Groupes de Barsotti-Tate, 2 et 3

Matthieu Romagny

Exposé du 3 février 2015 : parties 1 à 3 des notes.
Exposé 24 février 2015 : parties 4 et 5 des notes.

Table des matières

On travaille dans la catégorie des faisceaux fppf abéliens sur un schéma de base S. Si G est un tel faisceau, on note $G^\vee = \mathrm{Hom}(G, \mathbb{G}_m)$ son dual de Cartier. Si G est un groupe de BT, on note $G^\vee = \varinjlim G(n)^\vee$ son dual de Serre. Si M est un $\mathcal{O}_S$-module quasi-cohérent, on note $M^* = \mathrm{Hom}(M, \mathcal{O}_S)$ son dual linéaire, $\mathbb{W}(M)$ son extension à la catégorie des faisceaux définie par $\mathbb{W}(M)(T) = \Gamma(T, M_T)$, et $\mathbb{V}(M)$ le faisceau défini par $\mathbb{V}(M)(T) = \Gamma(T, (M_T)^*) = \mathrm{Hom}_{\mathcal{O}_T}(M_T, \mathcal{O}_T)$.

1 L'extension vectorielle universelle d'un groupe de Barsotti-Tate

1.1 Morphismes d'un groupe fini plat vers un module quasi-cohérent

Soit S un schéma. Pour tout S-schéma en groupes G on note $\omega_{G/S} = e^*\Omega^1_{G/S}$ ou simplement ω_G le *module des 1-formes différentielles invariantes*. Le premier voisinage infinitésimal de la section neutre est $G_1 = \mathrm{Spec}(\mathcal{O}_S \oplus \omega_G)$ où ω_G est de carré nul, *cf* Stacks Project, lemme 0474. En particulier, l'ensemble des morphismes de faisceaux pointés entre G_1 et $\mathbb{G}_m$ est $\mathrm{Hom}_{\mathrm{pt}}(G_1, \mathbb{G}_m) = \omega_G$.

1.1.1 Le morphisme α. Soit G un faisceau abélien dont le dual de Cartier $G^\vee = \mathrm{Hom}(G, \mathbb{G}_m)$ est représentable. On note $\alpha_G : G \to \omega_{G^\vee}$ le morphisme défini comme le composé suivant :

$$\alpha_G : G \longrightarrow \mathrm{Hom}(G^\vee, \mathbb{G}_m) \xrightarrow{\mathrm{res}} \mathrm{Hom}_{\mathrm{pt}}(G_1^\vee, \mathbb{G}_m) = \omega_{G^\vee}.$$

Notant dx/x la forme différentielle invariante canonique sur $\mathbb{G}_m$, la seconde flèche peut aussi être décrite par $\alpha(\varphi) = \varphi^*(dx/x)$, pour tout $\varphi : G^\vee \to \mathbb{G}_m$.

1.1.2 Proposition. ([MM74], chap. I, 1.4) *Soit G un faisceau abélien dont le dual de Cartier $G^\vee$ est représentable. Alors $f \mapsto f \circ \alpha_G$ induit un isomorphisme fonctoriel en le $\mathcal{O}_S$-module quasi-cohérent M :*

$$\mathrm{Hom}(\omega_{G^\vee}, M) \xrightarrow{\sim} \mathrm{Hom}(G, M).$$

Le point clé est que M s'identifie aux unités principales de l'algèbre de fonctions du schéma des nombres duaux $D = D_M = \mathrm{Spec}(\mathcal{O}_S \oplus M)$, avec $M^2 = 0$. Le terme « unités » explique l'apparition du dual de Cartier, et le terme « nombres duaux » explique l'apparition des 1-formes différentielles.

Preuve : Notons $\pi : D \to S$ le morphisme de structure et $\eta : S \to D$ la section canonique. On a $\mathcal{O}_D^\times = \mathcal{O}_S^\times \oplus M$ d'où une suite exacte $0 \to M \to \pi_*\mathbb{G}_{m,D} \to \mathbb{G}_{m,S} \to 0$. On en déduit :

$$\begin{aligned}
\mathrm{Hom}(G, M) &= \ker\big[\mathrm{Hom}(G, \pi_*\mathbb{G}_{m,D}) \to \mathrm{Hom}(G, \mathbb{G}_{m,S})\big] \\
&= \ker\big[\mathrm{Hom}(G_D, \mathbb{G}_{m,D}) \to \mathrm{Hom}(G, \mathbb{G}_{m,S})\big] \\
&= \ker\big[G^\vee(D) \to G^\vee(S)\big] \\
&= \{f : D \to G^\vee \ ; \ f \circ \eta = e_{G^\vee}\} \\
&= \{f : D \to G_1^\vee \ ; \ f \circ \eta = e_{G^\vee}\} \\
&= \mathrm{Hom}(\omega_{G^\vee}, M)
\end{aligned}$$

où le dernier Hom représente les morphismes de $\mathcal{O}_S$-modules quasi-cohérents. □

1.1.3 Quelques remarques sur les algèbres de Lie. Ce point n'était pas inclus dans l'exposé oral, et peut (voire doit) être sauté. En essayant de donner une construction alternative de α_G je suis arrivé aux remarques et questions suivantes, auxquelles je n'ai pas réfléchi pendant un temps exagéré. Rappelons qu'à tout S-faisceau en groupes G est associé un faisceau défini par $\mathrm{Lie}(G)(T) = \ker(G(T[\epsilon]) \to G(T))$. (Ce n'est une algèbre de Lie au sens habituel que pour certains faisceaux, *cf* les foncteurs *très bons* de SGA3, Exp. II, déf. 4.10.) Voici quelques exemples :

(1) Si G est un schéma en groupes, on a $\mathrm{Lie}(G) = \mathbb{V}(\omega_{G/S})$.

(2) Si M est un module quasi-cohérent, on a $\mathrm{Lie}(\mathbb{W}(M)) = \mathbb{W}(M)$. Ceci est élémentaire à voir.

(3) On a $\mathrm{Lie}(\mathbb{V}(M)) = \mathbb{V}(M)$. Vérifions ceci. Soit T un S-schéma et $u : M_{T[\epsilon]} \to \mathcal{O}_{T[\epsilon]}$ une forme $\mathcal{O}_{T[\epsilon]}$-linéaire. En utilisant le fait que $M_{T[\epsilon]} = M_T \oplus \epsilon M_T$ et qu'une forme $\mathcal{O}_{T[\epsilon]}$-linéaire est une forme $\mathcal{O}_T$-linéaire et ϵ-linéaire, on peut écrire $u(x + \epsilon y) = (a(x) + b(y)) + \epsilon(c(x) + d(y))$ où a, b, c, d sont des formes $\mathcal{O}_T$-linéaires sur M_T, et la ϵ-linéarité signifie que $a = 0$ et $b = d$. De plus, u est nulle lorsque $\epsilon = 0$ ssi $b = 0$, donc finalement $u(x + \epsilon y) = \epsilon c(x)$. Donc $u \in \mathrm{Lie}(\mathbb{V}(M))(T)$ est donné par un élément de $\Gamma(T, (M_T)^*) = \mathbb{V}(M)(T)$.

(4) On dispose d'un morphisme canonique $\mathbb{W}(M^*) \to \mathbb{V}(M)$ qui revient à tirer en arrière sur T une section locale de M^*. C'est un isomorphisme lorsque M est localement libre de rang fini. Question : ce morphisme est-il universel parmi les morphismes depuis un module quasi-cohérent variable vers $\mathbb{V}(M)$? Ou alors, parmi les morphismes depuis $\mathbb{W}(M^*)$ vers un schéma en groupes (ou un fibré vectoriel) variable ?

(5) Soit G un schéma en groupes. À tout T-point de G on peut associer un morphisme de T-schémas en groupes $\varphi : G^\vee \to \mathbb{G}_m$ puis la composée :

$$\omega^*_{G^\vee/S} = \mathbb{W}(\omega^*_{G^\vee/S}) \longrightarrow \mathbb{V}(\omega_{G^\vee/S}) = \mathrm{Lie}(G^\vee) \xrightarrow{\mathrm{d}\varphi} \mathbb{G}_a.$$

C'est une forme linéaire sur $\omega^*_{G^\vee/S}$ i.e. une section de $\omega^{**}_{G^\vee/S}$. On obtient un morphisme $G \longrightarrow \omega^{**}_{G^\vee/S}$. Est-ce la composée de α_G et du morphisme canonique $\omega_{G^\vee/S} \to \omega^{**}_{G^\vee/S}$?

1.2 L'extension vectorielle universelle d'un BT

On suppose maintenant qu'il existe un entier N tel que $p^N = 0$ dans S.

1.2.1 Définition. Soit G un BT sur S. On dit qu'une extension $0 \to V \to E \to G \to 0$ de G par un module quasi-cohérent V est *universelle* si pour toute extension $0 \to V' \to E' \to G \to 0$, il existe un unique morphisme $\varphi : V \to V'$ tel que $E' = \varphi_* E$.

1.2.2 Remarque. L'image directe φ_* n'est définie a priori que pour les *classes* d'extensions, mais ici l'extension $\varphi_* E$ a un sens pour la raison suivante. Si G est un BT et M est un module quasi-cohérent, alors du fait que G est p-divisible et que $p^N = 0$ il résulte que $\mathrm{Hom}(G, M) = 0$. Soit E une extension de G par M. Comme tout automorphisme d'extension diffère de l'identité par un morphisme $G \to M$, on conclut que E n'a pas d'automorphisme.

$$\begin{array}{ccccccccc} & & & & E & & & & \\ & & & \overset{i}{\nearrow} & \downarrow{\scriptstyle \varphi} & \overset{p}{\searrow} & & & \\ 0 & \longrightarrow & M & & & & G & \longrightarrow & 0 \\ & & & \underset{i}{\searrow} & & \underset{p}{\nearrow} & & & \\ & & & & E & & & & \end{array}$$

(Détail : soit $u = \varphi - \mathrm{id}$. Alors $p\varphi = p \Rightarrow u(E) \subset M$ et $\varphi i = i \Rightarrow u(M) = 0$, d'où $\bar{u} : G \to M$.) Ainsi chaque extension est déterminée à isomorphisme unique près par sa classe.

1.2.3 Proposition. ([Mes72], IV.1.10) *Pour tout $n \geqslant N$, l'extension obtenue par le pushout*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & G(n) & \longrightarrow & G & \xrightarrow{p^n} & G & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha_{G(n)}} & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & V(G) = \omega_{G(n)^\vee} & \longrightarrow & E(G) & \longrightarrow & G & \longrightarrow & 0 \end{array}$$

est une (l')extension universelle de G.

Preuve : Appliquons $\mathrm{Hom}(-, M)$ à la suite exacte définie par l'isogénie p^n sur G, on trouve :

$$0 = \mathrm{Hom}(G, M) \longrightarrow \mathrm{Hom}(G(n), M) \xrightarrow{\delta} \mathrm{Ext}^1(G, M) \longrightarrow \mathrm{Ext}^1(G, M).$$

Comme $p^n = 0$ et Ext est bi-additif, on voit que la dernière flèche est nulle. Il s'ensuit que δ est un isomorphisme. Comme par ailleurs $\mathrm{Hom}(G(n), M) = \mathrm{Hom}(\omega_{G(n)^\vee}, M)$ fonctoriellement en M, on obtient le résultat. □

1.2.4 Propriétés. (i) L'extension vectorielle universelle $E(G)$ est fonctorielle en G et sa formation commute au changement de base sur S ([Mes72], IV.1.13, IV.1.15). La vérification est formelle.

(ii) La proposition ci-dessus (appliquée à $G^\vee$) implique en particulier que le module $\omega_{G(n)}$ est stationnaire à partir de $n = N$ (ceci découle aussi du lemme [Mes72], II.3.3.17 selon lequel $\mathrm{Inf}^k(G) \subset G(n + N - 1)$ pour tous k, n tels que $k < p^n$, cf exposé de David). De plus $\omega_G := \omega_{\overline{G}} = \omega_{G(N)}$ est localement libre, comme il découle du fait que $\overline{G}$ est un groupe de Lie formel. En particulier, on voit

que $\mathrm{Lie}(G) := \mathbb{V}(\omega_G) = \omega_G^*$ et le faisceau $V(G) = \omega_{G^\vee} = \mathbb{V}(\omega_{G^\vee}^*)$ sont des modules localement libres, i.e. des fibrés vectoriels ([Mes72], II.3.3.19 et II.3.3.20).

(iii) Le faisceau $E(G)$ est formellement lisse, et son complété formel $\overline{E(G)}$ est un groupe de Lie formel. Ces faits découlent assez facilement des propriétés analogues pour G et $V(G)$ ([Mes72], IV.1.18 et IV.1.19).

2 Site cristallin et cristaux

Le site adapté à l'étude des cristaux de Dieudonné est le gros site cristallin muni de la topologie fppf. Nous travaillerons ici avec le petit site cristallin nilpotent, comme le fait Messing [Mes72].

2.1 Définition. Un *PD-anneau* est un triplet (A, I, γ) où A est un anneau, $I \subset A$ un idéal, et $\gamma = (\gamma_n : I \to A)_{n\geqslant 0}$ est une famille d'applications t.q. $\gamma_n(I) \subset I$ si $n \geqslant 1$ et pour tous $x \in I$ et $a \in A$:

(1) $\gamma_0(x) = 1$ et $\gamma_1(x) = x$,
(2) $\gamma_n(ax) = a^n\gamma_n(x)$,
(3) $\gamma_m(x)\gamma_n(x) = \frac{(m+n)!}{m!\,n!}\,\gamma_{m+n}(x)$,
(4) $\gamma_n(x+y) = \sum_{i=0}^{n} \gamma_i(x)\gamma_{n-i}(y)$,
(5) $\gamma_m(\gamma_n(x)) = \frac{(mn)!}{m!\,(n!)^m}\gamma_{mn}(x)$.

On note souvent $x^{[n]} = \gamma_n(x)$, et $I^{[n]}$ l'idéal engendré par les $x_1^{[i_1]} \cdots x_k^{[i_k]}$ avec $x_j \in I$ et $i_1 + \cdots + i_k \geqslant n$. On dit que I est *PD-nilpotent* si $I^{[n]} = 0$ pour un n. Un *PD-morphisme* $\varphi : (A, I, \gamma) \to (B, J, \delta)$ 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. Un *PD-schéma* $(T, \mathcal{I}, \gamma)$ est un schéma T avec un faisceau d'idéaux quasi-cohérent $\mathcal{I}$ et une PD-structure γ sur $\mathcal{I}$. Etc.

2.2 Remarque. Les axiomes (1) et (3) impliquent que $n!x^{[n]} = x^n$. En particulier, si A est un anneau sans torsion, il y a au plus une PD-structure sur un idéal I. Si A est une $\mathbb{Q}$-algèbre, $x^{[n]} := x^n/n!$ est une PD-structure sur n'importe quel idéal I. Pour $A = \mathbb{Z}_{(p)}$ et $I = (p)$, on vérifie que $x^{[n]} := x^n/n! \in I$ pour tout $x \in I$, est une PD-structure. Elle est nilpotente ssi $p \neq 2$.

2.3 Définition. Soit $\Sigma = \mathrm{Spec}(\mathbb{Z}_{(p)})$ muni de l'idéal $\mathcal{I} = (p)$ avec ses PD canoniques. Soit S un schéma sur lequel p est localement nilpotent. On note $\mathrm{Cris}(S/\Sigma)$ ou simplement $\mathrm{Cris}(S)$ le petit site Zariski cristallin nilpotent, défini ainsi.

(1) Les ouverts sont les paires $(U \hookrightarrow U', \gamma)$ composées d'un ouvert $U \subset S$, un Σ-schéma U', une nilimmersion $U \hookrightarrow U'$, et une PD-structure localement nilpotente γ sur l'idéal $\mathcal{I}$ de U dans U'.

(2) Les morphismes entre $(U \hookrightarrow U', \gamma)$ et $(V \hookrightarrow V', \delta)$ sont les PD-morphismes de Σ-schémas $g : U' \to V'$ qui prolongent une inclusion d'ouverts Zariski $f : U \hookrightarrow V$ (donnant un carré commutatif mais non nécessairement cartésien).

(3) Les recouvrements sont engendrés par les familles $(U_i \hookrightarrow U_i', \gamma_i) \to (U \hookrightarrow U', \gamma)$ telles que les $U_i' \to U'$ sont des immersions ouvertes et $U' = \cup U_i$. (Pour d'autres topologies, comme la topologie fppf, il faut demander en plus que $U_i = U \times_{U'} U_i'$ mais c'est automatique ici.)

2.4 Définition. Un *faisceau de groupes abéliens* F sur $\mathrm{Cris}(S)$ est la donnée de :

(1) un faisceau abélien $F_{U'} = F_{U\hookrightarrow U'}$ sur U', pour tout ouvert $U \hookrightarrow U'$,

(2) un morphisme de faisceaux abéliens $\rho_g : g^{-1}F_{V'} \to F_{U'}$ pour tout morphisme d'ouverts $g : U' \to V'$, tels que $\rho_{\mathrm{id}} = \mathrm{id}$, $\rho_{gh} = \rho_h \circ h^{-1}\rho_g$, et ρ_g est un isomorphisme si g est une immersion ouverte. Un *cristal* F de groupes abéliens sur $\mathrm{Cris}(S)$ est un faisceau tel que ρ_g est un iso pour *tout* $g : U' \to V'$.

2.5 Exemples. (1) Le *faisceau structural* $F = \mathcal{O}_S$ défini par $F_{U'} = \mathcal{O}_{U'}$ est un faisceau de groupes abéliens. C'est même un faisceau d'anneaux, en un sens évident. On a alors des notions évidentes de *faisceau de $\mathcal{O}_S$-modules* et de *cristal de $\mathcal{O}_S$-modules*, où dans la définition le foncteur d'image inverse g^{-1} est remplacé par le foncteur d'image inverse des modules g^*.
(2) Le faisceau $F = \Omega^1_{S/\mathbb{Z}}$ n'est pas un cristal.

3 Les cristaux $\mathbb{E}(G)$ et $\mathbb{D}(G)$

Le point clé pour construire $\mathbb{E}(G)$ et $\mathbb{D}(G)$ et démontrer leur propriété de cristal est le théorème suivant. On y note $i_G : V(G) \to E(G)$ le noyau de l'extension vectorielle universelle. La notion d'exponentielle, qui y apparaît, sera expliquée dans la section suivante.

3.1 Théorème. ([Mes72], IV.2.2) *Soit $S \hookrightarrow S'$ une nilimmersion à PD nilpotentes de schémas affines dans lesquels $p^N = 0$. Soient G, H deux BT sur S, $u : G \to H$ un morphisme et $v = E(u) : E(G) \to E(H)$ le morphisme associé. Soient G', H' des relèvements de G, H à S'. Alors, il existe un unique morphisme $v' : E(G') \to E(H')$ (qui ne respecte pas nécessairement la structure d'extension) satisfaisant :*

(i) *v' relève v,*

(ii) *pour tout morphisme $w' : V(G') \to V(H')$ qui relève $V(u)$, le morphisme $d = i_{H'} \circ w' - v' \circ i_{G'} : V(G') \to E(H')$, nul en restriction à S, est une exponentielle.*

$$\begin{array}{ccc} V(G') & \xrightarrow{i_{G'}} & E(G') \\ {\scriptstyle w'}\downarrow & \searrow^{d} & \downarrow{\scriptstyle v'} \\ V(H') & \xrightarrow[i_{H'}]{} & E(H') \end{array}$$

Preuve : La preuve occupe les paragraphes IV.2.6 et IV.2.7 de [Mes72]. Nous l'admettons. □

3.2 Remarques. (1) Un calcul facile montre qu'il est suffisant de demander que $d = i_{H'} \circ w' - v' \circ i_{G'} : V(G') \to E(H')$ soit une exponentielle pour *un seul* $w' : V(G') \to V(H')$ qui relève $V(u)$.
(2) La subtilité est qu'on ne sait pas s'il existe $u' : G' \to H'$ tel que $v' = E(u')$. En particulier, il faut bien noter qu'a priori le diagramme carré du théorème n'est pas commutatif, i.e. $d \neq 0$!

3.3 Corollaire. *La règle $u \mapsto v' = E_{S'}(u)$ est fonctorielle. En particulier elle envoie id_G sur $\mathrm{id}_{E(G')}$ et isomorphismes sur isomorphismes.*

Preuve : Ces faits découlent de l'assertion d'unicité dans 3.1. □

Dans la définition 2.4 et la remarque qui la suit, nous nous sommes limités aux faisceaux et aux cristaux de groupes abéliens et de modules. Nous aurons besoin ici de faisceaux à valeurs dans une autre catégorie. En fait, pour toute catégorie C qui est un champ au-dessus de $\mathrm{Cris}(S)$, on peut définir les notions de faisceaux et cristaux en objets de C. Prenons pour C la catégorie $\mathrm{Ab}^{\mathrm{fppf}}_{\mathrm{Cris}}$ dont les objets sont les paires $(U \hookrightarrow U', F_{U'})$ formées d'un ouvert cristallin $U \hookrightarrow U'$ et d'un faisceau fppf abélien $F_{U'}$ sur U', avec pour morphismes entre $(U \hookrightarrow U', F_{U'})$ et $(V \hookrightarrow V', F_{V'})$ les paires composées d'un morphisme d'ouverts cristallins $g : U' \to V'$ et d'un morphisme de faisceaux $\psi : F_{U'} \to g^* F_{V'}$. (La flèche ψ va bien dans ce sens, et non pas dans l'autre.)

3.4 Corollaire. *Il existe un unique cristal de $\mathrm{Ab}^{\mathrm{fppf}}_{\mathrm{Cris}}$-objets $\mathbb{E}(G)$ sur S tel que, pour tout ouvert cristallin $U \hookrightarrow U'$ tel que $G \times_S U$ s'étend en un BT $G_{U'}$ sur U', on ait $\mathbb{E}(G)_{U \hookrightarrow U'} = E(G_{U'})$.*

Preuve : Supposons d'abord que G s'étend en un BT sur S'. Soient G'_1, G'_2 deux tels relèvements de G à S'. Alors d'après 3.1, il existe un unique morphisme $v : E(G'_1) \to E(G'_2)$ qui relève $\mathrm{id}_G : G \to G$ et vérifie la condition (ii) de *loc. cit.* D'après le corollaire, c'est un isomorphisme. Dans le cas général, d'après le théorème de Grothendieck (voir [Gro74], VI.4.1 ou [Ill13], th. 4.2.1) il suffit de recouvrir S par des ouverts affines U_i pour que sur chaque ouvert le groupe $G \times_S U_i$ se relève, et que les faisceaux $E(G'_i)$ définis par choix d'un relèvement G'_i, canoniquement isomorphes sur les intersections, se recollent en un faisceau $\mathbb{E}(G)$ sur S. Pour faire de $\mathbb{E}(G)$ un cristal, il ne reste qu'à donner un isomorphisme canonique $\rho_g : g^*\mathbb{E}(G)_{V'} \simeq \mathbb{E}(G)_{U'}$ pour tout morphisme d'ouverts cristallins :

$$\begin{array}{ccc} U & \hookrightarrow & U' \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle g} \\ V & \hookrightarrow & V' \end{array}$$

Il suffit de construire un tel isomorphisme localement, donc on peut supposer que G se relève en $G_{U'}$ et $G_{V'}$ le long des épaississements considérés. Utilisant le fait (1.2.4) que la formation de $E(G)$ commute au changement de base, on a :

$$g^*\mathbb{E}(G)_{V'} = g^*E(G_{V'}) = E(g^*G_{V'}).$$

De plus, comme $g^*G_{V'}$ et $G_{U'}$ sont deux relèvements de $G \times_S U$ à U', d'après 3.1 encore on a un isomorphisme canonique

$$E(g^*G_{V'}) = E(G_{U'}) = \mathbb{E}(G)_{U'}.$$

On obtient ainsi l'isomorphisme ρ_g. □

4 Exponentielle d'un groupe de Barsotti-Tate

4.1 Cospectre des cogèbres

En tant que faisceaux, les BT et les groupes de Lie formels sont par définition des colimites filtrantes de schémas finis localement libres. Pour leur associer une exponentielle, qui est un objet d'algèbre commutative définie sur les algèbres de fonctions, on est gêné par le fait que le spectre ne commute pas aux colimites filtrantes. La situation s'améliore si on remplace les algèbres de fonctions par leur dual linéaire, une cogèbre. Plus précisément, soient R un anneau, A un R-module, et $A^* = \mathrm{Hom}_R(A, R)$ son dual. Une structure d'algèbre (associative, commutative) sur A est donnée par deux applications linéaires $m : A \otimes_R A \to A$ et $e : R \to A$ vérifiant certains axiomes. En dualisant, on obtient deux applications $m^* : A^* \to A^* \otimes_R A^*$ et $e^* : A^* \to R$ qui donnent à A^* une structure de cogèbre. De plus, pour toute R-algèbre R' on a :

$$\begin{aligned} \mathrm{Spec}(A)(R') &= \mathrm{Hom}_{R\text{- Alg}}(A, R') = \mathrm{Hom}_{R'\text{- Alg}}(A_{R'}, R') \\ &= \{f \in (A_{R'})^* \ ; \ f \circ m = f \otimes f \text{ et } f \circ e = 1\} \\ &= \{f \in (A^*)_{R'} \ ; \ m^*(f) = f \otimes f \text{ et } e^*(f) = 1\}. \end{aligned}$$

On voit que le foncteur $\mathrm{Spec}(A)$ peut s'exprimer entièrement en termes de la structure de cogèbre sur $U := A^*$. Précisément, on a $\mathrm{Spec}(A) = \mathrm{Cospec}(U)$ au sens de la définition suivante.

4.1.1 Définition. Soit U une R-cogèbre (coassociative, cocommutative), i.e. un R-module muni d'applications $\Delta : U \to U \otimes_R U$ et $\eta : U \to R$ satisfaisant les axiomes duaux des axiomes d'algèbre. On appelle *cospectre* de U le foncteur sur les R-algèbres défini par

$$\mathrm{Cospec}(U)(R') = \{f \in U_{R'} \ ; \ \Delta(f) = f \otimes f \text{ et } \eta(f) = 1\}.$$

4.1.2 Remarque. Pour un schéma S, une $\mathcal{O}_S$-algèbre finie localement libre $\mathscr{A}$ et sa cogèbre duale $\mathscr{U} = \mathscr{A}^*$, on a un diagramme de foncteurs :

$$\begin{array}{ccc} \mathrm{Cospec}(\mathscr{U}) & \subset & \mathbb{W}(\mathscr{U}) \\ \| & & \downarrow \\ \mathrm{Spec}(\mathscr{A}) & \subset & \mathbb{V}(\mathscr{A}). \end{array}$$

4.1.3 Lemme. *Le cospectre commute aux colimites filtrantes de cogèbres.*

Preuve : Si $U = \operatorname{colim} U_i$, alors tout point f du cospectre est dans un U_i et les égalités $\Delta(f) = f \otimes f$ et $\eta(f) = 1$ ont lieu dans un certain $U_j \otimes_R U_j$, $j \geqslant i$. Ainsi f est un point du cospectre de U_j. □

Dans la suite, nous utiliserons l'algèbre de Lie d'une cogèbre (co ?)augmentée U, qui est en fait un abus de terminologie pour désigner l'algèbre de Lie du foncteur $F = \mathrm{Cospec}(U)$. On se donne donc une (co ?)augmentation $\epsilon : R \to U$ et on pose $1 = 1_U = \epsilon(1)$. Par définition de l'algèbre de Lie d'un foncteur, si $f \in F(R') = \ker[\mathrm{Cospec}(U)(R'[\epsilon]) \to \mathrm{Cospec}(U)(R')]$, on peut écrire $f = 1 + \epsilon x \in U_{R'} + \epsilon U_{R'}$. Les conditions d'appartenance au cospectre donnent $\Delta(x) = x \otimes 1 + 1 \otimes x$ et $\eta(x) = 0$ mais un calcul facile montre qu'en fait la seconde égalité est conséquence de la première.

4.1.4 Définition. Soit U une R-cogèbre avec coaugmentation $\epsilon : R \to U$ et $1 = 1_U = \epsilon(1)$. On dit que $x \in U$ est *primitif* si $\Delta(x) = x \otimes 1 + 1 \otimes x$. On note $\mathrm{Lie}(U)$ le faisceau des éléments primitifs de U (notation plus correcte : $\mathrm{Lie}\,\mathrm{Cospec}(U)$). C'est un sous-foncteur en modules de $\mathbb{W}(U)$.

4.2 L'exponentielle

4.2.1 Lemme. *Soit S un schéma sur lequel $p^N = 0$ et G un BT sur S. Soit B_k l'algèbre de fonctions de $\mathrm{Inf}^k(G)$. Alors $U = \varinjlim B_k^*$ est une $\mathcal{O}_S$-bigèbre plate, i.e. elle est munie de structures de cogèbre (coassociative, cocommutative, counitaire), et d'algèbre (associative, commutative, unitaire) compatibles entre elles.*

Preuve : Comme colimite filtrante de cogèbres localement libres de rang fini, U est une cogèbre plate. Comme la multiplication de G envoie $\mathrm{Inf}^k(G) \times \mathrm{Inf}^l(G)$ dans $\mathrm{Inf}^{k+l}(G)$ (voir [Mes72], I.1.1.6), on a des applications $B_{k+l} \to B_k \otimes B_l$ puis $B_k^* \otimes B_l^* \to B_{k+l}^*$. Par passage à la limite on obtient une structure d'algèbre sur U, dont on montre qu'elle est compatible à la structure de cogèbre (i.e. les applications de structure de l'algèbre sont des morphismes de cogèbre ; ou alors, de manière équivalente, les applications de structure de la cogèbre sont des morphismes d'algèbre, voir proposition 6.2.3). Ceci fait de U une bigèbre. □

4.2.2 Lemme. *Soit (A, I, γ) un PD-anneau dont les PD sont nilpotentes. Alors, l'application* exp : $I \to (1 + I)^\times$ *définie par* $\exp(x) = \sum_{n \geqslant 0} x^{[n]}$ *est bien définie et un morphisme de groupes.*

Preuve : L'application est bien définie car les PD sont nilpotentes, et le fait que ce soit un morphisme de groupes est un calcul formel pour lequel on peut se ramener au cas universel sur une $\mathbb{Q}$-algèbre auquel cas $x^{[n]} = x^n/n!$ et le résultat est vrai. □

Soit (A, I, γ) un PD-anneau et B une A-algèbre. On dit que les PD *s'étendent à* B s'il existe une structure de PD γ_B sur IB telle que $(A, I, \gamma) \to (B, IB, \gamma_B)$ est un PD-morphisme.

4.2.3 Lemme. *Soit (A, I, γ) un PD-anneau et B une A-algèbre. Si les PD de A s'étendent à B, l'extension est unique. Si $A \to B$ est plate, les PD de A s'étendent à B. Si $B \to C$ est un morphisme de A-algèbres plates, que l'on munit de leur unique extension de γ, c'est un PD-morphisme.*

Preuve : L'unicité de l'extension est immédiate par les axiomes de puissances divisées. L'existence dans le cas plat est démontrée dans [Be74], I.2.7.4 ou par une autre méthode Stacks Project, lemme 07H1. Le fait que tout morphisme de A-algèbres plates est un PD-morphisme provient de l'expression explicite des PD étendues obtenue par utilisation des axiomes de PD, comme pour la preuve de l'unicité. □

4.2.4 Proposition. ([Mes72], III.2.4) *Soit $S_0 = \mathrm{Spec}(A_0) \hookrightarrow S = \mathrm{Spec}(A)$ une nilimmersion à PD nilpotentes, avec $A_0 = A/I$. Soit G un faisceau abélien sur S dont le complété formel $\overline{G}$ est un groupe de Lie formel. Soit V un $\mathcal{O}_S$-module localement libre de type fini. Alors, il existe une application exponentielle* $\exp : \mathrm{Hom}(V, I \cdot \mathrm{Lie}(G)) \hookrightarrow \ker\left[\mathrm{Hom}(V, G) \to \mathrm{Hom}(V_0, G_0)\right]$.

Intuitivement, on peut penser que chaque $u : V \to G$ nul en restriction à S_0 possède une application tangente $\theta : V \to I \cdot \mathrm{Lie}(G)$, et certains u sont l'exponentielle de leur application tangente.

Preuve : On conserve les notations du lemme 4.2.1. On sait que $\overline{G} = \varinjlim \mathrm{Cospec}(B_k^*) = \mathrm{Cospec}(U)$, et de plus $\mathrm{Lie}(G) = \mathrm{Lie}(\overline{G}) = \mathrm{Lie}(U) \subset U$. Comme U et $U \otimes U$ sont plates, les puissances divisées sur I s'étendent de manière unique à $I \cdot U$ et à $I \cdot U \otimes U$, et les morphismes $\Delta : U \to U \otimes U$ et $\eta : U \to \mathcal{O}_S$ leur sont compatibles (lemme 4.2.3). En particulier on peut définir l'exponentielle :

$$I \cdot \mathrm{Lie}(U) \subset I \cdot U \xrightarrow{\exp} (1 + I \cdot U)^\times \subset U.$$

Soit y une section locale de $I \cdot \mathrm{Lie}(U)$. Alors $\eta(\exp(y)) = \exp(\eta(y)) = \exp(0) = 1$ et de plus :

$$\begin{aligned}
\Delta(\exp(y)) &= \sum_{n \geqslant 0} (\Delta(y))^{[n]} \text{ car } \Delta \text{ est un morphisme de PD-algèbres,} \\
&= \sum_{n \geqslant 0} (y \otimes 1 + 1 \otimes y)^{[n]} \text{ car } y \in I \cdot \mathrm{Lie}(U), \\
&= \exp(y \otimes 1).\exp(1 \otimes y) \text{ par le lemme 4.2.2,} \\
&= (\exp(y) \otimes 1).(1 \otimes \exp(y)) \text{ car } I(U \otimes U) = (IU) \otimes U = U \otimes (IU), \\
&= \exp(y) \otimes \exp(y).
\end{aligned}$$

Ceci montre que $\exp(y) \in \mathrm{Cospec}(U) = \overline{G}$. Si on part d'un morphisme de faisceaux en modules $\theta : V \to I \cdot \mathrm{Lie}(U)$, par composition on obtient $\exp \circ \theta : V \to \overline{G} \subset G$. De plus, il est clair que modulo I l'exponentielle est triviale, donc $(\exp \circ \theta)_{|S_0}$ également. □

4.2.5 Remarques. (1) L'exponentielle ainsi construite est celle du théorème clef 3.1 avec $S = S'$, $V = V(G')$ et $G = E(H')$. Ceci étant dit, la preuve du théorème nécessite de construire l'exponentielle dans une situation un peu plus générale, ce qui est fait dans [Mes72], III.2.6.
(2) L'hypothèse que V soit localement libre de type fini semble inutile ici. Elle est en fait pertinente dans les calculs que fait Messing dans [Mes72], III.2.4, eux-mêmes utiles pour préparer III.2.6. Cependant, je dois dire que je n'ai pas compris toutes les subtilités des calculs, et de l'utilité, de III.2.4.

5 Déformations d'un groupe de Barsotti-Tate

Soient $S \hookrightarrow S'$ une nilimmersion à PD localement nilpotentes de schémas dans lesquels $p^N = 0$ et G un BT sur S. On considère l'extension vectorielle universelle $0 \to V(G) \to E(G) \to G \to 0$.

5.1 Lemme. ([Mes72], IV.1.22) *La suite d'algèbres de Lie* $0 \to V(G) \to \mathrm{Lie}(E(G)) \to \mathrm{Lie}(G) \to 0$ *est exacte.*

Preuve : La seule chose qui n'est pas évidente est la surjectivité à droite. C'est un énoncé local donc on peut supposer S affine. Compte tenu du fait que $\mathrm{Lie}(G) = \omega^*_{G(N)} = \mathrm{Lie}(G(N))$ et du diagramme

$$\begin{array}{ccc} \mathrm{Lie}(E(G) \times_G G(N)) & \longrightarrow & \mathrm{Lie}(G(N)) \\ \downarrow & & \downarrow \simeq \\ \mathrm{Lie}(E(G)) & \longrightarrow & \mathrm{Lie}(G), \end{array}$$

on voit qu'il suffit de montrer que $E(G) \times_G G(N) \to G(N)$ possède une section. Or il s'agit d'un torseur sous $V(G)$, et on a $H^1(G(N), V(G)) = 0$ puisque $G(N)$ est affine et $V(G)$ quasi-cohérent. □

Si G possède un relèvement $G' \in \mathrm{BT}(S')$, on a $\mathrm{Lie}(E(G')) = \mathbb{D}(G)_{S'}$ et 5.1 s'écrit :

$$0 \to V(G') \to \mathbb{D}(G)_{S'} \to \mathrm{Lie}(G') \to 0.$$

En particulier $V(G')$ est un sous-fibré vectoriel (i.e. localement facteur direct) de $\mathbb{D}(G)_{S'}$.

5.2 Définitions. On appelle *filtration admissible* de $\mathbb{D}(G)_{S'}$ un sous-fibré vectoriel $\mathrm{Fil}^1 \mathbb{D}(G)_{S'}$ qui relève $V(G)$. On note $\mathrm{DefBT}(S'/S)$ la catégorie suivante :
(1) les objets sont les paires $(G, \mathrm{Fil}^1 \mathbb{D}(G)_{S'})$ composées d'un BT sur S et d'une filtration admissible de $\mathbb{D}(G)_{S'}$,
(2) les morphismes $(G, \mathrm{Fil}^1 \mathbb{D}(G)_{S'}) \longrightarrow (H, \mathrm{Fil}^1 \mathbb{D}(G)_{S'})$ sont les morphismes $u : G \to H$ de groupes de BT tels que $\mathbb{D}(u)_{S'}$ respecte les filtrations.

5.3 Théorème. (Grothendieck, Messing) ([Mes72], V.1.6) *Le foncteur*

$$\begin{array}{ccc} \mathrm{BT}(S') & \longrightarrow & \mathrm{DefBT}(S'/S) \\ G' & \longmapsto & (G \times_{S'} S, V(G')) \end{array}$$

est une équivalence de catégories.

Preuve : Montrons que le foncteur est fidèle, i.e. que si $u' : G' \to H'$ est tel que $u = u'_{|S} = 0$ et $\xi' := V(u') = 0$ alors $u' = 0$. La question est locale donc on peut supposer S affine (pour appliquer 3.1). On note que $v_1 = E(u')$ et $v_2 = 0$ relèvent tous les deux $E(u) = E(0) = 0$. Par ailleurs $V(u') = 0$ implique que pour $j \in \{1, 2\}$ le morphisme v_j fait commuter le diagramme :

$$\begin{array}{ccc} V(G') & \longrightarrow & E(G') \\ {\scriptstyle w'=V(u')=0}\downarrow & \searrow^{d} & \downarrow{\scriptstyle v_j} \\ V(H') & \xrightarrow[i]{} & E(H'). \end{array}$$

De plus, on a $d = i \circ w' - v_{j\,|V(G')} = -v_{j\,|V(G')} = 0$ pour $j = 1, 2$. (Pour $j = 1$ ceci provient du fait que $v_{1|V(G')} = V(u') = 0$.) En particulier d est une exponentielle, et l'assertion d'unicité dans 3.1 jointe à la remarque 3.2 montre que $v_1 = v_2$ i.e. $E(u') = 0$. Il s'ensuit que $u' = 0$.

Montrons que le foncteur est plein, i.e. que si $u : G \to H$ est un morphisme dans $\mathrm{BT}(S)$ tel que $\mathbb{D}(u)_{S'} : \mathbb{D}(G)_{S'} = \mathrm{Lie}(E(G')) \to \mathbb{D}(H)_{S'} = \mathrm{Lie}(E(H'))$ est compatible aux filtrations admissibles i.e. induit un morphisme $\xi' : V(G') \to V(H')$, alors il existe $u' : G' \to H'$ qui relève u. Compte tenu de l'unicité d'un tel u' qui résulte de la fidélité, on peut supposer S affine. D'après le théorème 3.1, il existe un unique $v' : E(G') \to E(H')$ qui relève $v = E(u)$ et tel que $d = i \circ \xi' - v'_{|V(G')}$ est une exponentielle.

$$\begin{array}{ccc} V(G') & \longrightarrow & E(G') \\ {\scriptstyle w'=\xi'}\downarrow & \searrow^{d} & \downarrow{\scriptstyle v'} \\ V(H') & \xrightarrow[i]{} & E(H') \end{array}$$

Par construction du foncteur $\mathbb{D}$, on a $\mathrm{Lie}(v') = \mathbb{D}(u)_{S'}$ donc $\mathrm{Lie}(d) = 0$. Comme $E(H')$ est formellement lisse, ceci implique $d = 0$. En d'autres termes $v'_{|V(G')} = i \circ \xi'$, c'est-à-dire que v' envoie $V(G')$ dans $V(H')$ et donc passe au quotient en un morphisme $u' : G' \to H'$. Par unicité dans 3.1 on a $E(u') = v'$, donc $V(u') = \xi'$.

Il reste à montrer que le foncteur est essentiellement surjectif. Nous ne donnerons qu'une esquisse. Soit $(G, \mathrm{Fil}^1 \mathbb{D}(G)_{S'})$ un objet de $\mathrm{DefBT}(S'/S)$. On doit construire $G' \in \mathrm{BT}(S')$ qui relève G et tel que $V(G') = \mathrm{Fil}^1 \mathbb{D}(G)_{S'}$ comme sous-fibré de $\mathbb{D}(G)_{S'}$. Par unicité, la question est locale ; on peut supposer que S est affine et que G se relève en G'. Pour cela on commence par montrer que la donnée de la filtration $\mathrm{Fil}^1 \mathbb{D}(G)_{S'} \subset \mathrm{Lie}(E(G'))$ détermine un unique relèvement $V' \subset E(G')$ de $V(G)$; c'est une variante de la correspondance entre sous-algèbres de Lie et sous-groupes, qui fonctionne bien puisque $E(G')$ est formellement lisse. Ensuite on observe que s'il existe, le groupe G' est nécessairement $G' = E(G')/V'$ et le point principal restant à montrer est que le faisceau défini ainsi est bien un BT. Pour cela, on écrit $E(G') = \varinjlim E'(n)$ où $E'(n) = E(G') \times_{G'} G'(n)$ est représentable, plat et de présentation finie. On raisonne alors en utilisant les $E'(n)$. Les détails sont dans [Mes72], V.1.8. □

5.3.1 Remarques. Dans Messing, la rédaction est un peu rapide sur quelques points de détail. Dans la partie « fidélité », on part de $u' : G' \to H'$ tel que $u = u'_{|S} = 0$ et $\mathrm{Lie}(E(u')) = 0$, ce qui semble incorrect. Dans la partie « fidélité », le fait que $\mathrm{Lie}(d) = 0$ implique $d = 0$ est laissé au lecteur.

6 Algèbres, cogèbres et dualité

Le contenu de cette section n'a pas été mentionné dans l'exposé oral. Il s'agit de rappels de base visant à élucider un point de [Mes72], III.2.4. Précisément, on montre ci-dessous que le dual gradué

de l'algèbre symétrique $S(M)$ d'un module M, vue comme bigèbre, est l'algèbre à puissances divisées $\Gamma(M)$ de ce module. Pour obtenir ce résultat, l'hypothèse « projectif de type fini » ne semble pas nécessaire (il faudrait quand même vérifier). Sous cette hypothèse en tout cas, on déduit par bidualité que le dual gradué de $\Gamma(M)$ s'identifie à $S(M)$, et je ne sais pas si on peut l'obtenir directement (et sans hypothèse « projectif de type fini »). C'est ce dernier résultat qui est utilisé par Messing.

Dans cette section, on fixe un anneau commutatif R, non nécessairement unitaire. On rappelle les définitions de base sur les algèbres, cogèbres et bigèbres. Les références utiles sont : le chapitre III de Kassel [Ka95], les deux premiers chapitres de Brzezinski et Wisbauer [BW03] (qui présente l'avantage de présenter les al/co/bi-gèbres sur un anneau commutatif quelconque, contrairement à la plupart des sources de la littérature) et le § 11 de Bourbaki [Bo70] notamment pour la notion de dual gradué.

6.1 Algèbres

6.1.1 Définition. Une *R-algèbre* est un R-module A muni d'une application R-linéaire $m_A : A \otimes A \to A$. Elle est *associative* si $m \circ (m \otimes \mathrm{id}_A) = m \circ (\mathrm{id}_A \otimes m) : A \otimes A \otimes U \to A$. Elle est *commutative* si $m \circ \iota = m : A \otimes A \to A$, où $\iota : A \otimes A \to A \otimes A$ est l'échange des facteurs. Une *sous-R-algèbre* est un sous-R-module $A_0 \subset A$ tel que $m(A_0 \otimes A_0) \subset A_0$. Un *morphisme* entre deux R-algèbres A, B est une application R-linéaire $f : A \to B$ telle que $f \circ m_A = m_B \circ (f \otimes f) : A \otimes A \to B$. Le noyau et l'image de f sont des sous-R-algèbres. Une *unité* pour A est un morphisme de R-algèbres $e : R \to A$ tel que $m \circ (e \otimes \mathrm{id}_A) = m \circ (\mathrm{id}_A \otimes e) = \mathrm{id}_A$, où à la source on identifie $A \otimes R$ et A.

6.1.2 Remarque. Dans le cas où R est unitaire, une unité pour A est uniquement déterminée par l'élément $1 = 1_A = e(1_R)$ puisqu'alors $e(r) = r.1_A$.

6.1.3 Exemples d'algèbres. (1) Soit M un R-module. Alors $A = \mathrm{End}_R(M)$, munie de la multiplication $m(f, g) = f \circ g$, est une R-algèbre associative et unitaire, non commutative en général.

(2) Soit M un R-module et $M^* = \mathrm{Hom}_R(M, R)$ son dual. Alors $M^* \otimes M$, muni de la multiplication définie sur les tenseurs purs par $(\varphi \otimes m)(\varphi' \otimes m') = \varphi' \otimes \varphi(m')m$, est une algèbre associative, non unitaire (voir 6.1.5(2)) et non commutative en général.

(3) Soit A une R-algèbre. Alors $A^\circ = A$, munie de la multiplication $m_{A^\circ}(x, y) = m_A(y, x) = yx$, est une R-algèbre appelée *algèbre opposée* de A. De plus, l'identité $\mathrm{id}_A : A \to A^{\circ\circ}$ est un morphisme de R-algèbres (on écrit le plus souvent $A^{\circ\circ} = A$). L'identité $\mathrm{id}_A : A \to A^\circ$ est un morphisme de R-algèbres ssi A est commutative. Si $f : A \to B$ est un morphisme de R-algèbres, alors $f^\circ = f : A^\circ \to B^\circ$ est un morphisme de R-algèbres.

6.1.4 Exemples de sous-algèbres. (1) Soit A une R-algèbre et $S \subset A$ une partie. Alors $Z_A(S) = \{a \in A;\ as = sa,\ \forall s \in S\}$ est une sous-R-algèbre de A appelée le *commutant de S dans A*. En particulier $Z(A) = Z_A(A)$ est le *centre* de A. Si A possède une unité $e : R \to A$, alors $e(R) \subset Z(A)$ puisque les axiomes d'unité entraînent que pour tous $r \in R$ et $a \in A$ on a $ra = e(r)a = ae(r)$.

(2) Soit M un R-module et $A = \mathrm{End}_R(M)$. Alors le sous-module $A_0 \subset A$ des endomorphismes dont l'image est un module de type fini forme une sous-algèbre de A.

(3) Soient $f_1, \ldots, f_n : A \to B$ des morphismes d'algèbre. Alors $\mathrm{Eq}(f_1, \ldots, f_n) = \{a \in A;\ f_1(a) = \cdots = f_n(a)\}$ est une sous-R-algèbre de A.

6.1.5 Exemples de morphismes. (1) Soit A une R-algèbre. Pour tout $x \in A$, notons $g_x : A \to A$ l'application R-linéaire définie par $g_x(y) = xy$. Alors $g : A \to \mathrm{End}_R(A)$, $g(x) = g_x$ est un morphisme de R-algèbres. Notons $d_x : A \to A$ l'application R-linéaire définie par $d_x(y) = yx$. Alors $d : A \to \mathrm{End}_R(A)^\circ$, $d(x) = d_x$ est un morphisme de R-algèbres.

(2) Soit M un R-module, $M^* = \mathrm{Hom}_R(M,R)$ son dual. L'application $f : M^* \otimes M \to \mathrm{End}_R(M)$ définie sur les tenseurs purs par $f(\varphi \otimes m) = (x \mapsto \varphi(x)m)$ est un morphisme de R-algèbres. L'image par f d'un tenseur arbitraire $\sum_{i=1}^n \varphi_i \otimes m_i$ est un endomorphisme dont l'image est incluse dans $\langle m_1, \ldots, m_n \rangle$. Ainsi, l'image de f est incluse dans la sous-algèbre des endomorphismes dont l'image est module de type fini, cf 6.1.4(2). En particulier, si M n'est pas de type fini alors $\mathrm{id}_M \notin \mathrm{im}(f)$. Bien sûr, si M est projectif de type fini, f est un isomorphisme et $M^* \otimes M$ est unitaire.

6.2 Cogèbres

On dualise les définitions de la section 6.1, i.e. on y renverse le sens des flèches.

6.2.1 Définition. Une *R-cogèbre* est un R-module U muni d'une application R-linéaire $c = c_U : U \to U \otimes U$. Elle est *coassociative* si $(c \otimes \mathrm{id}_A) \circ c = (\mathrm{id}_A \otimes c) \circ c : U \to U \otimes U \otimes U$. Elle est *cocommutative* si $\iota \circ c = c : U \to U \otimes U$, où $\iota : U \otimes U \to U \otimes U$ est l'échange des facteurs. Un *morphisme* entre deux R-cogèbres U, V est une application R-linéaire $f : U \to V$ telle que $c_V \circ f = (f \otimes f) \circ c_U : U \to V \otimes V$. Une *sous-$R$-cogèbre* est un sous-$R$-module $U_0 \subset U$ muni d'une structure de R-cogèbre telle que l'inclusion est un morphisme de cogèbres. Une *counité* pour U est un morphisme de R-cogèbres $\eta : U \to R$ tel que $(\eta \otimes \mathrm{id}_U) \circ c = (\mathrm{id}_U \otimes \eta) \circ c = \mathrm{id}_U$, où au but on identifie $U \otimes R$ et U.

On prendra garde que dans la définition d'une sous-cogèbre, on ne peut pas simplement écrire que $c(U_0) \subset U_0 \otimes U_0$ puisque ce produit tensoriel n'est pas en général sous-module de $U \otimes U$.

6.2.2 Exemples de cogèbres. (1) cogèbre opposée de U.

(2) Soit I un ensemble et $U = R^{(I)}$ muni de sa base canonique $(e_i)_{i \in I}$. L'application $c : U \to U \otimes U$, $c(e_i)e_i \otimes e_i$ munit U d'une structure de cogèbre.

(3) Soit M un R-module et $T(M)$ son algèbre tensorielle. Il existe une unique application linéaire $c : T(M) \to T(M) \otimes T(M)$ telle que $c(x_1 \ldots x_n) = \sum_{i=0}^n (x_1 \ldots x_i) \otimes (x_{i+1} \ldots x_n)$, pour tous $x_i \in M$. Elle fait de $T(M)$ une cogèbre.

(4) Soit M un R-module et $S(M)$ son algèbre symétrique. La diagonale $M \to M \oplus M$ s'étend en une application linéaire $S(M) \to S(M \oplus M) \simeq S(M) \otimes S(M)$ qui fait de $S(M)$ une cogèbre.

(5) Soit U une R-cogèbre et $A = \mathrm{Hom}_R(U,R)$ le module dual. Alors la composée $A \otimes A = U^* \otimes U^* \to (U \otimes U)^* \xrightarrow{c^*} U^* = A$ munit A d'une structure d'algèbre.

(6) Soit A une R-algèbre dont le module sous-jacent est projectif de type fini, et $U = \mathrm{Hom}_R(A,R)$ le module dual. Comme $A^* \otimes A^* \to (A \otimes A)^*$ est un isomorphisme, on munit U d'une structure de cogèbre. Sans hypothèse projective de type fini, le module U n'hérite pas en général de structure de cogèbre.

(7) La cogèbre $U = \mathrm{M}_n(R)$.

(8) Produit tensoriel de deux cogèbres.

6.2.3 Proposition. *Soit A un R-module muni de structures de R-algèbre unitaire (m,e) et de R-cogèbre counitaire (c,η). Alors, les conditions suivantes sont équivalentes :*

(1) les applications m et e sont des morphismes de cogèbre,

(2) les applications c et η sont des morphismes d'algèbre.

6.2.4 Définition. Une R-bigèbre est un quintuplet (A, m, e, c, η) tel que (A, m, e) est une R-algèbre et (A, c, η) est une R-cogèbre satisfaisant les conditions de la proposition précédente.

6.2.5 Définition. Une R-algèbre de Hopf est une bigèbre qui possède une *antipode* S. (Voir la définition précise dans Kassel [Ka95].)

6.2.6 Exemples. Les exemples $T(M)$, $S(M)$, $\mathrm{M}_n(R)$ sont des algèbres de Hopf. Aussi bien sûr l'algèbre de groupe $k[G]$ d'un groupe G. Aussi l'algèbre de fonctions d'un groupe algébrique. Aussi l'algèbre de Hopf duale d'une algèbre de Hopf de dimension finie.

6.3 Dualité

On a vu que le dual linéaire d'une cogèbre est une algèbre, mais que le dual linéaire d'une algèbre n'est pas toujours une cogèbre. Pour faire fonctionner une bidualité, on doit faire appel aux stratagèmes habituels, par exemple ajouter des hypothèses « projectif de type fini », ou considérer des duaux continus, etc. Un autre cas favorable est celui des algèbres graduées dont les composantes homogènes sont localement libres de type fini ; on aura alors une notion utile de dual gradué. Voyons voir tout ça.

6.3.1 Définition. Algèbre graduée.

6.3.2 Définition. Une *R-cogèbre $\mathbb{N}$-graduée* est un R-module gradué $U = \oplus_{n\in\mathbb{N}} U_n$ muni d'une structure de cogèbre $c : U \to U \otimes U$ telle que $c(U_n) \subset \oplus_{p+q=n} U_p \otimes U_q$. Si U possède une counité $\eta : U \to R$, on demande en plus que η se factorise par U_0 i.e. $\eta(U_n) = 0$ si $n \geqslant 1$.

Remarque 1 : comme les U_n sont facteurs directs, les modules $\oplus_{p+q=n} U_p \otimes U_q$ sont bien des sous-modules de $U \otimes U$. Remarque 2 : les modules $\oplus_{p+q=n} U_p \otimes U_q$ sont localement libres de type fini (ce ne serait pas aussi simple pour les cogèbres graduées avec un autre semi-groupe de graduation).

6.3.3 Définition. Soit $A = \oplus_{n\in\mathbb{N}} A_n$ une R-algèbre graduée dont les composantes A_n sont localement libres de type fini. On définit la cogèbre duale graduée par $A^* = \oplus_{n\in\mathbb{N}} A_n^*$.

6.3.4 Définition. Soit $U = \oplus_{n\in\mathbb{N}} U_n$ une R-cogèbre graduée. On définit l'algèbre duale graduée par $U^* = \oplus_{n\in\mathbb{N}} U_n^*$.

6.4 Duale graduée d'une algèbre symétrique

Soit M un R-module et $S(M)$ son algèbre symétrique, qui est en fait une algèbre de Hopf. Nous allons montrer que l'algèbre sous-jacente à la bigèbre duale graduée de $S(M)$ est l'algèbre à puissances divisées de M.

On part de la comultiplication de $S(M)$, donnée par $c : S(M) \to S(M) \otimes S(M)$ qui correspond à la diagonale de M en degré 1. L'application

$$c_n : S^n(M) \longrightarrow (S(M) \otimes S(M))_n = \bigoplus_{p+q=n} S^p(M) \otimes S^q(M)$$

est donnée par

$$c_n(x_1 \dots x_n) = \sum_{I,J} \left(\prod_{i\in I} x_i \right) \left(\prod_{i\in J} x_i \right),$$

la somme portant sur les partitions $I \amalg J = \{1, \dots, n\}$. Si on projette sur la composante de bidegré (p, q) on trouve $c_{p,q} : S^n(M) \longrightarrow S^p(M) \otimes S^q(M)$ donnée par

$$c_{p,q}(x_1 \dots x_n) = \sum_{|I|=p, |J|=q} \left(\prod_{i\in I} x_i \right) \left(\prod_{i\in J} x_i \right).$$

En dualisant, on voit que $c^* : S^p(M)^* \otimes S^q(M)^* \to S^n(M)^*$ est l'application qui, pour toutes formes $\varphi \in S^p(M)^*$ et $\psi \in S^q(M)^*$, envoie $\varphi \otimes \psi$ sur la forme :

$$c^*(\varphi \otimes \psi) : x_1 \dots x_n \longmapsto \sum_{|I|=p,|J|=q} \varphi\left(\prod_{i\in I} x_i\right) \psi\left(\prod_{i\in J} x_i\right).$$

Plus généralement, l'application $(S^p(M)^*)^{\otimes k} \to S^{pk}(M)^*$ envoie $\varphi_1 \otimes \cdots \otimes \varphi_k$ sur la forme suivante :

$$c^*(\varphi_1 \otimes \cdots \otimes \varphi_k) : x_1 \dots x_n \longmapsto \sum_{I_1,\dots,I_k} \varphi_1\left(\prod_{i\in I_1} x_i\right) \dots \varphi_k\left(\prod_{i\in I_k} x_i\right)$$

où la somme porte sur les partitions de $\{1, \dots, n\}$ en k parts $I_1, \dots, I_k$ de taille p. En particulier :

$$c^*(\varphi^{\otimes k}) : x_1 \dots x_n \longmapsto \sum_{I_1,\dots,I_k} \varphi\left(\prod_{i\in I_1} x_i\right) \dots \varphi\left(\prod_{i\in I_k} x_i\right).$$

On reconnaît dans la somme des orbites sous l'action libre du groupe symétrique $\mathfrak{S}_k$ sur l'ensemble des partitions comme ci-dessus, par permutation des I_i. La somme est donc divisible par $k!$. Une autre manière de l'écrire est de choisir un représentant privilégié dans chaque $\mathfrak{S}_k$-orbite, par exemple la partition $I_1 \amalg \cdots \amalg I_k$ telle que $\min(I_1) < \cdots < \min(I_k)$.

Références

[Be74] P. Berthelot, *Cohomologie cristalline des schémas de caractéristique $p > 0$*, Lecture Notes in Mathematics 407, Springer, 1974.

[Bo70] N. Bourbaki, *Algèbre, Chapitre 3. Algèbres tensorielles, algèbres extérieures, algèbres symétriques*, Hermann, 1970.

[BW03] T. Brzezinski, R. Wisbauer, *Corings and comodules*, London Math. Society Lecture Note Series 309, Cambridge University Press, 2003.

[Gro74] A. Grothendieck, *Groupes de Barsotti-Tate et cristaux de Dieudonné*, Séminaire de Mathématiques Supérieures no. 45 (1970), Les Presses de l'Université de Montréal, 1974.

[Ill85] L. Illusie, *Déformations de groupes de Barsotti-Tate (d'après A. Grothendieck)*, Séminaire sur les pinceaux arithmétiques : la conjecture de Mordell (Paris, 1983/84), Astérisque 127 (1985), 151–198.

[Ill13] L. Illusie, *Grothendieck at Pisa : crystals and Barsotti-Tate groups*, www.math.u-psud.fr/ illusie/Illusie-Pisa5.pdf.

[Ka95] Ch. Kassel, *Quantum groups*, Graduate Texts in Math. 155, Springer, 1995.

[MM74] B. Mazur, W. Messing, *Universal extensions and one dimensional crystalline cohomology*, Lecture Notes in Mathematics 370, Springer, 1974.

[Mes72] W. Messing, *The crystals associated to Barsotti-Tate groups : with applications to abelian schemes*, Lecture Notes in Mathematics 264, Springer, 1972.