Classification des schémas en groupes formels et finis sur un corps parfait, d'après J.-M. Fontaine

Matthieu Romagny, le 2 mai 2012

Petit groupe de travail *Groupes formels et p-divisibles*, CIRM (Luminy), 16-20 avril 2012.

On suit J.-M. Fontaine, *Groupes p-divisibles sur un corps local*, Astérisque 47-48, SMF, 1977.

Table des matières

On fixe un corps parfait k de caractéristique $p > 0$. Toutes les références non précisées sont des références au mémoire de Fontaine : ainsi III.4.2 indique le chapitre III, paragraphe 4.2.

1 Groupes formels sur k

On appelle *k-foncteur (resp. en groupes)* un foncteur covariant de la catégorie des k-algèbres dans celle des ensembles (resp. des groupes abéliens). On appelle *k-algèbre finie* une k-algèbre de dimension finie, munie de la topologie discrète. On appelle *k-foncteur formel (resp. k-groupe formel)* un foncteur covariant de la catégorie des k-algèbres finies dans celle des ensembles (resp. des groupes abéliens). Par restriction à la catégorie des k-algèbres finies, tout k-foncteur (en groupes) induit donc un k-foncteur formel (en groupes) que l'on appelle son *complété*. Par exemple, la droite affine est le foncteur défini par $\mathbb{A}^1_k(R) = R$ pour toute k-algèbre R, et son complété est défini par $\widehat{\mathbb{A}}^1_k(R) = R$ pour toute k-algèbre finie R.

On appelle *k-algèbre profinie* une k-algèbre topologique dont le k-module sous-jacent est profini. Si A est une k-algèbre profinie, on note $\mathrm{Spf}(A)$ le k-foncteur formel défini par

$$\mathrm{Spf}(A)(R) = \mathrm{Homc}_k(A, R),$$

où Homc désigne les morphismes *continus*. Si X est un k-foncteur formel (en groupes), on appelle *algèbre affine* de X l'ensemble $\mathcal{O}_X^f = \mathrm{Hom}_{k\text{-Fct}}(X, \widehat{\mathbb{A}}^1_k)$ des morphismes de foncteurs formels, qui est muni d'une structure naturelle de k-algèbre (de Hopf) profinie. Pour tout k-foncteur (en groupes) X, il existe un morphisme canonique $\alpha_X : X \to \mathrm{Spf}(\mathcal{O}_X^f)$, et on dit que X est un *k-schéma (en groupes) formel* si α_X est un isomorphisme. Cela signifie donc que X est proreprésentable, ou limite inductive filtrante de k-foncteurs formels (en groupes) représentables. On montre (I, prop. 4.1) que ceci est encore équivalent au fait que X est exact à gauche, c'est-à-dire envoie $\{0\}$ sur $\{0\}$ et commute aux produits fibrés. On dit aussi *k-groupe formel* au lieu de k-schéma formel en groupes.

Soit G un k-groupe formel. On dit qu'il est *connexe* si son algèbre affine A est locale. On dit que G est un *p-groupe* si le morphisme $\varinjlim {}_{p^n}G \to G$, où ${}_{p^n}G$ désigne le noyau de multiplication par p^n, est un isomorphisme. Il est équivalent de demander que $G(k')$ est un groupe de p-torsion, pour toute extension finie k'/k, ou pour tout k-anneau fini k'. Tout groupe formel connexe est un p-groupe. Il existe une unique décomposition en produit $G = G^{\mathrm{c}} \times G^{\text{ét}}$ où G^{c} est connexe et $G^{\text{ét}}$ est étale.

2 Covecteurs de Witt

2.1 Motivation

Le théorème de classification de Dieudonné pour les groupes finis ou formels sur un corps parfait k, tel que formulé par Fontaine, possède une structure formelle analogue à celle d'un théorème de dualité. En notations simplifiées et abusives, à un groupe G on associe un module $M_G = \mathrm{Hom}(G, \widehat{\mathrm{CW}}_k)$, et a un module M on associe un groupe $G_M = \mathrm{Hom}(M, \widehat{\mathrm{CW}}_k)$. Pour deviner l'« objet dualisant » $\widehat{\mathrm{CW}}_k$, on s'inspire d'une théorie analogue qui est celle de la dualité de Pontryagin dans la catégorie des p-groupes abéliens finis. Là, l'objet dualisant est le groupe $\mathbb{Q}_p/\mathbb{Z}_p$ qui peut être vu comme la limite inductive des groupes $\mathbb{Z}/p^m\mathbb{Z}$ avec les applications de transition $p : \mathbb{Z}/p^m\mathbb{Z} \longrightarrow \mathbb{Z}/p^{m+1}\mathbb{Z}$. Cette application p n'est rien d'autre que le Verschiebung $V : W_m(\mathbb{F}_p) \to W_{m+1}(\mathbb{F}_p)$ sur les vecteurs de Witt tronqués à coefficients dans le corps premier. Pour classifier les groupes finis et formels, on est amené à considérer le groupe formel $\widehat{\mathrm{CW}}^{\mathrm{u}}_k = \varinjlim W_m$

avec applications de transition les Verschiebung $V : W_m \to W_{m+1}$. Ce groupe s'identifie naturellement à un ensemble de « vecteurs de Witt vers la gauche », à support fini, appelés *covecteurs de Witt unipotents*. En fait, cet objet ne joue le bon rôle qu'en restriction à la catégorie des groupes unipotents, car tout morphisme d'un groupe de type multiplicatif vers le groupe unipotent W_m est nul. C'est la volonté de formuler une classification uniforme pour tous les groupes formels qui a mené Fontaine à chercher un plus gros groupe de covecteurs de Witt, à support non fini : le *groupe formel des covecteurs de Witt* $\widehat{\mathrm{CW}}_k$. On remarquera que si on note W_{nr} l'extension maximale non ramifiée de $W(k)$ et K_{nr} son corps de fractions, on a $\widehat{\mathrm{CW}}_k(\overline{k}) = K_{\mathrm{nr}}/W_{\mathrm{nr}}$, cf II.2.3 et III.2.3, en analogie avec la dualité de Pontryagin.

2.2 Faisceau CW

Soient A un anneau commutatif unitaire, R une A-algèbre, $r \geqslant 0$, $s \geqslant 1$ des entiers. Pour toute famille $(a_{-i})_{i\in\mathbb{N}}$ d'éléments de R, on note $\mathfrak{a}_r$ l'idéal engendré par les a_{-i} avec $i \geqslant r$, et

$$\mathrm{CW}_{r,s}(R) = \{\ (a_{-i})_{i\in\mathbb{N}} \in R^{\mathbb{N}}\ ;\ (\mathfrak{a}_r)^s = 0\ \}.$$

On pose ensuite :

$$\mathrm{CW}(R) = \bigcup_{r,s} \mathrm{CW}(R)$$

et on appelle CW (resp. $\mathrm{CW}_{r,s}$) le *foncteur des covecteurs de Witt* (resp. *tronqués*). Il s'agit d'un faisceau pour la topologie fidèlement plate sur la catégorie des A-algèbres. Considérons l'anneau de polynômes $\Lambda = A[X_{-i}]_{i\in\mathbb{N}}$ et l'idéal $\mathfrak{v}_r$ engendré par les X_{-i} avec $i \geqslant r$. Le quotient $\Lambda_{r,s} = \Lambda/(\mathfrak{v}_r)^s$ représente le foncteur $\mathrm{CW}_{r,s}$. Pour $r' \geqslant r$ et $s' \geqslant s$, on a les inclusions encadrées ci-contre. Soit $\widehat{\Lambda}$ la limite projective des $\Lambda_{r,s}$. On a un morphisme injectif $\Lambda \to \widehat{\Lambda}$ qui permet de voir les idéaux $(\mathfrak{v}_r)^s$ dans $\widehat{\Lambda}$. Munissons les $\Lambda_{r,s}$ de la topologie discrète et Λ de la topologie limite projective : c'est la topologie la moins fine qui rend continues les projections $\Lambda \to \Lambda_{r,s}$. C'est une topologie linéaire dont une base de voisinages de 0 est composée des idéaux $(\mathfrak{v}_r)^s$. De plus $\widehat{\Lambda}$ s'identifie au complété de Λ. Pour toute A-algèbre discrète R, on a :

$$\begin{array}{ccc} (\mathfrak{v}_{r'})^{s'} & \subset & (\mathfrak{v}_{r'})^{s} \\ \cap & & \cap \\ (\mathfrak{v}_{r})^{s'} & \subset & (\mathfrak{v}_{r})^{s} \end{array}$$

$$\mathrm{CW}(R) = \mathrm{Homc}_A(\widehat{\Lambda}, R).$$

2.3 Sous-faisceau CW^{u} des covecteurs de Witt unipotents

Conservons les notations ci-dessus. On note

$$\mathrm{CW}^{\mathrm{u}}(R) = \{\ (a_{-i})_{i\in\mathbb{N}} \in \mathrm{CW}(R)\ ;\ a_{-i} = 0 \text{ pour presque tout i }\}.$$

En identifiant une suite $(\ldots, 0, 0, a_{-(m-1)}, \ldots, a_{-1}, a_0)$ à l'élément $(a_{-(m-1)}, \ldots, a_{-1}, a_0)$ de l'ensemble $W_m(R)$ des vecteurs de Witt tronqués de longueur m, on voit immédiatement qu'on construit un isomorphisme

$$\mathrm{CW}^{\mathrm{u}} = \varinjlim W_m$$

où les applications de transition sont les Verschiebung $V : W_m \to W_{m+1}$, $(a_{-(m-1)}, \ldots, a_{-1}, a_0) \mapsto (0, a_{-(m-1)}, \ldots, a_{-1}, a_0)$.

2.4 Topologie sur $\mathrm{CW}(R)$

Pour tout idéal nilpotent $\mathfrak{n}$ de R, notons

$$\mathrm{CW}(R,\mathfrak{n},r) = \{\ (a_{-i})_{i\in\mathbb{N}} \in \mathrm{CW}(R)\ ;\ a_{-i} \in \mathfrak{n} \text{ si } i \geqslant r\ \}.$$

Les applications coordonnées donnent une bijection $\mathrm{CW}(R,\mathfrak{n},r) \simeq R^r \times \mathfrak{n}^{\mathbb{N}}$ qui permet par transport de structure de munir $\mathrm{CW}(R,\mathfrak{n},r)$ de la topologie produit, où les facteurs R et $\mathfrak{n}$ sont discrets. Il est immédiat que

$$\mathrm{CW}(R) = \varinjlim \mathrm{CW}(R,\mathfrak{n},r)$$

où la limite inductive est prise sur tous les idéaux nilpotents de R et les entiers r, ce qui permet de munir $\mathrm{CW}(R)$ de la topologie limite inductive que l'on appelle sa *topologie naturelle*. Pour cette topologie, $\mathrm{CW}(R)$ est séparé et complet ; de plus, pour tout morphisme d'anneaux $\varphi : R \to S$, l'application $\mathrm{CW}(\varphi) : \mathrm{CW}(R) \to \mathrm{CW}(S)$ est continue.

2.5 Extension aux anneaux complets

Munissons A de la topologie discrète. On peut étendre CW à la catégorie des A-algèbres linéairement topologisées, séparées et complètes. Si R est une telle algèbre, on pose :

$$\mathrm{CW}(R) = \varinjlim \mathrm{CW}(R/\mathfrak{a})$$

où $\mathfrak{a}$ décrit l'ensemble des idéaux ouverts de R. Ce foncteur est décrit plus précisément dans II.1.7. Avec cette extension, la description $\mathrm{CW}(R) = \mathrm{Homc}_A(\widehat{\Lambda}, R)$ est encore valable.

2.6 Loi de groupe sur CW

Notons $S_n = S_n(X_0,\dots,X_n;Y_0,\dots,Y_n)$ les polynômes qui donnent l'addition dans le foncteur des vecteurs de Witt p-typiques. Quelques commentaires sur le calcul pratique de ces polynômes sont donnés dans la section 7. La loi de groupe sur le faisceau CW relative au nombre premier p est l'unique loi de groupe qui étend fonctoriellement la loi de groupe topologique sur le sous-foncteur dense $\mathrm{CW}^{\mathrm{u}} = \varinjlim W_m$. Elle est définie par la suite de polynômes $S_n(X_{-n},\dots,X_0;Y_{-n},\dots,Y_0)$. Cette suite converge dans $\widehat{\Lambda}\widehat{\otimes}\widehat{\Lambda}$ vers une série formelle notée $S(X_{-i};Y_{-j})_{i,j\geqslant 0}$, comme il est démontré dans II.1.5, lemme 1.3 et II.3.3, lemme 3.1. Nous ne reproduisons pas ici la démonstration, qui n'est pas difficile. Indiquons les premiers termes de cette suite, avec les notations introduites dans la section 7 :

$$* \ S_1 = \ R_0Z_0 + R_1Z_{-1},$$

$$* \ S_2 = \ R_0Z_0 + R_1Z_{-1} + R_2Z_{-2} + R_1(R_0Z_{-1}, R_{-1}Z_{-2}),$$

$$\begin{aligned} * \ S_3 = \ & R_0Z_0 + R_1Z_{-1} + R_2Z_{-2} + R_3Z_{-3} \\ & + R_1\big(R_0Z_{-1}, R_1Z_{-2}, R_2Z_{-3}, R_1(R_0Z_{-2}, R_1Z_{-3})\big) \\ & + R_2\big(R_0Z_{-2}, R_1Z_{-3}\big), \end{aligned}$$

$$\begin{aligned} * \ S_4 = \ & R_0Z_0 + R_1Z_{-1} + R_2Z_{-2} + R_3Z_{-3} + R_4Z_{-4} \\ & + R_1\,(R_0Z_{-1}, R_1Z_{-2}, R_2Z_{-3}, R_3Z_{-4}, \\ & \qquad R_1\big(R_0Z_{-2}, R_1Z_{-3}, R_2Z_{-4}, R_1(R_0Z_{-3}, R_1Z_{-3})\big), R_2\big(R_0Z_{-3}, R_1Z_{-4}\big)\big) \\ & + R_2\big(R_0Z_{-2}, R_1Z_{-3}, R_2Z_{-4}, R_1(R_0Z_{-3}, R_1Z_{-4})\big) \\ & + R_3(R_0Z_{-3}, R_1Z_{-4}). \end{aligned}$$

Pour $a = (a_{-i})$ et $b = (b_{-i})$ dans $\mathrm{CW}(R)$, on pose alors $a + b = c = (c_{-i})$ avec

$$c_{-i} = S(\dots, a_{-i-n}, \dots, a_{-i}; \dots, b_{-i-n}, \dots, b_{-i}).$$

Ceci définit l'addition dans CW.

2.7 Endomorphismes

Pour plus de détails sur cette sous-section, voir l'exposé de D. Tossici.

2.7.1 Verschiebung. (II.2.5) *Sans hypothèse sur A*, le foncteur CW est muni d'une action de $\mathbb{Z}[V]$ donnée par :

$$V(\dots, a_{-i}, \dots, a_{-1}, a_0) = (\dots, a_{-i-1}, \dots, a_{-2}, a_{-1}).$$

2.7.2 Frobenius. (II.2.2) *Si A est de caractéristique p*, le foncteur CW est muni aussi d'une action de l'anneau $\mathbb{Z}[F, V]$, dans lequel on a les relations $FV = VF = p$, par :

$$F(\dots, a_{-i}, \dots, a_{-1}, a_0) = (\dots, a_{-i}^p, \dots, a_{-1}^p, a_0^p).$$

2.7.3 Vecteurs de Witt de la base. (II, prop. 2.2) *Si A est parfait*, notons $\sigma : A \to A$ son Frobenius. Le foncteur CW possède une action de $W(A)$ d'où une action de l'anneau $W(A)[F, V]$, dans lequel on a les relations $FV = VF = p$ et $Fx = \sigma(x)F$, $V\sigma(x) = xV$, pour tout $x \in W(A)$. L'action de $W(A)$ est définie ainsi. Soit P_m le m-ième polynôme donnant la multiplication des vecteurs de Witt. Étant donnés une A-agèbre R, $x = (x_0, x_1, \dots, x_n, \dots) \in W(A)$, $a = (\dots, a_{-n}, \dots, a_{-1}, a_0) \in \mathrm{CW}(R)$ et un entier $n \geqslant 0$ fixé, la suite de m-ième terme

$$P_m(\sigma^{-n-m}(x_0), \dots, \sigma^{-n-m}(x_m); a_{-m-n}, \dots, a_{-n})$$

est stationnaire. Soit b_{-n} sa limite et $b = (\dots, b_{-n}, \dots, b_{-1}, b_0)$. Alors $b \in \mathrm{CW}(R)$ et on pose $xa := b$.

2.8 Complété de CW

Si k est un corps, toute k-algèbre de dimension finie R est artinienne et son radical $\mathfrak{r}$ est nilpotent. On déduit alors de la définition de CW que le complété formel $\widehat{\mathrm{CW}}_k$ est décrit par :

$$\widehat{\mathrm{CW}}_k(R) = \mathrm{CW}(R) = \{\ (a_{-i})_{i \in \mathbb{N}} \in R^{\mathbb{N}}\ ;\ a_{-n} \in \mathfrak{r} \text{ pour presque tout } n\ \}.$$

On a les décompositions connexes-étales (voir section 1) :

$$\widehat{\mathrm{CW}}_k = \widehat{\mathrm{CW}}_k^{\mathrm{c}} \times \widehat{\mathrm{CW}}_k^{\text{ét}} \quad \text{et} \quad \widehat{\mathrm{CW}}_k^{\mathrm{u}} = \widehat{\mathrm{CW}}_k^{\mathrm{u,c}} \times \widehat{\mathrm{CW}}_k^{\mathrm{u,ét}}.$$

3 Le théorème de classification

Dans cette section, l'anneau de base est un corps parfait k. On note $W = W(k)$ l'anneau des vecteurs de Witt de k. On note par la même lettre σ le Frobenius de k et le Frobenius de W, qui relève le précédent. On note $D_k = W[F, V]$ l'anneau de Dieudonné de k. C'est le quotient de l'anneau de polynômes non commutatif $W\{F, V\}$, dans lequel pas même les constantes ne commutent à F et V, par les relations $Fx = \sigma(x)F$, $V\sigma(x) = xV$ pour tous les $x \in W$, et $FV = VF = p$. L'anneau D_k n'est pas commutatif, sauf si $k = \mathbb{F}_p$.

3.1 Énoncé

On définit d'abord le *module de Dieudonné d'un k-groupe formel G* par :

$$\mathbb{M}(G) = \mathrm{Hom}_{k\text{-Gr}}(G, \widehat{\mathrm{CW}}_k),$$

le groupe des morphismes de k-groupes formels de G dans $\widehat{\mathrm{CW}}_k$. Si G est un p-groupe formel, alors $\mathbb{M}(G)$ est un D_k-module $W[F]$-profini.

On définit ensuite le *p-groupe formel d'un module de Dieudonné M* par $\mathbb{G}(M) = \mathrm{Homc}_{D_k}(M, \widehat{\mathrm{CW}}_k)$, qui est plus précisément le k-foncteur en groupes défini par

$$\mathbb{G}(M)(R) = \mathrm{Homc}_{D_k}(M, \widehat{\mathrm{CW}}_k(R)),$$

groupe des applications D_k-linéaires continues, pour toute k-algèbre finie ou profinie R. Il est facile de voir que $\mathbb{G}(M)$ est un k-foncteur formel exact à gauche, donc représentable, c'est-à-dire, un k-groupe formel.

La classification de Dieudonné des p-groupes formels et finis sur k est résumée dans l'énoncé suivant (voir section 6 pour des rappels sur l'adjonction pour les foncteurs contravariants).

3.1.1 Théorème.

(1) *Les foncteurs $\mathbb{M}$ et $\mathbb{G}$ sont adjoints à droite.*

(2) *Les foncteurs $\mathbb{M}$ et $\mathbb{G}$ induisent des anti-équivalences inverses l'une de l'autre :*

$$\begin{array}{ccc} \{p\text{-groupes formels sur } k\} & \underset{\mathbb{G}}{\overset{\mathbb{M}}{\rightleftarrows}} & \{D_k\text{-modules } W[F]\text{-profinis}\} \\ \bigcup & & \bigcup \\ \{p\text{-groupes finis sur } k\} & \underset{\mathbb{G}}{\overset{\mathbb{M}}{\rightleftarrows}} & \{D_k\text{-modules finis}\} \end{array}$$

où l'on dit qu'un D_k-module est fini *s'il est de longueur finie comme W-module.*

(3) *Le groupe G est fini d'ordre p^r si et seulement si le module $\mathbb{M}(G)$ est de W-longueur finie r.*

Noter que Fontaine dit *adjoints à gauche* au lieu de *adjoints à droite*, et je ne comprends pas bien ce choix.

3.2 L'adjonction

La preuve du point (1) n'est pas difficile. En effet, soient G un p-groupe formel sur k et M un D_k-module $W[F]$-profini. On a des bijections naturelles :

$$\begin{aligned} \mathrm{Hom}_{k\text{-Fct}}(G, \mathbb{G}(M)) &= \mathbb{G}(M)(B_G) \text{ par le lemme de Yoneda,} \\ &= \mathrm{Homc}_{D_k}(M, \widehat{\mathrm{CW}}_k(B_G)) \text{ par définition de } \mathbb{G}(M), \\ &= \mathrm{Homc}_{D_k}(M, \mathrm{Hom}_{k\text{-Fct}}(G, \widehat{\mathrm{CW}}_k)) \text{ par Yoneda encore.} \end{aligned}$$

Comme par définition la loi de groupe de $\mathbb{G}(M)$ est induite par celle de $\widehat{\mathrm{CW}}_k$, on voit facilement que dans cette identification, on a bijection entre les sous-ensembles $\mathrm{Hom}_{k\text{-Gr}}(G, \mathbb{G}(M))$ et $\mathrm{Homc}_{D_k}(M, \mathrm{Hom}_{k\text{-Gr}}(G, \widehat{\mathrm{CW}}_k)) = \mathrm{Homc}_{D_k}(M, \mathbb{M}(G))$, cqfd.

3.3 La décomposition étale-connexe

La classique décomposition de Fitting affirme que si M est un $W[F]$-module artinien (ou pro-artinien, par passage à la limite), il existe une unique décomposition $M = M^{\text{ét}} \oplus M^{\text{c}}$ en sous-modules tels que F est bijectif sur $M^{\text{ét}}$ et nilpotent sur M^{c}. On dit que M est *étale*, resp. *connexe*, ssi $M = M^{\text{ét}}$, resp. $M = M^{\text{c}}$. Explicitement,

- $M^{\text{ét}} = \cap_{n \geqslant 0} F^n M$ est la *composante étale* de M,
- $M^{\text{c}} = \{x \in M, F^n x \text{ tend vers } 0\}$ est la *composante connexe* de M.

Par exemple, pour tout k-algèbre profinie R, les composantes étale et connexe de $M = \widehat{\mathrm{CW}}_k(R)$ sont $\widehat{\mathrm{CW}}_k^{\text{ét}}(R)$ et $\widehat{\mathrm{CW}}_k^{\text{c}}(R)$ (voir II.4.5, prop.4.1). On en déduit que :

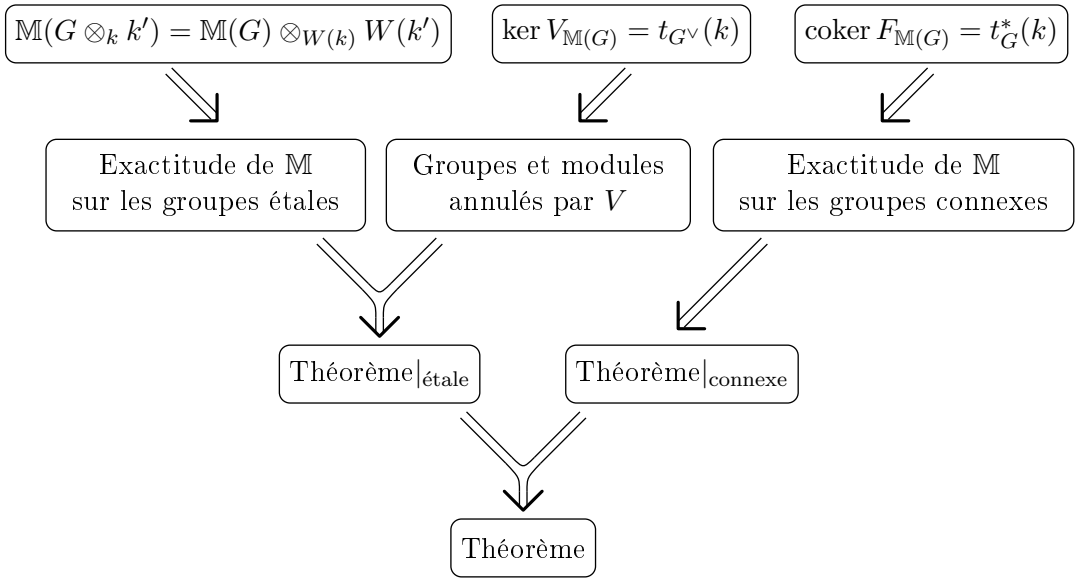
- si G est étale, resp. connexe, alors $\mathbb{M}(G)$ est étale, resp. connexe,
- si M est étale, resp. connexe, alors $\mathbb{G}(M)$ est étale, resp. connexe.

Tout ceci montre que les catégories des p-groupes formels sur k et des D_k-modules $W[F]$-profinis sont somme directe de leurs sous-catégories des objets étales et connexes, et que les foncteurs $\mathbb{M}$ et $\mathbb{G}$ respectent ces décompositions. Il suffit donc de démontrer le théorème de classification en restriction aux sous-catégories étale et connexe.

4 Preuve du théorème de classification

4.1 Stratégie de la preuve

Pour démontrer les points (2) et (3) du théorème, le plan suivi sera le suivant.



4.2 Conditions de finitude pour les anneaux et modules

Il s'agit de rappels sans preuve ; on renvoie à Bourbaki, Algèbre, Chapitre 8. Soit A un anneau et M un A-module. On dit que M est *artinien*, resp. *noethérien*, si ses sous-modules vérifient la condition des chaînes décroissantes, resp. croissantes. On dit que M est *de longueur finie* s'il possède une suite de composition de longueur finie. Les modules artiniens, resp. noethériens, resp. de longueur finie sont stables par sous-modules, quotients et extensions. Si $u : M \to M'$ est un morphisme entre modules de même longueur finie, alors les conditions suivantes sont équivalentes : u est bijectif ; u est injectif ; u est surjectif. Le $\mathbb{Z}$-module $\mathbb{Z}$ est noethérien non artinien ; le $\mathbb{Z}$-module

$\mathbb{Q}_p/\mathbb{Z}_p$ est artinien non noethérien. Un module est de longueur finie si et seulement s'il est artinien et noethérien. On dit que l'anneau A est *artinien*, resp. *noethérien*, resp. *de longueur finie*, s'il l'est comme A-module. Les conditions suivantes sont équivalentes : A est artinien ; A est noethérien de dimension 0 ; A est de longueur finie ; A est noethérien et $A_{\text{réd}}$ est un produit fini de corps ; A est un produit fini d'anneaux locaux à idéal maximal nilpotent. Si A est artinien, les conditions suivantes sont équivalentes : M est artinien ; M est noethérien ; M est de longueur finie ; M est de type fini. On dit qu'un anneau A est *proartinien* (Fontaine dit *pseudo-compact*) s'il est linéairement topologisé, séparé, complet, et si les quotients de A par ses idéaux ouverts sont artiniens. Si A est proartinien, on dit que M est *proartinien*, resp. *profini*, s'il est linéairement topologisé, séparé, complet, et si les quotients de M par ses sous-modules ouverts sont artiniens, resp. de longueur finie.

4.3 Isomorphisme $\mathbb{M}(G \otimes_k k') = \mathbb{M}(G) \otimes_{W(k)} W(k')$ (III.2.2)

4.3.1 *Soit k'/k une extension galoisienne et M un $W(k')$-module proartinien sur lequel $\mathcal{G} = \mathrm{Gal}(k'/k)$ agit continûment et semi-linéairement (i.e. M est un $W(k)[\mathcal{G}]$-module et $g(ax) = g(a)g(x)$ pour $a \in W(k')$, $x \in M$). Alors l'application $W(k') \otimes_{W(k)} M^{\mathcal{G}} \to M$, $a \otimes x \mapsto ax$ est un isomorphisme.*

Notons $W = W(k)$, $W' = W(k')$ et $\varphi : W' \otimes_W M^{\mathcal{G}} \to M$ le morphisme de l'énoncé. Soient $g_1, \ldots, g_n$ les éléments de $\mathcal{G}$. Soient $e_1, \ldots, e_n \in W'$ des éléments qui relèvent une k-base de k' ; ils forment une base du W-module libre W'. Il est clair que la matrice D des $g_i(e_j)$ est inversible, car $\det(D)^2$ est le discriminant de W'/W, qui est inversible car l'extension est non ramifiée. Le morphisme φ est injectif car un élément de $W' \otimes M^{\mathcal{G}}$ s'écrit d'une unique manière $\sum e_j \otimes x_j$, et si $\sum e_j x_j = 0$, alors pour tout i on a $\sum g_i(e_j)x_j = 0$, donc les x_j sont nuls.

Montrons que φ est surjectif. Remarque 1 : si $M \neq 0$ alors $M^{\mathcal{G}} \neq 0$, car pour $x \in M$ non nul, les éléments $u_j(x) = \sum_i g_i(e_j x) = \sum g_i(e_j) g_i(x)$ appartiennent à $M^{\mathcal{G}}$ et, utilisant l'inversibilité de la matrice D, ne sont pas tous nuls. Remarque 2 : si M est artinien, il est réunion des ${}_{p^r}M = \ker(p^r : M \to M)$, car si $x \in M$, la suite décroissante des sous-modules monogènes engendrés par $p^r x$ stationne en un entier R et on voit que $p^R x = 0$. Passons à la preuve du fait que φ est surjectif, d'abord dans le cas où M est de longueur finie, par récurrence sur $\lg_{A'}(M)$. Comme φ est injectif, il suffit de montrer que $\lg_A(M^{\mathcal{G}}) = \lg_{A'}(M)$. Si $\lg_{A'}(M) = 1$ alors $M \neq 0$ donc $M^{\mathcal{G}} \neq 0$ par la remarque 1, puis $\lg_A(M^{\mathcal{G}}) = 1$. Si $\lg_{A'}(M) > 1$, il existe $x \in M^{\mathcal{G}}$ non nul par la remarque 1, et on peut supposer que $px = 0$ par la remarque 2, i.e. x engendre un sous-module isomorphe à k'. On obtient une suite exacte $0 \to k' \to M \to N \to 0$ de W'-modules avec action semi-linéaire de $\mathcal{G}$. Comme $H^1(\mathcal{G}, k') = 0$ (rappel : ceci découle du théorème de la base normale qui montre que k' est un $\mathcal{G}$-module induit), on en déduit une suite exacte $0 \to k \to M^{\mathcal{G}} \to N^{\mathcal{G}} \to 0$. En utilisant l'hypothèse de récurrence pour N, il vient $\lg_A(M^{\mathcal{G}}) = \lg_A(N^{\mathcal{G}}) + 1 = \lg_{A'}(N) + 1 = \lg_{A'}(M) + 1$, cqfd. Supposons maintenant M artinien. Par la remarque 2, il est réunion des ${}_{p^r}M$ qui sont des modules artiniens sur l'anneau artinien $W_r(k')$, donc de longueur finie, et le résultat se déduit du cas précédent. Supposons enfin M proartinien. Alors, pour tout sous-module ouvert N, le sous-module $\cap g_i(N)$ est ouvert et $\mathcal{G}$-stable, ce qui montre que M est limite projective de modules artiniens avec action de $\mathcal{G}$, et le résultat se déduit du cas artinien.

4.3.2 *Avec les mêmes notations, le $\mathcal{G}$-module M est cohomologiquement trivial.*

En effet, on vient de montrer que c'est un module induit.

4.3.3 *Soit G un p-groupe formel sur k. Soit k'/k une extension finie (pas nécessairement galoisienne) et posons $M = \mathbb{M}(G)$ et $M' = \mathbb{M}(G \otimes_k k')$. Alors,*

(1) *l'application naturelle $W(k') \otimes_{W(k)} M \to M'$ est un isomorphisme,*

(2) *si k'/k est galoisienne, alors $\mathcal{G} = \mathrm{Gal}(k'/k)$ opère semi-linéairement sur M' et $M = (M')^{\mathcal{G}}$.*

Commençons par (2). Pour tout k-anneau profini R, le groupe $\mathcal{G}$ agit sur $R \otimes_k k'$ et $(R \otimes_k k')^{\mathcal{G}} = R$. De plus, $\mathcal{G}$ agit sur $\widehat{\mathrm{CW}}_{k'}(R \otimes_k k')$ par fonctorialité et on voit immédiatement qu'un covecteur $a = (\ldots, a_{-n}, \ldots, a_{-1}, a_0)$ est fixe sous $\mathcal{G}$ si et seulement si chacune de ses composantes l'est. Ceci montre que $\widehat{\mathrm{CW}}_{k'}(R \otimes_k k')^{\mathcal{G}} = \widehat{\mathrm{CW}}_k(R)$. Ceci dit, notons B_G l'algèbre affine de G. Notons Δ la comultiplication de la bigèbre des covecteurs de Witt. On a alors :

$$\mathbb{M}(G) = \mathrm{Hom}_{k\text{-Gr}}(G, \widehat{\mathrm{CW}}_k) = \left\{ a \in \widehat{\mathrm{CW}}_k(B_G)\,,\ \Delta a = a \mathbin{\widehat{\otimes}} 1 + 1 \mathbin{\widehat{\otimes}} a \right\}.$$

Il découle de ce qui précède, en prenant $R = B_G$, que $\mathbb{M}(G \otimes_k k')^{\mathcal{G}} = \mathbb{M}(G)$. Le point (1) s'en déduit lorsque k'/k est galoisienne grâce à 4.3.1. Lorsque k'/k n'est pas galoisienne, on obtient le résultat en plongeant k' dans sa clôture galoisienne.

4.4 Exactitude de $\mathbb{M}$ sur les groupes étales (III.2.3)

La restriction de $\mathbb{M}$ à la catégorie des p-groupes formels étales sur k est un foncteur exact. Autrement dit, le groupe $\widehat{\mathrm{CW}}_k^{\text{ét}}$ est un objet injectif de cette catégorie.

N.B. Ceci est en fait vrai sur la catégorie plus grande de tous les groupes formels étales.

Soit $\overline{k}$ une clôture algébrique de k et $\mathcal{G}_k = \mathrm{Gal}(\overline{k}/k)$. Pour tout k-groupe formel G, on note $G(\overline{k})$ la réunion des $G(k')$ pour k' sous-extension finie de $\overline{k}$. On sait que $G \mapsto G(\overline{k})$ est une équivalence entre la catégorie des k-groupes formels étales et la catégorie des $\mathcal{G}_k$-modules discrets. Par ailleurs, si l'on note W_{nr} la limite inductive des $W(k')$ et K_{nr} son corps de fractions, on sait que le $\mathcal{G}_k$-module $\widehat{\mathrm{CW}}_k^{\text{ét}}(\overline{k})$ s'identifie à $K_{\mathrm{nr}}/W_{\mathrm{nr}}$ (cf II.2.3). Nous devons donc montrer que $K_{\mathrm{nr}}/W_{\mathrm{nr}}$ est un objet injectif de la catégorie des $\mathcal{G}_k$-modules discrets. Soient $\mathcal{U}$ un sous-groupe ouvert distingué de $\mathcal{G}_k$, $k' = k^{\mathcal{U}}$, $\mathcal{G} = \mathrm{Gal}(k'/k) = \mathcal{G}_k/\mathcal{U}$, $W' = W(k')$ et K' le corps de fractions de W'. On a alors $(K_{\mathrm{nr}}/W_{\mathrm{nr}})^{\mathcal{U}} = K'/W'$. Nous admettons qu'il suffit de montrer que pour tous les $\mathcal{U}$ comme ci-dessus, le $\mathcal{G}$-module K'/W' est injectif (voir III.2.3, prop. 2.4). Soit $0 \to \Gamma_1 \to \Gamma_2 \to \Gamma_3 \to 0$ une suite exacte de $\mathcal{G}$-modules. Comme K'/W' est un groupe abélien divisible, la suite

$$0 \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\Gamma_3, K'/W') \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\Gamma_2, K'/W') \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\Gamma_1, K'/W') \longrightarrow 0$$

est exacte. Pour tout $\mathcal{G}$-module Γ, il y a sur le groupe $\mathrm{Hom}_{\mathbb{Z}}(\Gamma, K'/W')$ une structure de W'-module proartinien sur lequel le groupe $\mathcal{G}$ agit continûment et semi-linéairement, et $\mathrm{Hom}_{\mathbb{Z}[\mathcal{G}]}(\Gamma, K'/W') = \mathrm{Hom}_{\mathbb{Z}}(\Gamma, K'/W')^{\mathcal{G}}$. En prenant les points fixes, on en déduit que la suite

$$0 \longrightarrow \mathrm{Hom}_{\mathbb{Z}[\mathcal{G}]}(\Gamma_3, K'/W') \longrightarrow \mathrm{Hom}_{\mathbb{Z}[\mathcal{G}]}(\Gamma_2, K'/W') \longrightarrow \mathrm{Hom}_{\mathbb{Z}[\mathcal{G}]}(\Gamma_1, K'/W') \longrightarrow 0$$

est exacte, puisque $\mathrm{Hom}_{\mathbb{Z}}(\Gamma_3, K'/W')$ est cohomologiquement trivial par 4.3.2.

4.5 Isomorphisme $\ker V_{\mathbb{M}(G)} = t_{G^\vee}(k)$ (III.3.2)

Soit G un p-groupe formel sur k, $G^\vee$ son dual de Cartier, d'espace tangent $t_{G^\vee}(k)$. L'application qui à $a = (\ldots, a_{-n}, \ldots, a_{-1}, a_0)$ associe a_0 définit par restriction au noyau de V dans $\mathbb{M}(G)$ un isomorphisme de $k[F]$-modules topologiques

$$\ker V_{\mathbb{M}(G)} \simeq \mathrm{Hom}(G, \widehat{\mathbb{G}}_{\mathrm{a}}) = t_{G^\vee}(k).$$

Notons $B = B_G$ l'algèbre affine de G et $I = I_G$ son idéal d'augmentation. Considérons l'application $\pi : \widehat{\mathrm{CW}}_k(B) \longrightarrow B$, $a = (\dots, a_{-n}, \dots, a_{-1}, a_0) \mapsto a_0$. Puisque

$$\mathbb{M}(G) = \mathrm{Hom}_{k\text{-Gr}}(G, \widehat{\mathrm{CW}}_k) \subset \mathrm{Hom}_{k\text{-Fct}}(G, \widehat{\mathrm{CW}}_k) = \widehat{\mathrm{CW}}_k(B),$$

un élément $\varphi \in \mathbb{M}(G)$ peut être vu comme un $a = a_\varphi \in \widehat{\mathrm{CW}}_k(B)$. Comme le morphisme de groupes formels φ préserve le neutre, on voit que $a_{-n} \in I$ pour tout n. Comme φ commute au Verschiebung, le covecteur $Va = (\dots, a_{-n-1}, \dots, a_{-2}, a_{-1})$ est égal au covecteur $(\dots, V_B(a_{-n}), \dots, V_B(a_{-1}), V_B(a_0))$ où V_B est le Verschiebung de B. Il s'ensuit que $a_{-n} = V_B^n(a_0)$ pour tout n ; en particulier a est déterminé par a_0. Utilisant le fait que V_B est topologiquement nilpotent pour un p-groupe formel étale, on montre par ailleurs, sans supposer G étale, que pour tout $a_0 \in I$, la suite $a = (\dots, a_{-n}, \dots, a_{-1}, a_0)$ avec $a_{-n} = V_B^n(a_0)$ définit un élément de $\widehat{\mathrm{CW}}_k(B)$ (voir III.3.1). Ceci produit une application continue $I \to \widehat{\mathrm{CW}}_k(B)$ qui montre que $\mathbb{M}(G)$ est homéomorphe à son image dans I. Enfin, si $a \in \ker V_{\mathbb{M}(G)}$ alors $a = (a_0, 0, \dots)$ avec $a_0 \in I$ tel que $\Delta(a_0) = a_0 \widehat{\otimes} 1 + 1 \widehat{\otimes} a_0$. Un tel a_0 détermine un élément de $\mathrm{Hom}_{k\text{-Gr}}(G, \widehat{\mathbb{G}}_a)$, qui est isomorphe à $t_{G^\vee}(k)$ (voir I.8.6), cqfd.

4.6 Groupes et modules annulés par V (III.3.3)

(1) *Soit G un p-groupe fini sur k, d'ordre p^r, tel que $V_G = 0$. Alors $\mathbb{M}(G)$ est un D_k-module fini vérifiant $V\mathbb{M}(G) = 0$ dont la longueur comme W-module est égale à r.*

(2) *Soit M un D_k-module fini, de longueur comme W-module égale à r, vérifiant $VM = 0$. Alors $\mathbb{G}(M)$ est un groupe fini sur k, d'ordre p^r, tel que $V_{\mathbb{G}(M)} = 0$.*

(1) Notons $M = \mathbb{M}(G)$. Comme tout morphisme de groupes formels commute au Verschiebung, si $V_G = 0$ alors $VM = 0$. D'après 4.5, le module M s'identifie à $t_{G^\vee}(k)$. Par ailleurs $F_{G^\vee} = (V_G)^\vee = 0$, i.e. $G^\vee$ est de hauteur 1 et son algèbre B_G est de la forme $k[x_1, \dots, x_r]/(x_1^p, \dots, x_r^p)$. En particulier $t_{G^\vee}(k) = (I_{G^\vee}/I_{G^\vee}^2)^*$ est un k-espace vectoriel de dimension r.

(2) Notons $G = \mathbb{G}(M)$. Comme $VM = 0$, on a $pM = 0$ donc M est un $k[F]$-module, de dimension r sur k. Pour tout k-algèbre finie R, on a $G(R) = \mathrm{Hom}_{D_k}(M, \mathrm{CW}(R))$. Comme le noyau de V dans CW est formé des covecteurs de la forme $(\dots, 0, a_0)$, on voit que $G(R) = \mathrm{Hom}_{k[F]}(M, R)$ où R est muni de la structure de $k[F]$-module via $Fy = y^p$. Maintenant soit $u_1, \dots, u_r$ une base de M sur k, et posons $Fu_j = \sum a_{i,j} u_j$ avec $a_{i,j} \in k$. Si $\eta : M \to R$ est une forme k-linéaire, elle définit un élément de $G(R)$ ssi $\eta(Fu_j) = F\eta(u_j)$ pour tout j, i.e. $y_j^p = \sum a_{i,j} y_j$ en notant $y_j = \eta(u_j)$. Ceci montre que $B_G \simeq k[x_1, \dots, x_r]/(x_j^p - \sum a_{i,j} x_j)_{1 \leqslant j \leqslant r}$ qui est de dimension p^r. Comme enfin l'addition dans $G(R)$ est induite par l'addition dans R, on voit que le coproduit dans B_G est défini par $\Delta x_j = x_j \widehat{\otimes} 1 + 1 \widehat{\otimes} x_j$, i.e. G est un sous-groupe de $\mathbb{G}_a^r$. Il s'ensuit que $V_G = 0$.

4.7 Théorème$|_{\text{étale}}$ (III.3.4)

Pour prouver le théorème 3.1.1 pour les p-groupes formels étales, il nous reste à montrer :

(1) *Si G est un p-groupe fini étale d'ordre p^r, alors $\mathbb{M}(G)$ est un $W(k)$-module de longueur r.*

(2) *Pour tout p-groupe formel étale G, le morphisme d'adjonction $G \to \mathbb{G}(\mathbb{M}(G))$ est un isomorphisme.*

(3) *Pour tout D_k-module $W[F]$-profini étale M, le morphisme d'adjonction $M \to \mathbb{M}(\mathbb{G}(M))$ est un isomorphisme.*

(1) Si G est simple, c'est vrai d'après 4.6. Le cas général s'en déduit par récurrence sur la longueur de G, utilisant le fait que $\mathbb{M}$ est exact sur les groupes étales, cf 4.4.

(2) Un passage à la limite que nous ne détaillons pas (voir III.2.6) permet de se ramener à montrer le résultat pour G fini. Notons $u : G \to \mathbb{G}(\mathbb{M}(G))$ le morphisme d'adjonction. Si G est simple, d'ordre p^r, alors il n'est pas de type multiplicatif donc $V_G = 0$. D'après 4.6 le module $\mathbb{M}(G)$ est annulé par V et $\mathbb{G}(\mathbb{M}(G))$ est un groupe d'ordre p^r. Si u n'est pas un isomorphisme, alors $u = 0$ donc $\mathbb{M}(u) = 0$. Ceci n'est pas possible, car $\mathbb{M}(u) : \mathbb{M}(\mathbb{G}(\mathbb{M}(G))) \to \mathbb{M}(G)$ est un épimorphisme (voir 6.3.2) et $\mathbb{M}(G) \neq 0$. Donc u est un isomorphisme. Le cas général se démontre par récurrence sur la longueur de G : comme $\mathbb{M}$ est exact sur les groupes étales, à une suite exacte $0 \to G' \to G \to G'' \to 0$ correspond une suite exacte $0 \to \mathbb{M}(G'') \to \mathbb{M}(G) \to \mathbb{M}(G') \to 0$. On trouve un diagramme commutatif à lignes exactes

$$\begin{array}{ccccccccc} 0 & \longrightarrow & G' & \longrightarrow & G & \longrightarrow & G'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle u_{G'}} & & \downarrow{\scriptstyle u_G} & & \downarrow{\scriptstyle u_{G''}} & & \\ 0 & \longrightarrow & \mathbb{GM}G' & \longrightarrow & \mathbb{GM}G & \longrightarrow & \mathbb{GM}G''. & & \end{array}$$

Si $u_{G'}$ et $u_{G''}$ sont des isomorphismes, alors u_G l'est.

(3) La démonstration est à peine plus compliquée que celle de (2) et nous l'omettons. (Elle est un peu plus compliquée car on ne sait pas que $\mathbb{G}$ est exact sur les modules étales.)

4.8 Isomorphismes $\operatorname{coker} F_M = t_G^*(k)$ (III.4.2)

Le titre de cette sous-section est bien « Isomorphismes » car on y énonce deux résultats : le premier porte sur un groupe formel G et son module $\mathbb{M}(G)$, et le second porte sur un module de Dieudonné M et le groupe associé $\mathbb{G}(M)$. Nous admettrons ces deux résultats. La preuve du premier est un calcul assez volumineux (cf III.4.1, III.4.2) mais celle du second n'est pas difficile (III.4.3).

4.8.1 Isomorphisme $\operatorname{coker} F_{\mathbb{M}(G)} = t_G^*(k)$. Soit G un p-groupe formel sur k, $B = B_G$ son algèbre affine et $I = I_G$ l'idéal d'augmentation. On rappelle que $t_G^*(k) = I/\overline{I^2}$ où $\overline{I^2}$ est l'adhérence de I^2 (voir I.8.5), et que celui-ci possède une structure de $k[V]$-module topologique (voir I.8.7). Par ailleurs, si $b = (\ldots, b_{-n}, \ldots, b_{-1}, b_0) \in \mathbb{M}(G)$ alors les composantes b_{-n} appartiennent à I (voir 4.5). On peut alors énoncer :

Si G est un p-groupe formel sur k, l'application $\eta_G : \mathbb{M}(G) \to t_G^*(k)$ qui à $b = (\ldots, b_{-n}, \ldots, b_{-1}, b_0)$ associe l'image de b_0 dans $t_G^*(k)$ est une application D_k-linéaire continue surjective de noyau $F\mathbb{M}(G)$.

Ce résultat a le corollaire immédiat suivant :

4.8.2 *Si G est un p-groupe formel sur k tel que $F_G = 0$, alors $F\mathbb{M}(G) = 0$ et $\mathbb{M}(G)$ s'identifie canoniquement à $t_G^*(k)$. En particulier, si G est un p-groupe fini d'ordre p^r tel que $F_G = 0$, alors $\mathbb{M}(G)$ est un k-espace vectoriel de dimension r.*

4.8.3 Isomorphisme $t_{\mathbb{G}(M)}(k) \to \operatorname{coker}(F_M)^*$. Nous commençons par définir l'isomorphisme dont il est question. Soit M un D_k-module $W[F]$-profini et soit $G = \mathbb{G}(M)$. Soit $k[\epsilon]$ l'anneau des nombres duaux sur k et $\pi : k[\epsilon] \to k$, $\epsilon \mapsto 0$. On sait que $t_G(k) = \ker(G(\pi) : G(k[\epsilon]) \to G(k))$. Il est immédiat de voir que

$$\ker \widehat{\mathrm{CW}}_k(\pi) = \widehat{\mathrm{CW}}_k(\epsilon k[\epsilon]) = \widehat{\mathrm{CW}}_k^{\mathrm{c}}(k[\epsilon]).$$

Comme de plus $\widehat{\mathrm{CW}}_k^{\mathrm{c}}(k[\epsilon])$ est annulé par F, on a

$$t_G(k) = \mathrm{Homc}_{D_k}(M, \widehat{\mathrm{CW}}_k^{\mathrm{c}}(k[\epsilon])) = \mathrm{Homc}_{D_k}(M/FM, \widehat{\mathrm{CW}}_k^{\mathrm{c}}(k[\epsilon])).$$

Via cette identification, à $u \in t_G(k)$ est associé un morphisme continu $\widehat{u} : M/FM \to \widehat{\mathrm{CW}}^{\mathrm{c}}_k(k[\epsilon])$. Pour tout $a \in M/FM$, le covecteur $\widehat{u}(a)$ est de la forme $(\ldots, \mu_{-n}\epsilon, \ldots, \mu_{-1}\epsilon, \mu_0\epsilon)$. Nous noterons $\xi_M(u) : M/FM \to k$ l'application qui envoie a sur μ_0 ; c'est une forme linéaire continue, i.e. un élément du dual topologique $(M/FM)^*$. On peut alors énoncer :

L'application $\xi_M : t_{\mathbb{G}(M)}(k) \to (M/FM)^*$ est un isomorphisme de k-espaces vectoriels.

4.9 Exactitude de $\mathbb{M}$ sur les groupes connexes (III.4.2)

La restriction de $\mathbb{M}$ à la catégorie des k-groupes formels connexes est un foncteur exact.

Il suffit de montrer que si $G' \to G$ est un monomorphisme de k-groupes formels connexes, alors $\mathbb{M}(G) \to \mathbb{M}(G')$ est surjective. Le morphisme entre algèbres affines $B_G \to B_{G'}$ est surjectif, car G, G' sont limites de leurs noyaux de multiplication par p^n et pour tout n le morphisme ${}_{p^n}G' \to {}_{p^n}G$ est un monomorphisme de k-groupes finis, donc une immersion fermée. Il en découle que $t^*_G(k) \to t^*_{G'}(k)$ est surjectif. Les morphismes η de 4.8.1 s'insèrent dans un diagramme commutatif :

$$\begin{array}{ccc} \mathbb{M}(G) & \longrightarrow & \mathbb{M}(G') \\ \downarrow{\scriptstyle \eta_G} & & \downarrow{\scriptstyle \eta_{G'}} \\ t^*_G(k) & \longrightarrow & t^*_{G'}(k). \end{array}$$

On en déduit que l'application $\mathbb{M}(G) \to t^*_{G'}(k) \simeq \mathbb{M}(G')/F\mathbb{M}(G')$ est surjective. Notons $N \subset \mathbb{M}(G')$ l'image de $\mathbb{M}(G)$; c'est un sous-D_k-module fermé qui se surjecte sur $\mathbb{M}(G')/F\mathbb{M}(G')$. Comme $\mathbb{M}(G')$ est connexe, le Frobenius F y est localement topologiquement nilpotent et on en déduit que $N = \mathbb{M}(G')$, c'est-à-dire $\mathbb{M}(G) \to \mathbb{M}(G')$ est surjective.

4.10 Théorème$|_{\text{connexe}}$ (III.4.4)

Pour prouver le théorème 3.1.1 pour les p-groupes formels connexes, il nous reste à montrer :

(1) *Si G est un p-groupe fini connexe d'ordre p^r, alors $\mathbb{M}(G)$ est un $W(k)$-module de longueur r.*

(2) *Pour tout p-groupe formel connexe G, le morphisme d'adjonction $G \to \mathbb{G}(\mathbb{M}(G))$ est un isomorphisme.*

(3) *Pour tout D_k-module $W[F]$-profini connexe M, le morphisme d'adjonction $M \to \mathbb{M}(\mathbb{G}(M))$ est un isomorphisme.*

(1) Si G est un p-groupe fini connexe simple, on a $F_G = 0$ et le résultat provient de 4.8.2. Le résultat dans le cas général s'en déduit par récurrence sur r, utilisant le fait que $\mathbb{M}$ est exact, voir 4.9.

Nous allons montrer que la preuve de (2) et (3) se ramène aux cas où $F^n_G = 0$ et $F^n_M = 0$.

Pour tout k-groupe formel connexe, on a $G = \varinjlim G_n$ où $G_n = \ker(F^n_G)$. On a donc

$$\mathbb{M}(G) = \mathrm{Hom}_{kGr}(G, \widehat{\mathrm{CW}}_k) = \mathrm{Hom}_{kGr}(\varinjlim G_n, \widehat{\mathrm{CW}}_k) = \varprojlim \mathrm{Hom}_{kGr}(G_n, \widehat{\mathrm{CW}}_k) = \varprojlim \mathbb{M}(G_n).$$

Par ailleurs, comme $\mathbb{M}$ est exact on a $\mathbb{M}(G_n) = \mathbb{M}(G)/F^n\mathbb{M}(G)$.

Pour tout D_k-module $W[F]$-profini connexe M, on a $M = \varprojlim M_n$ où $M_n = M/F^nM$. Si R est une k-algèbre finie, son radical est nilpotent donc il existe un entier r tel que $F^r\widehat{\mathrm{CW}}^{\mathrm{c}}(R) = 0$. Comme M est connexe, on a :

$$\mathbb{G}(M)(R) = \mathrm{Homc}_{D_k}(M, \widehat{\mathrm{CW}}^{\mathrm{c}}(R)) = \mathrm{Homc}_{D_k}(M/F^rM, \widehat{\mathrm{CW}}^{\mathrm{c}}(R)) = \varinjlim \mathrm{Homc}_{D_k}(M_n, \widehat{\mathrm{CW}}^{\mathrm{c}}(R)).$$

Ainsi $\mathbb{G}(M) = \varinjlim \mathbb{G}(M_n)$. Comme par ailleurs $\mathbb{G}$ est exact à gauche, on voit que $\mathbb{G}(M_n) = (\mathbb{G}(M))_n$. Pour montrer que $G \to \mathbb{G}(\mathbb{M}(G))$ et $M \to \mathbb{M}(\mathbb{G}(M))$ sont des isomorphismes, on peut donc supposer que $G = G_n$ et $M = M_n$, respectivement.

(2) On procède par récurrence sur l'entier n tel que $F_G^n = 0$. Si $n = 1$ i.e. $F_G = 0$, alors $F\mathbb{M}(G) = 0$ et $F_{\mathbb{G}(\mathbb{M}(G))} = 0$. La source et le but de $u_G : G \to \mathbb{G}(\mathbb{M}(G))$ sont des groupes de hauteur 1 et il suffit donc de démontrer que u_G induit un isomorphisme sur les espaces tangents. Or $t_G(k)$ est isomorphe au dual topologique de $\mathbb{M}(G)$ d'après 4.8.2, et $t_{\mathbb{G}(\mathbb{M}(G))}$ également d'après 4.8.3 ; on peut vérifier que ces isomorphismes sont bien compatibles à u_G. Si $n \geqslant 2$, on considère la suite exacte :

$$0 \longrightarrow \ker(F_G) \longrightarrow G \longrightarrow \mathrm{im}(F_G) \longrightarrow 0.$$

On en déduit que u_G est un isomorphisme en utilisant l'hypothèse de récurrence pour $\ker(F_G)$ et $\mathrm{im}(F_G)$ et l'exactitude de $\mathbb{M}$, exactement comme pour la preuve de (2) dans 4.7.

(3) La preuve est similaire et laissée en exercice.

5 Exemples

5.1 Groupes finis unipotents. Si G est fini et unipotent, il est annulé par V^m pour un certain m ; on voit alors que tout morphisme de groupes formels $f : G \to \widehat{\mathrm{CW}}_k$ se factorise par le noyau de V^m dans $\widehat{\mathrm{CW}}_k$, c'est-à-dire le groupe W_m des vecteurs de Witt de longueur m.

5.2 Les groupes $W_{m,n}$. Soient $m, n \geqslant 1$ des entiers. Le noyau de V^m dans $\widehat{\mathrm{CW}}_k$ est le groupe W_m des vecteurs de Witt. Notons $W_{m,n}$ le noyau de F^n dans W_m. Alors par construction $V^m = F^n = 0$ dans $W_{m,n}$, et si G est un groupe tel que $(V_G)^m = (F_G)^n = 0$, on a $\mathbb{M}(G) = \mathrm{Hom}_{k\text{-Gr}}(G, \widehat{\mathrm{CW}}_k) = \mathrm{Hom}_{k\text{-Gr}}(G, W_{m,n})$. Par exemple,

$$\mathbb{M}(W_{m,n}) = \mathrm{End}_{k\text{-Gr}}(W_{m,n})$$

et on peut montrer que ceci est $D_k/(D_kF^m + D_kV^n)$. Par exemple,

$$\mathbb{M}(\alpha_{p^n}) = D_k/(D_kF^n + D_kV) = W(k)[F]/(F^n) = k[F]/(F^n)$$

en notant que $p = FV = 0$ dans ce module. Par ailleurs, on a $(W_{m,n})^\vee = W_{n,m}$. Par exemple, $\alpha_{p^n} = W_{1,n}$ et $(\alpha_{p^n})^\vee = W_{1,n}^\vee = W_{n,1} = \ker(F : W_n \to W_n)$.

5.3 Le groupe $\mathbb{Z}/p^n\mathbb{Z}$. En utilisant l'isogénie d'Artin-Schreier-Witt

$$0 \longrightarrow (\mathbb{Z}/p^n\mathbb{Z})_k \longrightarrow W_{n,k} \stackrel{F-\mathrm{id}}{\longrightarrow} W_{n,k} \longrightarrow 0,$$

on voit facilement que $\mathbb{M}(\mathbb{Z}/p^n\mathbb{Z}) = D_k/(D_kV^n + D_k(F-1))$.

5.4 Le groupe μ_p. Pour les groupes de type multiplicatifs, le calcul de $\mathbb{M}(G)$ en partant de la définition est beaucoup plus délicat. Regardons par exemple le cas $G = \mu_p$. Alors on a $F = 0$ et V est un isomorphisme ; en fait $\mu_p = \mathrm{Spec}(A)$ avec $A = k[z]/(z^p - 1)$ et $V : A \to A$ est l'endomorphisme semi-linéaire qui envoie z sur z et sur k vaut $x \mapsto x^{1/p}$, l'inverse du Frobenius. Comme $F_G = 0$ on voit que $FM = 0$, i.e. si $a \in \mathbb{M}(G)$ est un morphisme $G \to \widehat{\mathrm{CW}}_k$ vu comme covecteur de Witt $a = (\ldots, a_{-n}, \ldots, a_{-1}, a_0)$, on a :

(1) $a_{-n} = V^n(a_0) = \sum (b_i)^{1/p^n} z^i$ où $a_0 := \sum b_i z^i$,

(2) $(a_{-n})^p = 0$ pour tout n,

(3) $a(zz') = a(z) + a(z')$ où l'addition est celle des covecteurs de Witt.

En fait il est clair que la condition (2) pour tout n découle de la condition (2) pour $n = 0$. Malheureusement, les peu engageantes formules d'addition des covecteurs de Witt rendent l'exploitation de la relation (3) difficile.

6 Variance, exactitude et adjonction

6.1 Variance

Soient $\mathcal{C}$ et $\mathcal{D}$ deux catégories. Voici trois définitions de *foncteur contravariant* de $\mathcal{C}$ vers $\mathcal{D}$:

(1) c'est la donnée d'une fonction $F : \mathrm{Ob}(\mathcal{C}) \to \mathrm{Ob}(\mathcal{D})$ et pour chaque $A, B \in \mathrm{Ob}(\mathcal{C})$ de fonctions $F_{A,B} : \mathrm{Hom}_{\mathcal{C}}(A, B) \to \mathrm{Hom}_{\mathcal{D}}(FB, FA)$ satisfaisant les axiomes habituels ;

(2) c'est un foncteur $F : \mathcal{C} \to \mathcal{D}^\circ$;

(3) c'est un foncteur $F : \mathcal{C}^\circ \to \mathcal{D}$.

Bien sûr, dans (1) on note en général F au lieu de $F_{A,B}$, pour simplifier. Quelle que soit la définition utilisée, on note souvent $F : \mathcal{C} \to \mathcal{D}$ un foncteur contravariant, en précisant alors la variance. Si on ne précise pas la variance de $F : \mathcal{C} \to \mathcal{D}$, il s'agit par défaut d'un foncteur covariant, mais il vaut mieux le préciser pour éviter toute ambigüité.

La définition (1) est celle qui me semble la meilleure, car c'est la plus proche de l'intuition que l'on a : un foncteur contravariant est un foncteur qui envoie une flèche $f : A \to B$ dans $\mathcal{C}$ sur une flèche renversée $F(f) : FB \to FA$ dans $\mathcal{D}$. La définition (2) est très proche, mais présente l'inconvénient que son action sur les morphismes s'écrit $F_{A,B} : \mathrm{Hom}_{\mathcal{C}}(A, B) \to \mathrm{Hom}_{\mathcal{D}^\circ}(FA, FB)$; or on a envie de penser à $\mathcal{D}^\circ$ comme étant $\mathcal{D}$ avec flèches renversées et pas vraiment comme une catégorie à part entière. On peut néanmoins considérer (1) et (2) comme équivalentes d'un point de vue formel. La définition (3) est très familière notamment car c'est celle qui est (la plus) utilisée pour les foncteurs de points, mais présente l'inconvénient qu'on doit considérer les flèches à l'envers dans la catégorie de départ. On a coutume de dire que les trois définitions donnent le même objet, mais ce n'est pas tout à fait exact. En fait, le choix de l'une ou l'autre définition a de l'importance, par exemple lorsqu'on parle des propriétés d'exactitude, comme on va le voir.

6.2 Exactitude

Dans la suite, supposons que les catégories considérées possèdent les limites projectives et inductives finies (c'est-à-dire indicées par des ensembles finis). Soit $F : \mathcal{C} \to \mathcal{D}$ un foncteur covariant. On dit que F est *exact à gauche* si pour tout système projectif fini $(A_i)_{i \in I}$ dans $\mathcal{C}$, le morphisme canonique $F(\varprojlim A_i) \to \varprojlim F(A_i)$ est un isomorphisme. On dit parfois que F *transforme les limites projectives finies en limites projectives* ou *commute aux limites projectives finies*. On dit que F est *exact à droite* si pour tout système inductif fini $(A_i)_{i \in I}$ dans $\mathcal{C}$, le morphisme canonique $\varinjlim F(A_i) \to F(\varinjlim A_i)$ est un isomorphisme. On dit parfois que F *transforme les limites inductives finies en limites inductives*, mais on voit bien ici que ce raccourci d'expression fait perdre en précision car le morphisme canonique ne vas pas de $F(\varinjlim A_i)$ vers $\varinjlim F(A_i)$. Il est clair que $F : \mathcal{C} \to \mathcal{D}$ est exact à gauche (resp. à droite) si et seulement si $F^\circ : \mathcal{C}^\circ \to \mathcal{D}^\circ$ est exact à droite (resp. à gauche).

Soit $F : \mathcal{C} \to \mathcal{D}$ un foncteur contravariant dans le sens (2), c'est-à-dire un foncteur covariant $F : \mathcal{C} \to \mathcal{D}^\circ$. On dit alors que F est exact à gauche si pour tout système projectif fini $(A_i)_{i \in I}$ dans $\mathcal{C}$,

le morphisme canonique $\varinjlim F(A_i) \to F(\varprojlim A_i)$ est un isomorphisme ; et on dit que F est exact à droite si pour tout système inductif fini $(A_i)_{i\in I}$ dans $\mathcal{C}$, le morphisme canonique $F(\varinjlim A_i) \to \varprojlim F(A_i)$ est un isomorphisme.

Soit $F : \mathcal{C} \to \mathcal{D}$ un foncteur contravariant dans le sens (3), c'est-à-dire un foncteur covariant $F : \mathcal{C}^\circ \to \mathcal{D}$. Alors c'est tout le contraire : F est exact à gauche si les morphismes $F(\varinjlim A_i) \to \varprojlim F(A_i)$ sont des isomorphismes, et F est exact à droite si les morphismes $\varinjlim F(A_i) \to F(\varprojlim A_i)$ sont des isomorphismes. Donc il faut bien préciser une fois pour toutes ce qu'on entend par foncteur contravariant !

6.3 Adjonction

6.3.1 Définitions et conventions. Soient $F : \mathcal{C} \to \mathcal{D}$ et $G : \mathcal{D} \to \mathcal{C}$ deux foncteurs covariants. On dit que (F, G) est un *couple de foncteurs adjoints* s'il existe des bijections fonctorielles en $A \in \mathcal{C}$ et $B \in \mathcal{D}$:

$$\mathrm{Hom}_{\mathcal{D}}(FA, B) = \mathrm{Hom}_{\mathcal{C}}(A, GB).$$

On dit que F est *adjoint à gauche* de G, et G *adjoint à droite* de F. Un adjoint à gauche est toujours exact à droite : en effet, pour vérifier que la flèche $\varinjlim F(A_i) \to F(\varinjlim A_i)$ est un isomorphisme, comme le foncteur de Yoneda $\mathcal{D} \to \mathrm{Fonct}(\mathcal{D}, \mathrm{Ens})$ est pleinement fidèle il suffit de vérifier que l'application induite $\mathrm{Hom}_{\mathcal{D}}(F(\varinjlim A_i), B) \to \mathrm{Hom}_{\mathcal{D}}(\varinjlim F(A_i), B)$ est un isomorphisme de foncteurs en $B \in \mathcal{D}$. Or, on a :

$$\begin{aligned}
\mathrm{Hom}_{\mathcal{D}}(F(\varinjlim A_i), B) &= \mathrm{Hom}_{\mathcal{C}}(\varinjlim A_i, GB) \text{ par adjonction,} \\
&= \varprojlim \mathrm{Hom}_{\mathcal{C}}(A_i, GB) \text{ par définition de } \varinjlim \text{ dans } \mathcal{C}, \\
&= \varprojlim \mathrm{Hom}_{\mathcal{D}}(FA_i, B) \text{ par adjonction,} \\
&= \mathrm{Hom}_{\mathcal{D}}(\varinjlim F(A_i), B) \text{ par définition de } \varinjlim \text{ dans } \mathcal{D}.
\end{aligned}$$

On montre de même qu'un adjoint à droite est toujours exact à gauche.

Soient $F : \mathcal{C} \to \mathcal{D}^\circ$ et $G : \mathcal{D}^\circ \to \mathcal{C}$ deux foncteurs contravariants, au sens (2) et (3). On dit que (F, G) est un *couple de foncteurs adjoints à droite* s'il existe des bijections fonctorielles en $A \in \mathcal{C}$ et $B \in \mathcal{D}^\circ$:

$$\mathrm{Hom}_{\mathcal{D}}(B, FA) = \mathrm{Hom}_{\mathcal{C}}(A, GB).$$

Dans ce cas, F et G sont exacts à gauche au sens (3).

Soient $F : \mathcal{C}^\circ \to \mathcal{D}$ et $G : \mathcal{D} \to \mathcal{C}^\circ$ deux foncteurs contravariants, au sens (3) et (2). On dit que (F, G) est un *couple de foncteurs adjoints à gauche* s'il existe des bijections fonctorielles en $A \in \mathcal{C}^\circ$ et $B \in \mathcal{D}$:

$$\mathrm{Hom}_{\mathcal{D}}(FA, B) = \mathrm{Hom}_{\mathcal{C}}(GB, A).$$

Dans ce cas, F et G sont exacts à droite au sens (3).

Il semble donc que la convention (3) pour la définition des foncteurs contravariants permet de garantir en toutes circonstances la règle : « un adjoint à gauche est exact à droite, un adjoint à droite est exact à gauche ».

6.3.2 Une remarque sur les morphismes d'adjonction. La remarque est valable dans le contexte covariant ou le contexte contravariant ; pour simplifier, nous regardons un seul cas. Soient

$F : \mathcal{C} \to \mathcal{D}$ et $G : \mathcal{D} \to \mathcal{C}$ des foncteurs contravariants (peu importe ici en quel sens) adjoints à droite : on a donc des bijections

$$\mathrm{Hom}_{\mathcal{D}}(B, FA) = \mathrm{Hom}_{\mathcal{C}}(A, GB)$$

fonctorielles en A et B. Pour $B = FA$, à id_{FA} correspond par adjonction un morphisme $u_A : A \to GFA$ et pour $A = GB$, à id_{GB} correspond un morphisme $v_B : B \to FGB$. La bijection ci-dessus est alors donnée ainsi : à $p : B \to FA$ on associe $G(p) \circ u_A : A \to GFA \to GB$, et réciproquement à $q : A \to GB$ on associe $F(q) \circ v_B : B \to FGB \to FA$. Le fait que l'on ait bijection implique :

$$F(u_A) \circ v_{FA} = \mathrm{id}_{FA} \quad \text{et} \quad G(v_B) \circ u_{GB} = \mathrm{id}_{GB}\,.$$

En particulier $u_{GB} : GB \to GFGB$ et $v_{FA} : FA \to FGFA$ sont des monomorphismes, alors que $F(u_A) : FGFA \to FA$ et $G(v_B) : GFGB \to GB$ sont des épimorphismes.

7 Rappels sur l'addition des vecteurs de Witt

Cette section est une petite digression, pas strictement nécessaire dans ces notes, sur le calcul des polynômes de Witt. On fixe un nombre premier p. Les polynômes $S_n = S_n(X_0, \dots, X_n; Y_0, \dots, Y_n)$ qui donnent l'addition dans le foncteur des vecteurs de Witt p-typiques sont définis par les égalités

$$S_0^{p^n} + pS_1^{p^{n-1}} + \cdots + p^n S_n = \big(X_0^{p^n} + pX_1^{p^{n-1}} + \cdots + p^n X_n\big) + \big(Y_0^{p^n} + pY_1^{p^{n-1}} + \cdots + p^n Y_n\big).$$

Par exemple, on a $S_0(X_0; Y_0) = X_0 + Y_0$ et

$$S_1(X_0, X_1; Y_0, Y_1) = X_1 + Y_1 + \frac{X_0^p + Y_0^p - (X_0 + Y_0)^p}{p}.$$

Soit $A = \mathbb{Z}[[X_1, X_2, X_3, \dots]]$ l'anneau des séries formelles en un nombre dénombrable de variables, au sens de Bourbaki, Algèbre, Chapitre 4. En particulier $X_1 + X_2 + X_3 + \dots$ est une série formelle autorisée, alors que certains auteurs demandent qu'une série formelle en $X_1, X_2, X_3, \dots$ ait ses composantes homogènes qui soient des *polynômes*. En appliquant Bourbaki, Algèbre commutative, Chap. 9, § 1, no 2, prop. 2, c) avec l'endomorphisme d'anneaux $\sigma : A \to A$ défini par $\sigma(X_i) = (X_i)^p$, on voit qu'il existe une unique suite d'éléments $R_n \in A$ telle que pour tout $n \geqslant 0$ on a :

$$\sum_i (X_i)^{p^n} = R_0^{p^n} + pR_1^{p^{n-1}} + \cdots + p^n R_n.$$

Lorsqu'on a un nombre fini s de variables, on notera $R_n(X_1, \dots, X_s) = R_n(X_1, \dots, X_s, 0, 0, \dots)$. Par exemple, on a $R_0(X_1, \dots, X_s) = X_1 + \cdots + X_s$ et

$$R_1(X_1, \dots, X_s) = \frac{X_1^p + \cdots + X_s^p - (X_1 + \cdots + X_s)^p}{p}.$$

La proposition suivante montre qu'on peut ramener le calcul des S_n à celui des R_n, c'est-à-dire que toutes les congruences p-adiques difficiles de l'addition de vecteurs de Witt sont contenues dans les polynômes R_n.

7.1 Proposition. *Pour tout $n \geqslant 1$, le polynôme S_n est une somme de $2n$ termes :*

$$S_n = R_0 Z_n + R_1 Z_{n-1} + \cdots + R_n Z_0 + R_1 S_{n-1} + R_2 S_{n-2} + \cdots + R_{n-1} S_1,$$

où l'on note $R_i Z_j := R_i(X_j, Y_j)$ et

$$R_i S_j := R_i(R_0 Z_j, \dots, R_j Z_0, R_1 S_{j-1}, \dots, R_{j-1} S_1)$$

le résultat obtenu en évaluant le polynôme R_i en les $2j$ termes de S_j.

Preuve: Notons (T_n) la suite de polynômes définie inductivement par $T_1 = R_0Z_1 + R_1Z_0$ et par le procédé indiqué dans le membre de droite de l'égalité de l'énoncé. Pour démontrer que $S_n = T_n$ pour tout n, il suffit de démontrer que la suite (T_n) vérifie

$$T_0^{p^n} + pT_1^{p^{n-1}} + \cdots + p^nT_n = \big(X_0^{p^n} + pX_1^{p^{n-1}} + \cdots + p^nX_n\big) + \big(Y_0^{p^n} + pY_1^{p^{n-1}} + \cdots + p^nY_n\big),$$

puisque ces égalités déterminent (S_n). Pour $0 \leqslant i \leqslant n$, écrivons :

$$T_i = \sum_{\substack{u+v=i \\ 0\leqslant u,v\leqslant i}} R_uZ_v + \sum_{\substack{u+v=i \\ 1\leqslant u,v\leqslant i-1}} R_uS_v.$$

On convient qu'une somme indicée par l'ensemble vide est nulle ; c'est le cas pour la deuxième somme, pour $i = 0$. Utilisant la définition des polynômes R_n, on trouve :

$$T_i^{p^{n-i}} = \sum_{\substack{u+v=i \\ 0\leqslant u,v\leqslant i}} (R_uZ_v)^{p^{n-i}} + \sum_{\substack{u+v=i \\ 1\leqslant u,v\leqslant i-1}} (R_uS_v)^{p^{n-i}} - \sum_{1\leqslant u\leqslant n-i} p^u(R_uS_i)^{p^{n-i-u}}$$

où la dernière somme est nulle pour $i = n$. Lorsqu'on effectue la sommation $\sum_{i=0}^{n-1} p^i(-)$, on voit que les deux dernières sommes de l'égalité ci-dessus s'annulent. Finalement il reste seulement :

$$\sum_{i=0}^{n} p^iT_i^{p^{n-i}} = \sum_{i=0}^{n} p^i \sum_{\substack{u+v=i \\ 0\leqslant u,v\leqslant i}} (R_uZ_v)^{p^{n-i}} = \sum_{v=0}^{n} p^v \sum_{u=0}^{n-v} p^u(R_uZ_v)^{p^{n-u-v}} = \sum_{v=0}^{n} p^v(X_v^{p^{n-v}} + Y_v^{p^{n-v}}),$$

ce qu'il fallait démontrer. □

7.2 Exemples. Voici les S_n pour $n \geqslant 4$:

$$* \; S_1 = \; R_0Z_1 + R_1Z_0,$$

$$* \; S_2 = \; R_0Z_2 + R_1Z_1 + R_2Z_0 + R_1(R_0Z_1, R_1Z_0),$$

$$\begin{aligned} * \; S_3 = \; & R_0Z_3 + R_1Z_2 + R_2Z_1 + R_3Z_0 \\ & + R_1\big(R_0Z_2, R_1Z_1, R_2Z_0, R_1(R_0Z_1, R_1Z_0)\big) \\ & + R_2\big(R_0Z_1, R_1Z_0\big), \end{aligned}$$

$$\begin{aligned} * \; S_4 = \; & R_0Z_4 + R_1Z_3 + R_2Z_2 + R_3Z_1 + R_4Z_0 \\ & + R_1\big(R_0Z_3, R_1Z_2, R_2Z_1, R_3Z_0, R_1\big(R_0Z_2, R_1Z_1, R_2Z_0, R_1(R_0Z_1, R_1Z_0)\big), R_2\big(R_0Z_1, R_1Z_0\big)\big) \\ & + R_2\big(R_0Z_2, R_1Z_1, R_2Z_0, R_1(R_0Z_1, R_1Z_0)\big) \\ & + R_3(R_0Z_1, R_1Z_0). \end{aligned}$$