Groupes formels p-divisibles et théorie de Cartier-Zink

Laurent Fargues

18 novembre 2003

Table des matières

1 G-foncteurs formels

Dans cette section on démontre un cas particulier de pro-représentabilité de [2], le cas formellement lisse.

1.1 La catégorie $\mathbf{Nilp}_R$

Soit R un anneau commutatif unitaire.

Définition 1.1. *La catégorie* $\mathbf{Nilp}_R$ *est la catégorie des* R *algèbres (non nécessairement unitaires) nilpotentes, ou de façon équivalente la catégorie des* R *algèbres augmentées* $R \oplus I_R$ *où l'idéal* I_R *est nilpotent.*

Géométriquement les objets de $Nilp_R$ sont des épaississements infinitésimaux de $\boldsymbol{Spec}(R)$ munis d'une rétraction : $\boldsymbol{Spec}(R) \to \boldsymbol{Spec}(R \oplus I_R)$.

Remarque 1.1. *On se restreint à la catégorie des algèbres augmentées car via leur section unité les schémas en groupes, groupes formels... sont localement représentés par des spectres d'alèbres augmentées. Le lemme de Yoneda nous dit donc qu'il suffit de se restreindre à de telles algèbres.*

Définition 1.2. *Une suite de morphismes* $N' \to N \to N''$ *dans* $\mathbf{Nilp}_R$ *est dite exacte (resp. exacte à gauche) si elle est exacte comme suite de groupes abéliens (resp. exacte à gauche et si l'image de* N *est un idéal de* N''*)*

N' est alors un idéal de N, $N/N' \hookrightarrow N''$.

Remarque 1.2. $\mathbf{Nilp}_R$ *admet des sommes directes finies, et infinies pour des algèbres dont l'indice de nilpotence est borné*
$\mathbf{Nilp}_R$ *admet des produits fibrés*

On remarque que l'on a alors un plongement exacte de la catégorie mod $_R$ dans $\mathbf{Nilp}_R$ qui à M associe l'algèbre dont la loi multiplicative est la loi triviale i.e. $M^2 = 0$, ou encore l'algèbre augmentée $R \oplus M$ avec comme lois :

$$(x, m) + (x', m') = (x + x', m + m')$$

$$(x, m).(x', m') = (xx', xm' + xm)$$

Exemple fondamental : si $M = R$ alors l'algèbre augmentée associée est $R[\epsilon]$, l'algèbre des nombres duaux et plus généralement pour $M = R^n$, on a $R[\epsilon_1, \ldots, \epsilon_n]$, $\forall i\ \epsilon_i^2 = 0$.

Définition 1.3. *Un morphisme* $N_1 \overset{\alpha}{\to} N_2$ *dans* $\mathbf{Nilp}_R$ *est une petite surjection si c'est une surjection telle que* $N_1.\ker(\alpha) = 0$

L'intérêt des petites surjections est que toute surjection $N_1 \overset{\alpha}{\to} N_2$ se dévisse en une suite de petites surjections

$$N_1 = M_1 \twoheadrightarrow M_2 \twoheadrightarrow \cdots \twoheadrightarrow M_{n-1} \twoheadrightarrow M_n = N_2$$

Pour cela il suffit de regarder les $N_1/(N_1^k.\ker(\alpha))$. Les assertions faisant intervenir les surjections se ramènent donc par dévissage à des assertions sur les petites surjections.

1.2 Foncteurs sur $\mathbf{Nilp}_R$

Définition 1.4. *Soit* $H : \mathbf{Nilp}_R \to \mathbf{Ab}$ *un foncteur.*
- *H est dit exacte (resp. exacte à gauche) si ...*
- *H vérifie la propriété de Mayer Vietoris si* $\forall\ N' \to N \leftarrow N''$, $H(N' \times_N N'') \overset{\sim}{\to} H(N') \times_{H(N)} H(N'')$
- *H est dit lisse si pour toute surjection α, $H(\alpha)$ est une surjection*

Proposition 1.1. *H est exact à gauche ssi il vérifie la propriété de Mayer Vietoris.*

On vérifie d'abord que pour H vérifiant l'une des deux propriétés dont on veut montrer l'équivalence, $H(0) = 0$ (il suffit d'écrire $0 = 0 \oplus 0$). Soit H vérifiant M.V. Alors, pour tout morphisme $\alpha : N \to N'$, $\ker(\alpha) = N \times_{N'} 0$ et donc M.V. $\Rightarrow H(\ker(\alpha)) = \ker(H(\alpha))$ ce qui implique l'exactitude à gauche de H.

Soit réciproquement H exacte à gauche. Montrons tout d'abord que H préserve les sommes directes finies i.e. $H(N \oplus N') \overset{\sim}{\to} H(N) \oplus H(N')$. En effet, la suite exacte

$$0 \to N \to N \oplus N' \to N' \to 0$$

est transformée en une suite exacte à gauche

$$0 \to H(N) \to H(N \oplus N') \to H(N')$$

Mais la suite précédente était scindée via $N' \to N \oplus N'$, donc la suite est exacte scindée et donne l'isomorphisme voulu. Commençons par un lemme :

Lemme 1.1. *Soit*

$$\begin{array}{ccc} N & \longrightarrow & N_2 \\ \downarrow & & \downarrow{\scriptstyle i} \\ N_1 & \longrightarrow & N_3 \end{array}$$

où i est une injection faisant de N_2 un idéal de N_3.
Ce diagramme est cartésien ssi la suite suivante est exacte :

$$0 \to N \to N_1 \to N_3/N_3$$

La vérification de ce lemme est immédiate. On remarque que celui-ci est également vrai (en enlevant l'hypothèse "idéal") dans **Ab**.

On en déduit immédiatement en appliquant le lemme dans $\mathbf{Nilp}_R$, en appliquant H exact à gauche, puis en réappliquant le lemme dans **Ab** (car $H(i)$ est une injection) que H vérifie M.V. pour de tels diagrammes cartésien.

Pour un diagramme cartésien quelconque

$$\begin{array}{ccc} N & \longrightarrow & N_2 \\ \downarrow & & \downarrow{\scriptstyle i} \\ N_1 & \xrightarrow{u} & N_3 \end{array}$$

on peut toujours se ramener à ce que i soit une injection en le transformant en le diagramme cartésien

$$\begin{array}{ccc} N & \longrightarrow & N_1 \oplus N_2 \\ \downarrow & & \downarrow{\scriptstyle i'} \\ N_1 \oplus N_2 & \longrightarrow & N_1 \oplus N_2 \oplus N_3 \end{array}$$

où i' est injective mais l'image de i' n'est pas forcément un idéal . Comme H commute aux sommes directes finies, si ce diagramme est transformé en un diagramme cartésien, on en déduit que

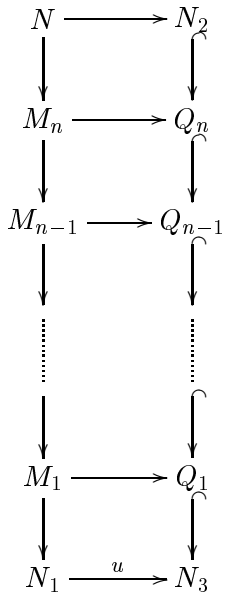
$$\begin{array}{ccc} H(N) & \longrightarrow & H(N_1) \oplus H(N_2) \\ \downarrow & & \downarrow{\scriptstyle H(i')} \\ H(N_1) \oplus H(N_2) & \longrightarrow & H(N_1) \oplus H(N_2) \oplus H(N_3) \end{array}$$

est cartésien et que donc (facile)

$$\begin{array}{ccc} H(N) & \longrightarrow & H(N_2) \\ \downarrow & & \downarrow \\ H(N_1) & \longrightarrow & H(N_3) \end{array}$$

est cartésien.

Il suffit donc de montrer que lorsque i est une injection on peut se ramener à ce que son image soit un idéal. Cela se fait par dévissage : on montre l'existence d'un diagramme



dans lequel chaque carré est cartésien et l'image du morphisme de droite est un idéal . Il suffit pour cela de choisir n tel que $N_2^{n+1} = 0$, de poser $Q_i = N_2 + N_3.N_2^i$ et $P_i = u^{-1}(Q_i)$. Si on prend H de ce diagramme, chaque carré est transformé en un carré cartésien par le cas précédent et donc le tout se recolle pour donner un carré cartésien (un carré cartésien n'étant qu'une limite projective, cela n'est rien d'autre le fait qu'une limite projective de limite projective est une limite projective). □

Définition 1.5. *Un G foncteur formel est un foncteur G : $\mathbf{Nilp}_R \to \mathbf{Ab}$ exact et qui commute aux sommes directes arbitraires.*

Cette définition s'interprète ainsi :
- L'exactitude à gauche est une condition nécessaire de pro-représentabilité
- On demande de plus la lissité ce qui veut dire lorsque G est pro-représentable que l'algèbre augmentée associée est une algèbre de séries formelles.
- la commutativité aux sommes directes quelconques est une sorte de continuité du foncteur (puisque l'exactitude implique déjà qu'il commute aux sommes finie)

1.3 Exemples

Soit $A = R \oplus I_R$ une R algèbre augmentée (non nécessairement nilpotente) . On vérifie que $\mathbb{G}_{mA}(N) = ((1 + I_A \otimes_R N), \times)$ (la restriction des scalaires de $\mathbb{G}_m$ sur A à R) est un G-foncteur formel lorsque I_A est plat sur R.
Par exemple si $A = R[t]$, $\mathbb{G}_{mR[t]}(N) = \{1 + tu_1 + \cdots + t^r u_r \mid u_i \in N\}$.

1.3.1 Foncteurs représentables et pro-représentables

Si $A = R \oplus I_A$ est une R-algèbre augmentée nilpotente on note $\boldsymbol{Spf}(A)$ le foncteur de $Nilp_R$ dans $\boldsymbol{\mathcal{E}ns}$ défini par $\boldsymbol{Spf}(A)(N) = \mathcal{H}\mathrm{om}_R(I_A, N) = \mathcal{H}\mathrm{om}_R(A, R \oplus N)$. Par le lemme de Yoneda on obtient ainsi un plongement de $\mathbf{Nilp}_R$ dans la catégorie des foncteurs sur $\mathbf{Nilp}_R$. De plus dans ce cas là, $\boldsymbol{Spec}(A) = \boldsymbol{Spf}(A)$ i.e. le foncteur est représenté dans la catégorie des schémas. On obtient ainsi un plongement des schémas en groupe affine finis sur R dans $\mathcal{H}\mathrm{om}(\mathbf{Nilp}_R, \mathbf{Ab})$.

Plus généralement, si A est une R algèbre augmentée complète (par rapport à son idéal d'augmentation), $A = \varprojlim A_i$, $\boldsymbol{Spf}(A)$ est le foncteur prolongé par continuité à partir des $\boldsymbol{Spf}(A_i)$ en posant

$$\boxed{\boldsymbol{Spf}(A)(N) = \varinjlim \boldsymbol{Spf}(A_i)(N) = \mathcal{H}\mathrm{om}_{\mathrm{Cont}}(I_A, N)}$$

où N est muni de la topologie discrète.
Par extension du lemme de Yoneda, cela donne un plongement des R-algèbres augmentées complètes dans les foncteurs sur $\mathbf{Nilp}_R$. De plus $\boldsymbol{Spf}(A)$ est représenté dans la catégorie des schémas formels (cf. EGA).

En particulier, le foncteur $N \mapsto N^n$ est pro-représenté par $R[[X_1, \ldots, X_n]]$. Ainsi on a un plongement des groupes formels sur R dans la catégorie des foncteurs pro-représentables à valeurs dans $\mathbf{Ab}$. Et l'on sait bien qu'un foncteur pro-représentable est lisse ssi c'est un groupe formel.

1.4 Foncteurs associés sur $\mathbf{Comp}_R$ et foncteurs continus

Soit $\mathbf{Comp}_R$ la catégorie des R algèbres augmentées complètes (par rapport à leur idéal d'augmentation). On s'intéresse aux foncteurs $H : \mathbf{Comp}_R \to \boldsymbol{\mathcal{E}ns}$ (ou $\mathbf{Ab}$) qui sont déterminés par leur restriction à $\mathbf{Nilp}_R$.

Définition 1.6. *H sera dit continu si $\forall N = \varprojlim N_i$, $H(N) \xrightarrow{\sim} \varprojlim H(N_i)$ est un isomorphisme.*

L'injection de la catégorie des foncteurs continus sur $\mathbf{Comp}_R$ dans celle des foncteurs sur $\mathbf{Nilp}_R$ possède un adjoint : si $H : \mathbf{Nilp}_R \to \boldsymbol{\mathcal{E}ns}$, le foncteur continu associé est

$$\boxed{\widehat{H} : N = \varprojlim N_i \longmapsto \varprojlim H(N_i).}$$

Il étend H à $\mathbf{Comp}_R$.

Dans le cas où $H = \boldsymbol{Spf}(A)$, on vérifie aussitôt que $\widehat{H}$ encore noté $\boldsymbol{Spf}(A)$ est défini par

$$\boxed{\boldsymbol{Spf}(A)(N) = \mathcal{H}\mathrm{om}_{\mathrm{Cont}}(A, N)}$$

où Cont signifie les morphismes continus pour A et N munis de leur topologie d'algèbre complète. Dorénavant, pour H un foncteur sur $\mathbf{Nilp}_R$ on notera encore H pour $\widehat{H}$ l'extension canonique de H.

On notera que l'on a encore un lemme de Yoneda : pour $H : \mathbf{Nilp}_R \to \boldsymbol{\mathcal{E}ns}$, $\mathcal{H}\mathrm{om}(\boldsymbol{Spf}(A), H) \simeq H(A)$.

1.5 Le foncteur tangent

Définition 1.7. *Pour $H : \mathbf{Nilp}_R \to \mathbf{Ab}$, on pose t_H le foncteur tangent égal à la restriction de H à mod $_R$ vue comme sous catégorie de $\mathbf{Nilp}_R$*

Soit l'hypothèse

$$(+) \quad t_H(M \times N) \simeq t_H(M) \times t_H(N)$$

où M et N sont des R-modules

Lemme 1.2. *Si H vérifie $(+)$ alors il se factorise à travers mod $_R$.*

En effet, les applications

$$+ : M \oplus M \to M$$

et $\forall r \in R$

$$r : M \xrightarrow{\times r} M$$

donnent par fonctorialité et le fait que $t_H(M \oplus M) \simeq t_H(M) \oplus t_H(M)$ une structure de R module sur $t_H(M)$ puisque les axiomes d'un R-module peuvent s'exprimer par des diagrammes commutatifs. On vérifie également que la loi $H(+)$ coïncide avec celle de $\mathbf{Ab}$. □

L'interprétation géométrique du foncteur tangent est que $t_H(R)$ est "l'espace tangent de Zariski" de H, puisque si H est représentable par N, $t_H(R) \simeq (N/N^2)^*$. Lorsque l'on cherche à (pro-)représenter H, un système de générateurs de $t_H(R)$ devrait correspondre à un système générateur de l'algèbre. Si H est lisse il n'y aura pas de relations. Dans le cas contraire le problème est plus compliqué (dans d'autres catégories que $\mathbf{Nilp}_R$, l'espace tangent est souvent interprété comme un H^1 tandis qu'un H^2 représente les relations).

Soit $M \in$ mod $_R$, H vérifiant $(+)$ et $m \in M$. L'application $c_m : r \to M$ de multiplication par m donne alors une application

$$\begin{aligned} M \otimes_R t_H(R) &\to t_H(M) \\ m \otimes \xi &\mapsto t(c_m)(\xi) \end{aligned}$$

dont on vérifie aussitôt que c'est un morphisme de R-modules.

Proposition 1.2. *Si de plus H est exacte à droite et commute aux sommes arbitraires alors cette application est un isomorphisme. On a donc un isomorphisme de foncteurs* $\boxed{\_ \otimes t_H(R) \xrightarrow{\sim} t_H(\_)}$

Pour $M = R$ l'application est clairement un isomorphisme. En particulier cela est vrai pour H un G-foncteur formel. H commutant aux sommes quelconques, $\forall I$ c'est vrai pour $R^{(I)}$. Si l'on choisit une résolution

$$R^{(I)} \to R^{(J)} \to M \to 0$$

Alors H et $\_ \otimes_R t_H(R)$ étant tous deux exactes à gauche

$$\begin{array}{ccccccc} t_H(R^{(I)}) & \longrightarrow & t_H(R^{(J)}) & \longrightarrow & t_H(M) & \longrightarrow & 0 \\ \downarrow \simeq & & \downarrow \simeq & & \downarrow & & \\ R^{(I)} \otimes_R t_H(R) & \longrightarrow & R^{(J)} \otimes_R t_H(R) & \longrightarrow & M \otimes t_H(R) & \longrightarrow & 0 \end{array}$$

commute avec deux lignes exactes. D'où le résultat par le lemme des cinq. □

Remarque 1.3. *Si H est exacte, alors par le lemme précédent $\_ \otimes_R t_H(R)$ l'est également et donc $t_H(R)$ est un R-module plat.*

1.6 Le théorème fondamental

Le but est de démontrer le théorème suivant :

Théorème 1.1. *Soit G un G-foncteur formel tel que $t_H(R)$ soit libre de rang n. Alors G est un groupe formel i.e. est pro-représentable par un $R[[X_1, \ldots, X_n]]$.*

Soit $H : \mathbf{Nilp}_R \to \mathbf{Ab}$ un foncteur.

Soit $\alpha : M \twoheadrightarrow N$ une petite surjection dans $\mathbf{Nilp}_R$. Notons $K = \ker(\alpha)$. On a donc, $K.M = 0$. En particulier $K^2 = 0 \Rightarrow K \in R - \text{ mod}$. Dès lors, $H(K) = t_H(K)$ est un R-module. On a de plus un diagramme cartésien dans $\mathbf{Nilp}_R$:

$$\begin{array}{ccc} K \times M & \xrightarrow{+} & M \\ \downarrow{\scriptstyle pr_2} & & \downarrow{\scriptstyle \alpha} \\ M & \xrightarrow{\alpha} & N \end{array}$$

où $+ : K \times M \to M$ est l'addition qui est une application d'algèbre puisque $M.K = 0$.

Supposons que H vérifie M.V.. Alors on vérifie que $H(+) : H(K) \times H(M) \to H(M)$ munie $H(M)$ d'une action de $H(K)$. Si pour $\xi \in H(N)$ on note $H(M)_\xi$ la fibre de $H(\alpha)$ au dessus de ξ on obtient alors pour tout ξ une action de $H(K)$ sur $H(M)_\xi$.

De plus le diagramme précédent est transformé en

$$\begin{array}{ccc} H(K) \times H(M) & \xrightarrow{H(+)} & H(M) \\ \downarrow{\scriptstyle pr_2} & & \downarrow{\scriptstyle H(\alpha)} \\ H(M) & \xrightarrow{H(\alpha)} & H(N) \end{array}$$

Et on vérifie immédiatement :

Lemme 1.3. *Ce diagramme est cartésien ssi pour tout $\xi \in H(N)$, $H(K)$ agit simplement transitivement sur $H(M)_\xi$. En particulier H vérifiant M.V., c'est le cas.*

Montrons maintenant :

Proposition 1.3. *Soit $\beta : H \to G$ un morphisme de foncteurs de $\mathbf{Nilp}_R$ dans $\mathbf{Ab}$ tel que β induise un isomorphisme des foncteurs tangents : $\beta : t_H \xrightarrow{\sim} t_G$. Supposons que H et G vérifient M.V. et que H est lisse. Alors β est un isomorphisme.*

Soit $N \in \mathbf{Nilp}_R$, décomposons la surjection $N \to 0$ en une suite de petites surjections :

$$NM_1 \xrightarrow{\alpha} \cdots\cdots \twoheadrightarrow M_k \twoheadrightarrow 0$$

Par récurrence sur k on peut supposer que $\beta : H(M_1) \xrightarrow{\sim} G(M_1)$.

On obtient alors un diagramme commutatif

$$\begin{array}{ccc} H(N) & \xrightarrow{u} & H(M_1) \\ {\scriptstyle\beta}\downarrow & & \downarrow{\scriptstyle\simeq\,\beta} \\ G(N) & \xrightarrow{v} & G(M_1) \end{array}$$

où u est surjective par lissité et où celle du bas est surjective par commutativité du diagramme et le fait que u et le β de droite est surjectif.

En fibrant ce diagramme au dessus d'un ξ dans la colonne de droite, il suffit donc de montrer que pour tout ξ l'application $H(N)_\xi \to G(N)_\xi$ entre les fibres est bijective. Mais si K désigne le noyau de α alors $H(K) = t_H(K) \simeq t_G(K) = G(K)$ qui agissent simplement transitivement sur $H(N)_\xi$ et $G(N)_\xi$ puisque H et G vérifient M.V. (et car ces deux ensembles sont non vides par surjectivité de u et v ! !). L'application $H(N) \to G(N)$ s'identifie alors à un isomorphisme d'espaces homogènes principaux. □

Montrons maintenant un lemme de "continuité" pour les foncteurs lisses.

Lemme 1.4. *Soit $\varphi : A \twoheadrightarrow B$ un morphisme surjectif de R algèbres augmentées complètes. Supposons que φ identifie B à un quotient de A comme algèbre complète (i.e. $A/\ker(\varphi) \simeq B$ est un homéomorphisme, ou encore φ envoie un système fondamental de voisinages de 0 dans A sur un de B). Soit H : $\mathbf{Nilp}_R \to \boldsymbol{\mathcal{E}}\mathbf{ns}$ un foncteur lisse vérifiant M.V.. Alors $H(\varphi) : H(A) \to H(B)$ est surjectif.*

La démonstration se fait bien sûr par construction d'une image réciproque par étapes. Par hypothèse on peut supposer que $A = \varprojlim A/I_i$ et $B = \varprojlim A/(I_i + J)$ où $J = \ker(\varphi)$. Considérons le diagramme commutatif suivant :

$$\begin{array}{ccc} A_{n+1} = A/I_{n+1} & \longrightarrow & A/(I_{n+1} + J) = B_{n+1} \\ \downarrow & & \downarrow \\ A_n = A/I_n & \longrightarrow & A/(I_n + J) = B_n \end{array}$$

L'application déduite $A_{n+1} \to A_n \times_{B_n} B_{n+1}$ est surjective. En effet, si $a_1, a_2 \in A$ et $a_1 \equiv a_2[I_n + J]$, donc $\exists u \in I_n\ \exists v \in J,\ a_1 - a_2 = u + v$. Alors $a_1 - u = a_2 + v$, $a_1 - u \equiv a_2[I_n]$ et $a_2 + v \equiv a_2[I_{n+1} + J]$.

Par lissité et M.V. on en déduit que l'application

$$H(A_{n+1}) \to H(A_n) \times_{H(B_n)} H(B_{n+1})$$

est surjective.

Dès lors, soir $(\xi_n)_n \in \varprojlim H(B_n) = H(B)$. La surjectivité de l'application précédente nous dit exactement que l'on peut construire une image réciproque $(\eta_n)_n \in H(A)$ par récurrence sur n. □

Nous pouvons maintenant démontrer le théorème voulu :

Théorème 1.2. *Si G est un G-foncteur formel tel que $t_G(R)$ soit libre de rang n alors G est un groupe formel de dimension n.*

Soit $M \in \text{ mod }_R$. D'après la proposition 1.2,

$$t_G(M) \simeq M \otimes t_G(R) \simeq \mathcal{H}\text{om}_R(\Omega, M)$$

où $\Omega = t_G(R)^*$ puisque $t_G(R)$ est libre.

Pour $M = \Omega$ cela donne $t_G(\Omega) = \mathcal{H}\text{om}_R(\Omega, \Omega)$. Soit ξ l'élément de $t_G(\Omega) = G(R \oplus \Omega)$ correspondant à l'identité. Par le lemme de Yoneda, ξ provient d'un morphisme $\boldsymbol{Spf}(R \oplus \Omega) \to G$ induisant l'identité sur l'espace tangent puisque

$$\forall M \in \text{ mod }_R,\ \boldsymbol{Spf}(R \oplus \Omega)(M) = \mathcal{H}\text{om}(\Omega, M) = t_G(M)$$

(bien sûr il y à là dedans des identifications faites ; il faut regarder le lemme de Yoneda de plus près pour voir que le fait que ξ corresponde à l'identité implique que l'isomorphisme ci dessus est "la composition avec l'identité").

Soit alors $\widehat{\boldsymbol{Sym}}_R(\Omega)$ l'algèbre des séries formelles associée. L'application surjective $\widehat{\boldsymbol{Sym}}_R(\Omega) \to \boldsymbol{Sym}_R(\Omega)$ induit grâce au lemme 1.4 une surjection

$$G(\widehat{\boldsymbol{Sym}}_R(\Omega)) \to G(\boldsymbol{Sym}_R(\Omega))$$

qui provient par le lemme de Yoneda d'un morphisme

$$\boldsymbol{Spf}(\widehat{\boldsymbol{Sym}}_R(\Omega)) \to G$$

Or ce morphisme induit un isomorphisme sur les foncteurs tangents puisque $\boldsymbol{Spf}(\widehat{\boldsymbol{Sym}}_R(\Omega)) \to \boldsymbol{Spf}(\boldsymbol{Sym}_R(\Omega))$ induit un isomorphisme sur les foncteurs tangents.

Par la proposition 1.3 ce morphisme est un isomorphisme. □

2 Théorie de Cartier

2.1 Introduction

Le module de Cartier associé à un groupe formel sur un anneau R est en quelque sorte une généralisation de l'algèbre de Lie associée à un groupe algébrique. La théorie de Cartier consiste alors à exprimer les liens entre le module et le groupe i.e. à récrire l'application exponentielle qui n'est valable elle que sur $\mathbb{Q}$.

Sur $\mathbb{Q}$ la théorie nous redonne le fait que tout groupe formel est isomorphe à un produit de $\widehat{\mathbf{G}_a}$

Sur un corps parfait de caractéristique p elle permet de déduire la classification des groupes p-divisibles connexes via leur module de Dieudonné.

2.2 Foncteurs admissibles

Notons $\sigma_i \in \mathbb{Z}[T_1, \ldots, T_n] = \mathbb{Z}[\underline{T}]$ les polynômes symétriques élémentaires définis par

$$\prod_{i=1}^{n}(1 - T_i t) = 1 - \sigma_1 t + \cdots + (-1)^n \sigma_n t^n$$

$\mathfrak{S}_n$ agit sur $\mathbb{Z}[T]$. Si $N \in \mathbf{Ab}$ notons $N[\underline{T}] = N \otimes_{\mathbb{Z}} \mathbb{Z}[\underline{T}]$ sur lequel $\mathfrak{S}_n$ agit. Rappelons le théorème de base :

Théorème 2.1. *Il y a un isomorphisme de groupes abéliens*

$$\begin{array}{ccc} N[X_1, \ldots, X_n] & \xrightarrow{\sim} & N[T_1, \ldots, T_n]^{\mathfrak{S}_n} \\ X_i & \mapsto & \sigma_i \end{array}$$

qui est un isomorphisme de R algèbres si N est une R algèbre.

Cet isomorphisme est un isomorphisme de groupes gradués si $N[\underline{T}]$ est muni de la graduation usuelle en posant $\deg(T_i) = 1$ et si $N[\underline{X}]$ est gradué par le poids : $\mathrm{pd}(X_i) = i$.

Notons $I_m = N[\underline{X}]_{\geq m}$ le sous groupe des éléments de poids supérieur ou égale à m et $J_m = N[\underline{T}]_{\geq m}$. L 'isomorphisme précédent induit un isomorphisme :

$$N[\underline{X}]/I_m \xrightarrow{\sim} (N[\underline{T}]/J_m)^{\mathfrak{S}_m}$$

qui en passant à la limite induit l'isomorphisme

$$\begin{array}{ccc} N[[X_1, \ldots, X_n]] & \xrightarrow{\sim} & N[[T_1, \ldots, T_n]]^{\mathfrak{S}_n} \\ X_i & \mapsto & \sigma_i \end{array}$$

Soit maintenant $H : \mathbf{Nilp}_R \to \boldsymbol{\mathcal{E}}\mathbf{ns}$ un foncteur. Rappelons que pour $A \in \mathbf{Nilp}_R$ augmenté $H(A[[X]]) = \varprojlim H(A[X]/I_m)$ et que plus généralement, si A est complet, $A = \varprojlim A/\mathfrak{a}_i$,

$$H(A[[\underline{X}]]) = \varprojlim_{i,m} H(A/\mathfrak{a}_i[X]/I_m)$$

Considérons la composée

$$H(A[[\underline{X}]]) = \varprojlim H(A[[\underline{X}]]/I_m) \to \varprojlim H(A[[\underline{T}]]/J_m) = H(A[[\underline{T}]]^{\mathfrak{S}_n}) \to H(A[[\underline{T}]])^{\mathfrak{S}_n}$$

Définition 2.1. *H est dit admissible si $\forall A \in \mathbf{Nilp}_R$ l'application naturelle*

$$H(A[[\underline{X}]]) \to H(A[[\underline{T}]])^{\mathfrak{S}_n}$$

est un isomorphisme

Exemples : Si M est un R-module soit H tel que $H(N) = M \otimes_R N$. Si $A = R \oplus N$ est l'algèbre augmentée associée, $A[[X]]^+ = R[[X]]^+ \oplus N[[X]]$ et donc $H(A[[X]]) = M \otimes_R R[[X]]^+ \oplus M \otimes_R N[[X]] = (M \otimes_R A)[[X]]^+$, donc H est admissible grâce au théorème 2.1.

Lemme 2.1. *Si H vérifie M.V. alors H est admissible.*

dem : En effet, pour tout $m \in \mathbb{N}$ considérons le diagramme

$$\begin{array}{ccc} A[\underline{X}]/I_m & \xrightarrow{\alpha} & A[\underline{T}] \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \Delta} \\ A[\underline{T}]/J_m & \xrightarrow{\varphi} & \prod_{\sigma\in\mathfrak{S}_n} A[\underline{T}]/J_m \end{array}$$

où $\varphi(x) = (x^\sigma)_{\sigma\in\mathfrak{S}_n}, \Delta(x) = (x, \ldots, x)$ et $\alpha : X_i \mapsto \sigma_i$. Le théorème 2.1 est équivalent à ce que ce diagramme soit cartésien. Donc

$$\begin{array}{ccc} H(A[\underline{X}]/I_m) & \xrightarrow{H(\alpha)} & H(A[\underline{T}]) \\ \downarrow{\scriptstyle H(\alpha)} & & \downarrow{\scriptstyle \Delta} \\ H(A[\underline{T}]/J_m) & \xrightarrow{H(\varphi)} & H(\prod_{\sigma\in\mathfrak{S}_n} A[\underline{T}]/J_m) = \prod_{\sigma\in\mathfrak{S}_n} H(A[\underline{T}]/J_m) \end{array}$$

est cartésien ce qui exprime exactement ce que l'on veut :

$$H(A[\underline{X}]/I_m) \xrightarrow{\sim} H(A[T_b]/J_m)^{\varphi=\Delta} = H(A[\underline{T}])^{\mathfrak{S}_n}$$

Donc en passant à la limite sur m, H est admissible. □

Par exemple,

$$\Lambda : N \mapsto (1 + R[t]^+ \otimes_R N)^\times = \{1 + tn_1 + \cdots + t^r n_r | n_i \in N\}$$

est admissible. Cet exemple est fondamental.

Soit $H : \mathbf{Nilp}_R \to \mathbf{Ab}$ admissible. Nous allons voir comment récupérer n indéterminées à partir d'une seule. Ceci nous permettra de voir plus tard que les groupes à un paramètre (une indéterminée) déterminent complètement tous les autres morphismes de groupes.

Notons

$$\begin{array}{rcl} u_i^n : R[[Y]] & \to & R[[T_1, \ldots, T_n]] \\ Y & \mapsto & T_i \end{array}$$

Soit la composée :

$$u_H^n : H(R[[Y]]) \xrightarrow{\sum_i H(u_i^n)} H(R[[T_1, \ldots, T_n]])^{\mathfrak{S}_n} \simeq H(R[[X_1, \ldots, X_n]])$$

En particulier,

$$\begin{array}{rcl} u_\Lambda^n : \Lambda(R[[Y]]) & \to & \Lambda(R[[\underline{X}]]) \\ 1 - Yt & \mapsto & 1 - X_1 t + \cdots + (-1)^n X_n t^n \end{array}$$

2.3 Le premier théorème fondamental

Celui ci dit qu'il y a une bijection entre groupes à un paramètres et éléments de $H(R[[Y]])$. A un groupe à un paramètre on associe sa dérivée en 0 : $\Phi(1-tY)$.

Théorème 2.2. *Soit $H : \mathbf{Nilp}_R \to \mathbf{Ab}$ admissible. On a un isomorphisme :*

$$\begin{array}{rcl} \lambda_H : \mathcal{H}om(\Lambda, H) & \xrightarrow{\sim} & H(R[[Y]]) \\ \Phi & \mapsto & \Phi_{R[[Y]]}(1-tY) \end{array}$$

dem : On vérifie immédiatement que λ_H est un morphisme de groupes.

L'idée est maintenant la suivante : soit $f \in \Lambda(N)$ pour un $N \in \mathbf{Nilp}_R$, $f = 1 + a_1 T + \cdots + a_n T^n$. Soit

$$\begin{array}{rcl} \rho_f^n : R[[X_1, \ldots, X_n]] & \to & N \\ X_i & \mapsto & (-1)^i a_i \end{array}$$

Alors,

$$\Lambda(\rho_f^n)(u_\Lambda^n(1-tY)) = \Lambda(\rho_f^n)(1 - X_1 t + \cdots + (-1)^n X_n t) = f$$

Or a priori, si $\Phi \in \mathcal{H}\mathrm{om}(\Lambda, H)$ par naturalité on a un diagramme commutatif

$$\begin{array}{ccccc} \Lambda(R[[Y]]) & \xrightarrow{u_\Lambda^n} & \Lambda(R[[X_1, \ldots, X_n]]) & \xrightarrow{\Lambda(\rho_f^n)} & \Lambda(N) \\ \downarrow{\scriptstyle \Phi_{R[[Y]]}} & & \downarrow{\scriptstyle \Phi_{R[[X]]}} & & \downarrow{\scriptstyle \Phi_N} \\ H(R[[Y]]) & \xrightarrow{u_H^n} & H(R[[X_1, \ldots, X_n]]) & \xrightarrow{H(\rho_f^n)} & H(N) \end{array}$$

et donc

$$\Phi_N(f) = H(\rho_f^n)(u_H^n(\theta)) \quad \text{où } \theta = \Phi_{R[[Y]]}(1-tY)$$

Ce qui montre que Φ est entièrement connu dès que l'on connaît θ.

Cela montre déjà l'injectivité de λ_H.

Montrons la surjectivité. Soit $\theta \in H(R[[Y]])$ on a vu que nécessairement $\forall N, f \;\; \Phi_N(f) = H(\rho_f^n)(\theta_n)$ où l'on a posé $\theta_n = u_H^n(\theta)$.

Prenons ceci comme définition de Φ.

Tout d'abord, cette définition est indépendante de n. En effet, si $m \geq n$ soit

$$\begin{array}{rcl} \beta_{n,m} : R[[X_1, \ldots, X_m]] & \to & R[[X_1, \ldots, X_n]] \\ X_i & \mapsto & \begin{cases} X_i \text{ si } i \leq n \\ 0 \text{ sinon} \end{cases} \end{array}$$

$$\rho_f^m = \rho_f^n \circ \beta_{n,m} \Rightarrow H(\rho_f^m)(\theta_m) = H(\rho_f^n)(H(\beta_{n,m})(\theta_m))$$

or

$$\begin{aligned} H(\beta_{n,m})(\theta_m) &= H(\beta_{n,m})(\sum_{i=1}^{m} H(u_i^m)(\theta)) \\ &= \sum_{i=1}^{m} H(\beta_{n,m} \circ u_i^m)(\theta) \\ &= \sum_{i=1}^{n} H(u_i^n)(\theta) = \theta_n \end{aligned}$$

car

$$\beta_{n,m} \circ u_i^m = \begin{cases} u_i^n \text{ si } i \leq n \\ 0 \text{ sinon} \end{cases}$$

et finalement

$$H(\rho_f^m)(\theta_m) = H(\rho_f^n)(\theta_n)$$

d'où l'indépendance par rapport à n.

Φ ainsi défini est une application naturelle de foncteur car si $u : N \to N'$ et $f \in N$ alors

$$\begin{aligned} H(u)[\Phi_N(f)] &= H(u)[H(\rho_f^n)(\theta_n)] \\ &= H(u \circ \rho_f^n)(\theta_n) \\ &= H(\rho_{\Lambda(u)(f)}^n)(\theta_n) \text{ car } u\rho_f^n = \rho_{\Lambda(u)(f)}^n \\ &= \Phi_{N'}(\Lambda(u)(f)) \end{aligned}$$

On a bien de plus $\lambda_H(\Phi) = \theta$ car

$$\lambda_H(\Phi) = \Phi_{R[[Y]]}(1 - tY) = H(\rho^1 1 - tY)(u_H^1(\theta)) = H(\rho_{1-tY}^1(\theta)) = \theta$$

car $\rho_{1-tY}^1 = Id$.

Reste à vérifier que Φ est un morphisme de groupes.

Par fonctorialité il suffit de le vérifier dans le cas universel : soient $\xi, \eta \in \Lambda(R[[X_1, \ldots, X_n; Y_1, \ldots, Y_n]])$ définis par

$$\begin{cases} \xi = 1 - X_1 t + \cdots + (-1)^n X_n t^n \\ \eta = 1 - Y_1 t + \cdots + (-1)^n Y_n t^n \end{cases}$$

Dès lors, ρ_ξ^n et ρ_η^n sont les inclusions :

$$R[[X]], R[[Y]] \xrightarrow{j_1, j_2} R[[X, Y]]$$

Il s'agit donc de démontrer que

$$H(j_1)(\theta_n) + H(j_2)(\theta_n) = H(\rho^{2n}_{\xi.\eta})(\theta_{2n})$$

Considérons pour cela l'application

$$\begin{array}{rcl} \alpha : R[[\underline{X},\underline{Y}]] & \to & R[[\underline{T},\underline{U}]] \\ X_i & \mapsto & \sigma_i(T_1,\ldots,T_n) \\ Y_i & \mapsto & \sigma_i(U_1,\ldots,U_n) \end{array}$$

Elle induit l'isomorphisme $\mathbb{R}[[\underline{X},\underline{Y}]] \simeq R[[\underline{T},\underline{U}]]^{\mathfrak{S}_n \times \mathfrak{S}_n}$.

On en déduit une série d'isomorphismes :

$$\begin{array}{rcl} H(R[[\underline{X},\underline{Y}]]) & \stackrel{\sim}{\to} & H(R[[\underline{T},\underline{U}]]^{\mathfrak{S}_n \times \mathfrak{S}_n}) \\ & = & H(R[[\underline{T}]]^{\mathfrak{S}_n}[[\underline{U}]]^{\mathfrak{S}_n}) \\ & \simeq & H(R[[\underline{T}]]^{\mathfrak{S}_n}[[\underline{U}]])^{\mathfrak{S}_n} \\ & = & H(R[[\underline{U}]][[\underline{T}]]^{\mathfrak{S}_n}) \\ & \simeq & H(R[[\underline{T},\underline{U}]])^{\mathfrak{S}_n \times \mathfrak{S}_n} \subset H(R[[\underline{T},\underline{U}]]) \end{array}$$

par admissibilité de H.

Il suffit donc de vérifier que :

$$H(\alpha)(H(j_1)(\theta_n) + H(j_2)(\theta_n)) = H(\alpha)H(\rho^{2n}_{\xi.\eta})(\theta_{2n})$$

Le membre de gauche est égal à :

$$H(\alpha j_1)(\theta_n) + H(\alpha j_2)(\theta_n)$$

or αj_1 est la composée de :

$$R[[\underline{X}]] \longrightarrow R[[\underline{T}]] \stackrel{i_1}{\hookrightarrow} R[[\underline{T},\underline{U}]]$$

$$X_i \longmapsto \sigma_i(T_1,\ldots,T_n)$$

De même pour αj_2.

Donc

$$\begin{array}{rcl} H(\alpha j_1)(\theta_n) + H(\alpha j_2)(\theta_n) & = & H(i_1)(\sum_{i=1}^{n} H(u_i^n)(\theta)) + H(i_2)(\sum_{i=1}^{n} H(u_i^n)(\theta)) \\ & = & \sum_{i=1}^{n} H(i_1 u_i^n)(\theta) + \sum_{i=1}^{n} H(i_2 u_i^n)(\theta) \\ & = & \sum_{i=1}^{2n} H(u_i^{2n})(\theta) \end{array}$$

qui est l'image de θ_{2n} dans l'isomorphisme standard.

Le membre de droite est égal à $H(\alpha\rho^{2n}_{\xi\eta})(\theta_{2n})$. Or

$$\alpha\rho^{2n}_{\xi\eta} : T_i \mapsto \alpha(\sum_{k+l=i} X_k Y_l) = \sum_{k+l=i} \sigma_k(\underline{T})\sigma_l(\underline{U}) = \sigma_i(\underline{T},\underline{U})$$

d'où le résultat. □

2.4 Modules de Cartier

Soit l'anneau

$$\mathbb{E}_R = \mathrm{End}(\Lambda)^{opp}$$

$$\mathbb{E}_R \xrightarrow{\sim\lambda_\Lambda} \Lambda(R[[Y]])$$

Si $H : \mathbf{Nilp}_R \to \mathbf{Ab}$ est un foncteur admissible notons

$$M_H = H(R[[Y]])$$

L'isomorphisme $\mathcal{H}\mathrm{om}(\Lambda, H) \xrightarrow{\sim\lambda_H} M_H$ permet de munir M_H d'une structure de $\mathbb{E}$-module à gauche :

$$\forall x \in \mathbb{E}_R \ \forall m \in M \ \ x.m = \lambda_H(\lambda_H^{-1}(m) \circ x)$$

Définition 2.2. *$V_n = \lambda_\Lambda^{-1}(1 - Y^n t)$, $F_n = \lambda_\Lambda^{-1}(1 - Yt^n)$, et $\forall c \in R$ $[c] = \lambda_\Lambda^{-1}(1 - cYt) \ \in \mathbb{E}$*

Lemme 2.2. *Si $\varphi_n, \psi_c : R[[Y]] \to R[[Y]]$ où $\varphi_n(Y) = Y^n, \psi_c(Y) = cY$, alors $\forall \gamma \in M_H$,*

$$V_n.\gamma = H(\varphi_n)(\gamma) \ \textit{et} \ [c].\gamma = H(\psi_c)(\gamma)$$

dem :

$$\begin{aligned}
V_n.\gamma &= \lambda_H(\lambda_H^{-1}(\gamma) \circ \lambda_\Lambda^{-1}(1 - Y^n t)) \\
&= (\lambda_H^{-1}(\gamma) \circ \lambda_\Lambda^{-1}(1 - Y^n t))_{R[[Y]]}(1 - tY) \\
&= \lambda_H^{-1}(\gamma)[1 - Y^n t] \\
&= \lambda_H^{-1}(\gamma)[\Lambda(\varphi_n)(1 - Yt)] \\
&= H(\varphi_n)(\lambda_H^{-1}(\gamma)(1 - Yt)) \text{ car } \lambda_H^{-1}(\gamma) \in \mathcal{H}\mathrm{om}(\Lambda, H) \\
&= H(\varphi_n)(\gamma)
\end{aligned}$$

De même pour $[c].\gamma$.

□

Corollaire 2.1.

$$V_n[c]F_m = \lambda_\Lambda^{-1}(1 - cY^n t^m)$$

Cela se déduit en appliquant le lemme précédent avec $H = \Lambda$ car alors :
$(V_n[c]F_m)(1 - Yt) = V_n[c](1 - Yt^m) = \Lambda(\varphi_n\psi_c)(1 - Yt^m) = 1 - cY^n t^m$

□

Supposons maintenant que H soit exacte. Son module de cartier M_H est alors muni d'une filtration décroissante

$$M_H^n = H(Y^n R[[Y]])$$

telle que

$$M_H^n / M_H^{n+1} \simeq H(Y^n R[[Y]]/Y^{n+1} R[[Y]])$$

Remarque 2.1.
- *M_H^n est un sous groupe de M_H mais non un sous module. Néanmoins, M_H/M_H^2 est un R module car $\mathbb{E}/\mathbb{E}_2$ est une R algèbre*
- *$\mathbb{E}_n \subset \mathbb{E}$ est un idéal à droite de $\mathbb{E}$*

Définition 2.3. *Un module de cartier V réduit est un $\mathbb{E}$ module à gauche M muni d'une filtration décroissante $(M^n)_{n\in\mathbb{N}^*}$, $M^1 = M$, telle que :*

1. *$V_m[c]M^n \subset M^{n+m}$*
2. *$\forall n, m\ \exists d\ F_m M^d \subset M^n$ (en d'autres termes $\forall m$, $F_m : M \to M$ est continu pour la topologie définie par la filtration)*
3. *$V_m : M/M^2 \xrightarrow{\sim} M^m/M^{m+1}$ est un isomorphisme*
4. *$M \xrightarrow{\sim} \varprojlim M/M^n$ i.e. M est séparé complet*

Proposition 2.1. *Si H est exacte alors M_H est un module de Cartier V-réduit.*

dem : (1) résulte du lemme 2.2.
Pour (3) :

$$\begin{array}{ccc} M/M^2 & \xrightarrow{\quad V_m \quad} & M^m/M^{m+1} \\ \| & & \| \\ H(YR[[Y]]/Y^2R[[Y]]) & \xrightarrow{H(\overline{\varphi}_m)} & H(Y^mR[[Y]]/Y^{m+1}R[[Y]]) \end{array}$$

or $\overline{\varphi}_m : YR[[Y]]/Y^2R[[Y]] \to Y^mR[[Y]]/Y^{m+1}R[[Y]]$ est un isomorphisme d'où le résultat.

(4) est vrai par définition de $H(R[[Y]])$ (Rappel : $H : \mathbf{Nilp}_R \to \mathbf{Ab}$ est étendu en un foncteur "continu" aux R algèbres augmentées complètes).

(2) demande un peu plus de travail : soit $\theta \in M_H = H(YR[[Y]])$.

$$F_m.\theta = \lambda_H^{-1}(\theta)(1 - Yt^m) = H(\alpha_m)(u_H^m(\theta))$$

par définition de λ_H^{-1} (cf. la preuve du théorème 2.2) où

$$\begin{aligned} \alpha_n : R[[X_1, \ldots, X_n]] &\to R[[Y]] \\ X_i &\mapsto 0 \text{ si } i < m \\ X_m &\mapsto Y \end{aligned}$$

Supposons que $\theta \in H(Y^{md}R[[Y]])$. Alors, $\forall i \leq m,\ H(u_i^m)(\theta) \in H(T_i^{md}R[[Y]])$ et donc

$$\sum_{i=1}^{n} H(u_i^m)(\theta) \in H(R[[\underline{T}]]_{deg \geq md})$$

Or $R[[\underline{X}]] \xrightarrow{\sim} R[[\underline{T}]]^{\mathfrak{S}_n}$ est un isomorphisme d'algèbres graduées où $R[[\underline{X}]]$ est graduée par le poids et $R[[\underline{T}]]$ par le degré.

Donc par exactitude de H,

$$u_H^n(\theta) \in H(R[[\underline{X}]]_{\text{poids} \geq md})$$

Or si $\text{poids}(P) \geq md, P(0, \ldots, 0, Y) \in Y^d R[[Y]]$. Donc $F_m.\theta \in M_H^d$ dès que $\theta \in M_H^{md}$. □

Soit M un module de Cartier V réduit et $(x_\alpha)_{\alpha \in M/M^2}$ un ensemble de représentants de M mod M^2. De la définition 2.3, 3 et 4 on déduit que tout élément $m \in M$ s'écrit de façon unique

$$\sum_{n \geq 0} V_n x_{\alpha_n}$$

Remarque 2.2. *On en déduit en particulier que la multiplication par V est injective sur M. Cela est faux pour la multiplication à droite par V sur $\mathbb{E}$, ou pour la multiplication par F.*

$\mathbb{E}/\mathbb{E}_2 = \Lambda(Y R[[Y]]/Y^2 R[[Y]])$ est l'espace tangent à Λ.

Lemme 2.3.

$$\begin{aligned} R^{(\mathbb{N}^*)} &\xrightarrow{\sim} \mathbb{E}/\mathbb{E}_2 \\ (x_i)_i &\mapsto \overline{\textstyle\sum_{i \geq 1} [x_i] F_i} \end{aligned}$$

dem : En effet, $\forall f \in \Lambda(R[\epsilon])$,

$$\begin{aligned} f &= 1 + a_1 \epsilon t + \cdots + a_n \epsilon t^n \\ &= \prod_{i=1}^{n} (1 + a_i \epsilon t^i) \\ &= \prod_{i=1}^{n} \lambda_\Lambda([a_i] F_i) \\ &= \lambda_\Lambda(\sum_{i=1}^{n} [a_i] F_i) \end{aligned}$$

écriture unique. D'où le résultat. □

Remarque 2.3. *On verra plus tard qu'en fait il existe un morphisme* $\Lambda \longrightarrow \widehat{\mathbf{G}_a}^{(\mathbb{N})}$.

Corollaire 2.2. *Tout élément de* $\mathbb{E}$ *s'écrit de façon unique*

$$\sum_{n,m} V_n[a_{n,m}]F_m$$

où $\forall n$ $a_{n,m}$ *est nul sauf pour un nombre fini de* m.

2.5 Quelques propriétés de F et V

Proposition 2.2. *1.* $V_1 = F_1 = 1$

2. $[c]V_n = V_n[c^n]$
3. $V_n V_m = V_{nm}$
4. $[c_1][c_2] = [c_1 c_2]$
5. $F_n V_n = n$
6. *Si* $p = 0$ *sur* R, $F_p V_p = V_p F_p = p$
7. $F_n[c] = [c^n]F_n$
8. $F_n F_m = F_{nm}$
9. $F_n V_m = F_m V_n$ *si* $n \wedge m = 1$
10. $[c_1 + c_2] = [c_1] + [c_2] + \sum_{n\geq 2} V_n[a_n(c_1, c_2)]F_n$ *où les* $a_n(X_1, X_2) \in \mathbb{Z}[X_1, X_2]$ *sont des polynômes "universels"*

Commençons tout d'abord par remarquer que $R \mapsto \mathbb{E}_R$ est fonctoriel en R au sens suivant : si $\varphi : R \to R'$ est un morphisme d'anneau il induit $\mathbf{Nilp}_{R'} \to \mathbf{Nilp}_R$ et donc un morphisme d'anneaux

$$\mathrm{End}_{\mathbf{Nilp}_R}(\Lambda)^{opp} \to \mathrm{End}_{\mathbf{Nilp}_{R'}}(\Lambda)^{opp}$$

On vérifie alors aisément que l'isomorphisme du premier théorème fondamental est naturel en R au sens où le diagramme suivant commute :

$$\begin{array}{ccc} \mathbb{E}_R & \xrightarrow{\sim\lambda_\Lambda} & \Lambda(R[[Y]]) \\ \downarrow & & \downarrow \\ \mathbb{E}_{R'} & \xrightarrow{\sim\lambda_\Lambda} & \Lambda(R[[Y]]) \end{array}$$

de plus l'élément $\sum_{n,m} V_n[c_{n,m}]F_m$ est envoyé sur $\sum_{n,m} V_n[\varphi(c_{n,m})]F_m$.

dem : Commençons par le (1) : $\forall \gamma, V_1.\gamma = H(\varphi_1)(\gamma)$ or $\varphi_1 = Id \Rightarrow V_1.\gamma = \gamma \Rightarrow V_1 = 1$. $F_1 = \lambda_\Lambda^{-1}(1 - Yt) = V_1 = 1$.

(2) : $\forall \gamma[c]V_n.\gamma = H(\psi_c\varphi_n) = H(\varphi_n\psi_{c^n})(\gamma) = V_n[c^n].\gamma$ car $\psi_c\varphi_n = \varphi_n\psi_{c^n}$
(3) résulte de la même façon de $\varphi_n\varphi_m = \varphi_{nm}$
(4) De même $\psi_{c_1}\psi_{c_2} = \psi_{c_1c_2}$.
(5) Étant donné que $V_n : \mathbb{E} \to \mathbb{E}$ est injectif il suffit de montrer que

$$V_nF_nV_n = NV_n$$

De plus il suffit de le montrer dans le cas universel par la remarque précédent la démonstration. En effet, si $\gamma = \sum_{n,m} V_n[c_{n,m}]F_m \in \mathbb{E}_R$, soit $\varphi : \mathbb{Z}[X_{ij}]_{i,j\in\mathbb{N}} \to R,\ X_{ij} \mapsto c_{i,j}$. Alors γ est l'image de $\sum_{n,m} V_n[X_{nm}]F_m$ dans le morphisme induit par $\varphi; \mathbb{E}(\varphi) : \mathbb{E}_{\mathbb{Z}[X_{ij}]} \to \mathbb{E}_R$.
Choisissons un plongement $\mathbb{Z}[X_{ij}] \hookrightarrow \mathbb{C}$. Il suffit donc de le démontrer sur $\mathbb{C}$.
Or sur $\mathbb{C}$,

$$V_nF_n = \lambda_\Lambda^{-1}(1 - Y^nt^n) = \sum_{i=0}^{n-1} \lambda_\Lambda^{-1}(1 - \zeta^iYt) = \sum_{i=0}^{n-1}[\zeta^i]$$

où ζ est une racine primitive n ième de l'unité. Donc :

$$\begin{aligned} V_nF_nV_n &= \sum_{i=0}^{n-1}[\zeta^i]V_n \\ &= \sum_{i=0}^{n-1} V_n[1] \text{ grâce au (2)} \\ &= n \end{aligned}$$

(6) :

$$V_pF_p = \lambda_\Lambda^{-1}(1 - Y^pt^p) = \lambda_\Lambda^{-1}((1 - Yt)^p) = p$$

(7) : De même qu'au (5) on travaille sur $\mathbb{C}$ et on utilise l'injectivité de V_n :

$$V_nF_n[c] = \sum_{i=0}^{n-1}[\zeta^i][c] = \sum_{i=0}^{n-1}[\zeta^ic] \text{ grâce au (4)}$$

$$= [c]\sum_{i=0}^{n-1}[\zeta^i] = [c]V_nF_n = V_n[c^n]F_n$$

d'où le résultat.

(8) On se place de nouveau sur $\mathbb{C}$:

$$\begin{aligned} V_{nm}F_nF_m &= V_m(V_nF_nn)F_m \\ &= V_m(\sum_{i=0}^{n-1}[\zeta_n^i])F_m \\ &= V_mF_m(\sum_{i=0}^{n-1}[\zeta_{nm}^i]) \text{ grâce au (7)} \\ &= (\sum_{j=0}^{m-1}[\zeta_m^j])(\sum_{i=0}^{n-1}[\zeta_{nm}^i]) \\ &= \sum_{i=0}^{n-1}\sum_{j=0}^{m-1}[\zeta_{nm}^{i+nj}] \\ &= \sum_{i=0}^{nm-1}[\zeta_{nm}^i] = V_{nm}F_{nm} \end{aligned}$$

(9) :

$$\begin{aligned} V_nF_nV_m &= \sum_{i=0}^{n-1}[\zeta_n^i]V_n \\ &= V_m\sum_{i=0}^{n-1}[\zeta_n^{mi}] \\ &= V_m\sum_{i=0}^{n-1}[\zeta_n^i] \text{ car } \overline{m} \in (\mathbb{Z}/n/\mathbb{Z})^\times \\ &= V_mV_nFF_n \\ &= V_nV_nF_n \text{ grâce au (3)} \end{aligned}$$

(10) : Il suffit de se placer sur $\mathbb{Z}[X_1, X_2]$:

$$\begin{aligned} \lambda_\Lambda([X_1+X_2]-[X_1]-[X_2]) &= (1-(X_1+X_2)t)(1-X_1t)^{-1}(1-X_2t)^{-1} \\ &= \prod_{i\geq 2}(1-a_i(X_1,X_2)t^i) \end{aligned}$$

□

2.6 Produit tensoriel réduit

Lemme 2.4. *Soit M un module de Cartier V réduit. $\overline{\mathbb{E}_nM} = M^n$. Si M est de type fini, $\mathbb{E}_n.M = M^n$.*

dem : En effet, $\forall m \in M^n, \exists m_{n+1} \in M^{n+1}\ \exists x_n \in M$,

$$m = V_n x_n + m_{n+1}$$

Et donc tout élément de M^n s'écrit $\sum_{r\geq n} V_r x_r \in \overline{\mathbb{E}_n M}$.

Si M est de type fini engendré par les $(e_i)_i$, tout $m \in M^n$ s'écrit $m = V_n \sum_i \lambda_{n,i} e_i + m_{n+1} \quad \lambda_{n,i} \in \mathbb{E}$ et donc

$$m = \sum_{r\geq n} V_r \sum_i \lambda_{r,i} e_i = \sum_i (\sum_{r\geq n} \lambda_{n,i}) e_i$$

car $\sum_n V_n \lambda_{n,i}$ converge dans $\mathbb{E}$ et appartient à $\mathbb{E}_r$. □

Remarque 2.4. *Si M est de type fini, dans la définition d'un module de Cartier V réduit , l'hypothèse de continuité des F_m est automatique. Elle se déduit de la continuité des F_m sur $\mathbb{E}$ puisque $F_m.M^n = F_m.(\mathbb{E}_n M) = (F_m \mathbb{E}_n).M$.*

Soit N un $\mathbb{E}$ module à <u>droite</u>. Notons

$$N_s = \{n \in N | n\mathbb{E}_s = 0\}$$

(ce n'est pas un sous module). Nous noterons $N_s \odot M^s$ l'image de $N_s \otimes_{\mathbb{Z}} M^s \to N \otimes_{\mathbb{E}} M$ i.e. le sous groupe (ce n'est pas un sous $\mathbb{E}$ module) de $N \otimes_{\mathbb{E}} M$ engendré par les $n_s \otimes m^s$.

Si $m^s \in M^s, \exists m^{s+1}, x,\ m_s = V_s x + m^{s+1} \Rightarrow \forall n_s \in N_s\ n - s \otimes m_s = n_s \otimes m_{s+1}$. Et donc

$$N_s \odot M^s \subset N_{s+1} \odot M^{s+1}$$

Définition 2.4. $(N \otimes_{\mathbb{E}} M)_\infty = \bigcup_s N_s \odot M^s$ *sous groupe de* $N \otimes_{\mathbb{E}} M$

Définition 2.5.

$$N \overline{\otimes}_{\mathbb{E}} M = (N \otimes_{\mathbb{E}} M)/(N \otimes_{\mathbb{E}} M)_\infty$$

Définition 2.6. *N est dit de torsion si tout élément de N est annulé par un $\mathbb{E}_s, s \in \mathbb{N}$.*

Remarque 2.5. *Si M est de type fini, $N \overline{\otimes}_{\mathbb{E}} M = N \otimes_{\mathbb{E}} M$*

Proposition 2.3. *Soit $N \in \mathbf{Nilp}_R$. Alors, $\Lambda(N)$ est un $\mathbb{E}$ module à droite de torsion*

dem : $\forall x \in \Lambda(N), \forall \Phi \in \mathbb{E} = \mathrm{End}(\Lambda)^{opp},\ \ x.\Phi = \Phi_N(x)$ muni $\Lambda(N)$ d'une structure de $\mathbb{E}$ module à droite.

Soit $t \in N$ tel que $N^t = 0$. Soit $f \in \Lambda(N), f = 1 + a_1 t + \cdots + a_n t^n$ et $\Phi \in \mathbb{E}_{nt}$.

$$\lambda_\Lambda(\Phi) \in Y^{nt} R[[Y]] \Rightarrow \theta_n = u^n_\Lambda(\theta) \in \Lambda(R[[X_1, \ldots, X_n]]_{poids \geq nt})$$

Or $F.\Phi = \Lambda(\rho^n_f)(\theta_n)$ où $\rho^n_f : X_i \mapsto (-1)^i a_i$.
Et donc

$$f.\Phi = 1 \pm \prod_i a_i^{\alpha_i^{(1)}}\ t \pm \cdots \pm \prod_i a_i^{\alpha_i^{(n)}}\ t^n$$

où $\sum_i i\alpha_i^{(k)} \geq nt \Rightarrow \sum_i \alpha_i^{(k)} \geq t \Rightarrow f.\Phi = 0$. □

2.7 Les exemples fondamentaux de produits tensoriels réduits

Lemme 2.5. $\mathbb{E}/\mathbb{E}_n \overline{\otimes}_{\mathbb{E}} M \simeq M/N^n$

dem : On remarque tout d'abord qu'étant donné que $\mathbb{E}_n$ est un idéal à droite de $\mathbb{E}$, $\mathbb{E}/\mathbb{E}_n$ est un $\mathbb{E}$ module à droite. Le lemme a donc bien un sens.

Soit l'application

$$\begin{array}{rcl} \mathbb{E}/\mathbb{E}_n \times & \to & M/M^n \\ (\bar{x}, m) & \mapsto & xm \end{array}$$

elle est bien définie car $\mathbb{E}_n.M \subset M^n$ et $\mathbb{E}$ bilinéaire. Elle induit donc $\mathbb{E}/\mathbb{E}_n \otimes_{\mathbb{E}} M \xrightarrow{u} M/M^n$.

$(\mathbb{E}/\mathbb{E}_n \otimes_{\mathbb{E}} M)_\infty = \mathbb{E}/\mathbb{E}_n \odot M^n$ et donc u est triviale sur $(\mathbb{E}/\mathbb{E}_n \otimes M)_\infty$ d'où une application $\mathbb{E}/\mathbb{E}_n \overline{\otimes}_{\mathbb{E}} M \to M/M^n$. Il est alors clair que cette application est un isomorphisme d'inverse $\bar{m} \mapsto 1 \otimes m$ (qui est bien défini car si $m \in M^n, 1 \otimes m \in \mathbb{E}/\mathbb{E}_n \odot M^n$). □

Corollaire 2.3. *Soit $N \in \mathbf{Nilp}_R, N^2 = 0$ et M un module de Cartier V réduit. Alors :*

$$\Lambda(N) \overline{\otimes}_{\mathbb{E}} M \simeq N \otimes_R M/M^2$$

dem : Λ est un foncteur exacte donc (? ?)

$$N \otimes_R \Lambda(YR[[Y]]/Y^2R[[Y]]) \xrightarrow{\sim} \Lambda(N)$$

isomorphisme de $R - \mathbb{E}_R$ bimodule. Et donc :

$$\begin{array}{rcl} \Lambda(N) \overline{\otimes}_{\mathbb{E}} M & \simeq & (N \otimes_R \mathbb{E}/\mathbb{E}_2) \overline{\otimes}_{\mathbb{E}} M \\ & \simeq & N \otimes_R (\mathbb{E}/\mathbb{E}_2 \overline{\otimes}_{\mathbb{E}} M) \\ & \simeq & N \otimes_R M/M^2 \end{array}$$

□

2.8 Groupes de torsion réduits

Définition 2.7. *Un morphisme de modules de Cartier V réduits est un morphisme de $\mathbb{E}$ modules, $\varphi : M_1 \to M_2$ tel que $\forall n\ \varphi(M_1^n) \subset M_2^n$.*

Par exemple si $\Phi : H_1 \to H_2$ est un morphisme de foncteurs admissibles il induit un morphisme de leurs modules de Cartier : $M_\Phi : M_{H_1} \to M_{H_2}$ où $M_\Phi = \Phi_{R[[Y]]}$.

Lemme 2.6.
- $\ker \varphi$ *muni de la filtration* $(\ker \varphi)^n = \ker \varphi \cap M_1^n$ *est un module de Cartier V réduit.*
- *φ surjectif* $\Leftrightarrow \forall n\ \varphi(M_1^n) = M_2^n \Leftrightarrow \bar{\varphi} : M_1/M_1^2 \to M_2/M_2^2$ *est surjectif.*

dem : Dans la définition 2.3 les propriétés 1,2,4 dont évidentes. Pour la 3 : on a un diagramme commutatif à lignes exactes

$$\begin{array}{ccccccc}
0 & \longrightarrow & (\ker\varphi)^n/(\ker\varphi)^{n+1} & \longrightarrow & M_1^n/M_1^{n+1} & \longrightarrow & M_2^n/M_2^{n+1} \\
 & & \uparrow{\scriptstyle V_n} & & \uparrow{\scriptstyle \simeq\ V_n} & & \uparrow{\scriptstyle \simeq\ V_n} \\
0 & \longrightarrow & \ker\varphi/(\ker\varphi)^2 & \longrightarrow & M_1/M_1^2 & \longrightarrow & M_2/M_2^2
\end{array}$$

D'où le résultat par le lemme des cinq.

Le reste du lemme est immédiat. □

Nous allons maintenant défini des modules de Cartier "libres" afin de pouvoir construire des présentations $N\overline{\otimes}_{\mathbb{E}}\_$ acycliques d'un module de Cartier.

Pour cela, soit I un ensemble, $\oplus_I\mathbb{E} = \mathbb{E}^{(I)}$ muni de la filtration $(\mathbb{E}_n^{(I)})_{n\in\mathbb{N}}$ possède toutes les propriétés d'un module de Cartier V réduite sauf la (4). Pour y remédier il suffit de le compléter :

$$\widehat{\mathbb{E}^{(I)}} = \varprojlim_n \mathbb{E}^{(I)}/\mathbb{E}_n^{(I)}$$

$\widehat{\mathbb{E}^{(I)}} = \{(x_i)_i \in \mathbb{E}^I$ telles que $x_i \to 0$ selon le filtre des complémentaires des parties finies de $I\}$.

$\widehat{\mathbb{E}^{(I)}}$ vérifie bien la propriété de présentation voulue au sens où :

Lemme 2.7.

$$\begin{array}{rcl}
\mathcal{H}om_{Cart}(\widehat{\mathbb{E}^{(I)}}, M) & \xrightarrow{\sim} & M^I \\
\varphi & \mapsto & \varphi(e_i)
\end{array}$$

Nous voulons définir des $\overline{Tor}_i^{\mathbb{E}}(N, M)$ pour N de torsion et M de Cartier grâce à des résolutions via les $\widehat{\mathbb{E}^{(I)}}$.

Soit donc N un module de torsion à droite et M de Cartier. Choisissons une résolution "libre" de M par des $P_k \simeq \widehat{\mathbb{E}^{(I_k)}}$.

$$P_k \to \cdots \to P_1 \to P_0 \to M \to 0$$

cela est possible grâce aux lemmes 2.6 et 2.7.

Les arguments standards d'algèbre homologique montrent que deux telles résolutions sont homotopes. Cela permet de définir :

$$\overline{Tor}_i^{\mathbb{E}}(N, M) = H_i(N\overline{\otimes}_{\mathbb{E}}P_\bullet)$$

A quoi ressemblent les $N\overline{\otimes}P_\bullet$?

Lemme 2.8. $\forall N$ *de torsion*

$$\begin{array}{rcl} N\overline{\otimes}\widehat{\mathbb{E}^{(I)}} & \simeq & N^{(I)} \\ n \otimes (x_i)_i & \mapsto & (nx_i)_i \end{array}$$

dem : La démonstration est facile. On remarque que $(nx_i)_i$ est à support fini justement parce que $x_i \to 0$. □

Toute suite exacte courte (cf. remarque 2.6) de modules de Cartier donne alors lieu à une suite exacte longue. Mais l'intérêt des groupes de torsion est de pouvoir balancer i.e. de pouvoir utiliser le fait que toute suite exacte courte de modules de torsion à droite donne lieu à une suite exacte longue. Cela résulte pour les $\overline{Tor}_i^{\mathbb{E}}$ du lemme précédent, du lemme qui suit et d'arguments standards d'algèbre homologique.

Lemme 2.9. *Soit*

$$N_1 \to N_2 \to N_3 \to 0$$

une suite exacte courte de $\mathbb{E}$ *modules de torsion. Alors*

$$N_1\overline{\otimes}M \to N_2\overline{\otimes}M \to N_3\overline{\otimes}M \to 0$$

est exacte $\forall M$ *module de Cartier.*

dem : Utilisant l'exactitude à droite du produit tensoriel on vérifie immédiatement que seule l'exactitude au milieu est non triviale. On vérifie aussitôt qu'elle est vraie si l'on montre que $(N_2\overline{\otimes}M)_\infty \twoheadrightarrow (N_3\overline{\otimes}M)_\infty$.
$(N_3 \otimes M)_\infty$ est engendré par les $n_s \otimes m^s$ où $n_s \in N_{3,s}, m^s \in M^s$. Par surjectivité de $N_2 \to N_3$ un tel n_s est l'image d'un $x \in N_2$. N_2 étant de torsion, $\exists t \geq s, x \in N_{2,t}$. Mais $n_s \otimes m^s = n_s \otimes m^t$ pour un $m^t \in M^t$ où $t \geq s$ et alors $n_s \otimes m^s$ est l'image de $x \otimes m^t$. □

Remarque 2.6. *La catégorie des modules de Cartier V réduits n'est pas une catégorie abélienne : l'image par un morphisme de modules de Cartier n'est pas un forcément un module de Cartier. Néanmoins on a une notion de suite exacte :* $M' \to M \to M''$ *est exacte pas seulement si elle l'est comme suite de* $\mathbb{E}$ *modules mais si de plus l'image du premier morphisme est égale au noyau du second comme module de Cartier (i.e. filtration y compris !). Cela entraîne forcément que l'image du premier morphisme est un sous module de Cartier. Dans le lemme qui suit, le foncteur est dit exacte s'il transforme une suite exacte en une suite exacte.*

Lemme 2.10. *Le foncteur* $M \mapsto M/M^2$ *est exacte.*

dem : Il suffit de vérifier que si $\varphi : M \to M'$ est un morphisme de modules de Cartier tel que l'image φ soit un sous module de Cartier alors $\ker(\varphi)/\ker(\varphi)^2 = \ker(\bar{\varphi})$ où $\bar{\varphi} : M/M^2 \to M'/M'^2$. L'inclusion $\subset$ est triviale. Dans l'autre ses : soit $\bar{m}$, $bar\varphi(\bar{m}) = 0 \Rightarrow \varphi(m) \in M'^2 \Rightarrow \varphi(m) \in \mathrm{im}(\varphi)^2$ car $\mathrm{im}(\varphi)$ est un sous module de Cartier. Et donc étant un module de Cartier, $\varphi(m) \in V.\mathrm{im}(\varphi) \Rightarrow \exists m' \in M'\ \varphi(m) = V.\varphi(m') = \varphi(V.m') \Rightarrow m - V.m' \in \ker(\varphi)$. □

Maintenant que nous avons défini nos objets $\overline{Tor}_i^{\mathbb{E}}(N,M)$ nous sommes prêts pour démontrer le théorème pour lesquels nous les avons introduits :

Théorème 2.3. *Soit $N \in \mathbf{Nilp}_R$, M de Cartier tel que M/VM soit R plat. Alors :*

$$\forall i > 0 \quad \overline{Tor}_i^{\mathbb{E}}(\Lambda(N), M) = 0$$

dem : Supposons d'abord que $N^2 = 0$. D'après le corollaire 2.3 $\forall Q$ de Cartier

$$\Lambda(N)\overline{\otimes}Q \simeq N \otimes_R Q/Q^2$$

Or si $Q \simeq \widehat{\mathbb{E}^{(I)}}$, Q/Q^2 est R libre (cf. lemme 2.3)

Donc grâce au lemme 2.10 :

$$\forall i \ \ \overline{Tor}_i^{\mathbb{E}}(\Lambda(N), M) \simeq Tor_i^R(N, M/M^2)$$

qui est bien nul si M/M^2 est plat.

Dans le cas général il suffit de dévisser N en :

$$0 \to N' \to N \to N'' \to 0$$

où $N'^2 = 0$ et où le théorème est connu pour N''.

On conclu grâce à la suite exacte longue associée. □

2.9 Le deuxième théorème fondamental de la théorie de Cartier

Définition 2.8. *Un module de Cartier M est dit V plat si M/VM est R plat.*

Théorème 2.4. *Le foncteur $H \mapsto M_H$ est une équivalence de catégories entre la catégorie des G foncteurs formels et celle des modules de Cartier V plats.*

Un quasi inverse est donné par le foncteur

$$M \mapsto \Lambda(-)\overline{\otimes}_{\mathbb{E}}M$$

De plus l'espace tangent à H s'identifie à M/VM.

Remarque 2.7. *Cette équivalence de catégories se restreint à une équivalence entre modules ce Cartier M tels que M/VM soit R libre et groupes formels/R. De même pour libre de type fini et groupes formels formellement de type fini/R. Même chose avec projectif de type fini et groupes de Lie formels.....*

dem : Si M est V plat d'après le théorème 2.8 $N \mapsto \Lambda(N)\overline{\otimes}_{\mathbb{E}}M$ est exacte. De plus on vérifie immédiatement qu'il commute aux sommes directes. Donc $\Lambda(-)\overline{\otimes}M$ est un G foncteur formel.

Les deux foncteurs $H \mapsto M_H$ et $M \mapsto \Lambda(-)\overline{\otimes}M$ sont donc bien définis. Reste à vérifier qu'ils sont quasi inverse.

Soit H un G foncteur formel. On a une application naturelle

$$\Lambda(-)\overline{\otimes}M_H \to H(-)$$

définie de la façon suivante : $\forall N \in \mathbf{Nilp}_R \; \forall f \in \Lambda(N) \; \forall m \in M_H = H(R[[Y]])$ considérons

$$\Gamma(f, m) = \lambda_H^{-1}(m)_N(f) \in H(N)$$

cette application est $\mathbb{E}$ bilinéaire car $\forall \Phi \in \mathbb{E} = \mathrm{End}(\Lambda)^{opp}$

$$\begin{aligned} \Gamma(f.\Phi, m) &= \Gamma(\Phi_N(f), m) \\ &= \lambda_H^{-1}(m)_N(\Phi_N(f)) \\ &= (\lambda_H^{-1}(m)_N \circ \Phi_N)(f) \\ &= \lambda_H^{-1}(\Phi.m)_N(f) \\ &= \Gamma(f, \Phi.m) \end{aligned}$$

Elle se factorise donc en $\Gamma : \Lambda(N) \otimes_{\mathbb{E}} M \to H(N)$. Montrons que $\Gamma((\Lambda(N) \otimes_{\mathbb{E}} M)_\infty) = 0$. Ils s'agit de montrer que si $f \in \Lambda(N), f.\mathbb{E}_s = 0$ et $m \in M^s$ alors $\Gamma(f \otimes m) = 0$. Mais $\Gamma(f \otimes \mathbb{E}_s M) = 0$ et donc il suffit de prouver que $\Gamma(f \otimes M^t) = 0$ pour $t >> 0, t \geq s$ ($m \in M^s$ s'écrit $m = V_s x + m', m' \in M^t$).

Soit donc $m \in M^t$

$$\Gamma(f \otimes m) = \lambda_H^{-1}(m)_n(f) = H(\rho_f^n)(\theta_n)$$

$m \in M^t \Rightarrow \theta_n \in H(R[[X_1, \ldots, X_n]])_{poids \geq t})$ On en déduit facilement que si $t \geq nr$ où r est tel que $N^r = 0$ alors $\Gamma(f \otimes m) = 0$.

On obtient alors une application naturelle (la naturalité est facile)

$$\Lambda(-)\overline{\otimes}M_H \to H(-)$$

Les deux membres sont des G foncteurs formels. Pour vérifier que cette application est un isomorphisme il suffit de prouver que c'est un isomorphisme sur les espaces tangents (cf. (? ?)). Mais cela résulte du corollaire (2.3).

Dans l'autre sens il s'agit de vérifier que le module de Cartier de $\Lambda(-)\overline{\otimes}M$ est canoniquement isomorphe à M. Mais ce module est $\Lambda(R[[Y]])\overline{\otimes}M = \mathbb{E}\overline{\otimes}_{\mathbb{E}}M$. C'est donc clair.

□

2.10 Théorie de Cartier sur $\mathbb{Q}$

L'application exponentielle est bien définie sur $\mathbb{Q}$ ce qui simplifie nettement la théorie.

Remarque 2.8. *Si R est un anneau et $n \in \mathbb{N}$, dans $\mathbb{E}_R$, en général, $[n] \neq n = [1] + \cdots + [1]$. Si R est une $\mathbb{Q}$ algèbre alors n est inversible dans $\mathbb{E}_R$ car la série*

$$(1 + Yt)^{\frac{1}{n}} = 1 + \sum_{k \geq 1} \binom{1/n}{k} Y^k t^k \in \Lambda(R[[Y]])$$

est bien définie. On notera alors $\frac{1}{n}$ cet élément.

Théorème 2.5. *Si R est une $\mathbb{Q}$ algèbre on a un isomorphisme*

$$\Lambda \simeq \bigoplus_{r=1}^{\infty} \widehat{\mathbb{G}}_a$$

Commençons par noter que $\bigoplus \widehat{\mathbb{G}}_a$ signifie $\varinjlim_N \left(\bigoplus_1^N \widehat{\mathbb{G}}_a \right)$ au sens des faisceaux Zariski i.e.

$$\forall N \in \mathbf{Nilp}_R \quad \left(\bigoplus_1^{\infty} \widehat{\mathbb{G}}_a \right)(N) = \bigoplus_1^{\infty} N$$

mais pour N complet

$$\left(\bigoplus_1^{\infty} \widehat{\mathbb{G}}_a \right)(N) = \{ (x_r) \in \prod_1^{\infty} N \mid \lim_{r \to \infty} x_r = 0 \}$$

dem : Le théorème se déduit des isomorphismes réciproques pour $N \in \mathbf{Nilp}_R$

$$(1 + tN[t])^{\times} \underset{\exp}{\overset{\log}{\rightleftarrows}} tN[T] \simeq \bigoplus_1^{\infty} \widehat{\mathbb{G}}_a(N)$$

□

L'idée qui suit est maintenant la suivante : $\mathbb{E} = \mathrm{End}(\bigoplus_1^{\infty} \widehat{\mathbb{G}}_a)$ est une "algèbre de matrices" dont les composantes sont des éléments de $\mathcal{H}\mathrm{om}(\widehat{\mathbb{G}}_a, \widehat{\mathbb{G}}_a) \simeq R$ (exo.). L'idée est alors de démontrer que pour les modules de Cartier, $\mathbb{E}$ est "Morita équivalente" à R grâce au projecteur

$$\begin{pmatrix} 1 & 0 & \dots & 0 & \dots \\ 0 & 0 & \dots & 0 & \dots \\ \vdots & \vdots & & & \\ 0 & 0 & & & \\ \vdots & \vdots & & & \end{pmatrix}$$

qui intervient dans l'équivalence de Morita "classique" entre $M_n(R)$ et R.

Commençons par quelques calculs :

Lemme 2.11. *L'action de* $\mathbb{E}$ *sur* $\bigoplus_1^\infty \widehat{\mathbb{G}}_a$ *est donnée par : si* $x = (x_n)_n$

- $(x.V_n)_m = nx_{nm}$
- $(x[c])_m = x_m c^m$
- $(xF_n)_m = \begin{cases} x_{\frac{m}{n}} \text{ si } n|m \\ 0 \text{ sinon} \end{cases}$

dem : Vérifions par exemple la première égalité. Le membre de droite définit un endomorphisme de $\bigoplus_1^\infty \widehat{\mathbb{G}}_a \simeq \Lambda$. D'après le premier théorème fondamental de la théorie de Cartier (th.2.2) pour voir que cet endomorphisme coïncide avec l'action de V_n à droite il suffit de le vérifier sur $1-tY \in \Lambda(R[[Y]])$. Or $\log(1-tY) = \sum_{k\geq 1} \frac{Y^k}{k} t^k$ et $\log(1-tY^n) = \sum_{k\geq 1} n\frac{Y^{nk}}{nk} t^k$ d'où le résultat.

□

Considérons alors $\frac{1}{n} V_n F_n : \bigoplus \widehat{\mathbb{G}}_a \to \bigoplus \widehat{\mathbb{G}}_a$. C'est un projecteur car

$$\frac{1}{n^2} V_n (F_n V_n) F_n = \frac{1}{n} V_n F_n \text{ (cf.prop.2.2 (5))}$$

Corollaire 2.4. $(x.\frac{1}{n} V_n F_n)_m = \begin{cases} x_m \text{ si } n|m \\ 0 \text{ sinon} \end{cases}$

C'est donc le projecteur sur les composantes d'indice $m|n$.

Corollaire 2.5.

$$P = \prod_{l \text{ premier}} (1 - \frac{1}{l} V_l F_l) \in \mathbb{E} \text{ (pdt. commutatif convergent)}$$

est le projecteur $x \to x_1$.

(La commutativité du produit résulte de la proposition 2.2)

Ce P est donc bien celui qui nous intéresse dans l'équivalence de Morita.

Définition 2.9. *Soit* M *un* $\mathbb{E}$ *module de Cartier.* $PM \subset M$ *est le sous groupe des éléments typiques*

Lemme 2.12.

- $m \in PM \Leftrightarrow \forall n > 1 \;\; F_n m = 0$
- PM *est un* R *module via*

$$\forall c \in R \;\; \forall m \in PM \;\; c.m = [c]m$$

dem : $\forall m \in PM,\; m = Pm \Rightarrow \forall n > 1 \; F_n m = (F_n P)m$ or $F_n P = F_n \prod_l (1 - \frac{1}{l} V_l F_l)$ or si $l|n \; F_n - \frac{1}{l} F_n V_l F_l = 0$ (cf.2.2). Donc $F_n m = 0$.

Réciproquement, si $\forall n > 1 \;\; F_n m = 0$ alors $\forall l$ premier $(1 - \frac{1}{l} V_l F_l)m = m - 0 = m$ donc $Pm = m$.

Soient maintenant $c_1, c_2 \in R$ et $m \in PM$ grâce à la proposition 2.2 :

$$[c_1 + c_2]m = [c_1]m + [c_2]m + \sum_{n>1} V_n [a_n(c_1, c_2)] \underbrace{F_n m}_{0}$$

$$= [c_1]m + [c_2]m$$

d'où la structure de R module.

□

Proposition 2.4. *Si M est un module de Cartier alors la composée*

$$PM \to M \to M/M^2$$

est un isomorphisme de R modules.

dem : Le fait que ce soit un morphisme de R modules est facile.

Montrons que $P : M \to PM$ est trivial sur M^2 : par continuité et le fait que $M^2 = \overline{\mathbb{E}^2.M}$ il suffit de montrer que $P.\mathbb{E}^2 = 0$, or $\forall n > 1 \ PV_n = 0$ (cf. prop.2.2). On a donc une factorisation $P : M/M^2 \to PM$ qui est l'inverse de celle qui nous est donnée car on vérifie aisément que $\forall m \in M \ \ Pm \equiv m[M^2]$. □

Lemme 2.13. *$\frac{1}{n}V_nPF_n : \bigoplus \widehat{\mathbb{G}}_a \to \bigoplus \widehat{\mathbb{G}}_a$ est le projecteur sur la n ième composante.*

dem : Cela se déduit du lemme 2.11 et du corollaire 2.5. □

Théorème 2.6. *Soit M un $\mathbb{E}$ module de Cartier. Alors, chaque $m \in M$ admet une représentation unique*

$$m = \sum_n V_n M_n \ \text{ où } m_n \in PM$$

Soient M_1, M_2 deux modules de Cartier, $\bar{\alpha} : M_1/M_1^2 \to M_2/M_2^2$ un morphisme de R modules. Alors, $\bar{\alpha}$ se relève uniquement en un $\mathbb{E}$ morphisme de modules de Cartier de M_1 dans M_2.

dem : D'après le lemme précédent

$$1 = \sum_{n \geq 1} \frac{1}{n} V_n P F_n$$

D'où l'écriture unique $m = \sum_{n \geq 1} V_n \left(\frac{1}{n} PF_n\right) m$. Donc $m_n = \frac{1}{n} PF_n M \in PM$ convient.

Soit maintenant $\bar{\alpha} : PM_1 \to PM_2$. $\bar{\alpha}$ se relève de façon unique en une application $\alpha : M_1 \to M_2$ définie par

$$\alpha(\sum V_n m_n) = \sum V_n \bar{\alpha}(m_n)$$

Pour montrer que α est $\mathbb{E}$ linéaire il suffit de vérifier que $\alpha(V_n.m) = V_n\alpha(m)$, $\alpha(F_n.m) = F_n\alpha(m)$, $\alpha([c]m) = [c]\alpha(m)$ ce qui découle facilement des relations entre F, V et de la R linéarité de $\bar{\alpha}$. □

Corollaire 2.6. *Soir R une $\mathbb{Q}$ algèbre. Alors, $H \mapsto t_H$ est une équivalence de catégories entre G foncteurs formels et R modules plats.*

Cette équivalence se restreint en une équivalence entre groupes formels et R modules libres de type fini.

En particulier tout groupe formel est isomorphe à $(\widehat{\mathbb{G}}_a)^{\dim G}$ et tout morphisme entre $\widehat{\mathbb{G}}_a^{r_1}$ et $\widehat{\mathbb{G}}_a^{r_2}$ est "linéaire".

dem : Il s'agit simplement d'une application du théorème précédent et du deuxième théorème fondamental de la théorie de Cartier. □

2.11 Théorie de Cartier sur $\mathbb{Z}_{(p)}$

$$\mathbb{Z}_{(p)} = \bigcup_{n \wedge p = 1} \mathbb{Z}[\frac{1}{n}] = \{x \in \mathbb{Q} \mid v_p(x) \geq 0\}$$

Soit R une $\mathbb{Z}_{(p)}$ algèbre i.e. un anneau dans lequel tout entier premier à p est inversible. C'est par exemple le cas si pour N grand $p^N = 0$ sur R. On remarque que dans $\mathbb{E}_R$, $\forall n$ premier à p $n = [1] + \cdots + [1] \in \mathbb{E}_R$ est inversible car la série

$$(1 + Yt)^{1/n} = 1 + \sum_{k \geq 1} \binom{1/n}{k} Y^k t^k$$

vérifie $v_p\left(\binom{1/n}{k}\right) \geq 0$.

Comme précédemment, grâce à des idempotents dans $\mathbb{E}$ on va essayer de trouver une équivalence de Morita entre modules de Cartier et modules sur un anneau "plus simple".

2.11.1 Idempotents

Définition 2.10.

$$\epsilon_1 = \prod_{l \neq p} (1 - \frac{1}{l} V_l F_l) \in \mathbb{E} \text{ (l premier)}$$

$$\forall n, n \wedge p = 1 \quad \epsilon_n = \frac{1}{n} V_n \epsilon_1 F_n$$

(Le produit convergent est commutatif)

Lemme 2.14. *Les ϵ_i sont des idempotents orthogonaux :*

$$\epsilon_n \epsilon_m = \delta_{n,m} \epsilon_n$$

Par fonctorialité de $R \to \mathbb{E}_R$ il suffit de le démontrer dans le cas universel $\mathbb{Z}[X_{i,j}]$ qui se plonge dans une $\mathbb{Q}$ algèbre. Il suffit donc de le vérifier dans le cas d'une $\mathbb{Q}$ algèbre. En utilisant le lemme 2.11 on trouve pour $x \in \bigoplus \widehat{\mathbb{G}}_a$:

$$\forall n \; n \wedge p = 1 \;\; (x.\epsilon_n)_m = \begin{cases} x_m \text{ si } \exists \alpha \in \mathbb{N} \; m = p^\alpha n \\ 0 \text{ sinon} \end{cases}$$

Les égalités affirmées s'en déduisent aussitôt.

□

Si $N \in \mathbf{Nilp}_R$, $\Lambda(N)$ est un $\mathbb{E}$ module de torsion à droite (proposition 2.3). Or $\epsilon_n \in \mathbb{E}_n$ donc $\forall x \in \Lambda(N) \;\; \exists n_0 \;\; \forall n \geq n_0 \;\; x\epsilon_n = 0$. Donc, si $\Lambda_n = \Lambda\epsilon_n$,

$$\boxed{\Lambda = \bigoplus_{n \wedge p = 1} \Lambda_n}$$

Définition 2.11. $\widehat{W} = \Lambda_1$ *qui est un G foncteur formel.*

Lemme 2.15. *L'application*

$$\begin{array}{ccc} \Lambda_n & \longrightarrow & \widehat{W} \\ x & \longmapsto & xV_n \end{array}$$

est un isomorphisme

dem : L'application est bien à valeurs dans $\widehat{W}$ car

$$\Lambda_n V_n = \Lambda \epsilon_n V_n = \Lambda \frac{1}{n} V_n \epsilon_1 F_n V_n = \Lambda V_n \epsilon_1 \subset \widehat{W}$$

L'inverse est donné par $x \mapsto x\frac{1}{n}F_n$. On a bien que si $x = y\epsilon_1 \in \widehat{W}$

$$x\frac{1}{n}F_n = y\frac{1}{n}\epsilon_1 F_n = \left(y\frac{F_n}{n}\right)\frac{1}{n}V_n\epsilon_1 F_n \in \Lambda_n$$

On vérifie aussitôt que ces deux applications sont réciproques l'une de l'autre.

□

Corollaire 2.7. $\Lambda \simeq \bigoplus_{n \wedge p = 1} \widehat{W}$ *isomorphisme de G foncteurs formels.*

Définition 2.12. *Si M est un module de Cartier les éléments de $\epsilon_1 M \subset M$ sont appelés les éléments p-typiques. Si $M = M_H$ est le module de Cartier du G foncteur formel H les éléments p-typiques s'appellent les courbes p-typiques.*

Lemme 2.16. *$m \in M$ est p-typique $\Leftrightarrow \forall n, n \wedge p = 1 \;\; F_n m = 0$*

La démonstration est la même que celle du lemme 2.12

□

Lemme 2.17. *Tout élément $m \in M$ s'écrit de façon unique $m = \sum_{n \geq 1} V_n m_n$ où m_n est p typique.*

Cela découle de

$$1 = \sum \epsilon_n = \sum V_n \epsilon_1 \left(\frac{1}{n}F_n\right)$$

□

Le but est maintenant de ré-énoncer les théorèmes fondamentaux de la théorie de Cartier en termes de $\widehat{W}$ à la place de Λ et $\mathrm{End}(\widehat{W})$ à la place de $\mathbb{E}$

2.11.2 Le premier théorème fondamental revisité

Théorème 2.7. *Soit H un G foncteur formel. Il y a un isomorphisme*

$$\begin{array}{ccc} \mathcal{H}om(\widehat{W}, H) & \xrightarrow{\simeq} & \epsilon_1 H(R[[Y]]) = \epsilon_1 M_H \\ \Phi & \mapsto & \epsilon_1 \Phi_{R[[Y]]}(1 - tY) \end{array}$$

dem : $\mathcal{H}\mathrm{om}(\widehat{W}, H) = \mathcal{H}\mathrm{om}(\Lambda\epsilon_1, H)$. Or si on écrit $\Lambda = \bigoplus_{n\wedge p=1} \Lambda_n$,

$$\mathcal{H}\mathrm{om}(\Lambda, H) \simeq \prod_{n\wedge p=1} \mathcal{H}\mathrm{om}(\Lambda_n, H)$$

et donc $\epsilon_1\mathcal{H}\mathrm{om}(\Lambda, H) = \mathcal{H}\mathrm{om}(\Lambda_1, H)$. puisque ϵ_1 tue tout morphisme partant de Λ_n, $n > 1$.

Le théorème est donc une conséquence du premier théorème fondamental (th.2.2).

□

2.11.3 $\mathbb{E}_p$ modules V réduits

Corollaire 2.8. $\mathbb{E}_p := End(\widehat{W}) = \epsilon_1\mathbb{E}\epsilon_1$ *et tout élément de* $\mathbb{E}_p$ *s'écrit de façon unique :*

$$\epsilon_1 \sum_{r,s\geq 0} V_{p^r}[x_{r,s}]F_{p^s} = \sum_{r,s\geq 0} V_{p^r}[x_{r,s}]F_{p^s}\epsilon_1$$

dem :

$$\mathrm{End}(\widehat{W}) = \mathcal{H}\mathrm{om}(\widehat{W}, \widehat{W}) = \epsilon_1\widehat{W}(R[[Y]]) = \epsilon_1\mathbb{E}\epsilon_1$$

Pour la seconde assertion remarquons grâce au lemme ? ? ? que $\forall r \geq 0$:

$$\begin{aligned} F_{p^r}\epsilon_1 &= \epsilon_1 F_{p^r} \\ V_{p^r}\epsilon_1 &= \epsilon_1 V_{p^r} \\ [c]\epsilon_1 &= \epsilon_1[c] \end{aligned}$$

et que si n n'est pas une puissance de p :

$$\begin{aligned} F_n\epsilon_1 &= 0 \\ \epsilon_1 V_n &= 0 \end{aligned}$$

Donc $\forall x = \sum_{r,s\geq 0} V_r[c_{r,s}]F_s \in \mathbb{E}$, $\epsilon_1 x\epsilon_1 = \sum_{r,s\geq 0} \epsilon_1 V_r[c_{r,s}]F_s\epsilon_1$ Expression dans laquelle ne subsistent que les termes où r et s sont une puissance de p d'après les remarques précédentes. Donc

$$\begin{aligned} \epsilon_1 x\epsilon_1 &= \sum_{r,s\geq 0} V_{p^r}\epsilon_1[c_{p^r,s}]\epsilon_1 F_{p^s} \\ &= \sum_{r,s\geq 0} V_{p^r}\epsilon_1[c_{p^r,s}]F_s \\ &= \sum_{r,s\geq 0} \epsilon_1 V_{p^r}[c_{p^r,p^s}]F_{p^s} \end{aligned}$$

D'où l'existence de l'écriture annoncée. Quant à l'unicité, soit $y = \sum_{r,s\geq 0} V_r[c_{r,s}]F_s$ et supposons que $\epsilon_1 y = 0$. On veut montrer que $y = 0$. $V_p : \mathbb{E} \to \mathbb{E}$ étant injectif (cf remarque

2.2) et commutant à ϵ_1 on peut supposer que $y \notin \mathbb{E}_{p^r}$ ($\Leftrightarrow y \notin \mathbb{E}_2 \Leftrightarrow \exists s\ x_{0,s} \neq 0$). Mais alors

$$\begin{aligned} y = \sum_{n\wedge p=1} \epsilon_n y &= \sum_{n\wedge p=1, n\geq 2} \epsilon_n y \text{ car } \epsilon_1 y = 0 \\ &= \sum_{n\wedge p=1, n\geq 2} V_n\left(\frac{1}{n}\epsilon_1 F_n y\right) \in \mathbb{E}_2 \end{aligned}$$

Contradiction. Donc $y = 0$.

□

Définition 2.13. *Notons*

$$V = \epsilon_1 V_p = V_p \epsilon_1 \in \mathbb{E}_p$$
$$F = \epsilon_1 F_p = F_p \epsilon_1 \in \mathbb{E}_p$$
$$\forall x \in R\ \ [x]_p = [x]\epsilon_1 = \epsilon_1 [x]$$

Donc,

$$\boxed{\mathbb{E}_p = \{\sum_{r,s\geq 0} V^r [x_{r,s}]_p F^s\}}$$

On a les relations

$$\begin{aligned} [1]_p &= 1 \\ FV &= p \\ F[x]_p &= [x^p]_p F \\ [x]_p V &= V[x^p]_p \\ [x]_p[y]_p &= [xy]_p \\ [x+y]_p &= [x]_p + [y]_p + \sum_{n\geq 1} V^n [a_{p^n}]_p F^n \end{aligned}$$

Les vecteurs de Witt ne sont pas très loin...

Définition 2.14. *Un $\mathbb{E}_p$ module M_p est V réduit si*
- *$V : M_p \to M_p$ est injectif*
- *$M_p \xrightarrow{\simeq} \varprojlim M_p/V^n M_p$ i.e. M_p est V complet.*

Remarque 2.9. *Cette définition est "équivalente" à dire que tout élément $m \in M_p$ s'écrit de façon unique $\sum_{r\geq 0} V^r m_{\alpha(r)}$ où $(m_i)_i$ est un système de représentants de M/VM.*

On déduit de cette remarque :

Proposition 2.5. *Si M est un module de Cartier V réduit, $\epsilon_1 M$ est un $\mathbb{E}_p$ module V réduit.*

Remarque 2.10. *La catégorie des $\mathbb{E}_p$ modules V-réduits a pour objets les objets définis ci dessus et pour morphismes les morphismes de $\mathbb{E}_p$ modules. Contrairement à la catégorie des $\mathbb{E}$ modules de Cartier V-réduits, il n'y a pas d'hypothèses sur les filtrations. En d'autres termes, un morphisme de $\mathbb{E}_p$ modules V réduits est automatiquement continu pour la topologie V-adique, tandis que si $f : M_1 \to M_2$ est un morphisme de $\mathbb{E}$ modules, $M_1^n = \overline{V_n M_1}$ et dire que $\forall n\ f(M_1^n) \subset M_2^n$ est équivalent à dire que f est continue puisqu'alors $f(\overline{V_n M_1}) \subset \overline{f(V_n M_1)} = \overline{V_n f(M_1)} \subset M_2^n$.*

Les $\mathbb{E}_p$ modules V-réduits sont des objets plus algébriques. C'est d'ailleurs pour cette raison que le produit tensoriel des $\mathbb{E}_p$ modules V-réduits n'a pas besoin du quotient par $(N \otimes M)_\infty$.

2.11.4 "Équivalence de Morita"

Théorème 2.8. *Le foncteur $M \longmapsto \epsilon_1 M$ est une équivalence de catégories entre les $\mathbb{E}$ modules V réduits et les $\mathbb{E}_p$ modules V réduits.*

dem : Construisons un quasi inverse. Soit M_p un $\mathbb{E}_p$ module V réduit. Posons

$$M = \widehat{(\mathbb{E}\epsilon_1 \otimes_{\epsilon_1 \mathbb{E} \epsilon_1} M_p)}$$

le complété pour la topologie définie par les $(\mathbb{E}_n \epsilon_1 \otimes_{\mathbb{E}_p} M_p)_{n \in \mathbb{N}}$ (ou plutôt leur image). Montrons que M esr V réduit. Soit $(m_i)_i$ un système de représentants de $M_p / V M_p$. Tout élément $m \in M_p$ s'écrit de façon unique

$$m = \sum_{s=0}^{\infty} V^s m_{\alpha(s)}$$

Donc tout élément de M s'écrit de façon unique

$$\sum_{r \wedge p = 1} V_r \epsilon_1 \otimes \sum_{s \geq 0} V_{p^s} m_{\alpha(s), r}$$

$$= \sum_{r \in \mathbb{N}} V_n \epsilon_1 \otimes m'_n$$

On en déduit facilement que M est V réduit et que $\epsilon_1 M = M_p$. On vérifie également que $\forall M$ V réduit on a un isomorphisme de $\mathbb{E}$ modules

$$\widehat{(\mathbb{E}\epsilon_1 \otimes_{\epsilon_1 \mathbb{E} \epsilon_1} \epsilon_1 M)} \xrightarrow{\simeq} M$$

□

2.11.5 Le second théorème fondamental

Théorème 2.9. *Soit M un $\mathbb{E}$ module de Cartier V réduit. On a alors un isomorphisme de G-foncteurs formels*

$$\boxed{\widehat{W}(-) \otimes_{\mathbb{E}_p} \epsilon_1 M \simeq \Lambda(-) \overline{\otimes}_{\mathbb{E}} M}$$

dem : On a un morphisme naturel

$$\widehat{W}(-) \otimes_{\mathbb{E}_p} \epsilon_1 M \to \Lambda(-) \otimes_{\mathbb{E}} M \twoheadrightarrow \Lambda(-) \overline{\otimes}_{\mathbb{E}} M$$

associé aux inclusions $\widehat{W} \hookrightarrow \Lambda$ et $\epsilon_1 M \hookrightarrow M$.

La difficulté vient de l'application réciproque. Soit

$$\begin{aligned} B : \Lambda(N) \times M &\to \widehat{W}(N) \otimes_{\mathbb{E}_p} \epsilon_1 M \\ (\lambda, m) &\mapsto \sum_{r \wedge p = 1} \lambda V_r \epsilon_1 \otimes m_r \end{aligned}$$

où $m = \sum_{r \wedge p = 1} V_r m_r$, m_r p-typique (cf. 2.17). On remarque que $\Lambda(N)$ étant de torsion (cf. 2.3) cette somme est finie.

Il s'agit maintenant de montrer que B est bilinéaire et triviale sur $(\Lambda(N) \otimes_{\mathbb{E}} M)_\infty$.

Pour montrer la bilinéarité, l'expression de B se ramenant à une somme finie il suffit de montrer que pour $a = [c], V_s, F_c$ $B(\lambda a, V_r m) = B(\lambda, a V_r m)$ si m est p typique et $r \wedge p = 1$. Pour $[c]$:

$$\begin{aligned} B(\lambda[c], V_r m) &= \lambda V_r \epsilon_1 \otimes m \\ &= \lambda V_r [c^r] \epsilon_1 \otimes m \\ &= \lambda V_r \epsilon_1 [c^r] \otimes m \\ &= \lambda V_r \epsilon_1 \otimes [c^r]_p \otimes m \\ &= \lambda V_r \epsilon_1 \otimes [c^r]_p m \text{ car } [c^r]_p \in \mathbb{E}_p \\ &= B(\lambda, V_r [c^r] m) = B(\lambda, [c] V_r m) \end{aligned}$$

Pour V_s, si $s \wedge p = 1$:

$$\begin{aligned} B(\lambda V_s, v_r m) &= \lambda V_s V_r \epsilon_1 \otimes m \\ &= \lambda V_{rs} \epsilon_1 \otimes m \\ &= B(\lambda, V_{rs} m) = B(\lambda, V_s V_r m) \end{aligned}$$

et si $s = p^\alpha$:

$$\begin{aligned} B(\lambda V_{p^\alpha}, V_r m) &= \lambda V_{p^\alpha} V_r \epsilon_1 \otimes m \\ &= \lambda V_r V_{p^\alpha} \epsilon_1 \otimes m \\ &= \lambda V_r \epsilon_1 V_{p^\alpha} \otimes m \\ &= \lambda V_r \epsilon_1 \otimes V^\alpha m \text{ car } V \in \mathbb{E}_p \\ &= B(\lambda, V_r V_{p^\alpha} m) = B(\lambda, V_{p^\alpha} V_r m) \end{aligned}$$

Donc $\forall s \;\; B(\lambda V_s, V_r m) = B(\lambda, V_s V_r m)$.

Pour F_s, supposons $s \wedge r = 1$:

$$\begin{aligned} B(\lambda F_s, V_r m) &= \lambda F_s \epsilon_1 \otimes m \\ &= \lambda V_r F_s \epsilon_1 \otimes m (2.29)) \\ &= \lambda V_r \epsilon_1 (\epsilon_1 F_s \epsilon_1) \otimes m \text{ car } F_s \epsilon_1 = \epsilon_1 F_s \epsilon_1 \\ &= \lambda V_r \epsilon_1 \otimes F_s m \text{ or } F_s m \text{ est p-typique} \\ &= B(\lambda, V_r F_s m) = B(\lambda, F_s V_r m) \end{aligned}$$

Si $s|r$:

$$\begin{aligned} B(\lambda F_s, V_r m) &= \lambda F_s F_v \epsilon_1 \otimes m \\ &= \lambda s V_{\frac{r}{s}} \epsilon_1 \otimes m \\ &= \lambda V_{\frac{r}{s}} \epsilon_1 \otimes sm \\ &= B(\lambda, s V_{\frac{r}{s}} m) \\ &= B(\lambda, F_s V_r m) \end{aligned}$$

D'où $\forall s \;\; B(\lambda F_s, V_r m) = B(\lambda, F_s V_r m)$.

D'où la bilinéarité. Il reste à voire que $B((\Lambda(N) \otimes_{\mathbb{E}} M)_\infty) = 0$.

Si $\lambda \mathbb{E}_s = 0$ et $m \in M^s \;\; m = \sum_{r \wedge p = 1} V_r m_r$.

$$\forall r \geq s \;\; m_r = \sum_{a \geq \alpha(r)} V_{p^a} m_{r,a} = V^{\alpha(r)} m'_r$$

où $\alpha(r) = inf\{a | p^a \geq \frac{s}{r}\}$ et où m'_r est p-typique. Donc

$$\begin{aligned} B(\lambda, m) &= \sum_{r \wedge p = 1} \lambda V_r \epsilon_1 \otimes m_r \\ &= \sum_{r \wedge p = 1} \lambda V_r \epsilon_1 \otimes V^{\alpha(r)} m'_r \\ &= \sum_{r \wedge p = 1} \lambda V_r \epsilon_1 V^{\alpha(r)} \otimes m'_r \text{ car } V \in \mathbb{E}_p \\ &= \sum_{r \wedge p = 1} \underbrace{\lambda V_{r p^{\alpha(r)}}}_{0} \epsilon_1 \otimes m'_r = 0 \end{aligned}$$

On a donc bien une application $\Lambda(N) \overline{\otimes}_{\mathbb{E}} M \to \widehat{W}(N) \otimes_{\mathbb{E}_p} \epsilon_1 M$ dont il est clair qu'elle est naturelle en $N \in \mathbf{Nilp}_R$ et dont on vérifie aussitôt qu'elle est un inverse à l'application canonique définie au début de la démonstration.

□

Théorème 2.10. *Si R est une $\mathbb{Z}_{(p)}$ algèbre il y a une équivalence de catégories entre les G foncteurs formels et les $\mathbb{E}_p$ modules V-réduits V-plats.*

$$H \longmapsto \mathcal{H}om(\widehat{W}, H) = \epsilon_1 M_H$$

qui est un $End(\widehat{W})^{opp} = \epsilon_1 \mathbb{E} \epsilon_1$ *module* V *réduit.*

$$M_p \longmapsto \widehat{W}(-) \otimes_{\mathbb{E}_p} M_p$$

De plus, $t_H \simeq M_p/VM_p$.

Cette équivalence se restreint en une équivalence entre groupes formels et $\mathbb{E}_p$ *modules tels que* M_p/VM_p *soit* R *libre de type fini.*

dem : Cela résulte des théorèmes précédents ainsi que du second théorème fondamental. □

2.12 $\widehat{W}$ et vecteurs de Witt

Proposition 2.6. *Les applications*

$$\begin{aligned}
\bigoplus_{i\geq 1} N &\to \Lambda(N) \\
(n_i)_i &\mapsto \prod_{i\geq 1}(1-n_i t^i) \\
\bigoplus_{j\geq 0} N &\to \widehat{W}(N) \\
(n_j)_j &\mapsto \prod_{j\geq 0}(1-n_j t^{(p^j)})\epsilon_1
\end{aligned}$$

donnent des isomorphismes de foncteurs d'ensembles :

$$\begin{aligned}
\bigoplus \widehat{\mathbb{G}}_a &\xrightarrow{\sim} \Lambda \\
\bigoplus \widehat{\mathbb{G}}_a &\xrightarrow{\sim} \widehat{W}
\end{aligned}$$

dem : Ces applications sont bien fonctorielles en $N \in \mathbf{Nilp}_R$. Puisque les deux membres sont des G foncteurs formels d'ensembles, pour montrer que ce sont des isomorphismes il suffit de montrer que ce sont des isomorphismes sur les foncteurs tangents (et non les espaces tangents car on ne parle pas ici de foncteurs à valeurs dans **Ab** : il faut tester tous les $N, N^2 = 0$; $R[\epsilon]^+$ ne suffit pas, on ne peux pas utiliser $t_H(N) = t_H(R[\epsilon]^+) \otimes N \ldots$).

Pour Λ, si $N^2 = 0$,

$$\prod_{i\geq 1}(1-n_i t^i) = 1 - \sum_{i\geq 1} n_i t^i$$

c'est donc bien un isomorphisme.

Pour $\widehat{W}$: Tout $x \in \widehat{W}(N)$ s'écrit d'après le cas précédent pour Λ

$$\begin{aligned}
\prod_{i\geq 1}(1-n_i t^i)\epsilon_1 &= \prod_{i\geq 1}(1-n_i t)F_i\epsilon_1 \\
&= \prod_{j\geq 0}(1-n_j t^{(p^j)})\epsilon_1
\end{aligned}$$

(car $F_i\epsilon_1 = 0$ si i n'est pas une puissance de p)

D'où la surjectivité.

Si $N^2 = 0$ supposons que $\prod_{j\geq 0}(1-n_j t^{(p^j)})\epsilon_1 = 1$. Alors,

$$\forall i \;\; n_i^2 = 0 \Longrightarrow \forall m > 1 \;\; (1-n_j t^{(p^j)})F_m = 1$$

$$\text{or } 1 = \sum_{n\wedge p=1} \epsilon_n \implies \prod_{j\geq 0}(1-n_j t^{(p^j)})$$

$$= \prod_{j\geq 0}(1-n_j t^{(p^j)})\epsilon_1 \times \prod_{n\wedge p=1, n>1}\left(\prod_{j\geq 0}(1-n_j t^{(p^j)})\right)\underbrace{\epsilon_n}_{F_n(\frac{1}{n}\epsilon_1 V_n)}$$

$$= 1\times 1 = 1$$

donc $\prod_{j\geq 0}(1-n_j t^{(p^j)}) = 1 \Longrightarrow \forall j\ n_j = 0$ par le cas de Λ. D'où l'injectivité. □

Maintenant que nous avons compris la structure ensembliste de $\widehat{W}$, un élément de $\widehat{W}$ étant donné par ses coordonnées dans $\oplus\widehat{\mathbb{G}}_a$, il faut comprendre la structure de groupe. Ensemblistement, le foncteur vecteurs de Witt $W_{|\mathbf{Nilp}_R} : \mathbf{Nilp}_R \to \boldsymbol{\mathcal{E}}\mathbf{ns}$ est isomorphe à $\prod\widehat{\mathbb{G}}_a$. Nous allons voire qu'en fait l'injection $\oplus\widehat{\mathbb{G}}_a \hookrightarrow \prod\widehat{\mathbb{G}}_a$ est un morphisme de groupe $\widehat{W} \hookrightarrow W$.

Définition 2.15. *(Polynômes de Witt généralisés)*

$$\forall m \geq 1 \quad U_m(X_1,\ldots,X_m) = \sum_{d|m}\frac{m}{d}X_{\frac{m}{d}}^d$$

Remarque 2.11. *On a donc :*

$$\forall n\in\mathbb{N} \quad U_{p^n}(X_1,\ldots,X_n) = W_n(Y_0,\ldots,Y_n) \text{ où } Y_i = X_{p^i}$$

les polynômes de Witt habituels.

Théorème 2.11. *Il y a des morphismes de foncteurs de groupes*

$$\begin{array}{rcl}\Lambda & \longrightarrow & \bigoplus_{m=1}^{\infty}\widehat{\mathbb{G}}_a \\ \prod_{i\geq 1}(1-n_i t^i) & \longmapsto & (U_m(n_1,\ldots,n_i))_{m\geq 1}\end{array}$$

$$\begin{array}{rcl}\widehat{W} & \longrightarrow & \bigoplus_{m=0}^{\infty}\widehat{\mathbb{G}}_a \\ \prod_{j\geq 0}(1-n_j t^{(p^j)})\epsilon_1 & \longmapsto & (W_m(n_0,\ldots,n_m))_{m\geq 0}\end{array}$$

dem : Ce sont bien des applications naturelles en $N \in \mathbf{Nilp}_R$. Pour montrer que ce sont des morphismes de groupe il suffit de le faire dans le cas universel. On peut donc supposer que R est une $\mathbb{Q}$ algèbre. On peut alors utiliser les applications exponentielle et logarithme (cf.2.5).

Pour Λ :

$$\begin{aligned}\log\left(\prod_{i\geq 1}(1-n_i t^i)\right) &= -\sum_{i\geq 1}\sum_{k\geq 1} n_i^k \frac{t^{ik}}{k} \\ &= -\sum_{m\geq 1}\sum_{d|m}\left(\frac{m}{d}n_i^d\right)\frac{t^m}{m} \\ &= -\sum_{m\geq 1} U_m(n_1,\ldots,n_m)\frac{t^m}{m}\end{aligned}$$

Il est clair sur cette expression que le morphisme donné est additif puisque le logarithme transforme produits en sommes.

Pour $\widehat{W}$: ϵ_1 est une projection sur les éléments dont l'indice est une puissance de p. Donc par restriction c'est un morphisme pour $\widehat{W}$.

□

Ainsi $\widehat{W}(N) \subset W(N)$ est l'ensemble des $(a_0,\ldots,a_n,\ldots)$ tels que $a_i = 0$ pour $i >> 0$. On peut d'ailleurs vérifier directement que $\widehat{W}(N)$ est bien stable par l'addition (ce qui est faux si N n'est pas nilpotente). En effet, l'addition dans $W(N)$ est donnée par des polynômes universels, $(a_i)_i + (b_i)_i = (P_i(a_0,\ldots,a_i;b_0,\ldots,b_i))_i$ dont on peut montrer qu'à $k \in \mathbb{N}$ fixé tout monôme faisant intervenir les $X_l, Y_l, l \leq k$ est de degré tendant vers l'infini lorsque i tends vers l'infini. N étant nilpotente on en déduit que $\widehat{W}(N) \subset W(N)$ est stable par l'addition.

On vérifie facilement le lemme suivant :

Lemme 2.18. *L'action de $V \in \mathbb{E}_p$ sur $\widehat{W}$ est la même que celle induite par le morphisme F usuels (cf. ? ? ?) sur W restreints à $\widehat{W}$. De même, les rôles de $F \in \mathbb{E}_p$ et V sont inversés. L'action de $[c] \in \mathbb{E}_p$ est la même que l'action de $[c] \in W(R)$ par multiplication.*

Remarque 2.12. *Il n'est pas étonnant que les rôles de F et V soient inversés puisque $\mathbb{E}_p$ agit à droite sur $\widehat{W}(N)$ tandis que les morphismes F et V des vecteurs de Witt agissent à gauche.*

Proposition 2.7. *L'ensemble des éléments de la forme $\sum_{n\geq 0} V^n[a_n]F^n$ est un sous anneau commutatif $\mathcal{W}$ de $\mathbb{E}_p$ et l'application*

$$\begin{aligned} W(R) &\longrightarrow \mathcal{W} \\ (a_0,\ldots,a_n,\ldots) &\longmapsto \sum_{n\geq 0} V^n[a_n]F^n\end{aligned}$$

est un isomorphisme d'anneaux.

$\mathbb{E}_p$ contient donc les vecteurs de Witt.

dem : Commençons par démontrer un lemme :

Lemme 2.19. *$\forall N \in \mathbf{Nilp}_R$, l'application*

$$\begin{aligned} W(R)\times\widehat{W}(N) &\longrightarrow W(R\oplus N) \\ (x,y) &\longmapsto xy\end{aligned}$$

est à valeurs dans $\widehat{W}(N)$ *et définit un morphisme*

$$W(R) \longrightarrow \mathbb{E}_p = End(\widehat{W})^{opp}$$

dem : Ici $R \oplus N$ est vu comme un anneau augmenté, $W(R), W(N), \widehat{W}(N) \subset W(R \oplus N)$. Montrons d'abord que $\forall x \in W(R)\ \forall y \in W(N)\ \ xy \in W(N)$ i.e. $W(N)$ est un idéal de $W(R \oplus N)$. Il existe des polynômes universels $(P_i)_i$ tels que

$$(x_i)_i.(y_i)_i = (P_i(x_0, \ldots, x_i; y_0, \ldots, y_i))_i$$

Or $P_i(\underline{X}, 0) = 0$ car $\forall R\ \forall x \in W(R)\ x.0 = 0$. Donc tout monôme de P_i fait intervenir des termes en Y_k pour au moins un k, or $R.N \subset N$, d'où le résultat.

Il s'agit maintenant de montrer que $W(R).\widehat{W}(N) \subset \widehat{W}(N)$. Or $\forall x \in N\ \forall m \in \mathbb{N}\ \ \forall \sum_{n\geq 0} V^n([a_n]) \in W(R)$

$$\sum_{n\geq 0} V^n([a_n]).V^m([x]) = \sum_{n\geq 0}([a_n]F^n(V^m([x])))$$

car $\forall a, b\ V(aF(b)) = V(a)V(b)$. Or si $n \geq m\ F^nV^m([x]) = p^{n-m}F^{n-m}([x]) = p^{n-m}[x^{(p^{n-m})}]$ (tout ceci est bien vrai même si R n'est pas de caractéristique p) qui est nul si $n >> 0$ car x est nilpotent. La somme sur n ci dessus est alors finie et appartient donc à $\widehat{W}(N)$.

Tout élément de $\widehat{W}(N)$ étant une somme finie de $V^m([x])$ on en déduit le résultat.

□

Montrons maintenant que l'application $W(R) \to \mathbb{E}_p$:

$$\sum_{n\geq 0} V^n([a_n]) \longmapsto \sum_{n\geq 0} V^n[a_n]F^n$$

est telle que l'élément associé de $\mathbb{E}_p = \mathrm{End}(\widehat{W})^{opp}$ agisse de la même façon que l'élément de $W(R)$:

$\forall N \in \mathbf{Nilp}_R\ \ \forall x \in \widehat{W}(N)$:

$$\begin{aligned}
(\sum_{n\geq 0} V^n([a_n])).x &= \sum_{n\geq 0} V^n([a_n]F^n(x)) \text{ car } V(aF(b)) = V(a)b \\
&= \sum_{n\geq 0} V^n(x.(V^n[a_n])) \text{ grâce au lemme 2.18} \\
&= \sum_{n\geq 0} x.(V^n[a_n]F^n) \text{ grâce au lemme 2.18} \\
&= x.\sum_{n\geq 0} V^n[a_n]F^n
\end{aligned}$$

D'où le résultat.

□

Remarque 2.13. *Au début et à la fin des égalités ci dessus V et F n'ont pas le même sens. D'après le lemme 2.18 il faut faire attention à ne pas s'emmêler les pinceaux.*

2.13 Quelques remarques sur le cas d'un corps parfait

Cette section est juste destinée à faire remarquer au lecteur certaines particularités du cas où R est un corps parfait k de caractéristique p.

La première chose à remarquer est qu'alors F et V commutent :

$$FV = VF = p$$

de plus F et V sont semi-linéaires linéaires :

$$\forall \lambda \in k \quad F[\lambda] = [\lambda^p]F \quad V[\lambda] = [\lambda^{p^{-1}}]V$$

On a vu que $W(k) = \{\sum_n V^n[a_n]F^n\} \subset \mathbb{E}_p$, mais ici

$$\sum_n V^n[a_n]F^n = \sum_n [a_n^{p^{-n}}]p^n$$

et de plus $W(k)$ est un anneau de valuation discrète d'uniformisante p et de corps résiduel k.

Si M est un module V-réduit, M/VM est un k-ev. Supposons M/VM de dimension finie. Étant donné que M est V-adiquement complet et que $p = VF$, M est p-adiquement complet.

Alors, M est sans p-torsion $\iff$ M est sans F-torsion (car $VF = p$ et V est injectif).

Dans tous les cas, M est un $W(k)$ module muni de deux opérateurs F et V σ et σ^{-1} linéaires tels que $FV = p$.

En particulier, si M est sans p torsion et de type fini sur $W(k)$, M est un $W(k)$ cristal.

La classification des groupes-p divisibles sur un corps parfait n'est plus très loin...

2.14 Présentations des modules V-réduits

Comme précédemment pour $\mathbb{E}$ on peut définir des modules de Cartier "libres" qui permettent de donner un sens à la notion de présentation d'un module de Cartier.

Définition 2.16. *Si I est un ensemble, notons $\widehat{\mathbb{E}_p^{(I)}}$ le complété de $\mathbb{E}_p^{(I)}$ pour la topologie V-adique.*

$\widehat{\mathbb{E}_p^{(I)}}$ est le module des courbes p-typiques du G-foncteur formel $\mathbb{E}_p^{(I)}$ (facile à voire).

$$\widehat{\mathbb{E}_p^{(I)}} = \{(x_i)_i \in \mathbb{E}_p^I \mid x_i \to 0\}$$

On montre facilement le lemme :

Lemme 2.20. *Si M est V-réduit alors*

$$\begin{array}{rcl} \mathcal{H}om(\widehat{\mathbb{E}_p^{(I)}}, M) & \xrightarrow{\sim} & M^I \\ f & \mapsto & (f(e_i))_i \end{array}$$

où $(e_i)_i$ est la base canonique de $\mathbb{E}^{(I)}$.

Lemme 2.21.
- *Tout sous module fermé d'un module V réduit est V-réduit.*
- *Si $f : M_1 \to M_2$ est un morphisme de $\mathbb{E}_p$ modules V-réduits tel que $\bar{f} : M_1/VM_1 \to M_2/VM_2$ ("l'application tangente") soit injective alors f est injectif. De plus M_2/M_1 est V-réduit.*

dem : La première assertion est claire.
$\forall n > 0$ le diagramme suivant commute :

$$\begin{array}{ccc} M_1/VM_1 & \xrightarrow{\bar{f}} & M_2/VM_2 \\ \simeq \downarrow V^n & & \simeq \downarrow V^n \\ V^nM_1/V^{n+1}M_1 & \longrightarrow & V^nM_2/V^{n+1}M_2 \end{array}$$

donc la flèche du bas est injective. f induisant pour tout n des morphismes de modules filtrés $M_1/V^nM_1 \to M_2/V^nM_2$ injectifs sur les quotients de la filtration, les applications $M_1/V^nM_1 \to M_2/V^nM_2$ sont injectives. M_1 étant V-séparé, f est injectif.

L'injectivité de $M_1/V^nM_1 \to M_2/V^nM_2$ est équivalente à ce que $V^nM_2 \cap M_1 = V^nM_1$ ce qui est équivalent à ce que V soit injectif sur M_2/M_1. On a alors des suites exactes

$$0 \to M_1/V^nM_1 \to M_2/V^nM_2 \to (M_2/M_1)/V^n(M_2/M_1) \to 0$$

qui montrent que M_2/M_1 est V-complet.

□

Soit maintenant M un module V-réduit tel que M/VM soit R libre de base $(\overline{m_i})_{i\in I}$ où $m_i \in M$ (M est donc le module d'un groupe formel).

Définition 2.17. *Les m_i forment une V-base de M.*

Tout élément $m \in M$ s'écrit de façon unique $\sum_{n,i} V^n[c_{n,i}]m_i$. Pour connaître complètement la structure de $\mathbb{E}_p$ module de M il suffit de connaître les Fm_i car on connaît déjà les relations liant F, V et $[c]$.

$$\exists c_{n,i,j} \quad Fm_i = \sum_{n,j} V^n[c_{n,i,j}]m_j$$

Appelons ces équations les équations structurales de M. Les coefficients $(c_{n,i,j})_{n,i,j}$ définissent la structure de M à isomorphisme près.

On peut voire cela d'un point de vue de la présentation du module M, les équation structurales fournissant un suite semi-exacte :

$$\widehat{\mathbb{E}_p^{(I)}} \longrightarrow \widehat{\mathbb{E}_p^{(I)}} \longrightarrow M \longrightarrow 0$$

$$e_i \longmapsto Fe_i - \textstyle\sum_{n,j} V^n[c_{n,i,j}]e_j$$

$$e_i \longmapsto m_i$$

En fait cette suite est exacte comme le montre le lemme suivant :

Lemme 2.22. *Soient $\alpha_{n,i,j} \in W(R) \subset \mathbb{E}_p$ des éléments tels que à n, i fixés $\alpha_{n,i,j} = 0$ pour presque tout j. Considérons l'application*

$$\begin{array}{rcl} \varphi : \widehat{\mathbb{E}_p^{(I)}} & \longrightarrow & \widehat{\mathbb{E}_p^{(I)}} \\ e_i & \longmapsto & Fe_i - \displaystyle\sum_{n,j} V^n \alpha_{n,i,j} e_j \end{array}$$

Alors, le conoyau de φ est un module de Cartier V-réduit M.

L'image des e_i dans M forment une V-base de M et on a une suite exacte

$$0 \to \widehat{\mathbb{E}_p^{(I)}} \xrightarrow{\varphi} \widehat{\mathbb{E}_p^{(I)}} \to M \to 0$$

dem : D'après le lemme 2.21 pour montrer l'injectivité de φ il suffit de montrer l'injectivité de $\bar{\varphi} : \widehat{\mathbb{E}_p^{(I)}}/V\widehat{\mathbb{E}_p^{(I)}} \to \widehat{\mathbb{E}_p^{(I)}}/V\widehat{\mathbb{E}_p^{(I)}}$. Si $\alpha_{0,i,j} \equiv [a_{i,j}]$ mod V dans $W(R)$ (le premier terme du développement de $\alpha_{0,i,j}$ sous la forme $\sum V^n[a_n]F^n$). Alors,

$$\varphi(e_i) \equiv Fe_i - \sum_j [a_{i,j}]e_i \bmod V\widehat{\mathbb{E}_p^{(I)}}$$

Or les $(F^n e_i)_{n,i}$ forment une V-base de $\widehat{\mathbb{E}_p^{(I)}}$. D'où l'injectivité de $\bar{\varphi}$.

De plus,

$$M/VM = \bigoplus_{n,i} R.F^n e_i / \sum_{n,i} R.\bar{\varphi}(F^n e_i)$$

or

$$\begin{aligned}\bar{\varphi}(F^n e_i) &\equiv F^n\varphi(e_i)\\ &\equiv F^{n+1}e_i - \sum_{j,m} F^n V^m \alpha_{m,i,j} e_j\\ &\equiv F^{n+1}e_i - \sum_{j,m\leq n} [b_{i,j,m}] F^{n-m} e_j\end{aligned}$$

Donc

$$\bigoplus_{n,i} R.F^n e_i = \left(\bigoplus_i R.e_i\right) \oplus \left(\bigoplus_{n\geq 1} R.\bar{\varphi}(F^n e_i)\right)$$

ce qui prouve que l'image des e_i dans M est une V-base.

□

Corollaire 2.9. *La donnée d'un module V-réduit M tel que M/VM soit libre est équivalente à la donnée d'équations structurales données par des $c_{n,i,j} \in R$.*

De plus ces équations engendrent librement les relations définissant la structure de M.

Remarque 2.14. *En particulier tout module V-réduit tel que M/VM soit libre de type fini possède une résolution libre de longueur deux. Un tel $\mathbb{E}_p$ module n'est donc pas quelconque puisque sa dimension cohomologique est inférieure ou égale à 1.*

Exemple : Considérons le groupe des vecteurs de Witt tronqués W_n. Une V-base de W_n est constituée des applications $(m_i)_{0\leq i\leq n}$:

$$\begin{aligned} m_i : \widehat{W} &\to W_n\\ (x_0,\dots,x_k,\dots) &\mapsto (0,\dots,0,x_0,\dots,x_{n-i})\end{aligned}$$

qui correspond à la base des $(0,\dots,0,1,\dots,1)$ de R^{n+1}. $F.m_i = m_i \circ V = m_{i+1}$ (rappel :les rôles de F et V sont échangés)

Les équations structurelles sont donc :

$$\begin{cases} Fm_i = m_{i+1}\\ Fm_n = 0\end{cases}$$

2.15 Changement de base dans les modules V-réduits

Voici l'analogue du théorème 2.8

Théorème 2.12. $\forall M$ *V-réduit* $\forall N \in \mathbf{Nilp}_R$ $\forall i > 0$

$$Tor_i^{\mathbb{E}_p}(\widehat{W}(N), M) = 0$$

La démonstration est la même que celle du théorème 2.8.

Proposition 2.8. *Soit $R \to R'$ un morphisme d'anneaux et M un $\mathbb{E}_{p,R}$ module V-plat (ss.entendu V-réduit). Posons*

$$M' = \mathbb{E}_{p,R'} \widehat{\otimes}_{\mathbb{E}_{p,R}} M$$

le complété V-adique de $M' = \mathbb{E}_{p,R'} \otimes_{\mathbb{E}_{p,R}} M$. Alors, M' est V-réduit, V-plat et

$$\forall N \in \mathbf{Nilp}_{R'} \quad \widehat{W}(N) \otimes_{\mathbb{E}_{p,R}} M \simeq \widehat{W}(N) \otimes_{\mathbb{E}_{p,R'}} M'$$

où N est vu comme R algèbre nilpotente via $R \to R'$.

De plus, si une V-base de M est $(m_i)_i$ dont les coefficients structurels sont les $c_{n,i,j} \in W(R)$ alors, les $(1 \widehat{\otimes} m_i)_i$ forment une V-base de M' et les coefficients structurels associés sont les images des $c_{n,i,j}$ dans $W(R) \to W(R')$.

Si H est un groupe formel de module des courbes p-typiques M alors M' est le module des courbes p-typiques de $H_{R'} = H \times_{\boldsymbol{Spf}(R)} \boldsymbol{Spf}(R')$.

dem : Considérons le cas où M/VM est libre (pour plat .....). Choisissons une V-base $(m_i)_i$ et soit

$$0 \to \mathbb{E}_{p,R}^{(I)} \to \mathbb{E}_{p,R}^{(I)} \to M \to 0$$

la présentation associée. Appliquant $\mathbb{E}_{p,R'}^{(I)} \otimes_{\mathbb{E}_{p,R}^{(I)}} -$ à cette suite on obtient grâce au théorème 2.12 une suite exacte

$$0 \to \mathbb{E}_{p,R'} \otimes_{\mathbb{E}_{p,R}} \mathbb{E}_{p,R}^{(I)} \to \mathbb{E}_{p,R'} \otimes_{\mathbb{E}_{p,R}} \mathbb{E}_{p,R}^{(I)} \to \mathbb{E}_{p,R'} \otimes_{\mathbb{E}_{p,R}} M \to 0$$

qui en passant aux V-complétés donne une présentation de M'. D'où une partie des assertions.

De plus, on a une application naturelle

$$\widehat{W}(N) \otimes_{\mathbb{E}_{p,R}} M \simeq \widehat{W}(N) \otimes_{\mathbb{E}_{p,R'}} \left(\mathbb{E}_{p,R'} \otimes_{\mathbb{E}_{p,R}} M\right) \to \widehat{W}(N) \otimes_{\mathbb{E}_{p,R'}} \left(\mathbb{E}_{p,R'} \widehat{\otimes}_{\mathbb{E}_{p,R}} M\right)$$

Il est facile de définir un inverse en utilisant le fait que $\widehat{W}(N)$ est de torsion...

□

Remarque 2.15. *On déduit aisément de la preuve que si M possède une V-base finie (i.e. M est associé à un groupe formel formellement de type fini) alors la complétion est inutile i.e.*

$$\mathbb{E}_{p,R'} \widehat{\otimes}_{\mathbb{E}_{p,R}} M \simeq \mathbb{E}_{p,R'} \otimes_{\mathbb{E}_{p,R}} M$$

2.16 Application aux relèvements des groupes formels et de leurs morphismes

Proposition 2.9. *Soit $R \twoheadrightarrow R'$ une surjection d'anneaux et H' un groupe formel sur R'. Alors il existe H un groupe formel sur R tel que $H_{R'} = H'$ i.e. tout groupe formel sur R' se relève en un groupe formel sur R.*

dem : Il suffit de relever les équations structurelles du module de H' en relevant les coefficients $c'_{n,i,j} \in R'$ en des $c_{n,i,j} \in R$.

□

Théorème 2.13. *Soit I un idéal de R tel que $pI = I^p = 0$ et G_1, G_2 deux groupes formels (formellement de type fini) sur R. Notons $R' = R/I$.*

- *Pour tout morphisme $\varphi : G_{1/R'} \to G_{2/R'}$, $p\varphi$ se relève en un morphisme de G_1 dans G_2.*
- *Soient $\varphi_1, \varphi_2 : G_1 \to G_2$ tels que $\varphi_{1/R'} = \varphi_{2/R'}$. Alors $p\varphi_1 = p\varphi_2$.*

dem : Notons $\mathbb{E}_{p,I} = \epsilon_1 \Lambda(I[[Y]])\epsilon_1$ qui est un idéal de $\mathbb{E}_{p,R}$ (cela est clair sur la définition de Λ).

$$\mathbb{E}_{p,I} = \{\sum_{m,n} V^n[c_{n,m}]F^m \mid c_{n,m} \in I\}$$

On a alors une suite exacte de $\mathbb{E}_p$ modules.

$$0 \to \mathbb{E}_{p,I} \to \mathbb{E}_{p,R} \to \mathbb{E}_{p,R'} \to 0$$

(cela est clair sur l'écriture unique $\sum_{n,m} V^n[c_{n,m}]F^m$)

Soit M un $\mathbb{E}_p$ module V-réduit tel que M/VM soit libre de type fini. Si on choisit une présentation associée à une V-base de M :

$$0 \to \mathbb{E}_{p,R}^I \to \mathbb{E}_{p,R}^I \to M \to 0$$

(où I est fini) on obtient en tensorisant par $\mathbb{E}_{p,R'}$ une suite exacte

$$0 \to \mathbb{E}_{p,R'}^I \to \mathbb{E}_{p,R'}^I \to M_{R'} \to 0$$

(cf.proposition 2.8). Donc,

$$\mathrm{Tor}^1_{\mathbb{E}_{p,R}}(\mathbb{E}_{p,R'}, M) = 0$$

Revenons à notre suite exacte

$$0 \to \mathbb{E}_{p,I} \to \mathbb{E}_{p,R} \to \mathbb{E}_{p,R'} \to 0$$

Appliquons lui $- \otimes_{\mathbb{E}_{p,R}} M$. On obtient grâce à la nullité du groupe de torsion ci dessus une suite exacte

$$0 \to \mathbb{E}_{p,I} \otimes_{\mathbb{E}_{p,R}} M \to M \to M_{R'} \to 0$$

ce qui montre que le noyau de $M \to M_{R'}$ est exactement l'ensemble des $\sum_{n,i} V^n[c_{n,i}]m_i$ où $c_{n,i} \in I$ et m_i est une V-base de M.

Montrons que ce noyau est annulé par p. $p \in W(R) \subset \mathbb{E}_p$, il existe donc des $a_n \in R$ tels que

$$p = [p] + \sum_{n \geq 1} V^n[a_n]F^n$$

Donc si $m = \sum_{n,i} V^n[c_{n,i}]F^n \in \mathbb{E}_{p,I} \otimes M$,

$$[p]m = \sum_{n,i} V^n[\underbrace{p^{(p^n)}c_{n,i}}_{0}]m_i = 0 \text{ car } pI = 0$$

et

$$\begin{aligned}\sum_{n\geq 1} V^n[a_n]F^n.m &= \left(\sum_{n\geq 1} V^n[a_n]F^{n-1}\right).\left(\sum_{n\geq 1,i} \underbrace{(FV)}_{p} V^{n-1}[c_{n,i}]m_i + \sum_i \underbrace{F[c_{n,i}]}_{[c_{n,i}^p]F=0} m_i\right)\\ &= \left(\sum_{n\geq 1} V^n[a_n]F^{n-1}\right).\left(\sum_{n\geq 1,i} V^{n-1}\left(p[c_{n,i}]\right)m_i\right)\end{aligned}$$

(on a utilisé $I^p = 0$). Or,

$$p[c_{n,i}] = \underbrace{[pc_{n,i}]}_{0} + \sum_{k\geq 1} V^k[a_k] \underbrace{F^k[c_{n,i}]}_{[c_{n,i}^{(p^k)}]F=0} = 0$$

Donc $pm = 0$ et p annule le noyau de $M \to M_{R'}$.

En conséquence, si M_1 et M_2 désignent les modules des courbes p-typiques de G_1 et G_2, et si $\varphi : M_{1,R'} \to M_{2,R'}$ alors $p\varphi$ de relève en un morphisme de M_2 dans M_2.

Et si $\varphi_1, \varphi_2 : M_1 \to M_2$ sont tels que $\varphi_{1/R'} = \varphi_{2/R'}$ alors $p\varphi_1 = p\varphi_2$.

□

Remarque 2.16. *Faire le lien avec la rigidité des quasi-isogénies.*

2.17 Le théorème des "diviseurs élémentaires"

Voici l'analogue du théorème de la base adaptée pour les modules libres de type fini sur un anneau de valuation discrète.

Théorème 2.14. *Soit $R = k$ un corps parfait de caractéristique p et $M' \subset M$ une inclusion de $\mathbb{E}_p$ modules V-réduits telle que M/VM soit de dimension finie sur k. Il existe alors une V-base $(m_i)_{i\in I}$ de M, un sous ensemble $J \subset I$ et des entiers $n(j), j \in J$ tels que $(V^{n(j)}m_j)_{j\in J}$ soit une V-base de M'.*

dem : $\forall n \in \mathbb{N}$ $V^n : M/VM \xrightarrow{\sim} V^nM/V^{n+1}M$ est une bijection Fr^n linéaire de k espaces vectoriels. k étant parfait on a donc

$$\forall n \ \ \dim_k(Gr^nM) = \dim_k(M/VM) < +\infty$$

Notons $G_n = M' \cap V^nM/M' \cap V^{n+1}M \subset Gr^nM$ sous espace vectoriel.

Puisque M' est un sous $\mathbb{E}_p$ module, $\forall n$ $VG_n \subset G_{n+1}$. Choisissons pour tout n un supplémentaire U_{n+1} de VG_n dans G_{n+1} :

$$G_{n+1} = VG_n \oplus U_{n+1}$$

et posons $U_0 = G_0$. Alors,

$$\forall n \ \ G_n = \bigoplus_{0\leq i\leq n} V^iU_{n-i}$$

Parce que k est parfait, $\dim_k(V^iU_{n_i}) = \dim_k(U_{n_i})$. Étant donné que $\dim(G_n) \leq \dim(Gr^nM) = \dim(M/VM)$, pour n grand $U_n = 0$, ce qui implique que pour n grand $VM' \subset M' \cap V^nM$: la topologie V-adique sur M induit la topologie V-adique sur M'.

Choisissons pour tout $n \in \mathbb{N}$ une base $(\overline{m'_j})_{j\in J_n}$ de U_n où $m'_j \in M' \cap V^nM$. Choisissons également des $m_j \in M$ tels que $m'_j = V^nm_j$. Notons $J = \amalg_j J_n$ (ensemble fini) et pour $j \in J$, $n(j)$ tel que $j \in J_{n(j)}$.

Les $(m_j)_{j\in J}$ sont V-linéairement indépendants car si pour des $\lambda_j \in k$

$$\sum_j [\lambda_j]m_j \equiv 0 \ [VM]$$

Appliquant V^N à cette égalité pour N grand (tel que $U_N = 0$) on obtient

$$\sum_j \lambda_j^{p^{-N}} V^{N-n(j)}m'_j = 0 \in V^NM/V^{N+1}M$$

ce qui grâce à la décomposition en sommes directes $\bigoplus_{0\leq i\leq n} V^iU_{n-i}$ implique que $\forall j$ $\lambda_j = 0$. D'où la V-indépendance linéaire.

De plus, le fait que pour $n >> 0$ $U_n = 0$ ajouté à la décomposition en sommes directes citée ci dessus implique que les $V^{n(j)}m_j = m'_j$ forment une V-base de M'.

Il suffit maintenant de compléter les $(m_j)_j$ V-linéairement indépendants en une base de M/VM pour conclure.

□

Remarque 2.17. *Soit G un groupe formel de module M et $(m_i)_{i\in I}$ une V-base de M. $m_i \in M = G(R[[Y]])$ donc $m_i : \boldsymbol{Spf}(R[[Y]]) \to G$.*

Le morphisme de G-foncteurs formels d'ensembles :

$$\begin{aligned}\bigoplus_{i\in I} \boldsymbol{Spf}(R[[Y]]) &\to G\\ (x_i)_i &\mapsto \sum_i m_i(x_i)\end{aligned}$$

Donne un isomorphisme de G-foncteur formel d'ensembles

$$\boldsymbol{Spf}(R[[\underline{Y}]]) \xrightarrow{\sim} G$$

puisque c'est un isomorphisme sur l'espace tangent.

Corollaire 2.10. *Soient G_1, G_2 deux groupes formels sur k corps parfait et $f : G_1 \to G_2$. Il existe des coordonnées X_i, Y_j i.e. des isomorphismes $G_1 \simeq \boldsymbol{Spf}(k[[\underline{X}]])$ $G_2 \simeq \boldsymbol{Spf}(k[[\underline{Y}]])$ telles que pour un r,*

$$\begin{cases}\forall i \le r\ f^*Y_i = X_i^{p^{\alpha(i)}} \text{ où } \alpha(i) \in \mathbb{N}\\ \forall i > r\ f^*Y_i = 0\end{cases}$$

dem : Supposons pour commencer que $f_* : M_{G_1} \hookrightarrow M_{G_2}$ soit une inclusion. Soit alors $(m_i)_{i\in I}, J \subset I$ et $n(j) \in \mathbb{N}$ comme dans le théorème 2.14. D'après la remarque précédente, les m_i définissent un isomorphisme

$$\boldsymbol{Spf}(k[[\underline{Y}]]) \xrightarrow{\alpha} G_2$$

Notons p_i la fonction i-ème coordonnée,

$$\begin{aligned}p_i : G_2 \xrightarrow{\alpha^{-1}} \boldsymbol{Spf}(k[[\underline{Y}]]) &\to \boldsymbol{Spf}(k[[T]])\\ y &\mapsto y_i\end{aligned}$$

Par définition de α , $\sum_i m_i p_i = Id_{G_2}$: on a une décomposition sur les coordonnées.

De la même façon, pour $j \in J$ notons $m'_j = V^{n(j)} m_j$ qui définissent un isomorphisme

$$\boldsymbol{Spf}(k[[\underline{X}]]) \xrightarrow{\beta} G_1$$

tel que si $q_j : G_1 \to \boldsymbol{Spf}(k[[T]])$ est la fonction j-ème coordonnée alors $\sum_j m'_j q_j = Id_{G_1}$.

Soit $g : G_1 \to G_2$ le morphisme défini sur les coordonnées par :

$$g^*Y_i = \begin{cases}0 \text{ si } i \notin J\\ X_i^{p^{n(i)}} \text{ si } i \in J\end{cases}$$

$g = (\sum_i m_i p_i) \circ g = \sum_i m_i p_i g$ est la décomposition de g sur les coordonnées. f étant un morphisme de groupes, $f = f(\sum_j m'_j q_j) = \sum_j f m'_j q_j$. Montrons que

$$m_i p_i g = \begin{cases}0 \text{ si } i \notin J\\ f m'_i q_i \text{ sinon}\end{cases}$$

i.e. les deux sont égaux coordonnées à coordonnées.

$$(m_i p_i g)^* Y_k = \begin{cases} 0 \text{ si } k \neq i \\ 0 \text{ si } i \notin j \\ X_i^{p^{n_i}} \text{ sinon} \end{cases}$$

$\forall j \in J\ f m'_j = f_* m'_j = V^{n(j)} m_j$ donc

$$\begin{aligned} (f m'_j q_j)^* Y_k &= (V^{n(j)} m_j q_j)^* Y_k \\ &= q_j^* (V^{n(j)} m_j)^* Y_j \\ &= q_j^* (m_j^* Y_k^{p^{n(j)}}) \text{ (par definition de V)} \\ &= \begin{cases} 0 \text{ si } k \neq j \\ X_j^{p^{n(j)}} \text{ sinon} \end{cases} \end{aligned}$$

Donc $g = \sum_i m_i p_i g = \sum_j f m'_j q_j = f$. D'où le résultat si $f_* : M_{G_1} \to M_{G_2}$ est injectif.

Dans le cas général on factorise f_* en une composée d'un surjection et d'une injection.

□

2.18 Applications aux groupes plats finis

Si A est une R algèbre augmentée plate telle que A^+ soit nilpotent , notons $\widehat{\mathbb{G}}_{m,A}$ le G-foncteur formel défini par

$$\forall N \in \mathbf{Nilp}_R \ \ \widehat{\mathbb{G}}_{m,A}(N) = (1 + A^+ \otimes_R N)^\times$$

Si A est un module projectif fini alors $\widehat{\mathbb{G}}_{m,A}$ est un groupe formel

$$\widehat{\mathbb{G}}_{m,A} \simeq \boldsymbol{Spf}(\widehat{\mathrm{Sym}}_R(A^{+*}))$$

Proposition 2.10. *Si $H = \boldsymbol{Spec}(A)$ est un groupe plat fini connexe sur R, il y a une suite exacte*

$$0 \longrightarrow G \xrightarrow{u} \widehat{\mathbb{G}}_{m,A^*} \xrightarrow{v} \widehat{\mathbb{G}}_{m,A^*\otimes A^*}$$

où A^* est l'algèbre duale de Cartier.

dem : Notons $\mu : A \otimes A \to A$, $\eta : R \to A$ les applications définissant la structure de R algèbre de A, et $\Delta : A \to A \otimes A$, $\iota : A \to A$, $\epsilon : A \to R$ celles définissant la structure d'algèbre de Hopf.

$(A^*)^+ = (A^+)^*$ est facile à voir.

Si $N \in \mathbf{Nilp}_R$ $G(N) = \mathcal{H}\mathrm{om}_{R-alg}(A^+, N) \subset A^{+*} \otimes N = \mathcal{H}\mathrm{om}_{R-mod}(A^+, N)$. Soit donc $\lambda \in G(N)$, posons $u(\lambda) = 1 + \lambda \in \mathbb{G}_{m,A^*}(N)$ via les identifications et inclusions ci dessus.

$\forall \lambda_1, \lambda_2 \in G(R)$ $\lambda_1.\lambda_2 = \lambda_1 + \lambda_2 + \lambda_1 \otimes \lambda_2 \circ \Delta'$ où

$$\begin{array}{rcl} \Delta_{|A^+} : A^+ & \to & (A^+ \otimes_R R) \oplus (R \otimes_R A^+) \oplus (A^+ \otimes_R A^+) \\ x & \mapsto & x \otimes 1 + 1 \otimes x + \Delta'(x) \end{array}$$

Δ' définit donc le produit sur l'anneau $(A^+)^*$.

Et $(\lambda_1 \otimes \lambda_2) \circ \Delta_{|A^+} = \lambda_1 + \lambda_2 + \lambda_1.\lambda_2 \Rightarrow u(\lambda_1.\lambda_2) = (1 + \lambda_1)(1 + \lambda_2)$. Donc u est un morphisme de groupe.

Si maintenant $1 + \lambda \in 1 + A^{*+}$, à quelles conditions a-t-on $\lambda \in \mathcal{H}\mathrm{om}_{R-alg}(A, N)$? Il faut et il suffit que $\lambda \circ \mu_{|A^+\otimes A^+} = \lambda \otimes \lambda \in \mathcal{H}\mathrm{om}(A^+ \otimes A^+, N) = (A^* \otimes A^*)^+ \otimes N$ Posons alors $v(1 + \lambda) = (1 + \lambda \circ \mu_{|A^+\otimes A^+})(1 + \lambda \otimes \lambda)^{-1} \in \widehat{\mathbb{G}}_{m,A^*\otimes A^*}(N)$. On vérifie que v est un morphisme de groupes.

□

Corollaire 2.11. *Tout groupe plat fini connexe est le noyau d'un morphisme de groupes formels*

Corollaire 2.12. *Pour tout groupe plat fini connexe $G = \boldsymbol{Spec}(A)$ sur un corps parfait de caractéristique p il existe un isomorphisme*

$$A \simeq k[X_1, \ldots, X_n]/(X_1^{p^{\alpha_1}}, \ldots, X_n^{p^{\alpha_n}})$$

Cela résulte du corollaire précédent et du corollaire 2.10.

2.19 Isogénies et module de Cartier

Dans toute cette partie on suppose R de caractéristique p.

2.19.1 Frobenius et module de Cartier

Rappelons que si $H : \mathbf{Nilp}_R \to \mathbf{Ab}$, $H^{(p^m)}$ est le foncteur défini par

$$\forall N \in \mathbf{Nilp}_R \; H^{(p^m)}(N) = H(N^{(p^m)})$$

où $N^{(p^m)}$ est la R algèbre telle que R opère via $R \xrightarrow{\mathrm{Fr}^m} R$ où Fr est le Frobenius.

$\forall N \in \mathbf{Nilp}_R$ l'application de R-algèbre

$$\begin{array}{ccc} N & \to & N^{(p^m)} \\ n & \mapsto & n^{p^m} \end{array}$$

induit un morphisme de Frobenius $\mathrm{Fr}^m : H \to H^{(p^m)}$.

$G \mapsto G^{(p^m)}$ est naturel au sens où $\forall \alpha : G \to H$ on a un diagramme commutatif

$$\begin{array}{ccc} G & \xrightarrow{\alpha} & H \\ \downarrow{\scriptstyle \mathrm{Fr}^m} & & \downarrow{\scriptstyle \mathrm{Fr}^m} \\ G^{(p^m)} & \xrightarrow{\alpha^{(p^m)}} & H^{(p^m)} \end{array}$$

On rappelle également (cf. ? ? ?) que si G est un groupe formel alors $\mathrm{Fr}^m : G \to G^{(p^m)}$ est une isogénie.

Lemme 2.23. *$\widehat{W} \xrightarrow{\sim} \widehat{W}^{(p^m)}$ et $Fr^m : \widehat{W} \to \widehat{W}$ est donné par la multiplication à droite par V^m.*

dem : En effet, $\widehat{W}$ est "sans équation" et $1+\sum_i n_i t^i \mapsto 1+\sum_i n_i t^i$ donne l'isomorphisme. Le fait que Fr^m soit donné par la multiplication à droite par V^m vient du lemme 2.18. □

Par fonctorialité de $R \to \mathbb{E}_R$, le morphisme d'anneau $\mathrm{Fr} : R \to R$ induit un morphisme

$$\begin{array}{ccc} \mathbb{E}_p & \to & \mathbb{E}_p \\ x & \mapsto & x^{f^m} \end{array}$$

vérifiant

$$\left(\sum_{n,m} V^n [c_{n,m}] F^m)\right)^f = \sum_{n,m} V^n [c_{n,m}^{p^m}] F^m$$

On en déduit aussitôt :

Lemme 2.24.

$$\forall x \in \mathbb{E}_p \quad xV = Vx^f \;\; et \;\; Fx = x^f F$$

Soit maintenant G un groupe formel. D'après la proposition 2.8

$$M_{G^{(p^m)}} \simeq \mathbb{E}_p \otimes_{f^m,\mathbb{E}_p} M_G \quad \text{(i.e. } x \otimes \lambda m = x\lambda^{f^m} \otimes m)$$

Lemme 2.25.

$$\begin{array}{rcl} Fr^m_{G*} : M_G & \to & M_{G^{(p^m)}} \simeq \mathbb{E}_p \otimes_{f,\mathbb{E}_p} M_G \\ x & \mapsto & V^m \otimes x \end{array}$$

(Cette application est bien $\mathbb{E}_p$ linéaire grâce au lemme précédent)
dem : $G \simeq \widehat{W}(-) \otimes_{\mathbb{E}_p} M_G$ et $\mathrm{Fr}^m : \widehat{W}(-) \to \widehat{W}$ est l'application $\lambda \mapsto \lambda V^m$ donc

$$\begin{array}{rcl} \mathrm{Fr}^m : \widehat{W}(-) \otimes_{\mathbb{E}_p} M_G & \to & \widehat{W}(-) \otimes_{f^m,\mathbb{E}_p} M_G \\ \lambda \otimes x & \mapsto & \lambda V^m \otimes x \end{array}$$

d'où le résultat.

□

Nous noterons $\mathrm{Fr}^m : M_{G^{(p^m)}} \to M_G$.

2.19.2 Verschiebung

Considérons l'application $\mathbb{E}_p$ linéaire

$$\begin{array}{rcl} \mathrm{Ver} : \mathbb{E}_p \otimes_{f^m,\mathbb{E}_p} M & \to & M \\ \lambda \otimes x & \mapsto & \lambda^{f^m} x \end{array}$$

On a :

$$\mathrm{VerFr} = \mathrm{FrVer} = p$$

Si $M = M_G$ pour un groupe formel G elle induit un morphisme $\mathrm{Ver} : G^{(p^m)} \to G$ dont on vérifie aisément qu'il s'agit du Verschiebung.

2.19.3 Le module V-divisé

Le module V-divisé associé à un module V-réduit est l'analogue pour le Frobenius remplaçant p de l'isocristal associé à un cristal. Les isomorphismes entre modules V-divisés correspondent aux quasi-isogénies (au sens où f est une quasi-isogénie si pour N grand $V^N f$ est une isogénie) entre groupes formels et donc deux groupes formels sont isogènes ssi leurs modules V-divisés sont isomorphes.

Définition 2.18. *Si M est un module V-réduit on notera*

$$\widetilde{M} = \varinjlim_m \mathbb{E}_p \otimes_{f^m,\mathbb{E}_p} M$$

Ainsi, si $M = M_G$, $\widetilde{M}_G = \varinjlim_m M_{G^{(p^m)}}$

On remarque que si R est réduit les morphismes de transition sont injectifs et donc $\widetilde{M_G} = \bigcup_m M_{G^{(p^m)}}$.

Considérons l'application $\mathbb{E}_p$ linéaire

$$\begin{aligned} \alpha : \mathbb{E}_p \otimes_{f^m,\mathbb{E}_p} M &\to \mathbb{E}_p \otimes_{f^{m+1},\mathbb{E}_p} M \\ \lambda \otimes x &\to \lambda^f \otimes x \end{aligned}$$

On a

$$\alpha(V.(\lambda \otimes x)) = \alpha(V\lambda \otimes x) = (V\lambda)^f \otimes x = \lambda V \otimes X$$

or dans la limite inductive $\lambda V \otimes x = \lambda \otimes x$. Il est donc naturel d'appeler V^{-1} l'application $\mathbb{E}_p$ linéaire induite par α sur le module V-divisé.

On notera les propriétés suivantes :

$$\begin{aligned} V^{-1}x &= x^f V^{-1} \\ V^{-1}V &= VV^{-1} = Id \end{aligned}$$

Le module V-divisé associé à $\mathbb{E}_p$, $\widetilde{\mathbb{E}}_p$ est un anneau qui peut être identifié au localisé de $\mathbb{E}_p$ par la partie multiplicative des $(V^n)_{n\geq 0}$:

$$\widetilde{\mathbb{E}}_p = \{xV^{-n}\}/\sim$$

où $xV^{-a} \sim yV^{-b}$ si $\exists N \in \mathbb{N}\ xV^{N-a} = yV^{N-b}$.

L'application $V^{-1} : \widetilde{\mathbb{E}}_p \to \widetilde{\mathbb{E}}_p$ est $x \mapsto x^f V^{-1}$.

Lemme 2.26. *Si M/VM est libre de type fini*

$$\widetilde{M} \simeq \widetilde{\mathbb{E}}_p \otimes_{\mathbb{E}_p} M$$

Cela se vérifie en prenant une V-base de M et ne utilisant la proposition 2.8.

2.19.4 Critère d'isogénie

Théorème 2.15. *Soit $\varphi : G_1 \to G_2$ un morphisme de groupes formels de même dimension sur un anneau de caractéristique p. Sont alors équivalents :*

1. *φ est une isogénie*
2. *Il existe un morphisme $\psi : G_2 \to G_1^{(p^m)}$ tel que $\psi \circ \varphi = Fr_{G_1}^m$*
3. *φ induit un isomorphisme des modules de Cartier V-divisés de G_1 et G_2*

dem : (1) $\Rightarrow$ (2) : Le noyau de φ est un groupe plat fini connexe de la forme $\boldsymbol{Spec}(R \oplus N)$ où $N \in \mathbf{Nilp}_R$. N étant nilpotent on en déduit qu'il est annulé par une puissance suffisamment grande du Frobenius. Donc, $\exists m$ $\ker(\varphi) \subset \ker(\mathrm{Fr}^m)$. φ étant une isogénie elle induit un isomorphisme $\alpha : G_1/\ker(\varphi) \xrightarrow{\sim} G_2$. Si l'on note

$$\psi : G_2 \xrightarrow{\alpha^{-1}} G_1/\ker(\varphi) \twoheadrightarrow G_2/\ker(\mathrm{Fr}^m) \xrightarrow{\mathrm{Fr}^m} G_2^{(p^m)}$$

Alors ψ convient.

(2) $\Rightarrow$ (1) : Fr est une isogénie (cf. ? ? ?), donc G_1 et G_2 étant des groupes formels de même dimension φ etψ sont des isogénies (cf ? ? ?).

(2) $\Rightarrow$ (3) : $\psi \circ \varphi = \mathrm{Fr}^m \Rightarrow \psi_* \circ \varphi_* = Id : \widetilde{M}_{G_1} \to \widetilde{M}_{G_1}$. Donc φ est injective. Mais on a vu lors de la démonstration de (2) $\Rightarrow$ (1) que (2) $\Rightarrow \psi$ est une isogénie donc en appliquant (1) $\Rightarrow$ (2) à ψ à la place de φ et le raisonnement précédent on en déduit que ψ_* est également injective. Donc φ_* est un isomorphisme des modules V-divisés.

(3) $\Rightarrow$ (1) résulte du théorème suivant :

Théorème 2.16. *Soient G_1, G_2 deux groupes formels et $\alpha : \widetilde{M}_1 \to \widetilde{M}_2$ un isomorphisme de leurs modules V-divisés. Il existe alors une isogénie $\varphi : G_1 \to G_2^{(p^m)}$ pour un $m \in \mathbb{N}$ qui induit α et une isogénie $\psi : G_2^{(p^m)} \to G_1^{(p^r)}$ telle que $\psi \circ \varphi = Fr^r_{G_1}$. De plus, tout morphisme $\varphi : G_1 \to G_2$ induisant α est une isogénie.*

dem : Soit $(m_i)_{1 \leq i \leq s}$ une V-base de M_1. Les images $\alpha(m_i)_{1 \leq i \leq s} \in \widetilde{M}_2$ étant en nombre fini sont dans l'image de $M_2^{(p^m)} \to \widetilde{M}_2$ pour m suffisamment grand. Soient donc $(n_i)_i \in M_2^{(p^m)}$ tels que les n_i s'envoient sur les $\alpha(m_i)$.

Montrons que quitte à choisir un $m' \geq m$, $m_i \mapsto n_i$ définit un morphisme de $\mathbb{E}_p$ module. Considérons pour cela les équations structurelles de M_1 :

$$F.m_i = \sum_{n,j} V^n[c_{n,i,j}]m_j$$

Pour montrer que $m_i \mapsto n_i$ définit un morphisme il suffit de montrer que les n_i satisfont aux mêmes équations (cf. ? ? ?) Or dans le module V-divisé ces équations sont satisfaite i.e. la différence entre les deux termes de l'égalité ci dessus est nulle . Étant donné qu'il n'y a qu'un nombre fini d'équations structurelles on peut choisir un $m' \geq m$ tel que tout ces différences soient nulles dans $M_2^{(p^m)}$ i.e. tel que les équations soient satisfaites.

D'où l'existence de φ induisant α.

On remarque de même en utilisant la finitude d'une V-base que si deux morphismes $f_1, f_2 : N_1 \to N_2$, entre des modules V-réduits N_1, N_2 tels que N_1/V_1 soit libre de type fini, vérifient $\widetilde{f_1} = \widetilde{f_2} : \widetilde{M_1} \to \widetilde{M_2}$, alors pour n grand $f_1 = f_2 : M_1 \to M_2^{(p^n)}$.

Considérons alors l'application composée $M_2^{(p^m)} \to \widetilde{M}_2 \xrightarrow{\alpha^{-1}} \widetilde{M}_1$. D'après ce qui a été fait précédemment cette application est induite par un morphisme $\psi : G_2^{(p^m)} \to G_1^{(p^k)}$ pour un $k \in \mathbb{N}$. On a alors $\psi_* \circ \varphi_* = Id : M_1 \to \widetilde{M}_1$ et donc par la remarque précédente pour un r suffisamment grand $\psi \circ \varphi_* : M_1 \to M_1^{(p^r)}$ est Fr^r.

D'où l'existence de ψ vérifiant la propriété voulue.

L'existence d'un tel ψ implique que φ et ψ soient des isogénies (cf. la démonstration de (2) $\Rightarrow$ (1) dans le théorème précédent).

La dernière assertion est claire.

□

2.20 Le cas d'un corps parfait

Dans toute cette section $R = k$ est un corps parfait de caractéristique p.

Remarque 2.18. *Si $\varphi : M_1 \to M_2$ est un morphisme de modules V-réduits alors $im(\varphi)$ est fermé i.e. est un module V-réduit (cela est vrai pour tout R)*

Théorème 2.17. *Un morphisme $\varphi : G_1 \to G_2$ entre groupes formels de même dimension est une isogénie ssi $\varphi_* : M_{G_1} \to M_{G_2}$ est injectif.*

dem : k étant un corps les applications de transition définissant les modules V-divisés sont injectives :

$$\widetilde{M} = \bigcup_m M^{(p^m)}$$

Soit donc φ une isogénie. D'après le théorème 2.15, $\varphi_* : \widetilde{M}_{G_1} \to \widetilde{M}_{G_2}$ est un isomorphisme, donc en restriction à M_{G_1} φ_* est injective.

Supposons réciproquement que $\varphi_* : M_{G_1} \to M_{G_2}$ soit injective. Alors, $\varphi_* : \widetilde{M}_{G_1} \to \widetilde{M}_{G_2}$ est injective. D'après le théorème des diviseurs élémentaires (th.2.14) il existe une V-base $(m_i)_{i\in I}$ de M_{G_1}, un ensemble $J \subset I$ et des $(n(j))_{j\in J}$ tels que $m'_j = V^{n(j)} m_j$ soit une V-base de M_{G_2}. Mais G_1 et G_2 ont même dimension, donc $J = I$!. Donc dans $\widetilde{M}_{G_2}$, $m_i = \varphi_*(V^{-n(i)} m'_i)$ d'où la surjectivité de $\varphi_* : \widetilde{M}_{G_1} \to \widetilde{M}_{G_2}$.

□

On remarque que l'on a démontré en même temps que M_{G_2}/M_{G_1} était de V-torsion. D'où :

Corollaire 2.13. *Si $\varphi : G_1 \to G_2$ est une isogénie alors M_{G_1}/M_{G_2} est annulé par une puissance de V.*

2.21 Classification des groupes formels p-divisibles sur un corps parfait

Le théorème 2.17 implique le corollaire suivant

Corollaire 2.14. *Si G est un groupe formel, G est un groupe formel p-divisible ssi M_G est sans p-torsion ssi M_G est sans F-torsion.*

Théorème 2.18. *Le foncteur $M \longmapsto M_G$ induit une équivalence de catégories entre la catégorie des groupes formels p-divisibles sur k et la catégorie des $k - \sigma^{-1}$ cristaux (M, V) tels que $pM \subset VM$ et V soit topologiquement nilpotent.*

dem : Soit G un groupe formel p-divisible et $M = M_G$. p étant une isogénie d'après le corollaire 2.13 M/pM est annulé par une puissance de V, M/VM étant de dimension finie (et k parfait impliquant M/V^nM est également de dimension finie...) M/pM est un $W(k)/pW(k) = k$-ev. de dimension finie. M est V-complet et $VF = p$, donc M est p-complet. D'après le lemme de Nakayama pour les modules complets sur un anneau complet on en déduit que M est un $W(k)$ module de type fini. Mais d'après le corollaire précédent M est sans p-torsion, donc M est un $W(k)$ module libre de type fini!! Il est muni de l'opérateur $V \in \mathbb{E}_p$ qui est σ^{-1} linéaire injectif. L'équation $p = VF$ montre alors que (M, V) est un cristal.

Réciproquement, soit (M, V) un σ^{-1} cristal tel que V soit topologiquement nilpotent et tel que $pM \subset VM$. $pM \subset VM \Leftrightarrow$ l'existence de $F : M \to M$ σ linéaire tel que $FV = p$. V étant topologiquement nilpotent, M est V-complet. On peut donc définir une action de $\mathbb{E}_p = \{\sum_{n,m} V^m[a_{n,m}]F^n\}$ sur M de façon tautologique. Etant donné que $F, V, [c] \in \mathbb{E}_p$ vérifient les mêmes équations de commutation que les opérateurs F, V sur M il est clair que cela munit M d'une structure de $\mathbb{E}_p$ module. Celui-ci est V-réduit car l'hypothèse d'injectivité de V fait partie de la définition d'un cristal.

Il est également clair que la correspondance construite fait se correspondre morphismes de $\mathbb{E}_p$ modules et morphismes de cristaux.

□

Remarque 2.19. *Un cristal (M, V) vérifie que V est nilpotent ssi les pentes de l'isocristal associé sont strictement positives. La partie de pente nulle correspond à la partie étale...La classification des groupes p-divisibles non forcément formels se déduit donc aisément du théorème précédent.*

Remarque 2.20. *Il résulte du corollaire 2.10 que la hauteur de G est égale à la dimension de M_G/pM_G. En résumé :*

$$ht(G) = \dim M_G/pM_G$$
$$\dim(G) = \dim M_G/VM_G$$

Proposition 2.11. *Le module V-divisé de M est isomorphe à l'isocristal associé à M_G comme $W(k)_{\mathbb{Q}}[F, V]$ module.*

dem : $pM \subset VM \subset M$ et pour N grand $V^N M \subset pM \subset M$. Le V-localisé coïncide donc avec le p-localisé puisque p et V sont sans torsion. □

Corollaire 2.15. *Les isocristaux classifient les groupes p-divisibles sur k à isogénie près. Si G_1, G_2 sont deux groupes p-divisibles, les isomorphismes entre $\widetilde{M}_{G_1}$ et $\widetilde{M}_{G_2}$ correspondent aux quasi-isogénies entre G_1 et G_2.*

2.22 Classification des groupes plats finis connexes sur un corps parfait

$R = k$ est un corps parfait de caractéristique p.

Proposition 2.12. *Tout groupe plat fini sur k est le noyau d'une isogénie de groupes formels.*

dem : Cela résulte du corollaire 2.10 du théorème 2.14 et du théorème 2.17. □

Soit donc G plat fini et soit $\varphi : G_1 \to G_2$ une isogénie de groupes formels telle que $\ker \varphi = G$. Notons M le conoyau de $\varphi_* : M_{G_1} \to M_{G_2}$. On a donc une suite exacte :

$$0 \to M_{G_1} \to M_{G_2} \to M \to 0$$

Pour retrouver $G(N)$ pour un $N \in \mathbf{Nilp}_R$ on procède de la façon suivante :

$$\forall N \in \mathbf{Nilp}_R \quad G(N) = \ker(G_1(N) \xrightarrow{\varphi_N} G_2(N))$$

Appliquons $\widehat{W}(N) \otimes_{\mathbb{E}_p} -$ à la suite exacte ci dessus. On obtient grâce au théorème 2.12 :

$$G(N) \simeq \mathrm{Tor}_1^{\mathbb{E}_p}(\widehat{W}(N), M)$$

De plus $\Lambda(N)$ est un module annulé par une puissance de V i.e. est un module de longueur finie. On montre alors sans problèmes :

Théorème 2.19. *Il y une équivalence de catégories entre la catégorie des groupes plats finis connexes sur k et la catégorie des $W(k)$ modules M de longueur finie munis d'un opérateur V σ^{-1} linéaire tel que $pM \subset VM$ et tels que V soit nilpotent.*

Dans cette correspondance, le noyau d'une isogénie de groupes formels $\varphi : G_1 \to G_2$ est associé à M_{G_2}/M_{G_1}.

On a $ht(G) = \dim(M/pM)$.

Définition 2.19. *M est appelé le module de Dieudonné covariant de G.*

On déduit par exemple aussitôt de tout cela que tout groupe plat fini connexe sur k est annulé par son ordre. En effet, il est clair que M est annulé par l'ordre de G. Or la multiplication par cet ordre sur $G(N) = \mathrm{Tor}_1(\widehat{W}(N), M)$ est induite par la multiplication par cet ordre sur M. (donc G est même annulé par p^α où $\alpha = sup\{\alpha_i\}$ (cf.2.12)).

3 Isocristaux

3.1 Définitions

Soit k un corps parfait de caractéristique p, $W = W(k)$, $K = \mathrm{Frac}(W)$. Notons $\sigma : K \to K$ le Frobenius.

Définition 3.1. *Un isocristal sur K de hauteur h est un couple (N, φ) où N est un K-e.v. de dimension h muni d'une application σ-linéaire $\varphi : N \to N$ bijective.*

Les isocristaux forment une catégorie. Si (N_1, φ_1) et (N_2, φ_2) sont deux isocristaux $\mathcal{H}\mathrm{om}((N_1, \varphi_1), (N_2, \varphi_2))$ est l'ensemble des applications K-linéaires $u : N_1 \to N_2$ vérifiant $u \circ \varphi_1 = \varphi_2 \circ u$. On notera $\boldsymbol{Isoc}_k$ la catégorie des isocristaux sur K. C'est une catégorie abelienne $\mathbb{Q}_p$ linéaire (mais non K-linéaire) au sens où les $\mathcal{H}\mathrm{om}$ sont des $\mathbb{Q}_p$-espaces vectoriels et la composition est $\mathbb{Q}_p$ bilinéaire.

De plus $\boldsymbol{Isoc}_k$ possède des $\mathcal{H}\mathrm{om}$ internes au sens où $\mathcal{H}\mathrm{om}_K(N_1, N_2)$ le K-e.v. des applications K linéaires entre N_1 et N_2 est un isocristal sur K si on le muni de l'opérateur $\varphi : u \mapsto \varphi_2 \circ u \circ \varphi_1^{-1}$. Dès lors,

$$\mathcal{H}\mathrm{om}_{\boldsymbol{Isoc}_k}((N_1, \varphi_1), (N_2, \varphi_2)) = (\mathcal{H}\mathrm{om}_K((N_1, \varphi_1), (N_2, \varphi_2)))^{\varphi}$$

Elle possède également des produits tensoriels

$$(N_1, \varphi_1) \otimes (N_2, \varphi_2) = (N_1 \otimes N_2, \varphi_1 \otimes \varphi_2)$$

Il s'agit d'une catégorie Tannakienne $\mathbb{Q}_p$-linéaire non neutre. Un foncteur fibre sur K est $(N, \varphi) \mapsto N$. Nous décrirons plus tard son lien et la gerbe associée lorsque $k = \overline{\mathbb{F}_p}$.

Si $(e_i)_i$ est une base de N, on peut définir la matrice de φ associée dans cette base. Les formules de changement de base pour la matrice de φ sont de la forme

$$A \mapsto \Lambda^{\sigma} A \Lambda^{-1}$$

La classification des isocristaux est donc équivalente à celle des classes de conjugaison tordues (par σ) dans $\mathbf{GL}_n(K)$. Nous verrons plus tard que lorsque k est algébriquement clos cette classification est plus simple que celle des classes de conjugaisons elle même (il n'y a pas de classes "unipotentes" au ses où elles sont toutes semi-simples).

Une autre formulation de la définition d'un isocristal est que φ soit un isomorphisme entre N est $N^{\sigma} = N \otimes_K K$ le K-e.v. tordu par σ.

Si $\mathcal{E}_k = K[F]$ où $F\lambda = \lambda^s F$, un isocristal sur K est la même chose qu'un $\mathcal{E}_k$-module non dégénéré de dimension finie sur K. Le centre de $\mathcal{E}_K$ est $\mathbb{Q}_p$.

On définit également une notion de cristal :

Définition 3.2. *Un cristal est un couple (N, φ) où N est un W module libre de rang fini et où $\varphi : N \to N$ est une application σ linéaire injective*

Comme pour les isocristaux les cristaux forment une catégorie $\mathbb{Z}_p$-linéaire.

Si (N, φ) est un cristal, $(K \otimes_W N, \sigma \otimes \varphi)$ est un isocristal. Et donc, les cristaux sont exactement les réseaux φ-stables des isocristaux.

Définition 3.3. *Un morphisme $u : (N_1, \varphi_1) \to (N_2, \varphi_2)$ de cristaux est une isogénie si $1 \otimes u : K \otimes_W N_1 \to K \otimes_W N_2$ est un isomorhisme. Deux cristaux sont dits isogènes s'il existe une isogénie entre eux. Cela est équivalent à ce que leurs isocristaux associés soient isomorphes (en particulier c'est une relation d'équivalence).*

On peut également formuler la définition d'une isogénie en disant que u est injectif et N_1 et N_2 sont de même hauteur. Ou bien encore en disant que u est injectif et $u(N_1)$ est un réseau de N_2. Le fait qu'un isomorphisme des isocristaux associés donne une isogénie est clair : si $u : K \otimes N_1 \xrightarrow{\sim} K \otimes N_2$, $p^m.u_{|N_1}$ est une isogénie pour $m \in \mathbb{N}$ grand.

Les isocristaux classifient donc les cristaux à isogénie près.

3.2 Exemples

Soit $\lambda = \dfrac{r}{s} \in \mathbb{Q}, s \wedge r = 1, s, r \geq 0$. Posons

$$\boxed{N^\lambda = K[F]/(F^r - p^s)}$$

sur lequel F opère σ linéairement i.e. une base de N^λ est $(1, F, \ldots, F^{r-1})$ et la matrice de F dans cette base est

$$\begin{pmatrix} 0 & 0 & \ldots & 0 & p^s \\ 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & & & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 0 \end{pmatrix}$$

Posons pour $\lambda \leq 0, N^\lambda = \mathcal{H}\mathrm{om}(N^{-\lambda}, K)$ le dual de N.

Les objets N^λ sont des examples fondamentaux puisque l'on montrera que si k est algébriquement clos, $\boldsymbol{Isoc}_k$ est semi-simple d'objets simples les N^λ.

On remarque que les N^λ sont définis à partir de cristaux "canoniques" puisque

$$N^\lambda = K \otimes_W W[F]/(F^r - p^s)$$

Plus précisément, si V est l'opérateur σ^{-1}-linéaire défini par $FV = VF = p$ alors une base de ce cristal est

$$1, F, \ldots, F^{s-r-1}, V, \ldots, V^r$$

et l'on remarque que si $0 \leq \lambda \leq 1$ alors ce cristal est également stable par l'action de V et on peut écrire

$$N^\lambda = K \otimes_W W[F, V]/(FV - p, F^{s-r} - V^r)$$

où F et V commutent. Ainsi, N^λ est associé à un cristal muni d'une application σ^{-1}-linéaire V telle que $FV = VF = p$. Et on montre qu'en fait, $N^\lambda = \boldsymbol{D}(G^\lambda)$ (module de Dieudonné contravariant) où

$$G^\lambda = \ker(F^{r-s} - V^s : \underset{\to k}{\boldsymbol{W}} \longrightarrow \underset{\to k}{\boldsymbol{W}})$$

3.3 Classification des isocristaux

3.3.1 Enoncé du théorème

Nous allons montrer le théorème suivant :

Théorème 3.1. *Si k est algébriquement clos la catégorie $\boldsymbol{Isoc}_k$ est semi-simple d'objets simples les N^λ. En d'autres termes, tout isocristal peut s'écrire $\bigoplus_{\lambda\in\mathbb{Q}} \left(N^\lambda\right)^{\oplus m_\lambda}$ où les N^λ sont ceux définis précédemment, où les m_λ sont définis de façon unique et où de plus les N^λ n'ont pas de sous modules (ou quotients) non triviaux.*

On verra de plus que si k n'est pas algébriquement clos, on a tout de même une décomposition $\bigoplus_{\lambda\in\mathbb{Q}} N_\lambda$ mais où les N_λ sont sommes directes de N^λ après extension des scalaires à $W\left(\bar{k}\right)_{\mathbb{Q}}$. Les N_λ sont les composantes isotypiques (nous dirons isoclin).

3.3.2 Démonstration

Première pente de Newton d'un isocristal Le groupe de Grothendieck des W-modules de torsion est muni d'une application longueure virtuelle à valeurs dans $\mathbb{Z}$. Pour deux réseaux M_1, M_2 d'un isocristal N nous noterons $[M_1 : M_2]$ la longueure de la différence virtuelle $[M_1] - [M_2]$ au sens elle vaut $\text{long}([M_1/N] - [M_2/N])$ pour un réseau N contenu dans $M_1 \cap N_2$ (cette quantité est indépendante de N (cf. Corps locaux)).

Définition 3.4. *La dimension de l'isocristal (N, F) est $\dim(N, F) = [M : F(M)]$ pour un réseau M de N (et on vérifie que cela ne dépend pas de M)*

Définition 3.5. *Soit (N, F) et $M \subset N$ un réseau de N. On note $ord_M(F) = max\{k \in \mathbb{Z} \mid F(M) \subset p^k M\}$ et pour $m \in M$, $ord_M(m) = max\{k \in \mathbb{Z} \mid m \in p^k M\}$*

Lemme 3.1. *Si M, M' sont deux réseaux de N et $c, c' \in \mathbb{Z}$ tels que $p^c M \subset M'$ et $p^{c'} M \subset M$. Alors :*

- $\forall m \in N, \mid ord_M(m) - ord_{M'}(m) \mid \leq max(c, c')$.
- $\mid ord_M(F) - ord_{M'}(F) \mid \leq c + c'$.

Posons $x = \text{ord}_M(m)$. Dès lors, $m \in p^x M \subset p^{x-c} M' \Rightarrow \text{ord}_{M'}(m) \geq \text{ord}_M(m) - c$. Par symétrie on obtient donc également $\text{ord}_M(m) \geq \text{ord}_{M'}(m) - c$. Ces deux inégalités nous donnent la première inégalité recherchée.

Soit $y = \text{ord}_M(F)$. $FM \subset p^y M \Rightarrow FM \subset p^{y-c} M'$. Or $M' \subset p^{-c'} M \Rightarrow FM' \subset p^{-c'} FM$. Et donc $FM' \subset p^{y-c-c'} M' \Rightarrow \text{ord}_{M'}(F) \geq \text{ord}_M(F) - c - c'$. Par symétrie on obtient également $\text{ord}_M(F) \geq \text{ord}_{M'}(F) - c - c'$. Ces deux inégalités nous donnent la deuxième inégalité cherchée. □

Définition 3.6. *Un isocristal (N, F) est dit effectif s'il contient un réseau M tel que $FM \subset M$ i.e. un cristal.*

Proposition 3.1. *Soit (N, F) un isocristal de hauteur h, $M \subset N$ un réseau tel que $F^{h+1}(M) \subset p^{-1} M$. Alors (N, F) est effectif.*

Soit

$$M' = \sum_{j=0}^{h+1} F^j M$$

qui est un réseau.

$$\sum_{j=0}^{h+1} F^j M' = \sum_{j=0}^{2h+1} F^j M$$
$$= M' + \sum_{j=0}^{h} F^j(F^{h+1}M) \subset M' + p^{-1}\sum_{j=0}^{h} F^j M \subset p^{-1}M'$$

On a donc un chaine de $h+2$ réseaux

$$M' \subset M' + FM' \subset \ldots \subset M' + FM' + \cdots + F^{h+1}M' \subset p^{-1}M'$$

Or $\text{long}(p^{-1}M'/M') = h$. Donc $\exists i, M' + \cdots + F^{i-1}M' = M' + \cdots + F^i M'$ ou encore

$$F^i M' \subset M + \cdots + F^{i-1}M'$$

Posons

$$M'' = \sum_{j=0}^{i} F^j M'$$

Alors $FM'' \subset M''$. □

Définition 3.7. *Soit (N, F) un isocristal. Posons*

$$\nu(N,F) = \sup\{\frac{1}{n} ord_M(F^n) \mid M \text{ réseau de } N, n \in \mathbb{N} \setminus \{0\}\}$$

D'après le lemme qui suit $\nu(N,F)$ est fini.

Lemme 3.2. *Soit (N,F) de dimension d et de hauteur h. Alors $\forall M$ réseau de N,*

$$\forall n \in \mathbb{N}^*,\ ord_M(F) \leq \frac{1}{n} ord_M(F^n) \leq \frac{d}{h}$$

De plus, s'il existe n tel que $ord_M(F) \neq \frac{1}{n} ord_M(F^n)$ on a alors $ord_M(F) + \frac{1}{h} \leq \frac{1}{h} ord_M(F^h)$.

dem : En effet,

$$F(M) \subset p^x M \Longrightarrow \forall n \geq 0\ \ F^n(M) \subset p^{nx} M$$

d'où $\forall n > 0\ \text{ord}_M(F) \leq \frac{1}{n}\text{ord}_M(F^n)$. Ce qui nous fournit la première inégalité.

Pour la seconde, si $F^n M \subset p^y M$ alors puisque $\forall i\ [M : FM] = [F^i M : F^{i+1}M]$ (car F est bijectif) :

$$n[M:FM] = [M:FM] + [FM:F^2M] + \cdots + [F^{n-1}M : F^n M] = [M : F^n M]$$
$$\geq [M : p^y M] = y[M : pM] = yh$$

Et donc $nd \leq yh$ ce qui est la seconde inégalité.

Pour la seconde partie du théorème, notons $x = \mathrm{ord}_M(F)$. Supposons donc que $\mathrm{ord}_M(F) \neq \frac{1}{n}\mathrm{ord}_M(F^n)$ ou ce qui est équivalent, $F^n M \subset pnx+1M$. Soit $M_i = \{m \in M \mid F^i m \in p^{ix+1}M\}$. On a donc une chaîne de réseaux

$$pM = M_0 \subset M_1 \subset \cdots \subset M_n = M$$

Montrons que

$$M_i = M_{i+1} \Rightarrow \forall j \geq 1\ M_i = M_{i+j}$$

En effet, si $F' = p^{-x}F$, $F'(M) \subset M$ et induit $\bar{F}' : M/pM \to M/pM$ dont les noyaux itérés $\ker(\bar{F}^i)$ ont pour image réciproque par $M \to M/pM$ les M_i. Donc le fait annoncé n'est rien d'autre que le fait que si les noyaux itérérés stagnent à une étape, ils stagnent après.

Maintenant, si $n > h$, étant donné que $[M : pM] = h\ \exists i \leq h, M_i = M_{i+1}$. ce qui implique $M_i = \cdots = M_h = \cdots = M$ donc $M_h = M$ ce qui est l'assertion annoncée.

Si $n \leq h$ alors l'assertion était déja claire. □

Lemme 3.3. *Soit M un réseau de (N, F). Alors $\nu(N, F) = \lim_{n\to+\infty} \frac{1}{n} ord_M(F^n)$.*

dem : Posons $\lambda = \nu(N, F)$. Soit M' un autre réseau de N. Choisissons i suffisemment grand tel que $p^i M \subset M'$ et $p^i M' \subset M$.

$$\begin{aligned}\lambda &\geq \sup_m \frac{1}{m}\mathrm{ord}_M(F^m)\\ &\geq \sup_k \frac{1}{kn}\mathrm{ord}_M(F^{kn}) \geq \sup_k \frac{1}{kn}(\mathrm{ord}_{M'}(F^{kn}) - 2i)\end{aligned}$$

La dernière inégalité résultant du lemme 3.1. Or $\mathrm{ord}_{M'}(F^{kn}) \geq k.\mathrm{ord}_{M'}(F^n)$. Donc

$$\begin{aligned}\sup_k \frac{1}{kn}(\mathrm{ord}_{M'}(F^{kn}) - 2i) &\geq \sup_k \left(\frac{1}{n}\mathrm{ord}_{M'}(F^n) - \frac{2i}{kn}\right)\\ &= \frac{1}{n}\mathrm{ord}_{M'}(F^n)\end{aligned}$$

On en déduit donc que

$$\forall n\ \sup_m \frac{1}{m}\mathrm{ord}_M(F^m) \geq \frac{1}{n}\mathrm{ord}_{M'}(F^n)$$

et que donc (appliquant la même égalité par symétrie entre M et M')

$$\sup_m \frac{1}{m}\mathrm{ord}_M(F^m) = \sup_m \frac{1}{m}\mathrm{ord}_{M'}(F^m)$$

Cela étant vrai pour tout réseau M' on en déduit que

$$\lambda = \sup_n \frac{1}{n}\mathrm{ord}_M(F^n)$$

Reste à montrer que ce sup est une limite. Soit donc $\epsilon > 0$ et $m \in \mathbb{N}$ tels que $\frac{1}{m}\mathrm{ord}_M(F^m) \geq \lambda - \epsilon$.

$$\forall k \geq 1 \, \forall 0 \leq r \leq m-1 \; \mathrm{ord}_M(F^{mk+r}) \geq k\mathrm{ord}_M(F^m) + r\mathrm{ord}_M(F)$$

et donc

$$\begin{aligned} \frac{1}{mk+r}\mathrm{ord}_M(F^{mk+r}) &\geq \frac{k}{mk+r}\mathrm{ord}_M(F^m) + \frac{r}{mk+r}\mathrm{ord}_M(F) \\ &\geq \frac{mk}{mk+r}(\lambda-\epsilon) + \frac{r}{mk+r}\mathrm{ord}_M(F) \end{aligned}$$

Soit A tel que pour $k \geq A$ et $0 \leq r \leq m-1$ on ait $\frac{1}{1+\frac{r}{mk}}(\lambda-\epsilon) \geq \lambda - 2\epsilon$ et $\frac{r}{mk+r} \leq \epsilon$ alors

$$\forall n \geq mA \;\; \frac{1}{n}\mathrm{ord}_M(F^n) \geq \lambda - 3\epsilon$$

□

Lemme 3.4. *Soit (N,F) un isocristal et $r/s \in \mathbb{Q}$ tels que $\nu(N,F) \geq \frac{r}{s}$. Il existe alors un réseau M de N tel que $F^sM \subset p^rM$.*

dem : Soit $F' = F^s p^{-r}$. Il faut montrer qye l'isocristal (N,F') est effectif. D'après la proposition 3.1 il suffit de montrer qu'il existe un réseau M de N tel que si $F'' = (F')^{h+1}$ alors $F''M \subset p^{-1}M$.

On vérifie facilement que $\nu(N,F'') = (h+1)(s\nu(N,F)-r)$. Donc ,l'hypothèse $\nu(N,F) \geq r/s$ implique que $\nu(N,F'') \geq 0$ et donc si $F''' = pF''$, $\nu(N,F''') \geq 1$. Soit M un réseau de N. Il existe donc $n \in \mathbb{N}$ tel que $(F''')^n \subset M$. Si $M' = M + F'''M + \cdots + (F''')^{n-1}M$ alors $F'''M' \subset M'$ d'où le résultat. □

Proposition 3.2. *Soit (N,F) un isocristal. Alors, $\nu(N,F) \in \mathbb{Q}$ et si $\nu(N,F) = \frac{r}{s}$ il existe un réseau M de N tel que $F^sM \subset p^rM$.*

dem : Il est bien connu (principe des tiroirs) qu'il existe un nombre rationel r/s tel que

$$|\nu(N,F) - \frac{r}{s}| \leq \frac{1}{s(h+1)} \text{ avec } 1 \leq s \leq h$$

Soit alors $F' = F^s p^{-r}$ et $F'' = F'^{h+1}$. On a donc $|\nu(N,F'')| \leq 1$ ce qui implique d'après le lemme précédent qu'il existe un réseau M de N tel que $F''M \subset p^{-1}M$ et donc d'après la proposition 3.1 qu'il existe un entier $n \geq 1$ tel que

$$\mathrm{ord}_{M'}(F') \neq \frac{1}{n}\mathrm{ord}_{M'}(F'^n)$$

D'après le lemme 3.2 on aurait

$$\mathrm{ord}_{M'}(F') \leq \frac{1}{h}\mathrm{ord}_{M'}(F'^h) - \frac{1}{h}$$

or $\nu(N, F'^h) \leq \frac{h}{h+1}$ et donc

$$\mathrm{ord}_{M'}(F') \leq \frac{1}{h+1} - \frac{1}{h} < 0$$

ce qui est une contradiction avec l'inclusion $F'M' \subset M'$. Donc,

$$\forall n \in \mathbb{N} \ \ \frac{1}{n}\mathrm{ord}_{M'}(F'^n) = \mathrm{ord}_{M'}(F')$$

Donc, $\nu(N, F') = \mathrm{ord}_{M'}(F')$ or il s'agit d'un entier de valeur absolue inférieure à $\frac{1}{h+1}$. On a donc $\nu(N, F') = 0$ ce qui implique que $\nu(N, F) = \frac{r}{s}$ et $F^s M' \subset p^r M'$. □

Décomposition en partie bijective et topologiquement nilpotente

Lemme 3.5. *Soit $(M.F)$ un cristal. Il existe une unique décomposition en somme de cristaux*

$$M = M_{ét} \oplus M_{nil}$$

où $F : M_{ét} \xrightarrow{\sim} M_{ét}$ est un isomorphisme et $F : M_{nil} \to M_{nil}$ est toplogiquement nilpotent (pour la toplogie p-adique).

dem : Soit $n \in \mathbb{N}$. considérons $M/p^n M$ muni de l'opérateur $\bar{F}$. Étant donné que k est parfait, $\forall k \in \mathbb{N}$ $\Im \bar{F}^k$ est un sous $W_n(k)$-module de $M/p^n M$. Le $W_n(K)$-module $M/p^n M$ étant de longeur finie, pour k grand

$$(M/p^n M)_{nil} = \bigcup_{i \geq 0} \ker \bar{F}^i \text{ et } (M/p^n M)_{\text{ét}} = \bigcap_{i \geq 0} \mathrm{Im}\bar{F}^i = \mathrm{Im}\bar{F}^k$$

et il est bien connu (identique au cas de espaces vectoriels) qu'alors

$$M/p^n M = (M/p^n M)_{nil} \oplus (M/p^n M)_{\text{ét}}$$

On vérifie aussitôt que les décompositions précédentes sont compatibles lorsque n varie. On pose alors $M_{nil} \varprojlim_n (M/p^n M)_{nil}$ et $M_{\text{ét}} \varprojlim_n (M/p^n M)_{\text{ét}}$. □

Isocristaux isoclins

Définition 3.8. *Un isocristal (N, F) de dimension d et hauteur h est isoclin si $\nu(N, F) = \frac{d}{h}$.*

Proposition 3.3. *Soit (N, F) un isocristal de dimension d et hauteur h. Les propriétés suivantes sont équivalentes :*

- *(N, F) est isoclin*
- *Il existe un réseau M dans N tel que $F^h M = p^d M$*
- *Il existe un réseau M dans N et $r/s \in \mathbb{Q}$ tels que $F^s M = p^r M$*

dem : De la proposition 3.2 il résulte que le premier point implique le second qui lui même entraîne trivialement le troisième.

Supposons donc le troisème point vérifié. Appliquons le lemme 3.3 :

$$\nu(N,F) = \lim_{n\to+\infty} \frac{1}{n}\mathrm{ord}_M F^n = \lim_{k\to+\infty} \frac{1}{ks}\mathrm{ord}_M F^{ks}$$

Or $\forall k \in \mathbb{N}\ F^{ks}M = p^{rk}M$ et donc $\mathrm{ord}_M F^{ks} = rk$, d'où $\nu(N,F) = \dfrac{r}{s}$. Mais, $[M : F^s M] = s[M : FM] = sd = [M : p^r M] = rh$, donc $r/s = d/h$. D'où le premier point. □

Décomposition en isocristaux isoclins sur un corps parfait

Lemme 3.6. *Soit (N,F) un isocristal, N_1 un sous-isocristal de N et N_2 un isocirstal quotient de (N,F). Alors,*

$$\forall i = 1,2\ \ \nu(N_i) \leq \nu(N,F)$$

avec égalité lorsque (N,F) est isoclin.

dem : Si $\nu(N,F) = \dfrac{r}{s}$, soit M un réseau de M tel que $F^r M \subset p^s M$. Alors, $M_1 = M \cap N_1$ est un réseau de N_1 vérifiant $F^r M_1 \subset p^r M_1$ avec égalité lorsque $F^r M = p^s M$. De même pour le réseau image de M dans le quotient N_2 de N. □

Corollaire 3.1. *Si $\nu(N_1) < \nu(N_2)$ alors $\mathcal{H}om(N_1,N_2) = 0$. Si N_1 et N_2 sont isoclins de pentes différentes alors $\mathcal{H}om(N_1,N_2) = 0$.*

Proposition 3.4. *Soit (N,V) un isocristal. Il existe une unique suite de nombres rationnels*

$$\lambda_1 > \lambda_2 > \cdots > \lambda_r$$

telle que

$$N = \bigoplus_{1\leq i\leq r} N_{\lambda_i}$$

où N_{λ_i} est isoclin de pente λ_i.

dem : Soit $\dfrac{r_1}{s_1} = \lambda_1 = \nu(N,F)$. Soit M un réseau de N vérifiant $F^{r_1}M \subset p^{s_1}M$. Soit $F' = F^{r_1}p^{-s_1}$. Le réseau M muni de F' est donc un cristal. Nous obtenons une décomposition $M = M_{\text{ét}} \oplus M_{nil}$. Par définition de $M_{\text{ét}}$, celui-ci est un réseau de $N_{\text{ét}}$ vérifiant $F^{r_1}M_{\text{ét}} = p^{s_1}M_{\text{ét}}$. D'après la proposition 3.3 on en déduit que $(N_{\text{ét}},F)$ est isoclin de pente λ_1. L'opérateur F' étant toplogiquement nilpotent sur M_{nil}, il existe un entier positif n tel que $F'^n M \subset pM$ et donc $F^{nr_1}M_{nil} \subset p^{1+ns_1}M_{nil}$ ce qui implique que $\nu(N_{nil},F) \leq \lambda_1 - \dfrac{1}{n} < \lambda_1$. D'où l'existence de la décomposition par récurrence sur la hauteur de (N,F).

L'unicité résulte de l'algorithme fourni pour construire une telle décomposition. □

Il résulte du corollaire 3.1 et de la proposition précédente que l'on a une décomposition orthogonale de la catégorie des k-isocristaux

$$\boldsymbol{Isoc}_k = \bigoplus_{\lambda\in\mathbb{Q}} \boldsymbol{Isoc}_{k,\lambda}$$

Décomposition sur un corps algébriquement clos L'isocristal N^λ est un module cyclique pour l'action de F, engendré par 1, d'annulateur $F^r - p^s$. Donc pour tout isocristal (N, φ),

$$\mathcal{H}\mathrm{om}(N^\lambda, N) \simeq \{x \in N \mid \varphi^r(x) = p^s x\}$$

Proposition 3.5. *Si $\lambda' \neq \lambda \in \mathbb{Q}$ alors $\mathcal{H}om(N^{\lambda'}, N^\lambda) = 0$*

Soient $\lambda = r/s, \lambda' = r'/s'$. Notons $(e_0, \ldots, e_{r-1}) = (1, F, \ldots, F^{r-1})$ la base canonique de N^λ. Un élément de $\mathcal{H}\mathrm{om}(N^{\lambda'}, N^\lambda)$ est équivalent à la donnée d'un $x = \sum_i a_i e_i \in N^\lambda$ tel que $F^{r'}x = p^{s'}x$.

Ecrivons $F^{rr'}(x)$ de deux manières :

$$F^r(x) = \sum_i a_i^{\sigma_i} p^s e_i$$

$$\Rightarrow F^{rr'}(x) = \sum_i a_i^{\sigma^{rr'}} p^{sr'} e_i$$

Puis de l'autre manière :

$$F^{r'}(x) = p^{s'}x \Rightarrow F^{rr'}(x) = p^{s'r}x$$

La comparaison des deux écritures donne :

$$\forall i \;\; p^{s'r} a_i = p^{sr'} a_i^{\sigma^{rr'}}$$

s'il existait un i tel que $a_i \neq 0$, la comparaison des valuations p-adiques donnerait (puisque $\forall y, y$ et y^σ ont même valuation) $s'r = sr'$ soit $\lambda = \lambda'$. □

Remarque 3.1. *Cela résulte également du corollaire 3.1 puisque N^λ est isoclin de pente λ.*

Lemme 3.7. *Pour tout λ, N^λ ne possède pas de sous-isocristal propre.*

dem : L'ioscristal N^λ est isoclin de pente $\lambda = \dfrac{d}{h}$ où d est la dimenison de N^λ et h sa hauteur avec $d \wedge h = 1$. Si N' est un sous-isocristal non nul de N alors N' est isoclin de pente λ (lemme 3.6) et donc si d' est la dimension de N' et h' sa hauteur, $\dfrac{d'}{h'}\dfrac{d}{h}$. Les entiers d et h étant premiers entre eux cela implique que h' est un multiple de h et donc $h' = h$, ce qui implique que $N' = N$. □

Lemme 3.8. *Soit k un corps algébriquement clos de caractéristique p, E/k un k-e.v. de dimension n. Soit $q = p^a$ pour un $a \in \mathbb{Z} \setminus \{0\}$ et $\varphi : E \to E$ une bijection additive telle que $\forall \lambda \in k \; \forall v \in E \;\; \varphi(\lambda v) = \lambda^q v$.*
Alors il existe une base $(e_1, \ldots, e_n)$ de E telle que $\forall i \; \varphi(e_i) = e_i$.

Quitte à prendre φ^{-1} on peut supposer $a > 0$

Commençons par montrer l'existence de $x \in E \setminus \{0\}$ tel que $\varphi(x) = x$.

Soit $v \in E, v \neq 0$ et $r \in \mathbb{N}^*$ le plus grand entier s tel que $(v, \varphi(v), \ldots, \varphi^{s-1}(v))$ soit libre. Il existe alors des $\alpha_i \in k$ tels que

$$\varphi^r(v) = \sum_{i=0}^{r-1} \alpha_i \varphi^i(v)$$

Pour $x = (x_1, \ldots, x_x) \in k^n$ posons $w = w(x) = \sum_{i=0}^{r-1} x_i \varphi^i(v)$. Cherchons à résoudre $\varphi(w) = w$.

Cela est èquivalent à :

$$\sum_{i=0}^{r-2} x_i^q \varphi^{i+1}(v) + \sum_{i=0}^{r-1} x_{r-1}^q \alpha_i \varphi^i(v) = \sum_{i=0}^{r-1} x_i \varphi^i(v)$$

On obtient donc un système linéaire

$$\begin{cases} x_0 = \alpha_0 x_{r_1}^q \\ x_1 = x_0^q + \alpha_1 x_{r_1}^q \\ \vdots \qquad\qquad \vdots \\ x_{r-1} = x_{r-2}^q + \alpha_{r-1} x_{r-1}^q \end{cases}$$

La condition pour que ce système admette une solution non nulle est qu'il y ait compatibilité lorque l'on remplace une ligne dans celle du dessous et que l'on boucle i.e. :

$$x_{n-1} = \alpha_0^{q^{n-1}} x_{n-1}^{q^n} + \cdots + \alpha_{n-1} x_{n-1}^q$$

Etant donné qu'il existe i, $\alpha_i \neq 0$, que $q > 0$ (car $a \neq 0$!) et que k est algébriquement clos, cette èquation possède bien une solution non nulle. D'où l'existence d'un x tel que $\varphi(x) = x$.

Soit maintenant $(e_1, \ldots, e_r)$ un sytème maximal de vecteurs linéairement indépendants tels que $\forall i\ \varphi(e_i) = e_i$. Notons $F \subset E$ le sous espace engendré par ces vecteurs. Si $F \neq E$, par le travail précédent $\exists \bar{f} \in E/F, \bar{\varphi}(\bar{f}) = \bar{f}$ où $f \in E$. Dès lors,

$$\exists \beta_i,\ \varphi(f) = f + \sum_{i=1}^{r} \beta_i e_i$$

Soit alors $e_{r+1} = f + \sum_{i=1}^{r} y_i e_i$ pour des $y_i \in k$.

Cherchons à résoudre $\varphi(e_{r+1}) = e_{r+1}$ en les inconnues y_i. Ceci est équivalent à

$$e_{r+1} + \sum_{i=1}^{r} (\beta_i + y_i^q) e_i = \epsilon_{r+1} + \sum_{i=1}^{r} y_i e_i$$

$$\Leftrightarrow \forall i\ y_i^q - y_i = -\beta_i$$

qui possède une solution puisque k est algébriquement clos. □

Nous pouvons maintenant démontrer le théorème de structure 3.1. Il reste à démontrer que si (N, F) est sioclin de pente λ et k algébriquement clos alors (N, F) est somme directe de copies de l'isocristal N^λ. Soit $\lambda = \frac{r}{s}$ et M un réseau de N tel que $F^r M = p^s M$. Soit $F' = F^r p^{-s} : M \xrightarrow{\sim} M$. D'après le lemme précédent, si $\bar{F}' : M/pM \to M/pM$ alors il

eciste une base $e_1, \ldots, e_n$ de M/pM telle que $\forall i\ \bar{F}' e_i = e_i$. Montrons qu'on peut relever les e_i en une base ϵ_i de M vérifiant $F'\epsilon_i = \epsilon_i$. Supposons construit un tel relévement $(\epsilon_i^{(n)})_i$ dans M/p^nM et cherchons à le relever dans $M/p^{n+1}M$ (de manière à ce qu'il satisfasse l'équation voulue). Soit $(\alpha_i)_i$ un relévement de $(e_i)_i$ dans $M/p^{n+1}M$. Matriciellement,

$$F'(\alpha_i)_i = (\alpha_i)_i + p^n A(\alpha_i)_i$$

où A est une matrice carrée à coefficients dans k. Cherchons une solution à notre problème sous la forme $(\epsilon_i^{(n+1)})_i = (\alpha_i)_i + p^n B(\alpha_i)_i$ où B est une matrice carré à coefficients dans k. Il vient alors

$$B^{(p)} - B = A$$

où $B^{(p)}$ est obtenue en mettant tous les coefficients de B à la puissance p. Cette équation possède bien sûr une solution puisque k est algébriquement clos.

Il existe donc une base $(e_i)_i$ de M telle que $\forall i\ F^r e_i = p^s e_i$. Celle-ci permet de construire un morphisme non-nul pour tout i, $N^\lambda \longrightarrow N$ envoyant 1 sur e_i. D'après le lemme 3.7 ces morphismes sont injectifs. On obtient donc $N = \sum_i N_i$ où $N_i \simeq N^\lambda$.

Soit J un sous-ensemble de l'ensemble des indices i tel que $N = \sum_{i\in J} N_i$ et que cette décomposition soit minimale. Cela implique que $\forall j \in J\ N_j \nsubseteq \sum_{i\neq j, i\in J} N_i$ et que donc d'après le lemme 3.7 $N_j \cap \sum_{i\neq j, i\in J} N_i = 0$. La somme est donc directe et l'on a une décomposition

$$N = \bigoplus_{j\in J} N_j \simeq \bigoplus_{j\in J} N^\lambda$$

□

3.4 Anneau des endomorphismes des isocristaux

Définition 3.9. *Nous noterons $\mathbb{Q}_{p^s} = W(\mathbb{F}_{p^s})_\mathbb{Q}$ l'extension non-ramifiée de degré s de $\mathbb{Q}_p$.*

On suppose dans cette section que le corps parfait k contient $\mathbb{F}_{p^s}$.

Rappelons que si $\lambda = \frac{r}{s}, r \wedge s = 1$ on note $(1, F, \ldots, F^{s-1})$ une base du k-isocristal N^λ.

Puisque N^λ est simple $\mathrm{End}(N^\lambda)$ est une algèbre à division sur $\mathbb{Q}_p$. Comme $\mathbb{Q}_p$-espace vectoriel, via l'application qui à un endomorphisme f associe $f(1)$

$$\mathrm{End}(N^\lambda) = \{x \in N^\lambda \mid F^s x = p^r x\ \}$$

Or, si $x = \sum_{i=0}^{s-1} \lambda_i F^i$,

$$F^s x = p^r x \Leftrightarrow \forall i\ \lambda_i^{\sigma^i} = \lambda_i \Leftrightarrow \forall i\ \lambda_i \in \mathbb{Q}_{p^s}$$

Et donc, $\mathrm{End}(N^\lambda)$ est un $\mathbb{Q}_{p^s}$-espace vectoriel de base $1, F, \ldots, F^{s-1}$ et même une $\mathbb{Q}_{p^s}$-algèbre puisque $\mathbb{Q}_{p^s} \xrightarrow{\sim} \mathbb{Q}_{p^s}.1$ induit un isomorphisme d'algèbre (mais $\mathbb{Q}_{p^s}.1$ n'est pas contenu dans le centre qui est $\mathbb{Q}_p$). Soit $\Pi \in \mathrm{End}(N^\lambda)$ l'endomorphisme associé à l'élément de base F. Alors, $\forall i \leq s-1$ Π^i est associé à l'élément de base F^i. Donc,

$$\mathrm{End}(N^\lambda) = \mathbb{Q}_{p^s}[\Pi] \text{ où } \forall x \in \mathbb{Q}_{p^s} \ \Pi x = x^\sigma \Pi \text{ et } \Pi^s = p^r$$

La norme réduite de Π est p^r. Soient donc $a, b \in \mathbb{Z}$ tels que $ar + bs = 1$ et posons $\Pi' = \Pi^a p^b$ de sorte que sa norme réduite soit p. Alors,

$$\Pi'^r = \Pi$$

et Π' est une uniformisante de $\mathrm{End}(N^\lambda)$ qui a pour ordre maximal $\mathbb{Z}_{p^s}[\Pi']$. Une autre présentation de $\mathrm{End}(N^\lambda)$ est alors

$$\mathbb{Q}_{p^s}[\Pi'] \text{ où } \forall x \in \mathbb{Q}_{p^s} \ x\Pi' = \Pi' x^{\sigma^r} \text{ et } \Pi'^s = p$$

Rappelons que $\mathrm{Br}(\mathbb{Q}_p) \simeq \mathbb{Q}/\mathbb{Z}$.

Proposition 3.6. *L'algèbre à division $D_\lambda = End(N^\lambda)$ est d'invariant λ mod $\mathbb{Z}$ dans le groupe de Brauer.*

dem : Il y a un isomorphisme de $\mathbb{Q}_{p^s}$-algèbres

$$\begin{array}{ccc} \mathrm{End}(N^\lambda) \otimes_{\mathbb{Q}_p} \mathbb{Q}_{p^s} & \xrightarrow{\sim} & M_s(\mathbb{Q}_{p^s}) \\ \Pi \otimes 1 & \mapsto & \begin{pmatrix} 0 & & & p^r \\ 1 & & & 0 \\ & \ddots & & \vdots \\ 0 & & 1 & 0 \end{pmatrix} \end{array}$$

(on peut le vérifier à la main ou bien utiliser le fait que $\mathrm{End}(N^\lambda) \otimes \mathbb{Q}_{p^s} = \{u \in \mathrm{End}_K(K^s \otimes_{\mathbb{Q}_p} \mathbb{Q}_{p^s}) \mid uF = Fu\}$ et l'isomorphisme $K \otimes_{\mathbb{Q}_p} \mathbb{Q}_{p^s} \xrightarrow{\sim} \prod_{i=0}^{s-1} K$ sur lequel $1 \otimes \sigma$ agit par permutation cyclique des composantes).

Rappelons maintenant que l'ismorphisme

$$H^2(\mathbb{Q}_{p^s}|\mathbb{Q}_p, \mathbb{Q}_{p^s}^\times) \xrightarrow{\sim} \frac{1}{s}\mathbb{Z}/\mathbb{Z} \subset \mathrm{Br}(\mathbb{Q}_p) = \mathbb{Q}/\mathbb{Z}$$

est réalisé par la valuation : $v_p : \mathbb{Q}_p^\times \longrightarrow \mathbb{Z}$:

$$H^2(\mathbb{Q}_{p^s}|\mathbb{Q}_p, \mathbb{Q}_{p^s}^\times) \xrightarrow{v_p} H^2(\mathbb{Q}_{p^s}|\mathbb{Q}_p, \mathbb{Z}) \simeq \widehat{H}^0(\mathbb{Q}_{p^s}|\mathbb{Q}_p, \mathbb{Z}) = \mathbb{Z}/s\mathbb{Z}$$

De plus, la classe dans le groupe de Brauer de $\mathrm{End}(N^\lambda)$ provient de l'application de bord suivante : soit la suite exacte $1 \to \mathbb{G}_m \to \mathrm{GL}_s \to \mathrm{PGL}_s \to 1$. Alors,

$$H^1(\mathbb{Q}_{p^s}|\mathbb{Q}_p, \mathrm{PGL}_s) \longrightarrow H^2(\mathbb{Q}_{p^s}|\mathbb{Q}_p, \mathbb{G}_m) \hookrightarrow \mathrm{Br}(\mathbb{Q}_p) \longrightarrow\!\!\!\!\!= \mathbb{Q}/\mathbb{Z}$$

$$[\mathrm{End}(N^\lambda)] \longmapsto \text{invariant de } \mathrm{End}(N^\lambda)$$

Il y un morphisme de suites exactes

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathbb{Q}_{p^s}^{\times} & \longrightarrow & \mathrm{GL}_s(\mathbb{Q}_{p^s}) & \longrightarrow & \mathrm{PGL}_s(\mathbb{Q}_{p^s}) & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle v_p} & & \downarrow{\scriptstyle v_p\circ\det} & & \downarrow{\scriptstyle v_p\circ\det} & & \\ 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{\times s} & \mathbb{Z} & \longrightarrow & \mathbb{Z}/s\mathbb{Z} & \longrightarrow & 1 \end{array}$$

d'où un diagramme commutatif :

$$\begin{array}{ccc} H^1(\mathbb{Q}_{p^s}|\mathbb{Q}_p, \mathrm{PGL}_s) & \xrightarrow{\delta} & H^2(\mathbb{Q}_{p^s}|\mathbb{Q}_p, \mathbb{Q}_{p^s}^{\times}) \\ \downarrow{\scriptstyle v_p\circ\det} & & \downarrow{\scriptstyle v_p} \\ H^1(\mathbb{Q}_{p^s}|\mathbb{Q}_p, \mathbb{Z}/s\mathbb{Z}) & \xrightarrow{\sim\delta} & H^2(\mathbb{Q}_{p^s}|\mathbb{Q}_p, \mathbb{Z}) \end{array}$$

et donc, si $f : \mathrm{End}(N^{\lambda}) \otimes_{\mathbb{Q}_p} \mathbb{Q}_{p^s} \xrightarrow{\sim} M_s(\mathbb{Q}_{p^s})$, si $c_\sigma = ff^{-\sigma}$ où $g_\sigma \in \mathrm{PGL}_s(\mathbb{Q}_{p^s})$ on doit vérifier que $v_p(\det(g_\sigma)) = r \bmod s\mathbb{Z}$ ce qui est bien le as car on vérifie que g_σ est la classe de $\begin{pmatrix} 0 & & & p^r \\ 1 & & & 0 \\ & \ddots & & \vdots \\ 0 & & 1 & 0 \end{pmatrix}$ □

3.5 La gerbe et le lien définis par la catégorie Tannakienne des isocristaux sur un corps algébriquement clos

3.5.1 Rappels champêtres

Rappelons que si $(\mathcal{T}, \otimes)$ est une catégorie Tannakienne $\mathbb{Q}_p$-linéaire on lui associe une gerbe fpqc $\mathcal{G}$ sur $\boldsymbol{Spec}(\mathbb{Q}_p)_{fpqc}$ telle que

$$\mathcal{G}(S) = \text{ le groupoïde des foncteurs fibres : } \mathcal{T} \longrightarrow \mathcal{O}_S\text{-mod. loc. libres de rg. fini}$$

Dire que c'est une gerbe signifie que localement sur $\boldsymbol{Spec}(\mathbb{Q}_p)_{fpqc}$ deux foncteurs fibres sont isomorphes : sur des corps cela signifie que $\forall \omega_1 \in \mathcal{G}(K_1), \omega_2 \in \mathcal{G}(K_2)$ $\exists K'|K_1$ et $K'|K_2$ telle que $\omega_1^{(K')} \simeq \omega_2^{(K')}$ et qu'il existe $K|\mathbb{Q}_p$ tel que $\mathcal{G}(K) \neq \emptyset$ (cette dernière condition est suffisante pour tous les schémas puisque tout schéma possède un point à valeurs dans un corps...). Soit $K|\mathbb{Q}_p$ telle que $\mathcal{G}(K) \neq \emptyset$ et $\omega \in \mathcal{G}(K)$. Il y a alors un morphisme couvrant

$$\boldsymbol{Spec}(K) \xrightarrow{\omega} \mathcal{G}$$

qui fournit une présentation i.e. un $\boldsymbol{Spec}(K)/\boldsymbol{Spec}(\mathbb{Q}_p)$-groupoide (au sens de l'appendice A de [1])

$$\left[\boldsymbol{Spec}(K) \times_{\mathcal{G}} \boldsymbol{Spec}(K) \underset{pr_2}{\overset{pr_1}{\rightrightarrows}} \boldsymbol{Spec}(K) \right]$$

(où la flêche du milieu est "l'identité") tel que $\mathcal{G}$ soit le quotient de ce groupoide i.e. le champ quotient associé (qui est le champ associé au préchamp quotient "naif" en forçant les $\mathcal{H}$om à être des faisceaux fpqc et les données de descentes à êtres effectives). Alors,

$$(\mathcal{T}, \otimes) \xrightarrow{\sim} \mathrm{Rep}(\mathcal{G}) = \mathcal{H}\mathrm{om}(\mathcal{G}, \mathrm{Vect})$$

où Vect désigne le champ des modules localement libres de rang fini sur un $\mathbb{Q}_p$-schéma quasicompact (étant donné que $\mathcal{G}$ possède un point sur un corps on peut se restreindre aux schémas qui sont des spectres de produits finis de corps extensions de $\mathbb{Q}_p$).

Remarque 3.2. *Lorsque $\mathcal{G}(K) \neq \emptyset$ pour $K|\mathbb{Q}_p$ de degré fini on peut remplacer partout fpqc par étale.*

Soit $\omega \in \mathcal{G}(K)$ et considérons le K-groupe pro-algébrique $G_\omega = \underline{\mathrm{Aut}}^{\otimes}(\omega)$. Dans le diagramme

$$\begin{array}{ccccc} & & \boldsymbol{Spec}(K) \times_{\boldsymbol{Spec}(\mathbb{Q}_p)} \boldsymbol{Spec}(K) & & \\ & \swarrow^{pr_1} & & \searrow^{pr_2} & \\ \boldsymbol{Spec}(K) & & & & \boldsymbol{Spec}(K) \end{array}$$

il existe un morphisme couvrant $f : T \longrightarrow \boldsymbol{Spec}(K) \times_{\boldsymbol{Spec}(\mathbb{Q}_p)} \boldsymbol{Spec}(K)$ et un isomorphisme $f^* pr_1^* \omega \xrightarrow{\sim} f^* pr_2^* \omega$. Quitte à élargir K on peut donc supposer que $pr_1^* \omega \simeq pr_2^* \omega$. Fixons un tel isomorphisme. Il induit un isomorphisme $\theta : pr_1^* G_\omega \xrightarrow{\sim} pr_2^* G_\omega$ qui vérifie

$$pr_{13}^* \theta = \gamma \circ (pr_{12}^* \theta \circ pr_{23}^* \theta)$$

où γ est un automorphisme intérieur de G_ω sur $\boldsymbol{Spec}(K) \times \boldsymbol{Spec}(K) \times \boldsymbol{Spec}(K)$ i.e. G_ω est un K-groupe muni d'une donnée de descente à automorphismes intérieures près : ce qu'on appelle un lien.

Exemple 3.1. *Si G_ω est abélien alors il s'agit d'une vrai donnée de descente. Le groupe G_ω se descent alors à $\mathbb{Q}_p$ en un $\mathbb{Q}_p$-groupe pro-algébrique qui ne dépend pas de ω (il est par exemple bien connu que pour un espace toplogique connexe par arcs de groupe fondamental abélien en un point, canoniquement ce groupe fondamental ne dépend pas de ce point).*

Soit $\mathcal{G}$ une S-gerbe étale ($S = \boldsymbol{Spec}(\mathbb{Q}_p)$ ici) de lien abélien G et $T \to S$ galoisien de groupe Γ tel que $\mathcal{G}(T) \neq \emptyset$. Soit $\omega \in \mathcal{G}(T)$. Il y a un morphisme couvrant

$$T \times_{\mathcal{G}} T \twoheadrightarrow T \times_S T \simeq T \times_S \Gamma$$

au dessus de T via la première projection. Ce morphisme a pour noyau $G \times_S T$ et fournit une suite exacte de groupe étales finis sur T qui sur les T-points donne une suite exacte

$$1 \to G(T) \to (T \times_{\mathcal{G}} T)(T) \to \Gamma \to 1$$

d'où un élément du $H^2(\Gamma, G(T))$.

Alors, cette correspondance induit une bijection entre classes de S-gerbes étales telles que $\mathcal{G}(T) \neq \emptyset$ de lien abélien G et $H^2(\Gamma, \mathcal{G}(T))$.

3.5.2 Le lien

Pour deux nombres rationnels λ_1 et λ_2 l'isocristal produit tensoriel $N^{\lambda_1} \otimes N^{\lambda_2}$ est isoclin de pente $\lambda_1\lambda_2$. On en déduit aussitôt que pour le foncteur fibre canonique $\omega : \boldsymbol{Isoc}_k \longrightarrow \mathrm{Vect}_K$ on a : $\mathrm{Aut}^{\otimes}(\omega)$ est le pro-tore $\mathbb{D}$ de groupe de cocaractères $\mathbb{Q}$ i.e.

$$\mathbb{D} = \lim_{\leftarrow} \mathbb{G}_m$$

où les morphismes de transition sont les multiplications pas les entiers (il s'agit du revétement simplement connexe de $\mathbb{G}_m$). Le groupe $\mathbb{D}$ agit sur la partie de pente λ via le caractère $z \mapsto z^{\lambda}$. Ce pro-tore est canoniquement défini sur $\mathbb{Q}_p$ et cette $\mathbb{Q}_p$-structure correspond à celle définie par la donnée de descente associée à la structure de lien.

Soit $s \in \mathbb{N} \setminus \{0\}$ et $\boldsymbol{Isoc}_k^{(s)}$ la sous-catégorie Tannakienne pleine de la catégorie $\boldsymbol{Isoc}_k$ formée des isocristaux de pentes à valeurs dans $\frac{1}{s}\mathbb{Z}/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$. Celle-ci est de type fini, engendrée par l'isocristal $N^{1/s}$. Son lien est donc un groupe algébrique (i.e. de type fini). Il s'identifie à $\mathbb{G}_m$ et le plongement $\boldsymbol{Isoc}_k^{(s)} \hookrightarrow \boldsymbol{Isoc}_k$ est associé à l'épimorphisme $\mathbb{D} \twoheadrightarrow \mathbb{G}_m$ défini par le caractère $1/s \in \mathbb{Q}$.
Remarquons que $\boldsymbol{Isoc}_k^{(s)}$ possède un foncteur fibre sur $\mathbb{Q}_{p^s}$. Etant donné que $\boldsymbol{Isoc}_k = \bigcup_s \boldsymbol{Isoc}_k^{(s)}$ cela implique que $\boldsymbol{Isoc}_k$ possède un foncteur fibre sur $\mathbb{Q}_p^{nr} \subset \overline{\mathbb{Q}_p}$.

3.5.3 La gerbe

Références

[1] J.S. Milne. The points on a Shimura variety modulo a prime of good reduction. In *The Zeta functions of Picard modular surfaces*, pages 151–253. Univ. Montréal, Montreal, PQ, 1992.

[2] M. Schlessinger. Functors of artin rings. *Trans. Amer. Math. Soc.*, 130 :208–222, 1968.