Site cristallin et cristaux de Dieudonné

Matthieu Romagny, le 2 mai 2012

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

Table des matières

1 Pourquoi le site cristallin ?

1.1 Pour quoi faire ?

Voici quelques-unes des motivations qui ont mené à la construction de la cohomologie cristalline d'une variété projective X définie sur un corps algébriquement clos k.

Lorsque k est le corps des complexes et X est lisse, Grothendieck a montré que l'hypercohomologie $\mathbb{H}^*(X, \Omega^*)$ du complexe de de Rham de X est isomorphe à la cohomologie singulière de X à coefficients complexes. Lorsque X est singulière, on peut choisir un plongement $X \hookrightarrow Y$ dans une variété lisse et considérer le complexe $(\Omega_Y^*)^{\wedge}_{/X}$, complété du complexe de de Rham de Y le

long de X. Deligne a montré que l'hypercohomologie de ce complexe ne dépend pas du plongement choisi. Grothendieck a alors posé la question de définir un site naturellement associé à X dont la cohomologie redonne la cohomologie précédente ; il a introduit une première approximation du site cristallin pour répondre à cette question : le *site infinitésimal*, dont les ouverts sont les paires composées d'un ouvert $U \subset X$ et d'une immersion fermée nilpotente $U \hookrightarrow T$. Sur un corps de caractéristique $p > 0$, pour donner une définition de cohomologie de de Rham, il faut en plus munir les idéaux des immersions $U \hookrightarrow T$ d'une structure de puissances divisées ; ce point est rapidement discuté ci-dessous.

Supposons maintenant k de caractéristique $p > 0$ et X lisse. Pour tout premier $\ell \neq p$, on dispose alors des groupes de cohomologie ℓ-adique $H^i_\ell(X) = H^i(X, \mathbb{Q}_\ell)$. Si X est la fibre spéciale d'un schéma propre et lisse $\mathcal{X}$ sur l'anneau des vecteurs de Witt $W(k)$ et si on fixe un plongement $W(k) \hookrightarrow \mathbb{C}$, on peut par ailleurs considérer les groupes de cohomologie ℓ-adique $H^i_\ell(\mathcal{X}_\mathbb{C}) = H^i(\mathcal{X}_\mathbb{C}, \mathbb{Q}_\ell)$ et les groupes de cohomologie singulière $H^i_{\text{sing}}(\mathcal{X}_\mathbb{C}) = H^i(\mathcal{X}_\mathbb{C}, \mathbb{Z})$. On sait que $H^i_\ell(X) \simeq H^i_\ell(\mathcal{X}_\mathbb{C})$, grâce aux théorèmes de changement de base dans la cohomologie étale, et que $H^i_\ell(\mathcal{X}_\mathbb{C}) \simeq H^i_{\text{sing}}(\mathcal{X}_\mathbb{C}) \otimes \mathbb{Q}_\ell$, grâce au théorème de comparaison entre la cohomologie étale et la cohomologie complexe. Ceci indique que de l'information sur X est contenue dans le groupe abélien $H^i_{\text{sing}}(\mathcal{X}_\mathbb{C})$. S'agissant de la torsion de ce groupe, on note que la tensorisation par $\mathbb{Q}_\ell$ tue toute la torsion première à ℓ, mais en faisant varier $\ell \neq p$ seule la partie de p-torsion ne peut pas être obtenue. Il est naturel de penser que la p-torsion de $H^i_{\text{sing}}(\mathcal{X}_\mathbb{C})$ est reliée à X, mais elle n'est pas accessible par les résultats précédents car ils ne sont plus valables lorsque $\ell = p$. La cohomologie cristalline fournit des groupes de cohomologie qui révèlent cette information de p-torsion.

1.2 Pourquoi c'est comme ça ?

Indiquons très brièvement comment vient l'idée d'introduire des puissances divisées sur les idéaux des immersions nilpotentes $U \hookrightarrow T$ du site infinitésimal. Reprenons le problème de définir un site naturellement associé à X et dont la cohomologie calcule $\mathbb{H}^*(X, (\Omega^*_Y)^\wedge_{/X}))$, maintenant lorsque le corps k est de caractéristique $p > 0$. Dans ce cas, le groupe d'hypercohomologie obtenu dépend de $X \hookrightarrow Y$, principalement car le lemme de Poincaré, qui nécessite d'inverser des factorielles, n'est plus vrai. Pour rétablir une forme de ce lemme, il faut introduire les puissances divisées qui permettent de faire des développements de Taylor. Une fois la définition du site cristallin convenablement modifiée, on démontre un lemme de Poincaré cristallin, on a une bonne définition de cohomologie de de Rham qui se calcule par la cohomologie cristalline ; ceci se trouve dans la thèse de Berthelot.

2 Anneaux à puissances divisées

2.1 Définitions

Comme on l'a expliqué, on veut faire du calcul différentiel dans une A-algèbre B, par quoi on entend, choisir un ensemble d'éléments « infinitésimaux » dans B pour lesquels on peut écrire une formule de Taylor :

$$P(x+h) = P(x) + P'(x)h + P''(x)h^{[2]} + \cdots + P^{(n)}(x)h^{[n]},\ x \in B,\ h \text{ infinitésimal.}$$

Si on est sur une $\mathbb{Q}$-algèbre, alors $h^{[n]} = h^n/n!$. Les infinitésimaux s'ajoutent et sont stables par multiplication par des éléments de B, i.e. ils forment un idéal. Dans la formule de Taylor, la puissance divisée d'un infinitésimal est un infinitésimal. Enfin, le souhait de pouvoir composer les développements limités nécessite de savoir composer les puissances divisées. On arrive à la définition suivante

des puissances divisées sur un idéal, dont l'idée essentielle est qu'il s'agit d'une famille d'applications qui vérifie toutes les propriétés formelles de la famille $\{x \mapsto x^n/n!\}_{n\geqslant 1}$.

2.1.1 Définition. Soit $I \subset A$ un idéal. Une structure de *puissances divisées* sur I est une famille d'applications $\gamma_n : I \to I$, $n \geqslant 1$, telles que :

(1) $\gamma_1(x) = x$; on pose aussi $\gamma_0(x) = 1$,

(2) $\gamma_n(\lambda x) = \lambda^n \gamma_n(x)$,

(3) $\gamma_m(x)\gamma_n(x) = (\!(m,n)\!)\, \gamma_{m+n}(x)$,

(4) $\gamma_n(x+y) = \sum_{i=0}^{n} \gamma_i(x)\gamma_{n-i}(y)$.

(5) $\gamma_m(\gamma_n(x)) = C_{m,n}\gamma_{mn}(x)$.

où $C_{m,n} := \frac{(mn)!}{m!\,(n!)^m}$ est le nombre de manières de regrouper mn éléments en m paquets de n. Un *anneau à puissances divisées*, ou *PD-anneau*, est un triplet (A, I, γ) où A est un anneau, $I \subset A$ un idéal, et $\gamma = (\gamma_n)_{n\geqslant 1}$ est une structure à puissances divisées sur I. Un *morphisme d'anneaux à puissances divisées*, ou *morphisme de PD-anneaux* $\varphi : (A, I, \gamma) \to (B, J, \delta)$ est un morphisme d'anneaux $\varphi : A \to B$ tel que $\varphi(I) \subset J$ et $\delta_n \circ \varphi = \varphi \circ \gamma_n$ pour tout n.

Pour munir d'une topologie (plate) la catégorie des immersions nilpotentes à puissances divisées $U \hookrightarrow T$ sur un ouvert de Zariski U de X, nous aurons besoin de la notion suivante.

2.1.2 Définition. Soient (A, I, γ) un anneau à puissances divisées et B une A-algèbre. On dit que γ *s'étend à* B s'il existe une structure de puissances divisées $\overline{\gamma}$ sur IB telle que $(A, I, \gamma) \to (B, IB, \overline{\gamma})$ est un morphisme de PD-anneaux.

Le foncteur $A \mapsto (A, 0, 0)$ plonge la catégorie des anneaux comme sous-catégorie pleine de la catégorie des PD-anneaux. Les morphismes de PD-anneaux de la forme $(A, I, \gamma) \to (B, IB, \overline{\gamma})$ sont ceux qui sont représentables par des anneaux, au même sens qu'un morphisme de champs algébriques ou d'espaces algébriques est représentable par des schémas, ou au même sens qu'un morphisme de schémas formels est adique.

2.1.3 Lemme. *Dans la situation de la définition précédente, si γ s'étend alors l'extension est unique. De plus γ s'étend dans chacune des situations suivantes :*

(1) *$IB = 0$,*

(2) *I est principal,*

(3) *$A \to B$ est plat.*

Preuve: Tout élément de IB s'écrit comme une somme finie $\sum_{1\leqslant i\leqslant r} b_i x_i$ avec $b_i \in B$ et $x_i \in I$. Si γ s'étend, les axiomes (3) et (4) des puissances divisées impliquent que

$$\overline{\gamma}(\sum b_i x_i) = \sum_{n_1+\cdots+n_r=n} b_1^{n_1} \dots b_r^{n_r} \gamma_{n_1}(x_1) \dots \gamma_{n_r}(x_r).$$

On voit que cette extension est uniquement déterminée par γ.

(1) est clair car si $IB = 0$ alors l'extension $\overline{\gamma}_n(0) = 0$ marche.

(2) Si $I = (x)$ posons $\overline{\gamma}_n(bx) = b^n\gamma_n(x)$. C'est bien défini, car si $bx = b'x$ i.e. $(b-b')x = 0$, alors

$$b^n\gamma_n(x) - (b')^n\gamma_n(x) = (b^n - (b')^n)\gamma_n(x) = (b^{n-1} + \cdots + (b')^{n-1})(b-b')\gamma_n(x) = 0$$

puisque $\gamma_n(x) \in I = (x)$. On montre ensuite que les axiomes de puissances divisées sont bien vérifiés.

(3) On commence par une remarque. D'après le théorème de Lazard, l'algèbre B est limite inductive de ses sous-A-modules libres de rang fini. En conséquence, si $z \in IB$ s'écrit de deux manières différentes comme somme finie $z = \sum x_i b_i$ et $z = \sum x'_{i'} b'_{i'}$, alors il existe $c_1, \ldots, c_s$ base d'un sous-A-module libre de rang fini de B et des coefficients $a_{i,j}, a'_{i',j} \in A$ tels que $b_i = \sum a_{i,j} c_j$ et $b'_{i'} = \sum a'_{i',j} c_j$ et $y_j = \sum x_i a_{i,j} = \sum x'_{i'} a'_{i',j}$ pour tout j. Définissons maintenant l'extension $\overline{\gamma}$. Soit $z = \sum_{1 \leqslant i \leqslant r} x_i b_i$ un élément de IB. On pose :

$$\overline{\gamma}_n(\sum x_i b_i) = \sum_{e_1 + \cdots + e_r = n} b_1^{e_1} \ldots b_r^{e_r} \gamma_{e_1}(x_1) \ldots \gamma_{e_r}(x_r).$$

Si z possède une autre écriture $z = \sum x'_{i'} b'_{i'}$, on utilise la remarque précédente et ses notations. Pour montrer que $\overline{\gamma}_n(z)$ est bien défini, il suffit de montrer que

$$\sum_{e_1 + \cdots + e_r = n} b_1^{e_1} \ldots b_r^{e_r} \gamma_{e_1}(x_1) \ldots \gamma_{e_r}(x_r) = \sum_{d_1 + \cdots + d_s = n} c_1^{d_1} \ldots c_t^{d_s} \gamma_{d_1}(y_1) \ldots \gamma_{d_s}(y_s).$$

Utilisant les axiomes des puissances divisées, on peut développer le membre de droite en une somme à coefficients dans $\mathbb{Z}[a_{i,j}]$ de termes $c_1^{d_1} \ldots c_t^{d_s} \gamma_{e_1}(x_1) \ldots \gamma_{e_r}(x_r)$. Alors, on observe que les coefficients à droite et à gauche de ces termes coïncident car c'est le cas dans l'anneau $\mathbb{Q}[x_1, \ldots, x_r, c_1, \ldots, c_s, a_{i,j}]$ muni de l'unique structure de puissances divisées sur l'idéal $(x_1, \ldots, x_r)$. □

2.2 Compatibilité

2.2.1 Définition. Soient (A, I, γ) et (B, J, δ) des anneaux à puissances divisées. Soit $A \to B$ un morphisme. On dit que δ est *compatible avec* γ s'il existe une structure d'idéal à puissances divisées $\overline{\gamma}$ sur $J + IB$ telle que les deux morphismes $(A, I, \gamma) \to (B, J + IB, \overline{\gamma})$ et $(B, J, \delta) \to (B, J + IB, \overline{\gamma})$ soient des PD-morphismes.

3 Sites cristallins d'un schéma

On fixe un schéma Σ muni d'un idéal quasi-cohérent à puissances divisées $(\mathcal{I}, \gamma)$. Soit S un Σ-schéma tel que p est localement nilpotent sur S et les puissances divisées γ s'étendent à S. Rappelons que les puissances divisées s'étendent toujours lorsque $\mathcal{I}$ est localement principal, ce qui sera le cas dans les cas qui nous intéressent le plus : $\Sigma = \mathrm{Spec}(\mathbb{Z}_{(p)})$ ou $\Sigma = \mathrm{Spec}(W(k))$ et $\mathcal{I} = (p)$ muni de ses puissances divisées canoniques.

3.1 Sites cristallins

3.1.1 Définition. On note $\mathrm{CRIS}(S/\Sigma, \mathcal{I}, \gamma)$ la catégorie définie ainsi :

(1) les objets sont les quadruplets (U, T, i, δ) où U est un S-schéma, T est un Σ-schéma sur lequel p est nilpotent, $i : U \hookrightarrow T$ est une immersion fermée, et δ est une structure d'idéal à puissances divisées sur l'idéal de $\mathcal{O}_T$ qui définit i, compatible à γ ;

(2) les morphismes $(U', T', i', \delta') \to (U, T, i, \delta)$ sont les paires (u, v) composées d'un S-morphisme $u : U' \to U$ et un Σ-morphisme $v : T' \to T$ commutant aux puissances divisées (i.e. un PD-

morphisme) tels que $v \circ i' = i \circ u$. On dit que ce morphisme est *cartésien* si le carré

$$\begin{array}{ccc} U' & \overset{i'}{\hookrightarrow} & T' \\ {\scriptstyle u}\downarrow & & \downarrow{\scriptstyle v} \\ U & \overset{i}{\hookrightarrow} & T \end{array}$$

est cartésien.

Le fait que p soit nilpotent dans $\mathcal{O}_T$ assure que l'immersion $U \hookrightarrow T$ est nilpotente. S'il ne faut retenir dans la notation qu'un élément d'un ouvert (U, T, i, δ), ce sera T.

3.1.2 Définition. Soit $\mathcal{T}_i$ l'ensemble des morphismes (u, v) de $\mathrm{CRIS}(S/\Sigma, \mathcal{I}, \gamma)$ tels que

(i) (u, v) est cartésien, et

(ii) v est une immersion ouverte ($i = 1$), un morphisme étale ($i = 2$), un morphisme plat localement de présentation finie ($i = 3$), un morphisme plat ($i = 3$).

On appelle *topologie de Zariski*, resp. *étale*, resp. *fppf*, resp. *fpqc*, la topologie sur $\mathrm{CRIS}(S/\Sigma, \mathcal{I}, \gamma)$ engendrée par les familles surjectives de morphismes de $\mathcal{T}_1$ et les familles finies surjectives de morphismes de $\mathcal{T}_i$ dont le but et la source sont affines. Si τ est l'une de ces topologies, on note $\mathrm{CRIS}(S/\Sigma, \mathcal{I}, \gamma)_\tau$ le site obtenu et $(S/\Sigma, \mathcal{I}, \gamma)_{\mathrm{CRIS},\tau}$ le topos correspondant.

3.1.3 Remarques. (1) On notera que pour vérifier les axiomes d'une topologie de Grothendieck, il faut pouvoir changer de base dans un recouvrement. Ceci est possible car tout morphisme $(u, v) : (U', T', i', \delta') \to (U, T, i, \delta)$ de $\mathcal{T}_i$ étant plat, l'existence d'extensions des puissances divisées (lemme 2.1.3) permet de voir qu'un produit fibré

$$(U', T', i', \delta') \times_{(U,T,i,\delta)} (U_1, T_1, i_1, \delta_1)$$

est représentable dans $\mathrm{CRIS}(S/\Sigma, \mathcal{I}, \gamma)$ par $U' \times_U U_1 \hookrightarrow T' \times_T T_1$.

(2) Par la théorie générale, la donnée d'un faisceau sur $\mathrm{CRIS}(S/\Sigma, \mathcal{I}, \gamma)_\tau$ est équivalente à la donnée d'un faisceau $F_{(U,T,\delta)}$ sur le petit site τ de T, pour tout ouvert (U, T, δ), et d'un morphisme de faisceaux $\rho_{(u,v)} : v^{-1}F_{(U,T,\delta)} \longrightarrow F_{(U',T',\delta')}$ pour tout morphisme $(u, v) : (U', T', \delta') \to (U, T, \delta)$ entre ouverts (où v^{-1} est le foncteur image inverse sur la catégorie des faisceaux d'ensembles), tels que :

(i) $\rho_{(\mathrm{id},\mathrm{id})} = \mathrm{id}$,

(ii) $\rho_{(uu',vv')} = \rho_{(u',v')} \circ (v')^{-1}\rho_{(u,v)}$,

(iii) $\rho_{(u,v)}$ est un isomorphisme si $(u, v) \in \mathcal{T}_i$.

3.2 Faisceaux fondamentaux

3.2.1 Définitions. (1) Le *faisceau structural* de $(S/\Sigma, \mathcal{I}, \gamma)_\tau$ est le faisceau $\mathcal{O}_{S/\Sigma}$ défini par

$$\Gamma((U, T, \delta), \mathcal{O}_{S/\Sigma}) = \Gamma(T, \mathcal{O}_T).$$

(2) L'*idéal à puissances divisées canonique* est le faisceau $\mathcal{I}_{S/\Sigma}$ défini par

$$\Gamma((U, T, \delta), \mathcal{I}_{S/\Sigma}) = \ker(\Gamma(T, \mathcal{O}_T) \to \Gamma(U, \mathcal{O}_U)).$$

(3) Le *faisceau des inversibles* est le faisceau $\mathcal{O}^\times_{S/\Sigma}$ défini par $\Gamma((U, T, \delta), \mathcal{O}^\times_{S/\Sigma}) = \Gamma(T, \mathcal{O}_T)^\times$.

On voudrait maintenant définir une sorte d'immersion fermée de S dans $(S/\Sigma, \mathcal{I}, \gamma)$. On va définir cela comme un morphisme de topos ; rappelons qu'un morphisme de topos noté $u : E \to E'$ est un triplet $u = (u_*, u^*, \varphi)$ où $u_* : E \to E'$, $u^* : E' \to E$ sont des foncteurs, avec u^* exact à gauche (condition de continuité), et φ est un morphisme d'adjonction entre u^* et u_* i.e. un morphisme de bifoncteurs $\varphi_{X',Y} : \mathrm{Hom}_E(u^*X', Y) \simeq \mathrm{Hom}_{E'}(X', u_*Y)$.

3.2.2 Définition. On note $\mathrm{Sch}\,/(S,\gamma)$ la sous-catégorie pleine de $\mathrm{Sch}\,/S$ dont les objets sont les S-schémas S' tels que les puissances divisées γ s'étendent à S'. On note $S_{\gamma,\tau}$ le topos des faisceaux sur $\mathrm{Sch}\,/(S,\gamma)$ pour la topologie τ.

3.2.3 Définition. On appelle *immersion* du topos τ dans le topos cristallin et on note

$$i_{S/\sigma} : S_{\gamma,\tau} \to (S/\Sigma, \mathcal{I}, \gamma)_{\mathrm{CRIS},\tau}$$

le morphisme de topos donné par le couple de foncteurs adjoints définis ainsi :

(1) pour tout faisceau F sur $\mathrm{CRIS}(S/\Sigma, \mathcal{I}, \gamma)$, $i^*_{S/\Sigma}F$ est le faisceau sur $\mathrm{Sch}\,/(S,\gamma)$ défini par $(i^*_{S/\Sigma}F)(U) = F(U,U)$ ce qui a un sens car pour $U \in \mathrm{Sch}\,/(S,\gamma)$, les puissances divisées γ s'étendent à $\mathcal{O}_U$ i.e. les puissances divisées 0 sont compatibles à γ ;

(2) pour tout faisceau G sur $\mathrm{Sch}\,/(S,\gamma)$, $i_{S/\Sigma *}G$ est le faisceau sur $\mathrm{CRIS}(S/\Sigma, \mathcal{I}, \gamma)$ défini par $(i_{S/\Sigma *}G)(U,T,\delta) = G(U)$.

3.2.4 Remarque. Pour tout faisceau G sur $\mathrm{Sch}\,/(S,\gamma)$, on a $i^*_{S/\Sigma} i_{S/\Sigma *} G = G$.

4 Cristaux de modules

On reprend les notations de la section 3 ; en particulier, on rappelle que p est localement nilpotent sur S.

4.1 Définition

Pour prolonger la remarque 3.1.3(2), la donnée d'un « $\mathcal{O}_{S/\Sigma}$-module pour la topologie τ », c'est-à-dire un faisceau de $\mathcal{O}_{S/\Sigma}$-modules sur $\mathrm{CRIS}(S/\Sigma, \mathcal{I}, \gamma)_\tau$, est équivalente à la donnée d'un faisceau de $\mathcal{O}_T$-modules $F_{(U,T,\delta)}$ sur le petit site τ de T, pour tout ouvert (U,T,δ), et d'un morphisme de faisceaux $\rho_{(u,v)} : v^*F_{(U,T,\delta)} \longrightarrow F_{(U',T',\delta')}$ pour tout morphisme $(u,v) : (U',T',\delta') \to (U,T,\delta)$ entre ouverts, où v^* est l'image inverse des faisceaux de modules.

4.1.1 Définition. Un *cristal en $\mathcal{O}_{S/\Sigma}$-modules* est un $\mathcal{O}_{S/\Sigma}$-module Zariski E tel que les morphismes de comparaison $\rho_{(u,v)}$ sont des isomorphismes. On dit que E est *quasi-cohérent, cohérent, localement libre* si pour tout (U,T,δ) le module $F_{(U,T,\delta)}$ vérifie cette propriété.

Dire qu'un faisceau est un cristal signifie donc en quelque sorte que « sa formation commute au changement de base »

Soit G un faisceau abélien sur $S_{\gamma,\tau}$, et notons $\underline{G} = i_{S/\Sigma *}G$ qui est un faisceau abélien sur $\mathrm{CRIS}(S/\Sigma)_\tau$. Dans la suite, nous définirons certains invariants de la forme $\mathbb{R}\mathcal{H}om_{S/\Sigma}(\underline{G}, E)$ ou $\mathcal{E}xt^i(\underline{G}, E)$ associés à G, pour divers faisceaux E. Notons $D^*(\mathrm{Ab}_{S/\Sigma})$, resp. $D^*(\mathcal{O}_{S/\Sigma})$, avec $* \in \{+, -, \varnothing\}$ les catégories dérivées de complexes de faisceaux abéliens sur $\mathrm{CRIS}(S/\Sigma)$, resp. de complexes de $\mathcal{O}_{S/\Sigma}$-modules. Lorsque E est un $\mathcal{O}_{S/\Sigma}$-module (cristal ou non), on a une formule d'adjonction

$$\mathbb{R}\mathcal{H}om_{\mathcal{O}_{S/\Sigma}}(\underline{G} \overset{\mathbb{L}}{\otimes} \mathcal{O}_{S/\Sigma}, E) = \mathbb{R}\mathcal{H}om_{S/\Sigma}(\underline{G}, E)$$

qui montre que $\mathbb{R}\mathcal{H}om_{S/\Sigma}(\underline{G},E)$ est muni d'une structure d'objet de $D^+(\mathcal{O}_{S/\Sigma})$, et ses groupes de cohomologie $\mathcal{E}xt^i(\underline{G},E)$ sont munis d'une structure de $\mathcal{O}_{S/\Sigma}$-module.

Notons maintenant F le Frobenius absolu de S et, pour tout $\mathcal{O}_{S/\Sigma}$-module E, notons $E^{(p)}=F^*E$. Supposons de plus que E est la préimage d'un faisceau sur $\mathrm{CRIS}(\mathbb{F}_p/\mathbb{Z}_p)$, ce qui est le cas pour les trois faisceaux fondamentaux $\mathcal{O}_{S/\Sigma}$, $\mathcal{I}_{S/\Sigma}$ et $i_{S/\Sigma *}\mathcal{O}_S$, et que G est un S-schéma en groupes plat commutatif. Alors on a $E^{(p)}=E$ et le Frobenius $F:G\to G^{(p)}$ induit par fonctorialité un morphisme

$$F:\mathbb{R}\mathcal{H}om_{S/\Sigma}(\underline{G},E)^{(p)}\simeq\mathbb{R}\mathcal{H}om_{S/\Sigma}(\underline{G}^{(p)},E^{(p)})\simeq\mathbb{R}\mathcal{H}om_{S/\Sigma}(\underline{G}^{(p)},E)\longrightarrow\mathbb{R}\mathcal{H}om_{S/\Sigma}(\underline{G},E).$$

De manière analogue, le Verschiebung $V:G^{(p)}\to G$ induit un morphisme

$$V:\mathbb{R}\mathcal{H}om_{S/\Sigma}(\underline{G},E)\to\mathbb{R}\mathcal{H}om_{S/\Sigma}(\underline{G},E)^{(p)}.$$

4.2 Cristaux de modules sur un schéma parfait

Pour les modules quasi-cohérents sur le site Zariski d'un schéma, un rôle particulier est joué par les schémas affines : le foncteur de sections globales induit une équivalence de catégories entre modules quasi-cohérents sur X et $\Gamma(X,\mathcal{O}_X)$-modules. Le rôle analogue pour les cristaux sur le site cristallin d'un schéma est joué par les schémas parfaits, i.e. ceux dont le Frobenius absolu est un isomorphisme. Pour simplifier, voici un énoncé dans le cas d'un schéma *affine* parfait.

4.2.1 Théorème. *Soit A un anneau de caractéristique p parfait, $S=\mathrm{Spec}(A)$, $\Sigma=\mathrm{Spec}(\mathbb{Z}_{(p)})$. Le foncteur sections globales $\Gamma(\mathrm{CRIS}(S/\Sigma),-)$ induit une équivalence de catégories entre la catégorie des cristaux de $\mathcal{O}_{S/\Sigma}$-modules quasi-cohérents et la catégorie des $W(A)$-modules séparés et complets pour la topologie p-adique.*

On a le même énoncé dans le cas d'un schéma parfait S non nécessairement affine.

Preuve: Nous nous contentons de donner un foncteur quasi-inverse. Pour tout entier n, on peut voir qu'il existe une unique structure de puissances divisées sur le noyau de $W_n(\mathbb{Z}_{(p)})\to\mathbb{Z}_{(p)}$; elle est définie par $\gamma_N(Vx)=p^{N-1}/N!V(X^N)$. Alors le schéma $S_n=\mathrm{Spec}(W_n(A))$ est un épaississement à puissances divisées de S. Maintenant soit M un $W(A)$-module séparé et complet pour la topologie p-adique. Pour tout épaississement à puissances divisées $U\hookrightarrow T$, le morphisme $T\to\Sigma$ se factorise par un certain $\mathrm{Spec}(W_n(\mathbb{Z}_{(p)})$ et un dispose d'un morphisme d'épaississements $f:(U,T)\to(S,S_n)$. On peut voir $M_n:=M\otimes_{W(A)}W_n(A)$ comme un module quasi-cohérent sur S_n. Alors le foncteur quasi-inverse associe à M le le cristal E défini sur $U\hookrightarrow T$ par $E_{(U,T)}=f^*M_n$. □

5 Le cristal de Dieudonné selon Berthelot-Breen-Messing

Ici encore, les notations de la section 3 sont en vigueur.

5.1 Le cristal de Dieudonné d'un schéma abélien

5.1.1 Théorème. *Soit $f:A\to S$ un schéma abélien de dimension relative n. Alors, on a :*

(1) $\mathcal{H}om_{S/\Sigma}(\underline{A},\mathcal{O}_{S/\Sigma})=0$,

(2) $\mathcal{E}xt^1_{S/\Sigma}(\underline{A},\mathcal{O}_{S/\Sigma})$ *est un cristal en $\mathcal{O}_{S/\Sigma}$-modules localement libre de rang $2n$,*

(3) $\mathcal{E}xt^2_{S/\Sigma}(\underline{A}, \mathcal{O}_{S/\Sigma})$.

C'est le théorème 2.5.6 de [BBM]. Le cristal $\mathbb{D}(A) = \mathcal{E}xt^1_{S/\Sigma}(\underline{A}, \mathcal{O}_{S/\Sigma})$ muni de ses morphismes F et V décrits plus haut est appelé le *cristal de Dieudonné de A/S*.

5.2 Le cristal de Dieudonné d'un groupe fini

5.2.1 Théorème. *Soit G un groupe fini localement libre sur S. Alors $\mathcal{E}xt^1_{S/\Sigma}(\underline{G}, \mathcal{O}_{S/\Sigma})$ est un cristal en $\mathcal{O}_{S/\Sigma}$-modules localement de présentation finie sur $\mathcal{O}_{S/\Sigma}$.*

Preuve: Il s'agit de [BBM], cor. 3.1.3. L'assertion à démontrer est locale sur S. D'après le théorème de plongement de Raynaud ([BBM], th. 3.1.1), on peut donc supposer que G se plonge dans un schéma abélien projectif A^0 ; notons $A^1 = A^0/G$ le schéma abélien quotient. On a donc une suite exacte

$$0 \longrightarrow G \longrightarrow A^0 \longrightarrow A^1 \longrightarrow 0$$

et, compte tenu de l'annulation de $\mathcal{E}xt^2$ dans le théorème 5.1.1, la suite exacte longue de cohomologie fournit une suite exacte

$$\ldots \longrightarrow \mathcal{E}xt^1_{S/\Sigma}(\underline{A}^1, \mathcal{O}_{S/\Sigma}) \longrightarrow \mathcal{E}xt^1_{S/\Sigma}(\underline{A}^0, \mathcal{O}_{S/\Sigma}) \longrightarrow \mathcal{E}xt^1_{S/\Sigma}(\underline{G}, \mathcal{O}_{S/\Sigma}) \longrightarrow 0.$$

On en déduit le résultat annoncé. □

Le cristal $\mathbb{D}(G) = \mathcal{E}xt^1_{S/\Sigma}(\underline{G}, \mathcal{O}_{S/\Sigma})$ muni de ses morphismes F et V est appelé le *cristal de Dieudonné de G/S*.

5.2.2 Remarque. On montre que le foncteur $\mathbb{D}$ sur les groupes finis localement libres est exact à droite. Plus précisément, si $0 \to G' \to G \to G'' \to 0$ est une suite exacte de groupes finis localement libres sur S, on montre en plongeant G dans un schéma abélien (localement sur S) que la suite $\mathbb{D}(G'') \to \mathbb{D}(G) \to \mathbb{D}(G') \to 0$ est exacte, cf [BBM], 3.1.6.

5.3 Le cristal de Dieudonné d'un groupe p-divisible

5.3.1 Théorème. *Soit G un groupe p-divisible sur S. Alors $\mathcal{E}xt^1_{S/\Sigma}(\underline{G}, \mathcal{O}_{S/\Sigma})$ est un cristal en $\mathcal{O}_{S/\Sigma}$-modules.*

Preuve: C'est [BBM], 3.3.3. On doit montrer que pour tout morphisme $(u, v) : (U', T', \delta') \to (U, T, \delta)$ dans CRIS(S/Σ), le morphisme de comparaison $\rho_{(u,v)}$ est un isomorphisme. Il existe n tel que $p^n \mathcal{O}_T = 0$, donc p^n est nul dans tous les schémas en jeu, puisqu'ils sont tous au-dessus de T. Notons $\Sigma_n \subset \Sigma$ le sous-schéma fermé où $p^n = 0$. Il suffit donc de montrer que le faisceau $\mathcal{E}xt^1_{S/\Sigma}(\underline{G}, \mathcal{O}_{S/\Sigma})_{(U,T,\delta)}$ sur CRIS(U/Σ_n). On voit ainsi qu'on peut se restreindre au site CRIS(S/Σ_n). Soit $m \geqslant n$. Alors

$$p^m : \mathcal{O}_{S/\Sigma} \to \mathcal{O}_{S/\Sigma}$$

est nul, donc aussi

$$p^m : \mathcal{E}xt^q_{S/\Sigma}(\underline{G}, \mathcal{O}_{S/\Sigma}) \to \mathcal{E}xt^q_{S/\Sigma}(\underline{G}, \mathcal{O}_{S/\Sigma})$$

pour tout q. De la suite exacte

$$0 \longrightarrow \underline{G}(m) \longrightarrow \underline{G} \xrightarrow{p^m} \underline{G} \longrightarrow 0,$$

on déduit alors des suites exactes courtes qui s'insèrent dans un diagramme commutatif

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{E}xt^q_{S/\Sigma}(\underline{G},\mathcal{O}_{S/\Sigma}) & \longrightarrow & \mathcal{E}xt^q_{S/\Sigma}(\underline{G}(n+m),\mathcal{O}_{S/\Sigma}) & \longrightarrow & \mathcal{E}xt^{q+1}_{S/\Sigma}(\underline{G},\mathcal{O}_{S/\Sigma}) & \longrightarrow & 0 \\ & & \| & & \downarrow & & \downarrow{\scriptstyle p^m=0} & & \\ 0 & \longrightarrow & \mathcal{E}xt^q_{S/\Sigma}(\underline{G},\mathcal{O}_{S/\Sigma}) & \longrightarrow & \mathcal{E}xt^q_{S/\Sigma}(\underline{G}(n),\mathcal{O}_{S/\Sigma}) & \longrightarrow & \mathcal{E}xt^{q+1}_{S/\Sigma}(\underline{G},\mathcal{O}_{S/\Sigma}) & \longrightarrow & 0 \end{array}$$

On en déduit que $\mathcal{E}xt^1_{S/\Sigma}(\underline{G},\mathcal{O}_{S/\Sigma}) = \mathrm{im}(\mathbb{D}(\underline{G}(n+m)) \to \mathbb{D}(\underline{G}(n)))$. Ce faisceau est simplement $\mathbb{D}(\underline{G}(n))$, par la remarque 5.2.2. On en déduit le théorème d'après 5.2.1. □

Le cristal $\mathbb{D}(G) = \mathcal{E}xt^1_{S/\Sigma}(\underline{G},\mathcal{O}_{S/\Sigma})$ muni de ses morphismes F et V est appelé le *cristal de Dieudonné de G/S*.

5.3.2 Remarque. Si $A \to S$ est un schéma abélien de dimension n, et G le groupe p-divisible associé, on a un isomorphisme canonique $\mathbb{D}(A) \to \mathbb{D}(G)$, voir [BBM], prop. 3.3.7. En particulier, dans ce cas $\mathbb{D}(G)$ est un cristal en modules localement libres de rang égal à la hauteur de G. On montre que ceci est en fait vrai pour tout groupe p-divisible, voir [BBM], 3.3.10.

5.4 Comparaison avec le module de Dieudonné de Fontaine

Supposons de plus que la base S est le spectre d'un corps parfait k ; notons σ le Frobenius de l'anneau de vecteurs de Witt $W(k)$. Pour comparer le cristal de Dieudonné et le module de Dieudonné construit par Fontaine, Berthelot, Breen et Messing construisent une extension canonique $\mathcal{E}_{S/\Sigma}$ de faisceaux sur $\mathrm{CRIS}(S/\Sigma,\mathcal{I},\gamma)_\tau$:

$$0 \longrightarrow \mathcal{O}_{S/\Sigma} \longrightarrow \mathcal{E}_{S/\Sigma} \longrightarrow (\mathrm{CW}_{S/\Sigma})^\sigma \longrightarrow 0,$$

où $\mathrm{CW}_{S/\Sigma}$ désigne le faisceau des covecteurs de Witt. Pour tout faisceau abélien G sur S, le cobord de la suite exacte des $\mathcal{E}xt$ associée à la suite exacte ci-dessus est un morphisme :

$$\mathcal{H}om_{S/\Sigma}(\underline{G},\mathrm{CW}_{S/\Sigma})^\sigma \longrightarrow \mathcal{E}xt^1_{S/\Sigma}(\underline{G},\mathcal{O}_{S/\Sigma}).$$

Si G est un groupe fini ou p-divisible, alors $\mathbb{M}(G) = \mathcal{H}om_{S/\Sigma}(\underline{G},\mathrm{CW}_{S/\Sigma})^\sigma$ s'identifie d'après le théorème 4.2.1 à un $W(k)$-module muni d'actions de F et de V qui n'est autre que le module de Dieudonné de G construit par Fontaine, et $\mathbb{D}(G) = \mathcal{E}xt^1_{S/\Sigma}(\underline{G},\mathcal{O}_{S/\Sigma})$ est le cristal de Dieudonné.

5.4.1 Théorème. *Le morphisme ci-dessus $\mathbb{M}(G)^\sigma \to \mathbb{D}(G)$ est un isomorphisme.*

Il s'agit du théorème 4.2.14 de [BBM].

6 Enveloppes à puissances divisées

Cette section est une note de lecture faite lors de la préparation de mes exposés au CIRM, qui n'a pas été intégrée aux exposés faits au CIRM.

Nous suivons les deux références suivantes : N. Roby, *Lois polynômes et lois formelles en théorie des modules*, Ann. Sci. É.N.S., Sér. 3, 80 no. 3 (1963), p. 213-348, et P. Berthelot, *Cohomologie Cristalline des Schémas de caractéristique $p > 0$*, Springer Lecture Notes 407, 1974.

6.1 Puissances divisées sur un module

6.1.1 Définition. Soit A un anneau commutatif unitaire. Une structure de *puissances divisées* sur un A-module M à valeurs dans une A-algèbre B_0 est une famille d'applications $\gamma_n : M \to B_0$ pour $n \geqslant 0$, telles que pour tous $x, y \in M$, $\lambda \in A$, et m, n entiers :

(1) $\gamma_0(x) = 1$,

(2) $\gamma_n(\lambda x) = \lambda^n \gamma_n(x)$,

(3) $\gamma_m(x)\gamma_n(x) = (\!(m,n)\!)\, \gamma_{m+n}(x)$,

(4) $\gamma_n(x+y) = \sum_{i=0}^{n} \gamma_i(x)\gamma_{n-i}(y)$.

où on a posé $(\!(m,n)\!) = \frac{(m+n)!}{m!\, n!}$.

Notons plus généralement $(\!(m_1, \ldots, m_r)\!) = \frac{(m_1+\cdots+m_r)!}{(m_1)!\ldots(m_r)!}$. On voit que (3) fournit

$$\gamma_{m_1}(x)\ldots\gamma_{m_r}(x) = (\!(m_1, \ldots, m_r)\!)\gamma_m(x)$$

lorsque $m = m_1 + \cdots + m_r$. En particulier $\gamma_1(x)^n = n!\, \gamma_n(x)$.

6.2 Enveloppe à puissances divisées sur un module

Considérons la catégorie $\mathcal{C} = \mathrm{PD}_A(\mathrm{Mod}, \mathrm{Alg})$ dont les objets sont les structures de puissances divisées sur un A-module N variable vers une A-algèbre B variable, notés $(\delta_n : N \to B)_{n\geqslant 0}$ ou plus simplement (B, N, δ). Soit $\mathcal{D} = \mathrm{Mod}$ la catégorie des A-modules, il y a donc un foncteur d'oubli $\omega : \mathcal{C} \to \mathcal{D}$ qui envoie (B, N, δ) sur N.

6.2.1 Proposition. *Le foncteur ω possède un adjoint à gauche noté $M \mapsto (M, \Gamma_A(M), \gamma)$ ou plus succinctement $M \mapsto \Gamma_A(M)$ et appelé* enveloppe à puissances divisées. *On a donc une bijection fonctorielle en (B, N, δ) :*

$$\mathrm{Hom}_{\mathcal{D}}(M, N) = \mathrm{Hom}_{\mathcal{C}}(\Gamma_A(M), (N, B, \delta)).$$

Preuve: Pour chaque $x \in M$ et chaque entier $n \geqslant 0$, on considère une indéterminée $X_{(x,n)}$. L'algèbre $\Gamma(M) = \Gamma_A(M)$ est quotient de l'algèbre de polynômes $A[X_{(x,n)}]_{x\in M, n\geqslant 0}$ par l'idéal engendré par les relations :

(1) $X_{(x,0)} - 1$,

(2) $X_{(\lambda x,n)} - \lambda^n X_{(x,n)}$,

(3) $X_{(x,m)}X_{(x,n)} - (\!(m,n)\!)X_{(x,m+n)}$,

(4) $X_{(x+y,n)} - \sum_{i=0}^{n} X_{(x,i)}X_{(y,n-i)}$.

On note $x^{[n]}$ l'image de $X_{(x,n)}$ dans $\Gamma(M)$. L'application $\gamma_n : M \to \Gamma(M)$ est définie par $x \mapsto x^{[n]}$. Il est facile de vérifier que $\Gamma(M)$ est une algèbre à puissances divisées et qu'elle vérifie la propriété universelle ad hoc. □

6.2.2 Remarques. (1) Par construction, $\Gamma(M)$ est engendrée par les $x^{[n]}$ pour $x \in M$, $n \geqslant 0$. Par ailleurs, d'après les propriétés (2) et (4), pour avoir un système générateur on peut se restreindre aux $x^{[n]}$ avec x dans un système de générateurs de M comme A-module. En revanche, en général on est obligé de considérer tous les entiers n, et il peut arriver que $\Gamma(M)$ ne soit pas une algèbre de type fini même si M est un module de type fini, cf 6.2.4.
(2) Il y a une unique graduation sur $\Gamma(M)$ telle que $\deg(x^{[n]}) = n$ pour tout $x \in M$. On note $\Gamma_n(M)$ le sous-module des éléments homogènes de degré n. On a des isomorphismes canoniques $\Gamma_0(M) = A$ et $\Gamma_1(M) = M$. L'idéal engendré par M dans $\Gamma(M)$ est inclus dans $\Gamma_+(M)$ mais ne lui est pas égal en général.

6.2.3 Une variante. On peut considérer une variante de $\mathcal{C} = \mathrm{PD}_A(\mathrm{Mod}, \mathrm{Alg})$ en considérant la catégorie $\mathcal{C}' = \mathrm{PD}_A(\mathrm{Mod} \subset \mathrm{Alg})$ des (B, N, δ) tels que N est un sous-A-module de B. Avec cette nouvelle catégorie, on a la même enveloppe à puissances divisées.

6.2.4 Cas des $\mathbb{Z}_{(p)}$-modules. Rappelons (voir lemme 7.1) que $v_p(n!) = (n - s(n))/(p-1)$, où $s(n)$ désigne la somme des chiffres de l'écriture p-adique de n. On en déduit immédiatement les faits suivants :

(i) soient $m_1, \ldots, m_r$ entiers non nuls d'écritures p-adiques $m_i = m_{i,0} + m_{i,1}p + \cdots + m_{i,d}p^d$. On peut choisir $d = d(i)$ égal au degré p-adique de m_i, i.e. $m_{i,d} \neq 0$, ou alors d égal au sup des degrés p-adiques, quitte à tolérer certains $m_{i,d}$ nuls. Si pour tout j la somme des $m_{i,j}$ est $\leqslant p-1$, en d'autres termes si lorsqu'on fait la somme des m_i en écriture p-adique il n'y a pas de retenue, alors $v((m_1, \ldots, m_r)) = 0$, voir 7.1(3).

(ii) les seuls entiers n tels que p divise $((i,j))$ pour tous $i, j \neq 0$ avec $i + j = n$ sont les puissances de p. En effet, notons k la valuation de n. Si $n = p^k$, pour $0 < i < n$ on a $v((i, p^k - i)) = k - v(i) > 0$. Sinon, d'après (i) on a $v((p^k, n - p^k)) = 0$, voir 7.1(5).

Supposons que A est une $\mathbb{Z}_{(p)}$-algèbre. On sait que $\Gamma(M)$ est engendré par les $x^{[n]}$ avec x dans un système de générateurs de M. D'après la relation (3) et ce qui précède, on peut en fait se restreindre aux $x^{[p^k]}$. Par exemple, prenons pour A un corps k de caractéristique $p > 0$ et M un A-module libre de rang 1 engendré par un élément x_1. Des relations entre les indéterminées $x_{p^k} := x^{[p^k]}$, il ne reste que celles provenant de $x^n = n!\, x^{[n]}$, soit $(x_{p^k})^p = 0$. On trouve :

$$\Gamma(M) \simeq \frac{k[x_1, x_p, x_{p^2}, \ldots]}{((x_1)^p, (x_p)^p, (x_{p^2})^p, \ldots)} .$$

En particulier ici A est intègre et M est libre ; $\Gamma(M)$ n'est pas de type fini sur k et non réduite, et l'idéal engendré par $M = \Gamma_1(M)$ n'est pas égal à $\Gamma_+(M)$.

6.2.5 Cas des $\mathbb{Q}$-modules. Il y a un morphisme canonique $S(M) \to \Gamma(M)$. En effet, on peut représenter $S(M)$ comme quotient de l'algèbre de polynômes $A[T_{(x,n)}]_{x \in M, n \geqslant 0}$ par l'idéal engendré par les relations :

(1) $T_{(x,0)} - 1$,

(2) $T_{(\lambda x, n)} - \lambda^n T_{(x,n)}$,

(3) $T_{(x,m)} T_{(x,n)} - T_{(x,m+n)}$,

(4) $T_{(x+y,n)} - \sum_{i=0}^{n} (i, n-i) T_{(x,i)} T_{(y,n-i)}$.

Le morphisme d'algèbres $A[T_{(x,n)}] \to A[X_{(x,n)}]$ défini par $T_{(x,n)} \mapsto n!X_{(x,n)}$ passe au quotient en un morphisme $S(M) \to \Gamma(M)$. Si A est une $\mathbb{Q}$-algèbre, ce morphisme est un isomorphisme. Plus généralement, si $S(M)$ est sans $\mathbb{Z}$-torsion, alors $\Gamma(M)$ est la sous-A-algèbre de $S(M) \otimes \mathbb{Q}$ engendrée par les $x^n/n!$ avec $x \in M$. En revanche, sur l'exemple ci-dessus avec $A = M = k$, ce morphisme n'est ni injectif ni surjectif.

6.3 Enveloppe à puissances divisées sur un idéal

En gros, l'utilité de l'enveloppe à puissances divisées est la suivante. Replaçons-nous dans le contexte de la section 1. Soit $X \hookrightarrow Y$ une immersion dans une variété lisse. En général, l'idéal qui définit X comme sous-schéma fermé de Y ne possède pas de structure de puissances divisées. Il convient alors d'ajouter des puissances divisées de manière formelle, en fait universelle. Pour cela, on remplacera Y par le voisinage infinitésimal à puissances divisées universel de X dans Y, qui est construit à partir de l'enveloppe à puissances divisées.

On va construire l'enveloppe à puissances divisées pour J, dans un cadre un peu plus général dans lequel l'anneau de base $A = (A, I, \gamma)$ est lui-même muni de puissances divisées. Soit la catégorie $\mathcal{C} = \text{PD- Alg}_{(A,I,\gamma)}$ dont les objets sont les (A, I, γ)-PD-algèbres (B, J, δ). Soit $\mathcal{D} = \text{Alg}$ la catégorie des couples (B, J) formés d'une A-algèbre avec un idéal $J \supset IB$.

6.3.1 Proposition. *Le foncteur d'oubli $\omega : \mathcal{D} \to \mathcal{C}$ possède un adjoint à gauche $(B, J, \delta) \mapsto D_\gamma(B, J, \delta)$.*

On appelle $D_\gamma(B, J, \delta)$ l'enveloppe à puissances divisées de (B, J, δ).

Preuve: Pour construire $D_\gamma(B, J)$, on considère l'algèbre à puissances divisées $\Gamma_B(J)$. Comme $\Gamma_+(J)$ est engendré par les $x^{[n]}$, les puissances divisées s'étendent à $\Gamma_+(J)$ par la formule de l'axiome (5). On considère l'idéal $K \subset \Gamma_B(J)$ engendré par les éléments $x^{[1]} - x$ pour $x \in J$ et les éléments $f(y^{[n]}) - f(y)^{[n]}$ pour $y \in I$. On pose $D_\gamma(B, J) = \Gamma_B(J)/K$. On vérifie que $K \cap \Gamma_+(J)$ est un sous-PD-idéal de $\Gamma_+(J)$, ce qui est une condition nécessaire et suffisante pour qu'il existe une structure de puissances divisées (alors unique) sur l'image de $\Gamma_+(J)$ dans $D_\gamma(B, J)$ telle que $\Gamma_B(J) \to D_\gamma(B, J)$ soit un PD-morphisme. Il n'est pas difficile de vérifier la propriété d'adjonction. □

6.3.2 Cas des $\mathbb{Z}_{(p)}$-algèbres. Si A est une $\mathbb{Z}_p$-algèbre, en itérant l'axiome (5) on trouve :

$$(\gamma_p)^k(x) = \frac{(p^k)!}{(p!)^{1+p+\cdots+p^{k-1}}}\, \gamma_{p^k}(x).$$

Le coefficient est de valuation nulle, de sorte que γ_{p^k} est déterminé par γ_p. Par exemple soit k un corps de caractéristique $p > 0$, soit $A = k[\epsilon]$ où $\epsilon^2 = 0$, soit I l'idéal engendré par $x_1 := \epsilon$. L'algèbre à puissances divisées est

$$\Gamma_A(I) \simeq \frac{A[x_1, x_p, x_{p^2}, \dots]}{(\epsilon x_1, (x_1)^p, (x_p)^p, (x_{p^2})^p, \dots)}$$

et les puissances divisées sont déterminées par la donnée de

$$\gamma_p(x_{p^k}) = \frac{p^{k+1}!}{p!\,(p^k!)^p}\, x_{p^{k+1}}.$$

Il semble que $\Gamma_1(I) \simeq I$ alors que $\Gamma_n(I) \simeq A$ pour $n \geqslant 2$, i.e. les relations dans I n'induisent pas de relations dans $\Gamma_n(I)$ (étonnant ?). L'enveloppe à puissances divisées de I est

$$D_\gamma(I) \simeq \frac{A[x_p, x_{p^2}, \dots]}{((x_p)^p, (x_{p^2})^p, \dots)}.$$

7 Quelques formules p-adiques

7.1 Lemme. *Soit $n_0 + n_1 p + n_2 p^2 + \dots$ le développement p-adique d'un entier $n \geqslant 1$. Alors, on dispose des formules suivantes pour les valuations et restes p-adiques :*

(1) *La valuation de $n!$ est $v(n!) = \sum_{k \geqslant 1} \lfloor n/p^k \rfloor = \frac{n-(n_0+n_1+n_2+\dots)}{p-1}$.*

(2) *Si l'on note $v = v(n!)$ alors le coefficient dominant dans le développement p-adique de $n!$ est*

$$(-1)^v n_0!\, n_1!\, n_2! \dots\, p^v.$$

(3) *La valuation du coefficient binômial $\binom{n}{k}$ est la somme des retenues dans l'addition de k par $n-k$.*

(4) *Si $\binom{n}{k}$ est premier à p, alors son reste modulo p est $\binom{n_0}{k_0}\binom{n_1}{k_1}\binom{n_2}{k_2}\dots$*

(5) *La valuation du coefficient binômial $\binom{p^n}{k}$ est $n - v(k)$, pour $k \geqslant 1$.*

Preuve: (1) Écrivons $n = n_0 + n_1 p + \dots + n_r p^r$. Il y a $\lfloor n/p^k \rfloor$ entiers $m \leqslant n$ divisibles par p^k et $\lfloor n/p^k \rfloor - \lfloor n/p^{k+1} \rfloor$ entiers $m \leqslant n$ de valuation k. Il s'ensuit que

$$v(n!) = \sum_{k \geqslant 1} k \left(\left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^{k+1}} \right\rfloor \right) = \sum_{k \geqslant 1} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

En utilisant le fait que $\lfloor n/p^k \rfloor = \sum_{i \geqslant k} n_i p^{i-k}$, on en déduit la formule

$$v(n!) = \frac{n - (n_0 + n_1 + \dots + n_r)}{p-1}.$$

(2) Voir aussi H. Hasse, *Number theory*, Classics in Mathematics, Springer-Verlag (2002), chapter 17, § 3. Pour tout ensemble fini M d'entiers positifs, notons $M!$ le produit des éléments de M et écrivons le coefficient dominant du développement p-adique de $M!$ sous la forme $\mu(M)p^{v(M!)}$. Nous souhaitons donc prouver que $\mu(\{1, \dots, n\}) = (-1)^{v(n!)} n_0! \dots n_r!$. Pour cela, il suffit de construire une partition $\{1, \dots, n\} = A_0 \sqcup \dots \sqcup A_r$ telle que

$$\mu(A_i) = (-1)^{n_i \frac{p^i - 1}{p-1}} n_i!.$$

Soit A_i l'ensemble des entiers $m \in \{1, \dots, n\}$ tels que $m_{i+1} = n_{i+1}, \dots, m_r = n_r$ et soit $v(m) = i$ soit $m_i < n_i$. C'est une partition, parce que n appartient à $A_{v(n)}$ et aucun autre A_i, et si $m < n$, il existe un i maximal tel que $m_i < n_i$ et alors m appartient à A_i et aucun autre. Les entiers $m \in A_i$ de valuation i sont déterminés par leur i-ième chiffre qui satisfait $1 \leqslant m_i \leqslant n_i$, et ils contribuent à $\mu(A_i)$ par un facteur $n_i!$. Les entiers $m \in A_i$ de valuation $k < i$ sont déterminés par leurs chiffres situés entre le k-ième et le i-ième, qui satisfont $1 \leqslant m_k \leqslant p-1$, $0 \leqslant m_j \leqslant p-1$ pour $k < j < i$, et $0 \leqslant m_i \leqslant n_i - 1$. Utilisant le fait que $(p-1)! \equiv -1 \mod p$, un calcul immédiat montre que ces m contribuent à $\mu(A_i)$ pour un facteur $(-1)^{n_i p^{i-k-1}}$. Finalement, la valeur de $\mu(A_i)$ est celle annoncée.

(3) Soit $k = k_0 + k_1 p + \cdots + k_r p^r$ et $l = n - k = l_0 + l_1 p + \cdots + l_r p^r$. L'algorithme d'addition p-adique pour additionner k et l s'écrit ainsi :

$$\begin{array}{ll} k_0 + l_0 = n_0 + \delta_0 p & \text{with } \delta_0 \in \{0,1\}, \\ k_1 + l_1 + \delta_0 = n_1 + \delta_1 p & \text{with } \delta_1 \in \{0,1\}, \\ \quad \vdots & \quad \vdots \\ k_r + l_r + \delta_{r-1} = n_r + \delta_r p & \text{with } \delta_r \in \{0,1\}, \\ n_{r+1} = \delta_r & \end{array}$$

où $\delta_0, \ldots, \delta_r$ sont les retenues. D'après (1), la valuation de $\binom{n}{k} = \frac{n!}{k!\,l!}$ multipliée par $(p-1)$ vaut

$$n - (n_0 + \cdots + n_{r+1}) - k + (k_0 + \cdots + k_r) - l + (l_0 + \cdots + l_r) = (p-1)(\delta_0 + \cdots + \delta_r).$$

(4) Ce que l'on vient de prouver montre que $\binom{n}{k}$ est premier à p si et seulement s'il n'y a pas de retenue. Si c'est le cas, alors $n_i = k_i + l_i$ pour tout i. Alors, le coefficient dominant dans le développement p-adique du coefficient binomial, qui dans le cas présent est aussi le reste p-adique, vaut

$$\frac{n_0! \ldots n_r!}{k_0! \ldots k_r!\, l_0! \ldots l_r!} = \binom{n_0}{k_0} \cdots \binom{n_r}{k_r}.$$

(5) Si $k = p^n$, le résultat est clair. Si $1 \leqslant k \leqslant p^n$, on a $v(p^n - k) = v(k)$. En prenant les valuations dans l'égalité

$$k! \binom{p^n}{k} = p^n (p^n - 1) \ldots (p^n - (k-1)),$$

on trouve $v(k!) + v\left(\binom{p^n}{k}\right) = n + v((k-1)!)$, d'où le résultat. □