à terme. Ça marche parce que $\Phi(F(X,Y))$ est dans $\mathbb{F}_p[\overline{X}, \overline{Y}]^{\mathbb{N}}$ ou $\mathbb{Z}[\ldots]^{\mathbb{N}}$. D'où $w_n(\varphi(a + a'))$

3.6 Racines de l'unité, $W(\mathbb{F}_p)$

Vincent pense que l'idée c'est de canoniser le lift de teichmüller. Ce qui est plutôt cohérent, i.e. le système de représentants du corps résiduel est donné par les $([i])_{i \in A}$.

Mais en fait il y'a une suite intéressante à cette histoire. Voir l'article de M. Hazewinkel

4 Anneaux de valuations

Une première remarque : les idéaux principaux ont valuation minorée > 0. En particulier $\mathfrak{m}_E$ est jamais principal. Ducoup de même $\alpha.\mathfrak{m}_E$ non plus pour $\alpha \in \mathfrak{m}_E$. Enfin si tu contiens α tu contiens $B(0, |\alpha|)$ de sorte que $\mathfrak{m}_E$ est le seul idéal de valuation 0 puis on a tout les idéaux !

5 Calcul en pratique

Donc on veut évaluer $\Phi(F(X,Y))_n =: f_n$. On a $f_n \in \mathbb{Z}[\bar{X}, \bar{Y}]$ ou $\in \mathbb{F}_p[\bar{X}, \bar{Y}]$. Mais en pratique en fait pour évaluer y faut écrire $f_n \in A[\bar{X}, \bar{Y}]$. Pour $a \in W(A) = A^{\mathbb{N}}$ je note $I_a := (X_i - a_i, i \in \mathbb{N})$.

5.1 L'intuition

Donc on veut écrire $p^n f_n(a,b) = (w_n(F(a,b)) - f_0^{p^n} - \ldots p^{n-1} f_{n-1}^p)$. Et ça on peut pas l'écrire dans A si A est de char $p > 0$.

En fait pour calculer $f_n(a,b)$ on peut simplement remarquer que la congruence

$$F(w_n(X), w_n(Y)) - (w_n(\Phi(F(X,Y))) - p^n\Phi(F(X,Y))_n) = 0 \mod p^n$$

implique que

$$F(w_n(b), w_n(a)) - (w_n(\Phi(F(a,b))) - p^n\Phi(F(a,b))_n) = 0 \mod p^n$$

en particulier, l'évaluation de f_n en (a,b) dépend seulement de l'évaluation des f_i en (a,b).