SÉMINAIRE DE MATHÉMATIQUES SUPÉRIEURES

DÉPARTEMENT DE MATHÉMATIQUES — UNIVERSITÉ DE MONTRÉAL

GROUPES DE BARSOTTI-TATE ET CRISTAUX DE DIEUDONNÉ

ALEXANDRE GROTHENDIECK

Institut des Hautes Études scientifiques de France

1974

LES PRESSES DE L'UNIVERSITÉ DE MONTRÉAL

C. P. 6128, Montréal 101, Canada

TABLE DES MATIERES

AVERTISSEMENT

Ces notes n'incluent que certaines des matières traitées par M. le professeur Alexandre Grothendieck dans son cours donné à Montréal à l'été 1970. On espère que les matières non publiées dans le présent travail, le seront dans une édition ultérieure.

Ce cahier comporte d'importantes lacunes: la première est l'absence d'un chapitre, qui se serait inséré entre les deux derniers chapitres, et qui devait porter sur les F-cristaux. On trouvera à la place une lettre de M. Grothendieck à M. Barsotti placée en appendice à la fin des notes et on consultera aussi utilement à ce sujet, les notes de M. Demazure[7] sur les groupes p-divisibles qui sont appelés ici les groupes de Barsotti-Tate par M. Grothendieck. La principale lacune est l'absence de deux autres chapitres qui devaient se situer à la fin du texte et traiter de la définition des foncteurs de Dieudonné généralisés et de leurs rapports avec les foncteurs classiques. Nous référons le lecteur à l'article (à paraître) de Barry Mazur et William Messing (réf. [23a] dans la bibliographie).

L'existence de ces Notes est due surtout aux efforts de Monique Hakim et Jean-Pierre Delale qui ont rédigé la plupart des chapitres. Nous les remercions bien sincèrement. Signalons cependant que les personnes ci-haut mentionnées ne sont pas responsables de l'incapacité de reproduire toutes les matières esquissées par M. Grothenkieck lors de son cours en 1970. Nous espérons toutefois que ces Notes, bien qu'incomplètes, donneront aux lecteurs une bonne introduction à la théorie des cristaux et des groupes de Barsotti-Tate.

Finalement, nous remercions Madame Thérèse Fournier pour son excellent travail de dactylographie de ces Notes.

Octobre 1973 J.P. Labute

CHAPITRE I

PRELIMINAIRES SUR WITT

1. Rappels sur les vecteurs de Witt

Dans tout ce qui suit, p désigne un nombre premier fixé une fois pour toutes.

Le schéma des vecteurs de Witt $\mathbb{W}$ et le schéma des vecteurs de Witt tronqués à l'ordre n $\mathbb{W}_n$ sont des schémas en anneaux, affines sur $\mathbb{Z}$ qui sont définis comme suit :

Soit $n \geq 1$ un entier et soit $\mathbb{E}^n = \operatorname{Spec} \mathbb{Z}[T_1, T_2, \ldots, T_n]$ d'espace affine de dimension n sur $\mathbb{Z}$. Le schéma $\mathbb{E}^n$ représente le foncteur $A \to A^n$ de la catégorie des schémas affines dans la catégorie des ensembles; il est donc muni d'une structure naturelle de schéma en anneaux. On note $\underline{0}^n$ le schéma $\mathbb{E}^n$ muni de cette structure. On démontre alors (c.f. J.-P. Serre, "Corps locaux", II, §6) qu'il existe une unique structure de schéma en anneaux sur $\mathbb{E}^n$ telle que le morphisme de schémas

$$\phi = (\phi_1, \phi_2, \ldots, \phi_n) : \mathbb{E}^n \to \underline{0}^n$$

défini par

$$\phi_i(x_1, x_2, \ldots, x_n) = x_1^{p^{i-1}} + p\, x_2^{p^{i-2}} + p^2\, x_3^{p^{i-3}} + \ldots + p^{i-1}\, x_i$$

soit un homomorphisme d'anneaux.

Par définition, $\mathbb{W}_n$ est le schéma $\mathbb{E}_n$ muni de cette structure de schéma en anneaux.

Les morphismes de restriction

$$R_n : \mathbb{W}_{n+1} \to \mathbb{W}_n \qquad (x_1,\ldots,x_n,x_{n+1}) \mapsto (x_1,\ldots,x_n)$$

sont alors des homomorphismes d'anneaux. En effet, il résulte de l'unicité de la structure d'anneau sur $\mathbb{W}_n$ qu'un morphisme $f : X \to \mathbb{W}_n$ est un morphisme d'anneaux (resp. de groupes) si et seulement si $\phi_i \circ f : X \to \underline{0}$ est un homomorphisme d'anneaux (resp. de groupes pour tout i, $1 \leq i \leq n$. Ici, on a $\phi_i R_n = \phi_i$, qui est par définition un homomorphisme d'anneaux.

On définit le schéma en anneau des vecteurs de Witt $\mathbb{W}$ par

$$\mathbb{W} = \lim_{\leftarrow n} (\mathbb{W}_n, R_n) \quad .$$

Le schéma sous-jacent à $\mathbb{W}$ est donc en particulier isomorphe à $\mathbb{E}^{\mathbb{N}}$.

2. Quelques morphismes remarquables

2.1. On définit

$$V = V_n : \mathbb{W}_n \to \mathbb{W}_n \qquad (x_1,x_2,\ldots,x_{n-1},x_n) \mapsto (0,x_1,\ldots,x_{n-1})$$

$$T = T_n : \mathbb{W}_n \to \mathbb{W}_{n+1} \qquad (x_1,x_2,\ldots,x_n) \mapsto (0,x_1,\ldots,x_n) \quad .$$

Le morphisme T est <u>additif</u> ; on a en effet $\phi_i T = p\, \phi_{i-1}$ pour $1 \leq i \leq n+1$.

On en déduit que $V_n = R_n T_n = T_{n-1} R_{n-1}$ est aussi un morphisme <u>additif</u>.

Par passage à la limite, les morphismes V_n définissent un morphisme additif

$$V : \mathbb{W} \to \mathbb{W}$$

appelé Verschiebung ou morphisme de décalage.

2.2. Le morphisme de Frobenius $F : \mathbb{W} \to \mathbb{W}$ est défini par passage à la limite à partir des morphismes

$$F_n : \mathbb{W}_n \to \mathbb{W}_n \qquad (x_1,x_2,\ldots,x_n) \to (x_1^p,x_2^p,\ldots,x_n^p) .$$

Ce morphisme n'est en général pas additif, mais par réduction en caractéristique p, il définit un homomorphisme d'anneau

$$F_{\mathbb{F}_p} : \mathbb{W}_{\mathbb{F}_p} \to \mathbb{W}_{\mathbb{F}_p} \qquad (\text{resp. } F_n \mathbb{F}_p)$$

où $\mathbb{F}_p$ désigne le corps premier $\mathbb{Z}/p\mathbb{Z}$ et $\mathbb{W}_{\mathbb{F}_p}$ désigne le schéma induit sur $\mathbb{F}_p$ par changement de base. En effet, les deux lois de composition sur $\mathbb{W}$ sont données par

$$(x_1,x_2,\ldots,x_n,\ldots) + (y_1,\ldots,y_n,\ldots) = (S_1,S_2,\ldots,S_n,\ldots)$$

$$(x_1,x_2,\ldots,x_n,\ldots) \cdot (y_1,\ldots,y_n,\ldots) = (P_1,\ldots,P_n,\ldots)$$

où les S_i et P_i sont des polynômes à coefficients entiers en $(x_1,x_2,\ldots,x_i, y_1,y_2,\ldots,y_i)$. Or, pour toute $\mathbb{F}_p$-algèbre, on a

$$P(x^p,y^p) = [P(x,y)]^p .$$

Proposition 2.3. En caractéristique p , on a les relations

$$F \cdot V = V \cdot F = p \, Id_{\mathbb{W}_{\mathbb{F}_p}}$$

(c.f. J.-P. Serre, "Corps locaux" II, §6, Cor. du th. 7). On peut donner la démonstration directe suivante : Posons

$$h = (h_1, h_2, \ldots, h_n, \ldots) = (p.Id_{\mathbb{W}} - VF)\ (x_1, \ldots, x_n, \ldots) \ .$$

On sait que $h_i \in \mathbb{Z}[x_1, x_2, \ldots, x_i]$, et il suffit de démontrer que h_i est divisible par p pour tout i pour prouver la proposition. Or on trouve que

$$\phi_i(h) = p\phi_i(x) - \phi_i(VF(x)) = p^i x_i$$

d'où l'on déduit que $h_1 = px_1$,

$$\phi_2(h) = h_1^p + ph_2 = p^2 x_2 \quad \text{d'où} \quad h_2 = p(x_2 - p^{p-2} x_1) \ ,$$

et par récurrence sur i , on en déduit que pour tout i on a $h_i = pk_i$.

Notons en particulier que dans $\mathbb{W}_{\mathbb{F}_p}$ on a $p = (0,1,0,\ldots)$ (car $(1,0,0,\ldots)$ est l'unité de $\mathbb{W}$).

3. L'ind-schéma $\vec{\mathbb{W}}$ et l'ind-schéma $\vec{\mathbb{W}}'$

On définit

$$\vec{\mathbb{W}} = \varinjlim_n (\mathbb{W}_n, T_n) \ .$$

C'est un ind-schéma en groupes dont le ind-schéma sous-jacent est isomor-

phe à $\mathbb{E}^{(\mathbb{N})}$, c'est-à-dire que pour tout anneau A ,

$$\underset{\rightarrow}{\mathbb{W}}(A) = A^{(\mathbb{N})} = \{(x_1,x_2,\ldots,x_n,\ldots) \ , \ x_i \in A \ , \ x_i = 0 \ \text{ sauf un nombre fini}\}$$

Mais ce foncteur a une structure additive qui n'est pas la structure habituelle de $\mathbb{E}^{(\mathbb{N})}$.

On peut définir un autre système inductif naturel à l'aide des morphismes

$$\mathbb{W}_n \xrightarrow{T_n F_n} \mathbb{W}_{n+1} \ .$$

On a alors des diagrammes commutatifs

$$\begin{array}{ccc} \mathbb{W}_n & \xrightarrow{T_n} & \mathbb{W}_{n+1} \\ \Big\downarrow{\scriptstyle F_n^{n-1}} & & \Big\downarrow{\scriptstyle F_{n+1}^{n}} \\ \mathbb{W}_n & \xrightarrow{T_n F_n = F_{n+1} T_n} & \mathbb{W}_{n+1} \end{array} \ ,$$

car $T_n F_n = F_{n+1} T_n$. Par définition, on pose

$$\underset{\rightarrow}{\mathbb{W}'} = \varinjlim (\mathbb{W}_n, T_n F_n) \ .$$

En caractéristique 0 , $\underset{\rightarrow}{\mathbb{W}'}$ n'a aucune structure naturelle de Groupe, mais en caractéristique p, $\underset{\rightarrow}{\mathbb{W}'}$ est un ind-schéma en groupes, et on a un morphisme additif

$$u : \underset{\rightarrow}{\mathbb{W}}_{\mathbb{F}_p} \to \underset{\rightarrow}{\mathbb{W}'}_{\mathbb{F}_p}$$

obtenu par passage à la limite des F^{n-1} .

Notons qu'en caractéristique p, les morphismes de transition TF ne sont autres que <u>la multiplication par</u> p puisque l'on a $TFR = FTR = FV = p.Id$

<u>Remarque</u>. Si A est un anneau <u>parfait</u> de caractéristique p, u induit un isomorphisme

$$u(A) : \mathbb{W}_{\overrightarrow{F}_p}(A) \to \mathbb{W}'_{\overrightarrow{F}_p}(A)$$

puisque c'est vrai pour chaque $F^n(A)$.

4. <u>L'anneau</u> W

4.1. On rappelle que (voir J.-P. Serre, "Corps locaux" II, §6, th.7) que si k est un corps parfait de caractéristique p, l'anneau

$$W = \mathbb{W}(k) = \varprojlim_{\leftarrow} W_n \qquad (W_n = \mathbb{W}_n(k))$$

est un anneau de valuation discrète, complet, de corps résiduel k, d'uniformisante $p = (0,1,0,0,\ldots)$, dont l'homomorphisme d'augmentation est donné par la projection canonique

$$W \to W_1 = k .$$

On peut d'ailleurs montrer (loc. cit. II, §5, th. 3) que ces propriétés caractérisent l'anneau W à un isomorphisme unique près (théorème de Cohen).

De plus, le corps des fractions de W,

$$K = W[1/p]$$

est de caractéristique nulle.

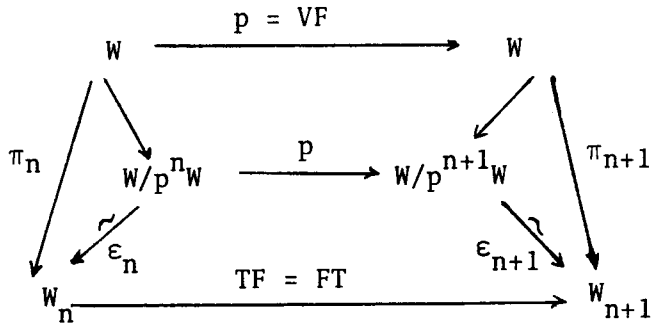
Comme k est parfait, l'homomorphisme u définit un isomorphisme de groupes

$$u(k) : \underset{\rightarrow}{\mathbb{W}}(k) \rightarrow \underset{\rightarrow}{\mathbb{W}}'(k) \quad .$$

Remarquons alors que la projection naturelle $\pi_n : W \rightarrow W_n$ définit un isomorphisme

$$\varepsilon_n : W/p^n W \xrightarrow{\sim} W_n$$

et l'on vérifie immédiatement que l'on a un diagramme commutatif



Utilisant alors l'isomorphisme naturel (de W-modules) valable pour tout anneau de valuation discrète

$$\varinjlim(W/p^n W, p) \xrightarrow{\sim} K/W$$

on déduit de ce qui précède que $\underset{\rightarrow}{\mathbb{W}}'(k)$ et donc $\underset{\rightarrow}{\mathbb{W}}(k)$ est isomorphe au module dualisant K/W . Comme K/W est un W-module, on déduit une structure de W-module sur $\underset{\rightarrow}{\mathbb{W}}(k)$ par transport de structure.

Proposition 4.2. Cetre structure se prolonge de manière unique en une structure de ind-schéma en groupes à anneau d'opérateurs W sur

$$\underset{\rightarrow}{\mathbb{W}}_k = \varinjlim(\mathbb{W}_n)_k, T)$$

en faisant opérer $\lambda \in W$ sur $(\mathbb{W}_n)_k$ par multiplication par $F^{1-n}(\lambda)$.

Remarquons que l'élément $F^{1-n}(\lambda) \in W$ est bien défini, car k étant parfait, $F : W \to W$ est un isomorphisme. Cette multiplication a un sens car, pour toute k-algèbre A , $\mathbb{W}_n(A)$ est une W-algèbre via le morphisme

$$W = \mathbb{W}(k) \xrightarrow{\pi_n} \mathbb{W}_n(k) \to \mathbb{W}_n(A) \ .$$

Pour que cette action se transporte à $\underset{\to k}{\mathbb{W}}$, il faut montrer que l'action de $\lambda \in W$ commute aux morphismes T . On vérifie immédiatement qu'il suffit de montrer que pour toute k-algèbre A , on a :

$$\forall\ x \in \mathbb{W}_n(A)\ ,\ \forall\ \lambda' \in \mathbb{W}_{n+1}(A)\ ,\ \lambda'.T(x) = T(FR(\lambda').x)$$

ou, ce qui revient au même, puisque R est une surjection :

$$\forall\ \lambda'\ ,\ y \in \mathbb{W}_{n+1}(A)\ ,\ \lambda'.V(y) = V(F(\lambda').y) \ .$$

Or, si A est un anneau parfait, F est un isomorphisme, et cette relation est vérifiée car

$$F(\lambda'.V(y)) = F(\lambda')\ FV(y) = F(\lambda').py = p[F(\lambda').y] = FV[F(\lambda').y] \ .$$

Dans le cas général, il suffit de remarquer que $\lambda'.V(y)$ et $V(F(\lambda').y)$ s'expriment à l'aide de polynômes à coefficients dans $\mathbb{Z}/p\mathbb{Z}$. D'après ce qui précède, ces polynômes prennent la même valeur si les variables sont prises dans un anneau parfait, par exemple la clôture algébrique de k . On en déduit qu'ils sont égaux.

Enfin, il faut montrer que cette structure sur $\underset{\rightarrow k}{\mathbb{W}}$ induit sur $\underset{\rightarrow}{\mathbb{W}}(k)$ la structure précédemment définie. Or il est immédiat (et cela prouve l'unicité de la structure sur $\underset{\rightarrow k}{\mathbb{W}}$) que la multiplication par $F^{1-n}(\lambda)$ sur $W_n(k) = W_n$ induit sur W/p^nW la multiplication par λ via les isomorphismes

$$W_n \xrightarrow[\sim]{F^{n-1}} W_n \xleftarrow[\sim]{\varepsilon_n} W/p^nW \ .$$

Remarques. Il n'y a pas en général d'action de $\mathbb{W}_k$ sur $\underset{\rightarrow k}{\mathbb{W}}$ mais seulement de $W = \mathbb{W}(k)$ sur $\underset{\rightarrow k}{\mathbb{W}}$.

Cette construction est fonctorielle en k et est valable pour tout anneau parfait A (mais $\mathbb{W}(A)$ n'est plus en général un anneau de valuation discrète).

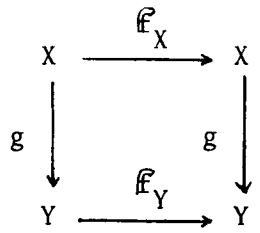
5. Les morphismes de Frobenius et de Verschiebung d'un schéma en groupes

Dans tout ce qui suit, on suppose que tous les schémas sont des schémas sur le corps premier $\mathbb{F}_p$.

5.1. Si X est un schéma, on appelle morphisme de Frobenius absolu de X et on note

$$\mathbf{f}_X : X \to X$$

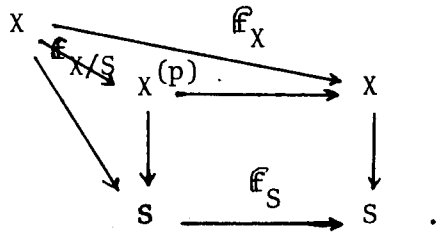
l'endomorphisme de X qui est l'identité sur l'espace sous-jacent et qui associe à une section s de $\underline{\mathcal{O}}_X$ la section s^p . Si Y est un autre schéma, et $g : X \to Y$ un morphisme, le carré suivant est commutatif :



On obtient donc un endomorphisme $\mathfrak{F}$ du foncteur identique de $Sch/\mathbb{F}_p$.

5.2. Soit S un schéma fixé et X un S-schéma. On note $X^{(p/S)}$ ou simplement $X^{(p)}$ le S-schéma image réciproque de X par le changement de base $\mathfrak{F}_S : S \to S$.

Le diagramme ci-dessus étant commutatif, il existe une flèche unique $\mathfrak{F}_{X/S}$ telle que le diagramme suivant soit commutatif :



On appellera le morphisme $\mathfrak{F}_{X/S}$ ainsi défini le <u>morphisme de Frobenius relatif de</u> X <u>au-dessus de</u> S .

L'application $X \to \mathfrak{F}_{X/S}$ est un morphisme fonctoriel du foncteur identique de Sch/S dans le foncteur $X \to X^{(p/S)}$. Ce dernier foncteur commute aux limites projectives finies, donc si X est un S-groupe, $X^{(p/S)}$ l'est aussi et, $\mathfrak{F}_{X/S}$ étant fonctoriel, est un morphisme de groupes.

La construction de $X^{(p/S)}$ commute aux changements de base, c'est-à-dire que pour tout morphisme $T \to S$, on a

$$(X \underset{S}{\times} T)^{(p/T)} \overset{\sim}{=} X^{(p/S)} \underset{S}{\times} T \ .$$

Enfin, si S est le spectre du corps premier $\mathbb{F}_p$, $X^{(p/S)} = X$ et $\mathfrak{f}_{X/S} = \mathfrak{f}_X$.

5.3. Soit G un S-chéma en groupes commutatifs plat.

On sait définir un homomorphisme canonique de groupes, fonctoriel en G

$$\mathbb{V}_G : G^{(p/S)} \to G$$

appelé homomorphisme de Verschiebung de G sur S qui a les propriétés suivantes :

$$\boxed{\mathfrak{f}_{G/S} \circ \mathbb{V}_G = p\ \mathrm{Id}_{G^{(p)}} \qquad \mathbb{V}_G \circ \mathfrak{f}_{G/S} = p\ \mathrm{Id}_G}$$

(pour la définition de $\mathbb{V}_G$ et la démonstration, voir S.G.A. 3, VII_A, 4.2-4.3).

Dans la plupart des cas, la seconde formule suffit pour calculer $\mathbb{V}_G$. En effet, si G est lisse alors $\mathfrak{f}_{G/S}$ est un épimorphisme. Si H se plonge dans un groupe lisse G, $\mathbb{V}_H$ est aussi déterminé car $\mathbb{V}_H$ est induit par $\mathbb{V}_G$. La plupart des groupes que l'on considérera sont finis localement libres sur la base, et on montrera plus loin qu'ils se plongent canoniquement dans un groupe lisse.

Le morphisme $\mathbb{V}_G$ est fonctoriel en G et commute aux changements de base. Si $S = \mathrm{Spec}(\mathbb{F}_p)$ et si G est le groupe $\mathbb{W}$ des vecteurs de Witt, le morphisme de Frobenius et la Verschiebung coïncident avec ceux définis au §2.

5.4. Pour tout $n \geq 1$, on définit les schémas

$$X^{(p^n)} = X^{(p^n/S)} = [X^{(p^{n-1}/S)}]^{(p/S)} .$$

On note $\mathcal{F}^n_{X/S}$ le morphisme composé

$$\mathcal{F}^n_{X/S} : X \xrightarrow{\mathcal{F}_{X/S}} X^{(p)} \xrightarrow{\mathcal{F}_{X^{(p)}/S}} X^{(p^2)} \to \ldots \xrightarrow{\mathcal{F}_{X^{(p^{n-1})}/S}} X^{(p^n)} .$$

De même, si G est un schéma en groupes commutatifs plat sur S, on note $\mathcal{V}^n_G$ le composé

$$\mathcal{V}^n_G : G^{(p^n)} \xrightarrow{\mathcal{V}_{G^{(p^{n-1})}}} G^{(p^{n-1})} \to \ldots \xrightarrow{\mathcal{V}_G} G .$$

On a alors la conséquence facile des relations de 5.3. (correspondant au cas $n = 1$) :

$$\mathcal{V}^n_G \circ \mathcal{F}^n_{G/S} = p^n \, Id_G , \quad \mathcal{F}^n_{G/S} \circ \mathcal{V}^n_G = p^n \, Id_{G^{(p^n)}} .$$

$\mathcal{F}^n_{X/S}$ et $\mathcal{V}^n_G$ s'appellent respectivement le <u>$n^{\text{ième}}$ itéré du Frobenius relatif de</u> G <u>sur</u> S et la <u>$n^{\text{ième}}$ itéré de la Verschiebung de</u> G <u>sur</u> S. Dans le cas où la base S est le spectre du corps premier $\mathbb{F}_p$, ce sont bien les itérés de $\mathcal{F}_{G/S}$, $\mathcal{V}_G$ au sens habituel.

CHAPITRE II

GROUPES FINIS LOCALEMENT LIBRES ET THEORIE CLASSIQUE DE DIEUDONNE

1. Rappels généraux sur les groupes finis localement libres

1.1. Soit S un schéma et soit G un schéma en groupes fini et localement libre sur S. Il est équivalent de dire que $G = \operatorname{Spec} A$, où A est une $\underline{\mathcal{O}}_S$-algèbre quasi cohérente finie localement libre, la structure de groupe étant décrite par des homomorphismes de $\underline{\mathcal{O}}_S$-algèbres

$$\Delta : A \to A \underset{\underline{\mathcal{O}}_S}{\otimes} A$$

$$I : A \to A$$

$$\varepsilon : A \to \underline{\mathcal{O}}_S$$

où Δ, I, ε correspondent respectivement à la loi de composition, à l'application $x \to x^{-1}$ et à la section unité, ces morphismes satisfaisant des relations évidentes exprimant l'associativité, etc. Ainsi, A muni de sa loi d'algèbre $\mu : A \otimes A \to A$ et de Δ devient une bigèbre.

Le noyau J de ε s'appelle l'idéal d'augmentation du groupe G.

Dans tout ce qui suit, on supposera, sauf mention contraire, que tous les groupes considérés sont commutatifs.

1.2. Si $s \in S$, on appelle rang de G en s le rang sur $k(s)$

de $A \otimes_{\underline{\mathcal{O}}_S} k(s)$. L'application $s \to$ rang de G en s est une application localement constante sur S . Si ce rang est constant égal à n , on dit que G est un groupe de rang n sur S .

1.3. Exemples de groupes finis localement libres

1.3.1. Soit G un groupe (abstrait) d'ordre n . Soit $\underline{G}_S$ le faisceau constant sur S défini par

$$\underline{G}_S(S') = G$$

pour tout S-schéma S' . $\underline{G}_S$ est un groupe libre de rang n sur S ; en effet son algèbre affine est isomorphe à $\underline{\mathcal{O}}_S^n$.

1.3.2. Soit $\mathbb{G}_{m|S}$ le groupe multiplicatif sur S , défini par

$$\mathbb{G}_{m|S}(S') = \Gamma(S', \underline{\mathcal{O}}_{S'})^*$$

pour tout S-schéma S' . Pour tout $n \geq 1$, on a l'isomorphisme

$$n\,\mathrm{Id} : \mathbb{G}_{m|S} \to \mathbb{G}_{m|S} \qquad x \to x^n .$$

Par définition, $\mu_{n|S}$, groupe des racines $n^{\text{ièmes}}$ de l'unité sur S , est le noyau de cet homomorphisme. C'est un groupe libre fini derang n sur S ; en effet, son algèbre affine est isomorphe à $\underline{\mathcal{O}}_S[T]/(T^n-1)$.

1.3.3. Soit $\mathbb{G}_{a|S}$ le groupe additif sur S , défini par

$$\mathbb{G}_{a|S}(S') = \Gamma(S', \underline{\mathcal{O}}_{S'})$$

pour tout S-schéma S' . Si S est un schéma sur le corps premier $\mathbb{F}_p$, on a un homomorphisme de Frobenius

$$F : \mathbb{G}_{a|S} \to \mathbb{G}_{a|S} \qquad x \to x^p .$$

On désigne par $\alpha_{p|S}$ le noyau de F. C'est un groupe libre fini de rang p sur S, d'algèbre affine isomorphe à $\underline{\mathcal{O}}_S[T]/T^p$.

1.4. Dualité de Cartier

Pour tout schéma en groupes (commutatif) G sur S, on pose :

$$G^* = \underline{\mathrm{Hom}}_{S\text{-gr}}(G, \mathbb{G}_{m|S}) .$$

On définit ainsi un foncteur contravariant $G \to G^*$ de la catégorie des groupes sur S dans elle-même ; ce foncteur commute aux changements de base.

Si $G = \mathrm{Spec}(A)$ est fini localement libre sur S, on montre (SGA 3, VII_A, 3.3.1) que l'on a

$$G^* = \mathrm{Spec}(\check{A})$$

avec

$$\check{A} = \underline{\mathrm{Hom}}_{\underline{\mathcal{O}}_S\text{-mod}}(A, \underline{\mathcal{O}}_S) ,$$

la structure de bi-algèbre sur $\check{A}$ étant définie à l'aide des transposés des morphismes Δ et μ de 1.1. G^* est donc aussi un groupe fini localement libre sur S, et G^* est de même rang que G. De plus, l'homomorphisme fonctoriel canonique $G \to (G^*)^*$ déduit de la définition de G^* est défini par l'isomorphisme $A \xrightarrow{\sim} (\check{A})^{\check{}}$, et est donc un isomorphisme :

$$G \xrightarrow{\sim} (G^*)^* .$$

On définit donc ainsi une anti-équivalence de la catégorie des S-schémas en groupes (commutatifs) finis localement libres avec elle-même, appelée dualité de Cartier.

Si l'on suppose que S est un schéma sur $\mathbb{F}_p$, on a défini (I.5) le schéma en groupes $G^{(p/S)}$ et les morphismes de Frobenius relatif $\mathfrak{F}_{G/S}$ et de Verschiebung $\mathfrak{V}_G$. Si G est fini localement libre sur S, $G^{(p/S)}$ l'est aussi et on montre alors (SGA 3, VII_A, 4.3.3) que la dualité de Cartier échange les morphismes de Frobenius relatif et de Verschiebung, i.e. on a :

$$(\mathfrak{V}_G)^* = \mathfrak{F}_{G^*/S} \quad ; \quad (\mathfrak{F}_{G/S})^* = \mathfrak{V}_{G^*} \quad .$$

1.5. Exemples

a) Soit $\underline{G}_S$ le groupe fini sur S attaché au groupe fini (abstrait) G (1.3.1). On vérifie aisément que l'algèbre affine de $(\underline{G}_S)^*$ est isomorphe à $\underline{\mathcal{O}}_S[G]$, la $\underline{\mathcal{O}}_S$-algèbre du groupe G, l'application diagonale provenant de l'application diagonale $G \to G \times G$. Si $G = \mathbb{Z}/n\mathbb{Z}$, on trouve

$$(\mathbb{Z}/n\mathbb{Z})^*_S \simeq \mu_{n|S} \quad ,$$

qui résulte aussi directement des définitions.

b) En caractéristique p, on montre que l'on a

$$(\alpha_{p|S})^* \simeq \alpha_{p|S} \quad .$$

1.6. Quotients de groupes finis localement libres

Soit $\mu : G' \to G$ un monomorphisme de groupes finis localement libres sur S, et soit $G'' = G/G'$ le faisceau quotient (pour la topologie f.p.p.f.). On a donc une suite exacte de faisceaux

$$0 \to G' \xrightarrow{\mu} G \xrightarrow{p} G'' \to 0 \quad .$$

On prouve (SGA 3, V, 4.1) que G'' est <u>représentable par un schéma en groupes finis localement libre sur</u> S, et que p est fidèlement plat, de sorte que G est fini localement libre sur G'', de rang relatif égal au rang de G'. Par transitivité, on en conclut donc que

$$\text{rang}(G) = \text{rang}(G') \cdot \text{rang}(G'') \ .$$

Par ailleurs, on montre que si dans la suite exacte de faisceaux ci-dessus, on suppose G' et G'' représentables par des schémas en groupes finis localement libres sur S, alors G est lui aussi représentable par un groupe fini localement libre sur S. C'est-à-dire qu'une extension de groupes finis localement libres est encore finie localement libre.

1.7. Soit ℓ un nombre premier. On appelle <u>composante ℓ-primaire</u> du groupe G sur S le sous-groupe

$$G(\ell) = \varinjlim_{n} \text{Ker}\{G \xrightarrow{\ell^n \text{Id}} G\} \quad ;$$

c'est le plus grand sous-groupe de ℓ-torsion de G.

Si G est fini localement libre sur S, on prouve que G est localement annulé par un entier n (SGA 3, VIII, 7.3), et donc chacune de ses composantes ℓ-primaires est localement annulée par une puissance de ℓ (i.e. est un ℓ-groupe), et G admet alors une décomposition canonique (comme faisceau f.p.p.f.) en ses composantes ℓ-primaires :

$$G = \coprod_{\ell} G(\ell) \ .$$

Si S est quasi compact, G est annulé par un entier n, et cette décomposition est finie. Par ailleurs, les $G(\ell)$ sont des schémas en groupes finis localement libres, en tant que facteurs directs de G qui l'est.

Nous nous intéresserons ici aux groupes pour lesquels on a $G = G(p)$, c'est-à-dire aux groupes finis localement libres sur S qui sont localement annulés par une puissance de p. Si G est un tel p-groupe, son dual G^* est aussi un p-groupe.

2. Types particuliers de groupes

2.1. Soit G un groupe fini localement libre sur une base quelconque S.

2.1.1. On dit que G est <u>infinitésimal sur</u> S (ou est <u>radiciel</u>) si l'une des conditions équivalentes suivantes est vérifiée :

- l'idéal d'augmentation J de G (1.1) est localement nilpotent.
- $\forall\, s \in S$, G_s est connexe.
- $\forall\, s \in S$, G_s ne possède qu'un seul point.
- $\forall\, s \in S$, $G_{\overline{s}}$ ne possède qu'un seul point, (où $G_{\overline{s}}$ désigne la fibre géométrique de G au-dessus de s).

2.1.2. On dit que G est <u>étale</u> au-dessus de S si le morphisme structural de G est étale. Il est équivalent de dire que $\forall\, s \in S$, G_s est étale sur $k(s)$, ou encore que $G_{\overline{s}}$ est réduit pour tout $s \in S$, ou encore que G est localement (pour la topologie étale, ou f.p.p.f.) isomorphe à un groupe constant.

2.1.3. On dit que G est <u>unipotent</u> si G^* est infinitésimal (voir SGA 3, XVII, pour une définition générale des groupes unipotents).

2.1.4. On dit que G est de <u>type multiplicatif</u> sur S si G^* est étale. Cela équivaut au fait que pour tout $s \in S$, G_s est de type multiplicatif, ou encore à ce que G se plonge localement pour la topologie étale dans $(\mathbb{G}_{m|S})^r$.

2.1.5. On dit que G est <u>bi-infinitésimal</u> sur S s'il est infinitésimal et unipotent (i.e. G et G^* sont infinitésimaux).

2.2. Si G est étale et localement annulé par une puissance de p sur un $\mathbb{F}_p$-schéma S, alors G^* est infinitésimal. En d'autres termes, sur une base de catactéristique p, tout p-groupe de type multiplicatif est infinitésimal. En effet, pour tout $s \in S$, $G_{\overline{s}}$ est isomorphe au groupe constant $G(\overline{k})_{\overline{k}}$ (où l'on désigne par $\overline{k}$ la clôture algébrique du corps résiduel en s). D'après 1.5.1 l'algèbre affine de $(G_{\overline{s}})^* = (G^*)_{\overline{s}}$ s'identifie à l'algèbre $\overline{k}[G(\overline{k})]$ du groupe $G(\overline{k})$. On vérifie alors immédiatement que l'idéal de $\overline{k}[G(\overline{k})]$, formé des éléments $\sum_{g \in G(\overline{k})} \lambda_g . g$, $\lambda_g \in \overline{k}$ tels que $\sum_g \lambda_g = 0$, est maximal et nilpotent car $G(\overline{k})$ est annulé par une puissance de p et $\overline{k}$ est de caractéristique p. Donc $(G^*)_{\overline{s}}$ se réduit à un point et G^* est infinitésimal.

2.3. Soit

$$0 \to G' \xrightarrow{\mu} G \xrightarrow{\pi} G'' \to 0$$

une suite exacte de groupes finis localement libres. Alors G est infinitésimal (resp. étale, resp. unipotent, resp. de type multiplicatif, resp.

bi-infinitésimal) si et seulement si G' et G'' sont infinitésimaux (resp. étales, resp. unipotents, resp. de type multiplicatif, resp. bi-infinitésimaux).

On vérifie aisément l'assertion dans le cas infinitésimal et dans le cas étale en se ramenant au cas où S est le spectre d'un corps algébriquement clos. Les autres cas s'en déduisent par dualité de Cartier.

2.4. Exemples de p-groupes en caractéristique p .

$(\mathbb{Z}/p\mathbb{Z})_S$ est étale sur S et $\mu_{p|S} = (\mathbb{Z}/p\mathbb{Z})^*_S$ est donc de type multiplicatif. Par ailleurs, $\alpha_{p|S} = (\alpha_{p|S})^*$ est bi-infinitésimal. Parmi ces 3 groupes, $\alpha_{p|S}$ et $(\mathbb{Z}/p\mathbb{Z})_S$ sont les groupes unipotents tandis queles groupes infinitésimaux sont $\alpha_{p|S}$ et $\mu_{p|S}$.

L'intérêt de ces trois groupes réside dans le résultat suivant : si S est le spectre d'un corps algébriquement clos et de caractéristique p , tout groupe annulé par une puissance de p et fini sur S admet une suite de composition finie

$$G \supset G_0 \supset G_1 \supset G_2 \ldots \supset G_{n-1} \supset G_n$$

où les G_i/G_{i+1} sont isomorphes à l'un des groupes α_p , μ_p , $\mathbb{Z}/p\mathbb{Z}$. De plus, il résulte de 2.4. que G est infinitésimal (resp. étale, resp. unipotent, resp. de type multiplicatif, resp. bi-infinitésimal) si et seulement si tous les G_i/G_{i+1} sont isomorphes à α_p ou μ_p (resp. $\mathbb{Z}/p\mathbb{Z}$, resp. $\mathbb{Z}/p\mathbb{Z}$ ou α_p , resp. μ_p , resp. α_p). (cf. SGA 3, XVII, 1.7. et 4.2.1).

2.5. Supposons que S soit un $\mathbb{F}_p$-schéma. Pour tout groupe fini localement libre sur S on définit alors les morphismes de Frobenius relatif et de Verschiebung (I,5). On a les critères suivants :

2.5.1. G est infinitésimal $\Leftrightarrow$ $\mathfrak{f}_{G/S}$ est localement nilpotent.

2.5.2. G est unipotent $\Leftrightarrow$ $\mathfrak{v}_G$ est localement nilpotent.

2.5.3. G est bi-infinitésimal $\Leftrightarrow$ $\mathfrak{f}_{G/S}$ et $\mathfrak{v}_G$ sont localement nilpotents.

2.5.4. G est étale $\Leftrightarrow$ $\mathfrak{f}_{G/S}$ est un isomorphisme.

2.5.5. G est de type multiplicatif $\Leftrightarrow$ $\mathfrak{v}_G$ est un isomorphisme.

Il suffit de prouver les assertions 2.5.1. et 2.5.4., les autres s'en déduisant, d'après 1.4. par dualité de cartier.

Démonstration de 2.5.1.

Soit $\varepsilon : S \to G$ la section unité de G (G est considéré comme schéma en "ensembles pointés" grâce à cette section ε). Nous allons caractériser le "noyau" de $\mathfrak{f}^n_{G/S}$ pour tout S-schéma G muni d'une section. On vérifie immédiatement que le noyau de $\mathfrak{f}^n_{G/S}$ est défini par l'idéal engendré par $F^n(J) \subset \underline{O}_G$, image de l'idéal d'augmentation par le morphisme $x \to x^{p^n}$; désignons par J_n cet idéal. On a évidemment $J_n \subset J^{p^n}$. Si J est de type fini, on peut supposer qu'il a moins de p^k générateurs, pour un entier k convenable, et on vérifie immédiatement que l'on a alors

$$J^{p^{n+k}} \subset J_n ,$$

de sorte que les J_n forment un système cofinal aux J^{p^n} .

On en déduit donc que, si G est localement de type fini sur S, $\mathfrak{f}_{G/S}$ est localement nilpotent si et seulement si J est localement nilpotent. Pour un groupe fini localement libre sur S cela équivaut au fait qu'il est infinitésimal.

Démonstration de 2.5.4.

On montre d'une manière générale (SGA 5, XIV (Houzel)) que si G est un schéma localement de présentation finie sur S, $\mathfrak{f}_{G/S}$ est un isomorphisme si et seulement si G est étale sur S.

3. Décomposition d'un p-groupe fini localement libre sur une base de caractéristique p réduite à un point s.

3.1. G étant un groupe fini localement libre sur S, on a une suite exacte canonique, fonctorielle en G

$$(*) \qquad 0 \to G^0 \to G \to G^{et} \to 0$$

où G^0 est la composante neutre de G et $G^{et} = G/G^0$. Le sous-groupe G^0 est ouvert dans G (SGA_3, VI_B, 3.9), il est donc fini localement libre sur S et c'est le plus grand sous-groupe infinitésimal de G. Le groupe quotient G^{et} est étale, (SGA 3, VI_A, 5.5) et il est fini localement libre sur S, d'après 1.6.

Appliquant la même construction à G^*, on obtient un sous-groupe $G^{mult} = (G^*/(G^*)^0)^*$, qui est le plus grand sous-groupe de type multiplicatif de G.

Si $k(s)$ est de caractéristique p et si G est annulé par une puissance de p, G^{mult} est infinitésimal (2.2) et on a donc des inclusions

$$0 \subset G^{mult} \subset G^0 \subset G$$

où $G/G^0 = G^{et}$ est étale, G^0/G^{mult} est bi-infinitésimal (car c'est un quotient d'un groupe infinitésimal et son dual s'identifie à $((G^0)^*)^0$.

Cette suite de composition de G est fonctorielle en G, et on vérifie qu'elle commute aux produits finis.

3.2. Si S est le spectre d'un corps parfait de caractéristique p, la projection canonique $G \to G^{et}$ induit un isomorphisme de G_{red} sur G^{et} et la suite exacte (*) splitte canoniquement (SGA 3, XVII, 1.6), et on a donc

$$G = G^0 \times G^{et} .$$

De même la suite exacte

$$0 \to G^{mult} \to G^0 \to G^0/G^{mult} \to 0$$

est splittée car la suite duale l'est. On obtient donc une décomposition canonique, fonctorielle en G :

$$G = G^{mult} \times G^{bi} \times G^{et}$$

où G^{mult}, $G^{bi} = G^0/G^{mult}$, G^{et} sont respectivement de type multiplicatif, bi-infinitésimal et étale. La partie unipotente de G est alors $G^{bi} \times G^{et}$ et la partie infinitésimale est $G^{mult} \times G^{bi}$.

On a les équivalences :

G est infinitésimal $\Leftrightarrow G^{et} = 0$

G est étale $\Leftrightarrow G^{mult} = G^{bi} = 0$

G est unipotent $\Leftrightarrow G^{mult} = 0$

G est bi-infinitésimal $\Leftrightarrow G^{mult} = G^{et} = 0$

G est de type multiplicatif $\Leftrightarrow G^{bi} = G^{et} = 0$.

3.3. La catégorie des p-groupes étales finis sur un corps parfait k est bien connue. Elle est équivalente à la catégorie des p-groupes finis sur lesquels opère le groupe fondamental $\pi_1(k) = Gal(\overline{k}/k)$. Par dualité de Cartier, la catégorie des p-groupes finis de type multiplicatif est équivalente à la catégorie opposée de celle des p-groupes étales. Par ailleurs, la catégorie des p-groupes finis sur lesquels opère $\pi_1(k)$ est équivalente à sa propre opposée par dualité de Prontryagin. On en déduit une équivalence de catégories entre la catégorie des p-groupes finis de type multiplicatif avec celle des p-groupes finis sur lesquels opère $\pi_1(k)$.

4. Théorie de Dieudonné sur un corps parfait

4.1. Soit k un corps parfait de caractéristique $p > 0$ et soit p-Gr-fin(k) la catégorie des schémas en groupes finis sur k et annulés par une puissance de p . Le but de la théorie de Dieudonné est d'établir une anti-équivalence entre la catégorie p-Gr-fin(k) et une catégorie de modules que nous allons définir.

On appelle anneau de Dieudonné $\mathcal{D}$ l'anneau W[F,V] (non commutatif) engendré sur l'anneau local $W = W(k)$ (I,4) par des indéterminées

F et V satisfaisant les relations suivantes :

$$F \cdot \lambda = \lambda^{\sigma} \cdot F$$

$$\lambda \cdot V = V \cdot \lambda^{\sigma}$$

$$F \cdot V = V \cdot F = p \ ,$$

pour tout $\lambda \in W$ et où l'on note par λ^{σ} l'image de λ par le morphisme de Frobénius de W .

On appelle <u>catégorie des modules de Dieudonné</u> la catégorie $\underline{\mathrm{Mod}}_{\mathcal{D};W\ \ell.f.}$ des $\mathcal{D}$-modules à gauche tels que le W-module sous-jacent soit de longueur finie. On voit en particulier qu'un tel module est annulé par une puissance de p .

Un objet de $\underline{\mathrm{Mod}}_{\mathcal{D};W\ \ell.f.}$ est donc un W-module M de longueur finie, muni de deux morphismes de W-modules

$$F_M : M^{\sigma} \to M$$

$$V_M : M \to M^{\sigma} \ ,$$

en posant

$$M^{\sigma} = M \otimes_{W} (W,\sigma) \ ,$$

(σ étant le morphisme de Frobénius de W), F_M et V_M vérifiant

$$F_M \cdot V_M = p \cdot \mathrm{Id}_M \ , \ V_M F_M = p \cdot \mathrm{Id}_M \ .$$

<u>Théorème 4.2</u>. (Dieudonné)

Il existe une équivalence de catégories

$$D^* : [p\text{-Gr-fin}(k)]^0 \xrightarrow{\approx} \underline{\mathrm{Mod}}_{\mathcal{D},W\ \ell.f.}$$

telle que l'on ait un isomorphisme canonique $[D^*(G)]^{\sigma} \approx D^*(G^{(p)})$

donnant lieu aux identifications suivantes:

$$D^*(\mathbf{f}_{G/k}) = F_{D^*(G)}$$
$$D^*(\mathbf{v}_G) = V_{D^*(G)} .$$

Corollaire 4.2.1. On a les équivalences suivantes :

G est infinitésimal <=> F opère de façon nilpotente sur $D^*(G)$.

G est unipotent <=> V opère de façon nilpotente sur $D^*(G)$.

G est bi-infinitésimal <=> F et V opèrent de façon nilpotente.

G est étale <=> F opère bijectivement sur $D^*(G)$.

G est de type multiplicatif <=> V opère bijectivement sur $D^*(G)$.

Pour une démonstration complète du théorème, se reporter au livre de P. Gabriel et M. Demazure, "Groupes algébriques". Dans ce qui suit, on donnera seulement la construction du foncteur D^* .

On observe tout d'abord que, d'après 3.2., la catégorie p-Gr-fin(k) est équivalente à la catégorie produit de la sous-catégorie pleine de p-Gr-fin(k) dont les objets sont les groupes unipotents et de la sous-catégorie pleine de p-Gr-fin(k) dont les objets sont les groupes de type multiplicatif. Il suffira donc de construire D^* séparément sur ces deux sous-catégories.

4.3. Cas des groupes unipotents

4.3.1. Pour tout groupe unipotent sur k , on pose par définition

$$D^*(G) = \mathrm{Hom}_{k\text{-}Gr}(G, \underset{\rightarrow}{\mathbb{W}})$$

où, pour abréger, on écrit $\underset{\rightarrow}{\mathbb{W}}$ pour $\underset{\rightarrow k}{\mathbb{W}}$ (I,3). On sait que W agit sur $\underset{\rightarrow}{\mathbb{W}}$ (I,4.2) et donc $D^*(G)$ est un W-module, qui est de longueur finie si G est fini sur k .

L'action de F et V sur $D^*(G)$ se définit en posant, pour tout $u \in D^*(G)$

$$F \cdot u = F_{\underset{\rightarrow}{W}} \circ u$$
$$V \cdot u = V_{\underset{\rightarrow}{W}} \circ u$$

où $F_{\underset{\rightarrow}{W}}$ et $V_{\underset{\rightarrow}{W}}$ sont les endomorphismes de Frobénius et de Verschiebung de $\underset{\rightarrow}{W}$, définis par passage à la limite des morphismes correspondant sur W_n.

On vérifie immédiatement, en revenant à la définition de l'action de W sur $\underset{\rightarrow}{W}$ et en utilisant les propriétés de $F_{\underset{\rightarrow}{W}}$ et $V_{\underset{\rightarrow}{W}}$, que ces actions font de $D^*(G)$ un $\mathcal{D}$-module.

4.3.2. Montrons que l'on a un isomorphisme canonique

$$D^*(G^{(p)}) \xrightarrow{\sim} (D^*(G))^{\sigma}$$

tel que

$$D^*(\mathfrak{F}_{G/k}) = F_{D^*(G)}$$
$$D^*(\mathfrak{V}_G) = V_{D^*(G)} \quad .$$

En effet, k étant parfait, le changement de base $k \xrightarrow{\sigma} k$ induit un isomorphisme σ-linéaire

$$\mathrm{Hom}(G, \mathbb{W}) \xrightarrow{\sim} \mathrm{Hom}(G^{(p)}, \mathbb{W}^{(p)}) \quad .$$

Mais $\underset{\rightarrow}{W}$ étant défini sur le corps premier $\mathbb{F}_p$, on a $\underset{\rightarrow}{W}^{(p)} = \underset{\rightarrow}{W}$ (car la formation de $\underset{\rightarrow}{W}^{(p)}$ commute aux changements de base, cf. I, 5.2). Par ailleurs

$$D^*(\mathfrak{F}_{G/k}) \doteq \mathrm{Hom}(G^{(p)}, \underset{\rightarrow}{W}) \to \mathrm{Hom}(G, \underset{\rightarrow}{W})$$
$$u \to u \circ \mathfrak{F}_{G/k}$$

s'identifie à $F_{D^*(G)}$ car $u \circ \tilde{f}_{G/k} = f_{\underset{\rightarrow}{W}} \circ u$ et $f_{\underset{\rightarrow}{W}}$ n'est autre que $F_{\underset{\rightarrow}{W}}$ (I, 5.3).

On fait un raisonnement analogue pour établir l'assertion relative à $D^*(\mathfrak{v}_G)$.

Si G est unipotent, il résulte de ce que $\mathfrak{v}_G$ est nilpotent (2.5.2) que $V_{D^*(G)}$ opère de façon nilpotente. On peut alors montrer, plus généralement, que le foncteur D^* définit une équivalence de catégories entre la catégorie des p-groupes affines unipotents sur k avec la catégorie des $\mathcal{D}$-modules sur lesquels V est localement nilpotent. On a en particulier :

Corollaire 4.3.3 On a des équivalences de catégories :

$$\left(\begin{array}{l}\text{p-groupes finis}\\ \text{unipotents sur } k\end{array}\right)^0 \xrightarrow[\approx]{D^*} \left(\begin{array}{l}\text{sous-catégorie pleine de } \underline{\mathrm{Mod}}_{\mathcal{D},W}\ \ell.f\\ \text{formée des objets } M \text{ où } V \text{ est nilpotent}\end{array}\right)$$

$$\left(\begin{array}{l}\text{p-groupes finis}\\ \text{étales sur } k\end{array}\right)^0 \xrightarrow[\approx]{D^*} \left(\begin{array}{l}\text{sous-catégorie pleine de } \underline{\mathrm{Mod}}_{\mathcal{D},W}\ \ell.f.\\ \text{formée des objets } M \text{ où } F \text{ est un isomorphi}\end{array}\right)$$

$$\left(\begin{array}{l}\text{p-groupes finis}\\ \text{bi-infinitésimaux}\end{array}\right)^0 \xrightarrow[\approx]{D^*} \left(\begin{array}{l}\text{sous-catégorie pleine de } \underline{\mathrm{Mod}}_{\mathcal{D},W}\ \ell.f.\\ \text{formée des objets où } F \text{ et } V \text{ sont nilpoten}\end{array}\right)$$

Cela résulte de la description de F et V (4.3.2) et de la caractérisation de chaque type de groupes à l'aide des morphismes $\tilde{f}$ et $\mathfrak{v}$ (2.5).

4.4. Cas des groupes de type multiplicatif

On désire construire une équivalence de catégories.

$$\left(\begin{array}{l}\text{p-groupes finis sur } k\\ \text{de type multiplicatif}\end{array}\right)^0 \xrightarrow[\approx]{D^*} \left(\begin{array}{l}\text{sous-catégorie pleine de } \mathrm{Mod}_{D,W\ \ell.f.}\\ \text{formée des objets où } V \text{ est un}\\ \text{isomorphisme}\end{array}\right)$$

La catégorie de droite est équivalente à la catégorie des W-modules de longueur finie munis d'un isomorphisme (W-linéaire)

$$M \xrightarrow{V} M^{\sigma} = M \otimes_W (W,\sigma)$$

(en effet, F est alors déterminé de façon unique par la relation $FV = p$). En considérant l'isomorphisme inverse, cette catégorie est encore équivalente à la catégorie des W-modules de longueur finie munis d'un isomorphisme

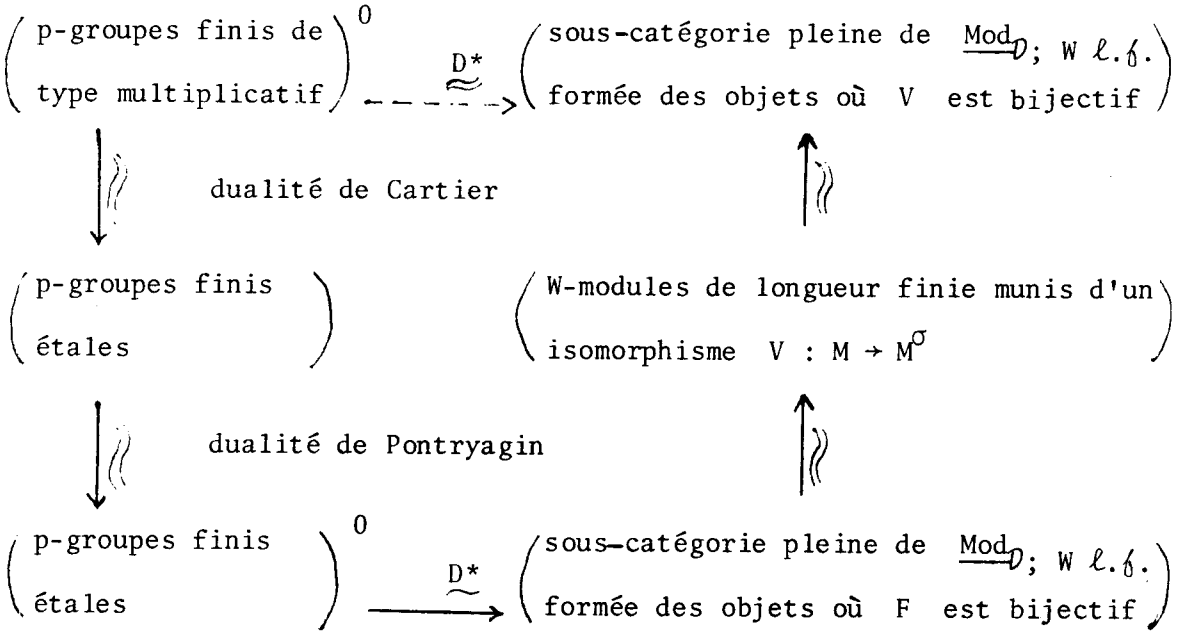
$$M^{\sigma} \xrightarrow{V^{-1}} M .$$

Mais, d'après le corollaire 4.3.3, cette catégorie est anti-équivalente à la catégorie des p-groupes finis étales sur k, qui est elle-même anti-équivalente, par dualité de Cartier, à la catégorie des p-groupes finis de type multiplicatif sur k.

Pour obtenir en définitive la bonne variance pour le foncteur D^* cherché, il suffit de remarquer qu'il existe une anti-équivalence de la catégorie des p-groupes finis étales sur k avec elle-même, donnée par la dualité de Pontryagin

$$G \to \underline{\mathrm{Hom}}_{gr}(G, \mathbb{Q}_p/\mathbb{Z}_p) .$$

Le foncteur D^* recherché est alors donné par la composition de toutes ses équivalences. La situation est résumée par le diagramme suivant :



(4.3.3)

4.5. Cas général

Si G est un p-groupe fini quelconque, on écrit, (d'après 3.2)

$$G = G^{uni} \times G^{mult}$$

où G^{uni} et G^{mult} sont respectivement unipotent et de type multiplicatif, et on pose

$$D^*(G) = D^*(G^{uni}) \times D^*(G^{mult}) .$$

Le théorème de Dieudonné 4.2. sera démontré si l'on prouve que l'on a une équivalence de catégories

$$\underline{\mathrm{Mod}}_{\mathcal{D};W\ \ell.f.} \xrightarrow{\sim} \left(\begin{array}{l}\text{sous-catégorie pleine}\\ \text{de } \underline{\mathrm{Mod}}_{\mathcal{D};W\ \ell.f.} \text{ formée}\\ \text{des objets où } V \text{ est}\\ \text{nilpotent}\end{array}\right) \times \left(\begin{array}{l}\text{sous-catégorie pleine}\\ \text{de } \underline{\mathrm{Mod}}_{\mathcal{D};W\ \ell.f.} \text{ formée}\\ \text{des objets où } V \text{ est}\\ \text{bijectif}\end{array}\right)$$

Cela résulte du lemme suivant :

Lemme. Tout $\mathcal{D}$-module M de longueur finie sur W se décompose d'une manière unique (et fonctorielle) en une somme directe

$$M = M' \times M''$$

telle que $V|M'$ est nilpotent et $V|M''$ est bijectif.

Preuve. Soit N un entier suffisamment grand pour que

$$\bigcup_{n>0} \mathrm{Ker}\ V^n = \mathrm{Ker}\ V^N \quad \text{et} \quad \bigcap_{n>0} \mathrm{Im}\ V^n = \mathrm{Im}\ V^N .$$

On a évidemment $V|\mathrm{Ker}\ V^N$ nilpotent et $V|\mathrm{Im}\ V^N$ bijectif et de plus $M = \mathrm{Ker}\ V^N \oplus \mathrm{Im}\ V^N$. Il est clair que cette décomposition est unique et fonctorielle.

5. Corollaires et compléments

Corollaire 5.1

Le foncteur D^* commute aux changements de base définis par toute extension parfaite K de k : Pour un objet G de $p\text{-Gr-fin}(k)$, on a un isomorphisme fonctoriel

$$D^*(G_K) \xleftarrow{\sim} W(K) \otimes_{W(k)} D^*(G) .$$

Preuve (d'après Oda et Oort).

On a une flèche évidente. Il suffit de considérer le cas où G est unipotent, et en considérant alors la suite de composition formée des $\mathrm{Im}\, v_G^n \subset G$, on se ramène au cas où $v_G = 0$.

Pour un tel groupe G, on a

$$D^*(G) = \mathrm{Hom}_{k\text{-}Gr}(G, \vec{\mathbb{W}}) = \mathrm{Hom}_{k\text{-}Gr}(G, \mathbb{G}_a) .$$

Par ailleurs, on a un isomorphisme

$$\mathrm{hom}_{k\text{-}Gr}(G, \mathbb{G}_a) \overset{\sim}{=} \mathrm{Ker}\{H^0(G, \underline{\mathcal{O}}_G) \xrightarrow{\Delta^* - pr_1^* - pr_2^*} H^0(G, \underline{\mathcal{O}}_G) \otimes_k H^0(G, \underline{\mathcal{O}}_G)\}$$

où $\Delta : G \times G \to G$ désigne la multiplication de G. Par le changement de base $k \to K$, on a un isomorphisme analogue, d'où l'on déduit le corollaire.

Corollaire 5.2

Pour tout p-groupe fini sur k, on a

$$\mathrm{rang}(G) = p^{\mathbf{long}_W(D^*(G))} .$$

Preuve. Il suffit de considérer le cas où G est unipotent, et par le Corollaire 5.1 on peut supposer k algébriquement clos. Alors G admet une suite de composition ne faisant intervenir que $\mathbb{Z}/p\mathbb{Z}$ et α_p (2.4). Or on établit aisément que

$$D^*(\alpha_p) \overset{\sim}{\to} k = W/pW \quad \text{avec} \quad F = V = 0$$

$$D^*(\mathbb{Z}/p\mathbb{Z}) \overset{\sim}{\to} k = W/pW \quad \text{avec} \quad V = 0 , \ F(\lambda) = \lambda p ,$$

et la formule est trivialement vérifiée.

5.3. Remarques

5.3.1. Les groupes formels et les groupes de Barsotti-Tate sur k peuvent être considérés comme limites inductives de p-groupes finis sur k. La théorie de Dieudonné permet donc de décrire ces groupes en termes de limites projectives de $\mathcal{D}$-modules de longueur finie sur W. Par exemple, on montrera (III, 5.6) que l'on a une équivalence de catégories entre la catégorie des groupes de Barsotti-Tate sur k et la catégorie des $\mathcal{D}$-modules qui sont libres et de type fini sur W.

5.3.2. Pour un p-groupe G fini sur k, il existe un isomorphisme canonique de $\mathcal{D}$-modules, fonctoriel en G :

$$D^*(G^*) \xrightarrow{\sim} \mathrm{Hom}_W(D^*(G), K/W) ,$$

où K/W désigne le module dualisant de W (c.f. Gabriel et Demazure). La structure de $\mathcal{D}$-module sur le membre de droite est définie comme suit :

Pour tout $\alpha \in \mathrm{Hom}_W(D^*(G), K/W)$ et tout $x \in D^*(G)$, on pose

$$F\cdot\alpha(x) = [\alpha(V(x))]^{\sigma}$$

$$V\cdot\alpha(x) = [\alpha(F(x))]^{\sigma^{-1}} .$$

6. Annexe: Construction du foncteur quasi inverse de D^*

Il suffit de construire le foncteur quasi inverse du foncteur

$$D^* : \left(\begin{array}{l}\text{groupes finis}\\ \text{unipotents}\end{array}\right)^0 \longrightarrow \left(\begin{array}{l}\text{sous-catégorie de } \underline{\mathrm{Mod}}_{\mathcal{D}};\ W \text{ l.f. for-}\\ \text{mée des objets où } V \text{ est nilpotent}\end{array}\right)$$

défini en 4.3. On montrera que le foncteur que l'on va construire est un

adjoint à gauche de D^* , il résultera du fait que D^* est une équivalence de catégories que c'est un foncteur quasi inverse de D^* .

6.1. Soit M un $\mathcal{D}$-module de longueur finie sur W et où V est nilpotent sur M . On lui associe le foncteur en groupes $\mathbb{E}(M)$ sur (sch/k) défini par

$$\mathbb{E}(M)(S) = \mathrm{Hom}_{\mathcal{D}}(M, \vec{\mathbb{W}}(S))$$

pour tout k-schéma S .

Il faut démontrer que $\mathbb{E}(M)$ est représenté par un p-groupe fini unipotent et que le foncteur $\mathbb{E}$ ainsi défini est adjoint à gauche de D^* .

6.2. $\mathbb{E}(M)$ est représentable par un schéma affine

On choisit un entier N suffisamment grand pour que V^{N+1} soit nul sur M et on considère les polynômes P_N et S_N qui définissent respectivement la dernière coordonnée de la multiplication et de l'addition dans $\mathbb{W}_{N+1}$ (ce sont des polynômes sur $\mathbb{Z}$ à $2N+2$ variables).

On définit alors la k-algèbre A comme quotient de $k[T_x, x \in M]$ par les relations suivantes :

i) $T_{F(x)} = T_x^p$

ii) $T_{x+y} = S_N(T_{V^N(x)}, \ldots, T_x ; T_{V^N(y)}, \ldots, T_y)$

iii) $T_{\lambda x} = P_N(\lambda_1^{p^{-N}}, \lambda_2^{p^{-N}}, \ldots, \lambda_{N+1}^{p^{-N}} ; T_{V^N(x)}, \ldots, T_x)$.

Pour prouver que $\mathrm{Spec}(A)$ représente le foncteur $\mathbb{E}(M)$, on remarque que pour tout $x \in M$ et tout $u \in \mathrm{Hom}_{\mathcal{D}}(M, \vec{\mathbb{W}}(S))$, on a

$V^{N+1}(u(x)) = 0$ car $V^{N+1}(x) = 0$; l'élément $u(x)$ provient par la limite inductive d'un élément $(y_1,y_2,\ldots,y_r) \in \mathbb{W}_r(S)$ et on a $V^{N+1}(y_1,\ldots,y_r) = 0$ car $\mathbb{W}_r$ se plonge dans $\vec{\mathbb{W}}$; on a donc $y_1 = y_2 = \ldots y_{r-N-1} = 0$, ce qui implique que $(y_1,y_2,\ldots,y_r)$ provient d'un élément unique de $\mathbb{W}_{N+1}(S)$ par le morphisme de transition T^{r-N-1} .

On en déduit que tout homomorphisme $u \in \mathrm{Hom}_{\mathcal{D}}(M, \mathbb{W}(S))$ se factorise de manière unique par $W_{N+1}(S) \hookrightarrow \vec{\mathbb{W}}(S)$.

On est donc ramené au problème de construire un isomorphisme fonctoriel en S

$$\phi_S : \mathrm{Hom}_{\mathcal{D}}(M, \mathbb{W}_{N+1}(S)) \to \mathrm{Hom}_k(A, \Gamma(\underline{\mathcal{O}}_S)) .$$

Pour tout $u \in \mathrm{Hom}_{\mathcal{D}}(M, \mathbb{W}_{N+1}(S))$, $\phi_S(u) : A \to \Gamma(\mathcal{O}_S)$ est le morphisme qui associe à T_x la dernière coordonnée de $u(x) \in \mathbb{W}_{N+1}(S) = \Gamma(\mathcal{O}_S)^{N+1}$. Il est clair que $\phi_S(u)$ est bien défini sur A et est un morphisme d'algèbres (à cause des relations vérifiées dans A). On définit une application inverse en associant à $\bar{u} \in \mathrm{Hom}_k(A, \Gamma(\mathcal{O}_S))$ l'homomorphisme de $\mathcal{D}$-modules $u : M \to W_{N+1}(S)$ qui à x fait correspondre $u(x) = (\bar{u}(T_{V^N(x)})\ldots, \bar{u}(T_x))$.

6.3. Le schéma $\mathbb{E}(M)$ est un p-groupe fini unipotent

Par définition même de $\mathbb{E}(M)$ (6.1), $\mathbb{E}(M)$ est un schéma en groupes, dépendant additivement de M . Comme M est annulé par une puissance de p (car V est nilpotent), il en est de même de $\mathbb{E}(M)$. Montrons que $\mathbb{E}(M)$ est fini.

Soit $\{x_1,\dots,x_r\}$ un système de générateurs du W-module M ; les relations vérifiées dans l'anneau A entraînent que l'on peut trouver un système de monômes en les variables $T_{x_1},\dots,T_{x_r}$, $T_{Vx_1},\dots,T_{Vx_r},\dots$, $T_{V^N x_1},\dots,T_{V^N x_r}$ et de degrés bornés, tels que cette famille de monômes engendre A en tant que k-espace vectoriel.

D'après 2.5.2 il suffit de montrer que $v_{\mathbb{E}(M)} = v$ est nilpotent pour prouver que $\mathbb{E}(M)$ est unipotent. Comme $\mathbb{E}(M)$ est un sous-groupe d'un groupe lisse (l'espace affine de dimension $r(N+1)$), v est déterminé de manière unique (I.5.3) par la relation $v \circ \mathbb{F}_{\mathbb{E}(M)|k} = p$; nous allons exhiber un morphisme v satisfaisant à cette relation. On montre que l'on a le diagramme commutatif suivant

$$\begin{array}{ccc} \mathrm{Hom}_{\mathcal{D}}(M, \mathbb{W}_{n+1}(S)) & \xrightarrow{\alpha \to \alpha \circ F} & \mathrm{Hom}_{\mathcal{D}}(M, \mathbb{W}_{N+1}(S,\sigma)) \\ \Big\downarrow \phi_S & & \Big\downarrow \phi_{S,\sigma} \\ \mathrm{Hom}_{k\text{-alg}}(A, \Gamma(\mathcal{O}_S)) & \xrightarrow{\mathbb{F}_{\mathbb{E}(M)|k}(S)} & \mathrm{Hom}_{k\text{-alg}}(A \otimes_k (k,\sigma), \Gamma(\mathcal{O}_S)) \end{array}$$

où (S,σ) désigne le k-schéma $S \to \mathrm{Spec}(k) \xrightarrow{\sigma} \mathrm{Spec}(k)$.

On construit alors un morphisme fonctoriel en S

$$v : \mathrm{Hom}_{\mathcal{D}}(M, \mathbb{W}_{N+1}(S,\sigma)) \to \mathrm{Hom}_{\mathcal{D}}(M, \mathbb{W}_{N+1}(S))$$
$$u \to u \circ V \quad .$$

D'après ce qui a été dit, ce morphisme s'identifie à la Verschiebung. Comme V est nilpotent sur M , v est nilpotent et $\mathbb{E}(M)$ est unipotent.

6.4. Le foncteur $\mathbb{E}$ est adjoint à gauche de D^*

On veut construire un isomorphisme fonctoriel en G et M

$$\mathrm{Hom}_{k\text{-}Gr}(G, \mathbb{E}(M)) \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{D}}(M, D^*(G)) .$$

Si l'on pose

$$\mathrm{Prim}((G) = \mathrm{Ker}\ \{\underset{\rightarrow}{\mathbb{W}}(G) \xrightarrow{\Delta^*\text{-}pr_1^*\text{-}pr_2^*} \underset{\rightarrow}{\mathbb{W}}(G \times G)\}) ,$$

on vérifie que l'on a :

$$D^*(G) = \mathrm{Hom}_{k\text{-}Gr}(G, \underset{\rightarrow}{\mathbb{W}}) \overset{\sim}{\sim} \mathrm{Prim}(G) .$$

Par ailleurs, d'après la définition même de $\mathbb{E}(M)$, on a

$$\mathrm{Hom}_k(G, \mathbb{E}(M)) = \mathbb{E}(M)(G) = \mathrm{Hom}_{\mathcal{D}}(M, \underset{\rightarrow}{\mathbb{W}}(G)) ,$$

ce qui définira l'isomorphisme désiré si l'on montre qu'un élément $u \in \mathrm{Hom}_{\mathcal{D}}(M, \underset{\rightarrow}{\mathbb{W}}(G))$ définit un morphisme de groupes $G \to \mathbb{E}(M)$ si et seulement si u se factorise par $\mathrm{Prim}(G)$.

En effet $\mathrm{Hom}_{k\text{-}Gr}(G, \mathbb{E}(M))$ s'identifie à la partie de $\mathrm{Hom}_{k\text{-}alg}(A, \Gamma(\underline{\mathcal{O}}_G))$ formée des morphismes α tels que le diagramme suivant soit commutatif :

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & \Gamma(\underline{\mathcal{O}}_G) \\ {\scriptstyle\Delta}\downarrow & & \downarrow{\scriptstyle\Delta} \\ A \otimes A & \xrightarrow{\alpha \otimes \alpha} & \Gamma(\underline{\mathcal{O}}_G) \otimes \Gamma(\underline{\mathcal{O}}_G) \end{array} .$$

Mais le morphisme $\Delta : A \to A \otimes A$ est donné par la formule

$$\Delta(T_x) = S_N(T_{V^N(x)} \otimes 1, \ldots, T_x \otimes 1 \ ; \ 1 \otimes T_{V^N(x)}, \ldots, 1 \otimes T_x)$$

pour tout $x \in M$, car pour u , $u' \in \mathrm{Hom}_{\mathcal{D}}(M, \mathbb{W}_{N+1}(S))$, on a $\phi_S(u + u')(T_x) = S_N(u(x), u'(x))$ et, toujours d'après la définition de ϕ_S , on a, en posant $\overline{u} = \phi_S(u)$, $\overline{u}' = \phi_S(u')$

$$S_N(u(x),u'(x)) = S_N[\overline{u}(T_{V^N(x)}),\ldots,\overline{u}(T_x) \; ; \; \overline{u}'(T_{V^N(x)}),\ldots,\overline{u}'(T_x)] \quad .$$

De sorte que $\overline{u}$ est un morphisme de groupe si et seulement si pour tout $x \in M$, on a

$$\Delta(\overline{u}(T_x)) = S_N[\overline{u}(T_{V^N(x)}) \otimes 1,\ldots,\overline{u}(T_x) \otimes 1; \; 1 \otimes \overline{u}(T_{V^N(x)}),\ldots,1 \otimes \overline{u}(T_x)] \quad .$$

Ce dernier élément n'est autre que la $N+1^{\text{ième}}$ coordonnée dans $\mathbb{W}_{N+1}(\Gamma(\underline{\mathcal{O}}_G) \times \Gamma(\underline{\mathcal{O}}_G))$ de l'élément $u(x) \otimes 1 + 1 \otimes u(x)$.

Le même raisonnement appliqué à x , $V(x),\ldots,V^N(x)$ montre alors que $\overline{u}$ définit un morphisme de groupes $G \to \mathbb{E}(M)$ si et seulement si $u(x)$ appartient au noyau de $\mathbb{W}_{N+1}(\Gamma(\underline{\mathcal{O}}_G)) \xrightarrow{\Delta^*\text{-}pr_1^*\text{-}pr_2^*} \mathbb{W}_{N+1}(\Gamma(\underline{\mathcal{O}}_G) \otimes \Gamma(\underline{\mathcal{O}}_G))$ qui est lui-même contenu dans $\mathrm{Prim}(G)$.

CHAPITRE III

GROUPES DE BARSOTTI-TATE

1. Notations et définitions préliminaires

Soit S un schéma. On munit la catégorie Sch/S des schémas au dessus de S d'une topologie $\mathcal{T}$ que l'on suppose plus fine que la topologie f.p.p.f. (fidèlement plate et de présentation finie) et moins fine que la topologie f.p.q.c. (fidèlement plate et quasi compacte) (SGA 3 IV, 6.3). L'introduction de cette topologie est technique et n'est pas essentielle dans les énoncés finaux (voir 5.1).

Pour abréger, nous dirons ici que G est un groupe si G est un faisceau en groupes commutatifs sur Sch/S pour la topologie $\mathcal{T}$.

Pour tout entier $n \geq 1$ et pour tout groupe G, on pose:

$$\Lambda_n = \mathbf{Z}/p^n\mathbf{Z}$$

$$G(n) = \mathrm{Ker}\ \{G \xrightarrow{p^n Id} G\}\ ,$$

et

$$G(\infty) = \varinjlim_n G(n)\ ;$$

$G(n)$ est un Λ_n-module (i.e. un $\mathcal{T}$-faisceau en Λ_n-modules);
$G(\infty)$ est le plus grand sous-groupe de p-torsion de G. On a évidemment:

$$G(n)(n') = G(n') \quad \text{pour} \quad n' \leq n \leq \infty$$

Si l'on veut indiquer qu'un groupe est annulé par p^n, c'est-à-dire est un Λ_n-module, on pourra donc le noter $G(n)$ au lieu de G sans entraîner de confusions.

2. Platitude et critère de représentabilité

2.1. Soit G un Λ_n-module. On dit que G est plat sur Λ_n si le produit tensoriel par G au dessus du faisceau constant Λ_n préserve les monomorphismes; on a alors le critère suivant:

2.2. Proposition: Soit $G(n)$ un groupe annulé par p^n. On a les équivalences:

(a) $\forall i \quad 1 \leq i \leq n$, $G(i)$ est un Λ_i-module plat

(b) $G(n)$ est un Λ_n-module plat

(c) $\forall i$, $1 \leq i \leq n-1$, $p^{n-i} G(n) = G(i)$

(i.e. l'application $G(n) \xrightarrow{p^{n-i}Id} G(i)$ est un épimorphisme)

(d) $\exists i$, $1 \leq i \leq n-1$, tel que $p^{n-i}G(n) = G(i)$

(e) $p\, G(n) = G(n-1)$

(f) Le morphisme canonique

$$\gamma: \Lambda_1[T]/T^n \underset{\Lambda_1}{\otimes} G(n)/p\, G(n) \to gr_p G(n) = \bigoplus_{i=0}^{i=n-1} p^i G(n)/p^{i+1}G(n)$$

(où $\gamma^i: G(n)/p\, G(n) \to p^i G(n)/p^{i+1}G(n)$ est induit par la multiplication par p^i) est un isomorphisme.

(g) Le morphisme

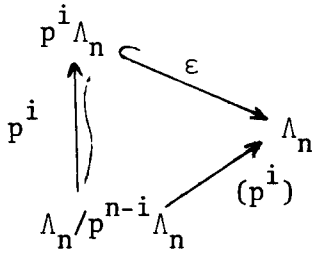
$$\beta: gr_p G(n) \to \Lambda_1[T]/T^n \underset{\Lambda_1}{\otimes} G(1)$$

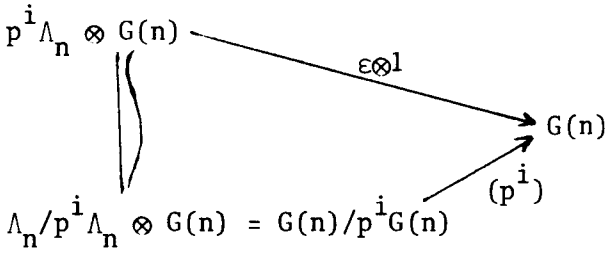
(où $\beta^i: p^i G(n)/p^{i+1}G(n) \to G(1)$ est induit par la multiplication par p^{n-i-1}) est un isomorphisme.

Démonstration:

(b) <=> (c) Pour tout i, $1 \leq i \leq n-1$, on a des triangles commutatifs

canoniques de Λ_n-modules constants qui donnent, par produit tensoriel avec $G(n)$ les diagrammes suivants:

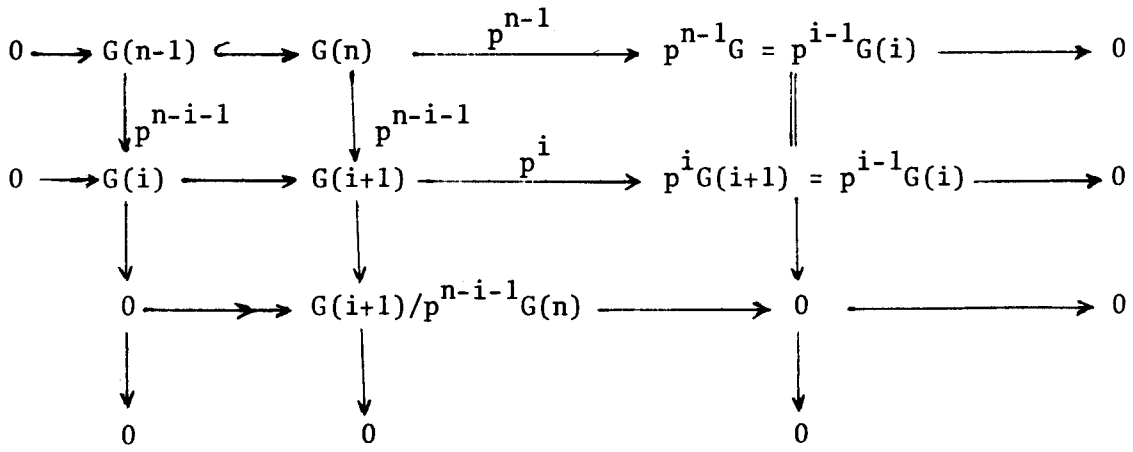




les seuls idéaux de Λ_n étant les $p^i\Lambda_n$, $G(n)$ est plat si et seulement si $\varepsilon \otimes 1$ est injectif pour tout i, ou encore si et seulement si (p^i) est injectif, ce qui équivaut à (c).

(c) => (a) Les relations analogues à (c) sont alors vérifiées par tous les $G(i)$ qui sont donc plats sur Λ_i, d'après ce qui précède.

(d) => (e) Montrons que si $G(i) = p^{n-i}G(n)$, pour un certain i, $1 \le i \le n-1$ alors on a $G(i+1) = p^{n-i-1}G(n)$. Cela se voit directement sur le diagramme suivant où les trois lignes sont des suites exactes.



(e) <=> (f) Soit λ^i: $p^iG(n)/p^{i+1}G(n) \to p^{i+1}G(n)/p^{i+2}G(n)$, $0 \le i \le n-2$

l'épimorphisme induit par la multiplication par p. On a

$$\gamma^i = \lambda^{i-1} \circ \lambda^{i-2} \circ \dots \circ \lambda^0, \quad 1 \leq i \leq n-1$$

on en déduit que l'épimorphisme γ est un isomorphisme si et seulement si γ^{n-1} est un monomorphisme, i.e. si on a (e).

(e) => (g) => (c) Avec les notations précédentes, on a:

$$\beta^i = j \circ \lambda^{n-2} \circ \lambda^{n-3} \circ \dots \circ \lambda^i$$

(où j désigne l'injection canonique $p^{n-1}G(n) \to G(1)$). D'après ce qui précède, (e) entraîne que tous les λ^i sont des isomorphismes, i.e. β est un monomorphisme. Nous allons montrer par récurrence que si β est un monomorphisme, on a (c), d'où l'on déduit immédiatement que j et donc β, sont des isomorphismes.

Si $\beta^0 = j \circ \gamma^{n-1}$ est un monomorphisme, on a alors $pG(n) = G(n-1)$. Comme β^i est un monomorphisme, on a:

$$[p^iG(n)](n-i-1) = p^{i+1}G(n) \ ;$$

mais $p^iG(n) = G(n-i)$ par l'hypothèse de récurrence, et donc $G(n-i-1) = p^{i+1}G(n)$.

2.3. Supposons maintenant que $G(n)$ soit un Λ_n-module plat et qu'il soit représentable par un schéma fini localement libre sur S. Alors $G(i)$, noyau de la multiplication par p^i, est représentable, fini et localement de présentation finie. Mais, $G(n)$ étant supposé Λ_n-plat, on a un épimorphisme $G(n) \xrightarrow{p^{n-1}} G(i)$. Fibre à fibre, cette application est surjecti

et donc (fidèlement) plate.

Par le critère de platitude fibre à fibre (EGA, IV, 11.3.1) on en déduit que $G(i)$ est plat sur S. Alors $G(i)$ est plat, fini, localement de présentation finie sur S, et est donc localement libre.

Inversement, si $G(1)$ est représentable par un schéma fini localement libre sur S et si $G(n)$ est Λ_n-plat, alors $G(n)$ admet une suite de décomposition finie $p^iG(n)/p^{i+1}G(n) \approx G(1)$ et $G(n)$ est représentable par un schéma fini localement libre (II, 1.6). On a donc:

2.4. Proposition: Soit $G(n)$ un groupe annulé par p^n et plat sur Λ_n. Alors $G(n)$ est représentable par un schéma fini localement libre sur S si et seulement si l'un des $G(i)$, $1 \leq i \leq n$, l'est.

3. Groupes de Barsotti-Tate tronqués d'échelon n

3.1. Nous allons voir que la définition d'un groupe de Barsotti-Tate tronqué d'échelon n fait intervenir la platitude sur Λ_n. Pour $n = 1$ cette condition est vide et il est nécessaire d'introduire une condition supplémentaire que l'on justifiera a posteriori (3.3).

Soit G un schéma en groupes (commutatifs) plat sur S. On considère le $\mathbb{F}_p$-schéma fermé $S_o \subset S$ défini par l'idéal $p\mathcal{O}_S$ et soit G_o le schéma sur S_o obtenu par changement de base. On peut alors construire les morphismes $\mathbf{f}_{G_o/S_o}$ et $\mathbf{v}_{G_o}$. Si G_o est un Λ_1-module, on a $\mathbf{f}_{G_o/S_o} \circ \mathbf{v}_{G_o} = 0$.

3.2. Définition. Soit $n \geq 1$ un entier. On appelle p-groupe de Barsotti-Tate tronqué d'échelon n sur S (ou groupe Barsotti-Tate tronqué d'échelon n) un schéma en groupes (commutatifs) G fini et localement libre sur S, annulé par p^n et plat sur Λ_n. Si $n = 1$, on suppose de plus que l'on a (avec les notations de 3.1):

$$(*) \qquad \text{Ker } \mathbf{f}_{G_o/S_o} = \text{Im } \mathbf{v}_{G_o}$$

(c'est une condition qui se vérifie fibre à fibre).

3.3. Si G(n) est un groupe de BT tronqué d'échelon n, alors G(i), $1 \leq i \leq n$, est un groupe de BT tronqué d'échelon i.

Pour $i > 1$, cela résulte de 2.4; pour $i = 1$, nous allons montrer que la condition (*) est aussi vérifiée.

Au dessus de $S_o \subset S$, nous avons déjà remarqué que l'image de $\mathbf{v}_{G(1)_o} : G(1)_o^{(p)} \to G(1)_o$ était contenue dans le noyau K de $\mathbf{f}_{G(1)_o/S_o} : G(1)_o \to G(1)_o^{(p)}$, de sorte que l'on a un diagramme commutatif

$$\begin{array}{ccc} G(1)_o^{(p)} & \xrightarrow{\mathbf{v}} & K \\ \downarrow & & \downarrow \\ & & G(1)_o \\ & & \downarrow \\ G(2)_o^{(p)} & \xrightarrow{\mathbf{v}_{G(2)_o}} & G(2)_o \end{array}$$

dont on vérifie immédiatement qu'il est cartésien car $G(2)_o^{(p)}(1) \simeq G(1)_o^{(p)}$ Par ailleurs l'image de $\mathbf{v}_{G(2)_o}$ contient $G(1)_o$, car $\mathbf{v}_{G(2)_o} \circ \mathbf{f}_{G(2)_o} = p$ a pour image $G(1)_o$, et l'on en déduit que $\mathbf{v}: G(1)_o^{(p)} \to K$ est surjectif.

4. Groupes de Barsotti-Tate

La terminologie de groupe de Barsotti-Tate est préférée à celle de "groupe p-divisible" employée par Tate (J.T. Tate, p-divisible groups, in Proceedings of a Conference on Local Fields, Driebergen 1966 (Springer)), la notion de groupe p-divisible étant beaucoup plus générale:

4.1. Définition. On dit qu'un groupe G ($\mathcal{C}$-faisceau en groupes) est p-divisible si $p.Id: G \to G$ est un épimorphisme.

Si G est p-divisible, $G(n)$ est un Λ_n-module plat d'après 2.2 (e), et le groupe de p-torsion $G(\infty)$ est lui aussi p-divisible. Plus généralement, si on se donne un système inductif

$$G_1 \hookrightarrow G_2 \hookrightarrow \dots G_n \hookrightarrow G_{n\,1} \hookrightarrow \dots$$

tel que G_n est annulé par p^n et $G_n(n-1) = G_{n-1}$ (on appelle un tel système de groupes un système co-p-adique) et tel que de plus G_n soit un Λ_n-module plat, alors $\varinjlim G_n$ est un groupe p-divisible et de p-torsion.

4.2. Définition. Un p-groupe de Barsotti-Tate sur S (ou groupe de Barsotti-Tate) est un groupe G ($\mathcal{C}$-faisceau en groupes commutatifs) p-divisible et de p-torsion tel que $G(1)$ soit un schéma fini localement libre sur S.

Il est équivalent de dire que l'un quelconque des $G(n)$ est un schéma fini localement libre sur S (2.4).

Si G est un groupe de BT, alors, pour tout $n \geq 1$, $G(n)$ est un groupe de BT tronqué d'échelon n. Il se trouve que sur un corps algébriquement clos, la réciproque est vraie: si G' est un groupe de BT tronqué d'échelon n, il existe un groupe de BT G tel que $G' = G(n)$ (la condition (*) de 3.2 est nécessaire si $n = 1$).

5. Sorites sur les groupes de Barsotti-Tate

5.1. La catégorie des groupes de Barsotti-Tate peut se décrire sans référence à la topologie $\mathcal{T}$ car elle est équivalente à la catégorie des systèmes co-p-adiques $\{G_n\}$ où G_n est un S-schéma en groupes fini localement libre qui est un Λ_n-module plat.

La catégorie des groupes de BT est une catégorie additive. Si S' est un schéma sur S et si G est un groupe de BT sur S, alors son image réciproque G' sur S' (restriction de G aux S'-schémas) est un groupe de BT sur S'. (On a en effet $G' = \varinjlim G(n) \times_S S'$ et les $G(n) \times_S S'$ sont des groupes de BT tronqués).

5.2. Proposition. Soit $0 \to G' \to G \to G'' \to 0$ une suite exacte de groupes; alors

a) Si G' et G'' sont des groupes de BT, il en est de même de G;

b) Si G' et G sont des groupes de BT, il en est de même de G'';

a) Une extension de groupes p-divisibles (resp. de p-torsion) est p-divisible (resp. de p-torsion) et la suite exacte induit (lemme du Serpent) une suite exacte $0 \to G'(1) \to G(1) \to G''(1) \to G'/pG' \to \ldots$ mais

comme G' est p-divisible, $G(1)$ est une extension de groupes finis localement libres et est donc de même nature.

b) Un quotient d'un groupe p-divisible (resp. de p-torsion) est p-divisible (resp. de p-torsion). Comme précédemment, $G''(1)$ est quotient de deux schémas en groupes finis localement libre, ce qui implique que $G''(1)$ l'est aussi (II, 1.6).

Remarque. Si G et G'' sont des groupes de BT, il est en général faux que le noyau soit un groupe de BT. Par exemple, on a la suite exacte $0 \to G(1) \to G \xrightarrow{p} G \to 0$ où $G(1)$ n'est pas p-divisible!

5.3. Rang (ou hauteur) d'un groupe de Barsotti-Tate. $G(1)$ est un groupe fini localement libre annulé par p. Pour tout $s \in S$, on a donc

$$\text{rang } (G(1)_s) = p^{r(s)}$$

où la fonction $s \mapsto r(s)$ est localement constante. Des suites exactes $0 \to G(1) \to G(n) \xrightarrow{p} G(n-1) \to 0$ on tire immédiatement que

$$\text{rang } (G(n)_s) = [\text{rang } (G(1)_s)]^n = p^{nr(s)}$$

L'entier $r(s)$ décrit donc le rang de tous les $G(n)$. Par définition $r(s)$ s'appelle le rang (ou la hauteur) du groupe de Barsotti-Tate G au point $s \in S$.

5.4. On a décrit la catégorie des groupes de BT sur S à l'aide de systèmes co-p-adiques. Signalons qu'on peut le faire à l'aide de systèmes p-adiques: Si G est un groupe de Barsotti-Tate, on lui fait

correspondre bi univoquement le système projectif p-adique

$$T_p(G) = (G(n)_{n\geq 1} \; ; \; G(n+1) \xrightarrow{p} G(n))$$

où la multiplication par p identifie $G(n)$ à $G(n+1)/p^nG(n+1)$ et où $G(1)$ est annulé par p et est représentable par un schéma fini localement libre sur S.

5.5. Dual d'un groupe de Barsotti-Tate. A tout groupe de BT G sur S, on associe donc le système p-adique $T_p(G)$. Ce système projectif définit par dualité de Cartier un système co-p-adique de groupes finis localement libres $G(n)^*$, annulés par p^n et plats sur Λ_n (2.2). Par définition, le dual de G est le groupe de BT G^* associé à ce système co-p-adique:

$$G^* = \varinjlim_n G(n)^* \; .$$

On a en particulier $G^*(n) = G(n)^*$, et on obtient ainsi un foncteur contravariant, compatible aux changements de base, qui définit une équivalence entre la catégorie $BT(S)$ des p-groupes de Barsotti-Tate sur S et son opposée, car on a un isomorphisme fonctoriel canonique

$$G \xrightarrow{\sim} (G^*)^* \; .$$

5.6. Module de Dieudonné associé à un groupe de BT sur un corps parfait. Reprenant les notations de II, 4.1 et désignant par $BT(k)$ la catégorie des p-groupes de BT sur le corps parfait k, on a le

Théorème (cf. II, 5.3.1) Il existe une équivalence de catégories

$$D^*: [BT(k)]^o \xrightarrow{\sim} (\mathcal{D}\text{-modules, libres et de type fini sur } W)$$

Telle que

$$[D^*(G)]^\sigma \simeq D^*(G^{(p)}); \quad D^*(f_{G/k}) = F_{D^*(G)}; \quad D^*(v_G) = V_{D^*(G)}$$

Soit G un groupe de BT sur un corps parfait. On pose

$$M(n) = D^*(G(n)),$$

où D^* est le foncteur "classique" défini en II, 4. Comme $G(n)$ est annulé par p^n, $M(n)$ est annulé par p^n et c'est donc un module sur $W/p^nW = W_n$.

Pour tout i, $1 \leq i \leq n-1$, les épimorphismes $G(n) \xrightarrow{p^i} G(n-i)$ définissent des monomorphismes

$$M(n)/p^{n-i}M(n) = M(n-i) \xrightarrow{p^i} M(n) .$$

Ceci équivaut au fait que $M(n)$ est <u>plat sur</u> W_n (démonstration analogue à celle de 2.2).

Enfin, le système co-p-adique des $G(n)$ définit un système p-adique des modules $M(n)$: Les injections $G(n) \to G(n+1)$ définissent des surjections

$$M(n+1) \to M(n)$$

qui identifient $M(n)$ à $M(n+1)/p^nM(n+1)$.

Par définition, on pose:

$$D^*(G) = \varprojlim M(n)$$

$D^*(G)$ est un module sur $W = \varprojlim W_n$; comme limite p-adique de W_n-modules plats, il est plat sur l'anneau local W et est donc libre. Les $M(n)$ étant de longueur finie, $D^*(G)$ est de type fini. De plus, $D^*(G)$ est muni de morphismes semi-linéaires F et V induits par les morphismes correspondants sur $M(n)$.

6. Exemples et types particuliers de groupes de Barsotti-Tate

6.1. Soit A un schéma abélien sur S (i.e. un schéma en groupes commutatifs, propre et lisse sur S, et à fibres connexes). Un schéma abélien est p-divisible: c'est bien connu dans le cas où la base est le spectre d'un corps algébriquement clos (cf. S. Lang, "Abelian Varieties") et, si S est quelconque, la surjectivité de $p\mathrm{Id}_A$ résulte de ce cas particulier grâce au critère de platitude fibre par fibre (EGA, IV, 11.3.10).

Si d désigne la dimension relative de A sur S, on peut montrer que

$$\text{rang } A(1) = p^{2d} .$$

Le groupe $A(1)$ est donc fini; il est évidemment de présentation finie et, étant plat, il est localement libre. On en déduit que $A(\infty) = \varinjlim_n A(n)$ est un groupe de BT de rang $2d$. C'est le p-groupe de BT associé au schéma abélien A, et cette construction peut se faire pour tout nombre premier p.

Si toutes les caractéristiques résiduelles de S sont diffé-

rentes de p, on montre que A(1) est étale sur S, et on dira alors que $A(\infty)$ est ind-étale.

Notons par ailleurs qu'il existe une notion de dualité pour les variétés abéliennes. Si A^* désigne la variété duale de la variété abélienne A, on montre aisément que son groupe de BT associé $A^*(\infty)$ s'identifie au dual, en tant que groupe de BT, de $A(\infty)$.

6.2. Par définition, on dit qu'un groupe de BT sur S est <u>un groupe de Barsotti-Tate ind-étale</u> si G(1) est étale. Il est équivalent de dire (les G(n) admettant une suite de composition en groupes isomorphes à G(1)) que tous les G(n) sont étales.

Le foncteur $G \mapsto T_p(G)$ (5.4) définit une équivalence de catégories entre la catégorie des groupes de BT ind-étales et la catégorie des <u>faisceaux p-adiques constants tordus sans torsion</u> (i.e. systèmes p-adiques de groupes finis localement libres G_n, étales sur S et plats sur Λ_n).

Si S est connexe, la catégorie des faisceaux p-adiques constants tordus sans torsion est bien connue: si l'on choisit un point géométrique $\bar{s} \in S$, on définit une équivalence de cette catégorie avec la catégorie des $\mathbf{Z}_p$-modules libres de type fini sur lesquels le groupe fondamental $\pi_1(S,\bar{s})$ opère continûment en associant au système $(G_n)_{n\geq 1}$ le $\mathbf{Z}_p$-module $\varprojlim (G_n)_{\bar{s}}$, $\pi_1(S,\bar{s})$ opérant par monodromie sur $(G_n)_{\bar{s}}$.

6.3. <u>Exemple</u>. On dit qu'un schéma en groupes T sur S est un <u>tore</u> s'il est, localement pour la topologie étale, isomorphe à $\mathbb{G}_{m,S}^r$.

Un tore T est p-divisible et $T(1)$ est un groupe fini localement libre de rang p^r, r étant la dimension relative de T sur S (ces propriétés sont locales et sont vérifiées par $\mathbb{G}_{m,S}^r$). On en déduit que $T(\infty)$ est un groupe de BT de rang r.

Comme exemple particulier important, on a le groupe de BT

$$\boldsymbol{\mu} = \mathbb{G}_{m,S}(\infty) = \varinjlim_n \boldsymbol{\mu}_{p^n,S} .$$

6.4. Exemple. Soit G un schéma en groupes sur S, extension d'un schéma abélien A par un tore T. Alors G est p-divisible, $G(1)$ est fini localement libre sur S et $G(\infty)$ est un groupe de BT de rang $2d+r$ (d et r désignant respectivement les dimensions relatives de A et T sur S). De plus, on a une suite exacte

$$0 \to T(\infty) \to G(\infty) \to A(\infty) \to 0 .$$

6.5. Comme y incite l'exemple (6.3), on dira qu'un groupe de BT G est toroïdal si $G(1)$ est de type multiplicatif. Il est équivalent de dire que tous les $G(n)$ sont de type multiplicatif, ou encore que le dual G^* (5.5) est ind-étale.

Le foncteur $G \mapsto T_p(G^*)$ définit une anti-équivalence entre la catégorie des groupes de BT toroïdaux et celle des faisceaux p-adiques constants tordus sans torsion. Composant ce foncteur avec la dualité dans les faisceaux p-adiques constants tordus sans torsion

$$T_p(G^*) \mapsto \underline{\mathrm{Hom}}_{gr}(G^*, \mathbb{Z}_p) \overset{\text{def}}{=\!=} (\underline{\mathrm{Hom}}_{gr}(G(n)^*, \Lambda_n))_{n\geq 1} ,$$

on obtient une équivalence au lieu d'une anti-équivalence. Cette équivalence peut s'expliciter comme suit:

$$G \longmapsto \underline{\mathrm{Hom}}_{gr}(\mu, G) \overset{\text{def}}{=\!=} (\underline{\mathrm{Hom}}_{gr}(\mu(n), G(n)))_{n\geq 1}$$

6.6. On dit qu'un groupe de BT G sur S est <u>à fibres connexes</u> si $G(1)$ est infinitésimal. Il revient au même de dire que tous les $G(n)$ sont infinitésimaux.

Si toutes les caractéristiques résiduelles de S sont égales à p, les groupes de BT toroïdaux sont à fibres connexes (II,2.2).

On montrera plus loin que, si p est localement nilpotent sur S, un groupe de BT est à fibres connexes si et seulement si il est aussi un groupe de Lie formel.

Nous allons donner ici une première définition élémentaire des groupes de Lie formels et étudier à quelles conditions un groupe de Lie formel est un groupe de BT.

6.7. On appelle <u>variété de Lie formelle ponctuée</u> (ou <u>augmentée</u>) sur S un faisceau X sur S (pour la topologie $\mathcal{C}$, (f.p.p.f.) $\leq \mathcal{C} \leq$ (f.p.q.c. muni d'une section $S \overset{\varepsilon}{\to} X$ et tel que localement (pour la topologie de Zariski) sur X, on ait

$$X \simeq \varinjlim_n \mathrm{Spec}\ \underline{\mathcal{O}}_S[[T_1,\ldots,T_r]]/(T_1,\ldots,T_r)^n .$$

<u>Remarques</u>. 1) On peut expliciter ce dernier isomorphisme en disant que pour tout $S' \to S$, S' quasi compact, on a

$$X(S') = \varinjlim_n \mathrm{Hom}_S\ (S',\ \mathrm{Spec}\ \underline{\mathcal{O}}_S[[T_1,\ldots,T_r]]/(T_1,\ldots,T_r)^n)$$

$$= \varinjlim_n \{f_1,f_2,\ldots,f_r \in \Gamma(S',\underline{\mathcal{O}}_S) \mid f_i^n = 0,\quad 1 \leq i \leq r\}$$

2) X est en particulier limite inductive de schémas finis et radiciels au dessus de S.

On appelle <u>groupe de Lie formel sur S</u> un faisceau en groupes sur S tel que sa section unité lui donne une structure de variété de Lie formelle. Comme le produit de deux variétés de Lie formelles est encore une variété de Lie formelle, il est équivalent de dire qu'un groupe de Lie formel est un objet en groupes de la catégorie des variétés de Lie formelles sur S.

Dans ce qui suit, tous les groupes de Lie formels seront supposés commutatifs.

Soit G un groupe de Lie formel sur S. On vérifie aisément que, si p est localement nilpotent sur S, G est de p-torsion, c'est-à-dire que

$$G = G(\infty) = \varinjlim_n G(n)\ ,$$

de sorte que G est un groupe de Barsotti-Tate si et seulement si les deux conditions suivantes sont vérifiées:

1) G est p-divisible.

2) $G(1)$ est représentable par un schéma fini localement libre.

Il se trouve que <u>si S est artinien local</u>, d'unique point $s \in S$,

ces deux conditions sont équivalentes et équivalent à chacune des conditions (ne faisant intervenir que la fibre géométrique de G):

3) $G_{\overline{s}}$ est p-divisible.

4) Il est impossible de plonger le groupe formel additif $\overline{\mathbb{G}}_a$ (complété formel de $\mathbb{G}_a$ le long de sa section unité) dans $G_{\overline{s}}$.

Dans le cas général, on pense que les conditions 1) et 2) sont encore équivalentes; cela résulterait de la conjecture suivante, vraie dans le cas artinien local (SGA 3, VII,):

Si $u: G \to G'$ est un S-morphisme de variétés de Lie formelles de même dimension relative sur S, on a les équivalences:

- u est un épimorphisme
- Ker (u) est représentable par un schéma fini
- Ker (u) est représentable par un schéma fini localement libre.

Par contre, le fait que le groupe de Lie formel G soit un groupe de BT ne se vérifie pas en général sur les fibres, comme le montre l'exemple du groupe de Lie formel associé à la courbe elliptique modulaire A sur une courbe S de caractéristique p, puisqu'il y a des points $s \in S$ tels que l'invariant de Hasse de A_s est nul.

Cet exemple suggère cependant la conjecture suivante: Pour qu'un groupe de Lie formel G sur S soit de BT, il faut et il suffit que ses fibres G_s soient des groupes de BT et que le rang de G_s (en tant que BT) soit une fonction localement constante en $s \in S$.

7. Suite de composition d'un groupe de Barsotti-Tate

7.1. Supposons d'abord S réduit à un point s. Si G est un groupe de Barsotti-Tate sur S, on pose par définition

$$G^o = \varinjlim_n G(n)^o \qquad (G(n)^o = \text{composante neutre de } G(n))$$

$$G^{et} = \varinjlim_n G(n)/G(n)^o ,$$

et l'on obtient une suite exacte

$$0 \to G^o \to G \to G^{et} \to 0$$

On vérifie immédiatement que G^o est un groupe de BT, d'où l'on déduit (5.2) que G^{et} l'est aussi, de sorte que l'on obtient G comme extension d'un groupe de BT ind-étale par un groupe de BT à fibre connexe. Cette décomposition est évidemment canonique et fonctorielle en G.

7.2. Si la caractéristique résiduelle de S est p et si l'on pose

$$G^{tor} = \varinjlim_n G(n)^{mult}$$

où $G(n)^{mult}$ désigne le plus grand sous-groupe de type multiplicatif de $G(n)$, $G(n)^{mult} \subset G(n)^o$, on obtient une filtration

$$\{0\} \subset G^{tor} \subset G^o \subset G$$

Il est immédiat que G^{tor} est un groupe de BT; c'est le plus grand sous-groupe de BT toroïdal de G.

On en déduit que G^o/G^{tor} est un groupe de BT; c'est un

groupe à fibre connexe et ind-unipotent (i.e. $G^o/G^{tor}(1) = G(1)^o/G(1)^{mult}$ est unipotent). Cette suite de composition canonique est fonctorielle en G, commute aux changements de base et par passage au dual, on vérifie que, par construction même, on a des isomorphismes canoniques

$$(G/G^o)^* \simeq (G^*)^{tor}, \quad (G/G^{tor})^* \simeq (G^*)^o .$$

7.3. Si la base S est quelconque, on en peut pas en général écrire un groupe de BT G comme extension d'un groupe de BT ind-étale G'' par un groupe de BT à fibres connexes G'.

En effet, si on a une telle extension, on sait que l'on obtient alors une suite exacte

$$0 \to G'(1) \to G(1) \to G''(1) \to 0 .$$

Pour tout $s \in S$, considérons alors le rang séparable de $G(1)_s$. On a:

$$\text{rang sep } (G(1)_s) = \text{card } G(1)(\bar{s}) = \text{rang sep } (G'(1)_s) \times \text{rang sep } (G''(1)_s).$$

Mais le rang séparable de $G'(1)_s$ est 1 car $G'(1)$ est infinitésimal et le rang séparable de $G''(1)_s$ est une fonction localement constante de $s \in S$ car $G''(1)$ est étale sur S, de sorte que l'on en déduit que le rang séparable de $G(1)_s$ est une fonction localement constante de s.

Or cela n'est pas vrai en général, comme le montre l'exemple de la variété elliptique modulaire A sur une courbe S en caractéristique

p, où l'on a des points isolés s où l'invariant de Hasse de A_s est nul. On a cependant le résultat suivant: (c.f.[24] chap.II, prop.4.9) :

7.4. Proposition. Soit G un groupe de Barsotti-Tate sur S. Les propriétés suivantes sont équivalentes:

i) G est extension d'un groupe de BT ind-étale par un groupe de BT à fibres connexes.

ii) Pour tout $n \in \mathbb{N}$, G(n) est extension d'un groupe fini étale par un groupe fini infinitésimal.

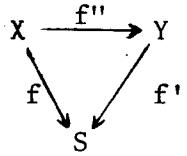
ii)^{bis} G(1) est extension d'un groupe fini étale par un groupe fini infinitésimal.

iii) Pour tout $n \in \mathbb{N}$, la fonction $s \mapsto$ rang sep $G(n)_s$ est localement constante.

iii)^{bis} La fonction $n \mapsto$ rang sep $G(1)_s$ est localement constante.

L'équivalence de (iii) et (iii)^{bis} résulte de ce que le rang séparable de $G(n)_s$ est la puissance n-ième du rang séparable de $G(1)_s$. D'autre part, (i) résulte immédiatement de (ii), et, d'après ce qui précède, la seule implication à démontrer est (iii) => (ii). On utilise pour cela le lemme suivant (c.f.[24] chap.II lemme 4.8) :

Lemme. Soit $f: X \to S$ un morphisme fini localement libre de schémas. Pour que f se factorise en f' étale et f'' radiciel et surjectif, il faut et il suffit que la fonction $s \mapsto$ rang sep (X_s) soit localement constante. La factorisation est alors unique et fonctorielle en f.



(De la fonctorialité, il résulte que si X est un schéma en groupes sur S, Y l'est aussi.)

CHAPITRE IV

CRISTAUX

1. Rappels sur les puissances divisées.

1.1. Définition. Soient A un anneau et J un idéal de A. On dit que J est muni de puissances divisées si on s'est donné une feuille d'applications

$$\gamma_n : J \longrightarrow J \quad , \quad \text{pour } n \in \mathbb{N}, \quad n \geq 1.$$

Vérifiant les axiomes suivants:

1) $\gamma_1(x) = x$, pour tout $x \in J$.

2) $\gamma_n(x+y) = \gamma_n(x) + \sum_{i=1}^{n-1} \gamma_{n-i}(x)\gamma_i(y) + \gamma_n(y)$

pour $x \in J$, $y \in J$

3) $\gamma_n(xy) = x^n \gamma_n(y)$ pour $x \in A$, $y \in J$

4) $\gamma_m \circ \gamma_n(x) = \frac{(mn)!}{(n!)^m m!} \gamma_{mn}(x)$

(5) $\gamma_m(x)\ \gamma_n(x) = \frac{(m+n)!}{m!n!} \gamma_{m+n}(x)$.

L'axiome 5 donne encore la relation

$$\gamma_{m_1+m_2+\ldots+m_p}(x) \cdot \frac{(m_1+m_2+\ldots+m_p)!}{m_1!m_2!\ldots m_p!} = \prod_{i=1}^{p} \gamma_{m_i}(x) \quad .$$

En particulier on a

$$x^n = (\gamma_1(x))^n = n!\ \gamma_n(x) \quad .$$

Cette dernière formule est la motivation principale pour l'introduction des puissances divisées. Si l'anneau A est de caractéristique 0, on a nécessairement

$$\gamma_n(x) = \frac{x^n}{n!} \qquad \text{pour tout} \quad n \in N.$$

Donc l'idéal J a au plus une structure de puissances divisées. Mais il est aussi immédiat que pour un anneau de caractéristique 0, les applications $\gamma_n(x) = \frac{x^n}{n!}$ définissent sur un idéal arbitraire une structure de puissances divisées.

Pour écrire d'une manière plus commode certaines formules, on définit $\gamma_0(x) = 1$ et on note quelquefois $x^{(n)}$ au lieu de $\gamma_n(x)$, la puissance divisée $n^{\text{ème}}$.

Les puissances divisées ont été introduites par H.Cartan pour l'étude des espaces d'Eilenberg-MacLane, et en algèbre abstraite par N.Roby dans sa thèse.

1.2. Exponentielle et logarithme.

Soient A un anneau et (J, γ_n) un idéal muni de puissances divisées. On définit alors les applications exponentielle et logarithme

$$\exp: J \to 1 + J \quad , \qquad \exp(x) = \sum_{n\geq 0} x^{(n)}$$

$$\log: 1 + J \to J \quad , \qquad \log(1+x) = \sum_{n\geq 1} (-1)^{n-1}(n-1)!\, x^{(n)}$$

où on suppose, pour que ces applications soient définies, que $x^{(n)}$ resp. $(n-1)!x^{(n)}$ est nul pour n assez grand. Si cette hypothèse est réalisée, la vérification habituelle montre alors que exp et log sont des isomorphismes réciproques

$$J^{+} \underset{\log}{\overset{\exp}{\rightleftarrows}} (1+J)^{*}$$

On introduit sur J la filtration

$$J = J^{(1)} \supset J^{(2)} \supset \ldots \supset J^{(n)} \supset \ldots .$$

définie comme suit: $J^{(n)}$ est l'idéal engendré par les monômes $x_1^{(a_1)} \; x_2^{(a_2)} \ldots x_r^{(a_r)}$ avec $\Sigma\, a_i \geq n$. On dit que (J, γ_n) est p.d. nilpotent s'il existe un n tel que $J^{(n)} = \{0\}$. Dans ce cas $x^{(n)} = 0$ pour tous les $x \in J$ et l'exponentielle et le logarithme sont donc définis. S'il existe un n tel que

$$(n - 1)!\; J^{(n)} = \{0\}$$

le logarithme est défini. Cette condition a été introduite par P. Berthelot en cohomologie cristalline; nous l'appellerons condition de Berthelot.

1.3. Quelques exemples de structure de puissances divisées.

Ex. 1) Si A est de caractéristique 0, nous avons déja vu que tout idéal possède une et une seule structure de puissances divisées:

$$\gamma_n(x) = \frac{x^n}{n!}$$

Ex. 2) Si A est un anneau sans torsion, il existe au plus une structure de puissances divisées sur J, puisqu'on a

$$n!\,\gamma_n(x) = x^n \quad .$$

Elle existe si et seulement si $J \subset J \otimes \mathbb{Q} \subset A \otimes \mathbb{Q}$ est stable par les opérations $x \mapsto x^n/n!$.

Ex. 3) Soient $W = W(k)$ l'anneau des vecteurs de Witt d'un corps parfait k et $J = pW$. Par la méthode classique de Gauss soit

$$n = a_o + a_1 p \quad + \ldots + a_\ell \; p^\ell$$

$0 \leq a_j \leq p - 1$, $j = 0, 1, \ldots \ell$, le développement p-adique de n et soit $s_n = \sum_{j=0}^{\ell} a_j$; la valuation p-adique de n! est donnée par

$$v_p(n!) = \frac{n - s_n}{p-1} \leq n - 1 \quad .$$

D'où $\gamma_n(p) = \frac{p^n}{n!} \in p\,W$. Il y a donc une unique structure de puissances divisées sur p W. De plus, on voit que si $p \neq 2$, $\frac{p^n}{n!}$ tend vers 0 dans W, et comme W est complet, on peut encore définir l'exponentielle par

$$\exp px = \sum_{n=0}^{\infty} \frac{p^n x^n}{n!} \quad .$$

Mais pour $p = 2$, ceci n'est plus vérifié, puisque par exemple on a

$$\frac{2^{2^n}}{2^n!} \equiv 2 \pmod{2^2} \quad .$$

De même sur $W_n = W/p^n W$, les puissances divisées sont nilpotentes pour $p \neq 2$ et on peut définir l'exponentielle et le logarithme. Pour $p = 2$, comme la condition de Berthelot est vérifiée on peut encore définir le logarithme, mais pas l'exponentielle.

Ex. 4) Extensions des puissances divisées.

Définition. Soient (A,J,γ) et (A',J',γ') deux anneaux munis d'idéaux avec puissances divisées, un p.d. homomorphisme

$$\varphi : (A, J, \gamma) \to (A', J', \gamma')$$

est un homomorphisme d'anneaux $\varphi: A \to A'$ tel que $\varphi(J) \subset J'$ et que, pour tout $x \in J$, on ait $\varphi(\gamma_n(x)) = \gamma'_n(\varphi(x))$.

Définition. Si (A, J, γ) est un anneau avec idéal muni de p.d. et si $\varphi: A \to B$ est un homomorphisme d'anneaux, on dit que γ s'étend à B s'il existe sur l'idéal JB une structure de puissances divisées γ' telle que

$$\varphi: (A, J, \gamma) \to (B, JB, \gamma')$$

soit un p.d. homomorphisme. (Cette structure γ' est alors unique).

Proposition. Soit (A, J, γ) un anneau avec idéal muni de p.d.
Si J est principal, γ peut toujours s'étendre.

Démonstration. Supposons que $J = (j)$ et soit $\varphi: A \to B$ un homomorphisme. Si γ s'étend en γ', on a nécessairement

$$\gamma'_n (b\ \varphi(j)) = b^n\ \varphi(\gamma_n(j)) \quad ,$$

qui est bien défini puisque si $b\ \varphi(j) = b'\ \varphi(j)$, comme $\gamma_n(j) = a_n j$, on a

$$b^n\ \varphi(\gamma_n(j)) - b'^n\ \varphi(\gamma_n(j)) = c(b - b')\ \varphi(j) = 0.$$

Il est immédiat que γ' ainsi défini donne une structure de puissances divisées extension de γ.

Proposition. Soient (A, J, γ) un anneau avec un idéal J muni de p.d. et B une A-algèbre plate. Alors γ s'étend à JB. (En fait il suffit que $J \otimes B \to JB$ soit un isomorphisme.)

Démonstration. Pour construire $\gamma'_n : JB \to JB$, on considère le module libre $\mathbb{Z}^{(J\times B)}$ de base $J\times B$ et on définit une application $g'_n : \mathbb{Z}^{(J\times B)} \longrightarrow JB$.

par

$$g'_n(a_1(j_1,b_1)+\ldots+a_\ell(j_\ell,b_\ell)) = \sum_{\substack{i_1+i_2+\ldots+i_\ell=n \\ i_k\geq 0}} (a_1b_1)^{i_1}\gamma_{i_1}(j_1)\ldots(a_\ell b_\ell)^{i_\ell}\gamma_{i_\ell}(j_\ell).$$

Comme par l'hypothèse de platitude, on a

$$J \otimes_A B \simeq JB$$

pour montrer que γ'_n bien définie, il suffit donc de la définir sur $J \otimes_A B$, par passage au quotient de g'_n. Il suffit donc de prouver que si $\alpha \in \mathbf{Z}^{(J\times B)}$, pour tout élément $\beta \in \mathbf{Z}^{(J\times B)}$ des formes suivantes

1) $(j' + j'', b) - (j',b) - (j'',b)$

2) $(j, b+b') - (j,b) - (j, b')$

3) $(aj,b) - (j, ab)$,

on a $g'_n(\beta + \alpha) = g'_n(\alpha)$.

Cette vérification est laissée au lecteur.

Les deux énoncés précédents sont dûs à P. Berthelot.

Ex.5) Cas d'un anneau de valuation discrète.

Soit V un anneau de valuation discrète d'inégale caractéristique, de caractéristique résiduelle p. Soit e l'indice de ramification absolu donné par

$$pV = \underline{m}^{e} \quad ,$$

où $\underline{m}$ est l'idéal maximal de V. Alors $\underline{m}$ est stable par puissances divisées si et seulement si on a

$$e \leq p - 1 \quad .$$

On a des puissances divisées topologiquement nilpotentes si et seulement si $e < p - 1$. C'est une conséquence immédiate de la formule donnant la valuation de n! déjà utilisée plus haut.

Ex.6) Si A est une algèbre sur $\mathbb{Z}_{(p)}$, les γ_n sont connus quand on connaît la seule opération $\gamma_p = \pi$. En effet γ_0, $\gamma_1, \ldots, \gamma_{p-1}$ sont connus parce que (p-1)! est inversible dans A. Posant alors pour tout n

$$n = a_0 + a_1 p + \ldots + a_r p^r \qquad 0 \leq a_i \leq p - 1, \quad a_r \neq 0,$$

on aura

$$\gamma_n(x) = c_n x^{a_0} \quad \pi(x)^{a_1} \quad (\pi^2(x))^{a_2} \quad \ldots \quad (\pi^r(x))^{a_r} \quad ,$$

où π^i est l'itéré i.ème de π et où

$$c_n = \frac{1}{n!} \quad (p!)^{\sum a_i (1+p+\ldots+p^{i-1})}$$

qui est bien un élément inversible de $\mathbb{Z}_{(p)}$.

Pb: conditions générales sur π pour que π soit de la forme γ_p ?

Si on suppose que $J^2 = pJ = \{0\}$, on trouve que pour que

$$\pi : J \longrightarrow J$$

soit égal à un γ_p pour un système convenable de puissances divisées, il faut et il suffit que π soit additif et p-linéaire.

2. Site cristallin d'un schéma

Soient S un schéma, I un idéal quasi cohérent de O_S et γ un système de puissances divisées sur I. On suppose de plus réalisée la condition de Berthelot $(n-1)!\, I^{(n)} = 0$ pour n assez grand. Soit X un S-schéma. On définit <u>le site cristallin</u> associé aux données $\{X, S, I, \gamma\}$ comme suit:

2.1 <u>Objets du site</u>. Les objets consistent en les triples $(U \subset U', \gamma_{U'})$/S où U est un ouvert de Zariski de X, $U \subset U'$ est une nilimmersion (on dit encore que U' est un <u>épaississement de</u> U), et $\gamma_{U'}$ est une structure de puissances divisées sur l'idéal J de $O_{U'}$, qui définit U dans U', "compatible" avec la structure γ de I.

La condition de compatibilité sur les structures à p.d. qui est exigée est de nature locale sur X et sur U et s'exprime dans le cas affine $X = \operatorname{Spec} A$, $U = \operatorname{Spec} B$, $U' = \operatorname{Spec} B'$ par les deux conditions.

(i) Sur IB', on suppose qu'il existe des puissances divisées qui prolongent celles de I (ce qui sera le cas par exemple si B' est A-plat ou si I est principal).

ii) Les puissances divisées sur IB' et sur J coïncident dans l'intersection $J \cap IB'$.

Les conditions (i) et (ii) sont équivalentes à l'existence de puissances divisées sur $J + IB'$ qui soient compatibles avec les puissances divisées de J et de I.

2.2 Morphismes du site. Un morphisme de (U, U') dans (V, V') consiste en une inclusion $U \subset V$ et la donnée d'un morphisme de schémas $U' \to V'$ qui rende commutatif le diagramme

$$\begin{array}{ccc} U & \hookrightarrow & U' \quad J \\ \cap & & \downarrow \\ V & \hookrightarrow & V' \quad K \end{array}$$

et qui soit telle que les structures à puissances divisées sur J et sur K soient compatibles.

2.3. Topologie du site. On met sur le site cristallin la topologie "de Zariski", à savoir la topologie la moins fine telle que, pour tout objet $U \hookleftarrow U'$, les familles de morphismes

$$\begin{array}{ccc} U_i & \hookrightarrow & U'_i \\ \downarrow & & \downarrow \\ U & \hookrightarrow & U' \end{array}$$

où $\{U'_i \hookleftarrow U'\}_{i \in I}$ est un recouvrement de U' par des ouverts de Zariski et où $U_i = U \times_{U'} U'_i$, soient des familles couvrantes.

2.4 Le topos associé au site cristallin s'appelle le topos cristallin et on le note $(X \mid S, I, \gamma)_{cris}$ ou, s'il n'y a pas de confusion possible, $(X \mid S)_{cris}$ et même X_{cris}.

2.5 Description d'un objet du topos cristallin.

Soit $F \in \mathrm{Ob}\, X_{cris}$, c'est-à-dire un faisceau d'ensemble sur le site cristallin. A tout objet (U,U') du site cristallin [on devrait en réalité écrire $(U \subset U', \gamma_{U'})$] on associe un faisceau $F_{(U,U')}$ si U' muni de la topologie de Zariski en posant:

$$F_{(U,U')}(V') = F(U \underset{U'}{\times} V', V') \qquad \text{pour tout ouvert } V' \subset U'$$

A tout morphisme $u = (u,u') : (V,V') \to (U,U')$, on associe le morphisme de faisceau

$$u^{\natural} : u'^{*} F_{(U,U')} \longrightarrow F_{(V,V')} .$$

Ces morphismes satisfont aux conditions de transitivité vis-à-vis de la composition et $u^{\natural}$ est un isomorphisme si u' est une immersion ouverte.

Inversement, la donnée d'une telle famille de faisceaux $F_{(U,U')}$ avec des morphismes de transition $u^{\natural}$ vérifiant les propriétés ci-dessus détermine un unique objet de X_{cris}.

Remarque. Nous n'introduisons pas ici les autres variantes quelquefois utilisées. Mentionnons pour mémoire le topos infinitésimal (même définition mais sans puissances divisées) et le topos stratifiant où on prend comme objets les épaississements $U \subset U'$ munis d'une rétraction.

2.6 Le faisceau d'anneaux $O_{X/S}$.

Si à chaque couple (U, U') nous associons le faisceau $O_{U'}$ on définit sur X_{cris} un faisceau d'anneaux locaux qu'on note $\underline{O}_{X/S}$. C'est encore le faisceau associé au préfaisceau

$$(U, U') \longmapsto \Gamma(U', O_{U'}) .$$

On a donc une notion de faisceau de $\underline{O}_{X/S}$-modules sur le site cristallin. Un tel objet F est déterminé par la donnée d'une structure de $O_{U'}$ - module sur les $F_{(U, U')}$, en sorte que pour $u : (V, V') \longrightarrow (U, U')$, le morphisme $u^{\natural}$ induise un homomorphisme de $O_{V'}$ - modules (encore noté $u^{\prime}$) $u^*F_{(U,U')} \to F_{(V,V')}$, l'image réciproque étant ici calculée en tant que module. Un faisceau de modules sur X_{cris} tel que tous les $u^{\natural}$ soient des isomorphismes est appelé un faisceau de modules spécial.

2.7. Cristaux.

Définition. Un faisceau en modules spécial F s'appelle un cristal en modules. Si, de plus, pour tout (U, U') les $F_{(U, U')}$ sont des $O_{U'}$ - modules quasi cohérents (resp. localement libres), on dit que F est un cristal en modules quasi cohérents (resp. localement libres).

Proposition. Un $\underline{O}_{X/S}$ - module est quasi cohérent (resp. localement libre) si et seulement si c'est un cristal en modules quasi cohérents (resp. localement libres).

Vérification immédiate.

2.8. F-Cristaux.

Plus généralement, soit F une catégorie fibrée sur Sch/S. Un F-cristal consiste en la donnée, pour tout objet (U,U') du site cristallin, d'un objet $F_{(U,U')}$ de $Ob F(U')$ où $F(U')$ désigne la catégorie fibre de F au-dessus de U' et, pour tout $v : (V,V') \longrightarrow (U,U')$, d'un isomorphisme

$$u \quad : \quad u^* F_{(U,U')} \longrightarrow F_{(V,V')} \quad ,$$

ces données étant soumises aux conditions de transitivité habituelles. La notion de cristal est souvent plus intéressante que celle de faisceau cristallin.

3. Relation entre cristaux et vecteurs de Witt.

Soit S un schéma sur $\Lambda_n = \mathbb{Z}/p^n\mathbb{Z}$. On désignera par S_{Zar} le topos Zariskien de S et par $S_{n\text{-cris}}$ le topos $(S|\Lambda_n, p\Lambda_n, \gamma)_{cris}$, c'est-à-dire le topos annelé cristallin (de Berthelot) de S relativement à Λ_n et à l'idéal $p\Lambda_n$ muni de la structure à puissances divisées canonique.

Soit W_n le schéma des vecteurs de Witt de longueur n et soit $W_n(\underline{O}_S)$ le faisceau d'anneaux

$$U \longmapsto W_n(\Gamma(U,\underline{O}_U))$$

sur S_{Zar}. On désignera par $S_{n\text{-Witt}}$ le topos annelé

$$S_{n\text{-Witt}} = (S_{Zar}\ ,\ W_n(\underline{O}_S)) \quad .$$

Si l'on suppose que S est de caractéristique p, nous allons définir des morphismes de topos annelés φ_n et Ψ_n

$$S_{n\text{-Witt}} \underset{\Psi}{\overset{\varphi_n}{\rightleftarrows}} S_{n\text{-cris}}$$

vérifiant $\varphi_n \Psi_n = F^n_{\mathbb{W}_n}$, c'est-à-dire est le morphisme identité sur les objets du topos $S_{n\text{-Witt}}$ et est défini sur les sections de $\mathbb{W}_n(\underline{O}_S)$ par l'homomorphisme induit par la puissance $n^{\text{ème}}$ de l'endomorphisme de Frobenius de $\mathbb{W}_{nF_p}$.

3.1 Lemme. Sur l'idéal d'augmentation $\ker\{\mathbb{W}_n(\underline{O}_{\mathbb{Z}_{(p)}}) \to \underline{O}_{\mathbb{Z}_{(p)}}\}$ de $\mathbb{W}_n(\underline{O}_{\mathbb{Z}_{(p)}})$, il existe une unique structure de puissances divisées.

Pour l'existence, on remarque d'abord que pour définir γ_N sur l'idéal d'augmentation de $\mathbb{W}_{n\mathbb{Z}_p}$, il suffit de définir $\gamma_N V$ sur tout $\mathbb{W}_n$, puisqu'en effet on a $V(\mathbb{W}_n(B) \xrightarrow{\sim} \ker\{\mathbb{W}_n(B) \to B\}$ pour tout anneau B.

Pour toute $\mathbb{Z}_{(p)}$-algèbre B et tout $x \in \mathbb{W}_n(B)$, on pose

$$\gamma_N V(x) = p^{N-1}/N! \quad V(x^N)$$

ce qui a bien un sens car $p^{N-1}/N! \in \mathbb{Z}_{(p)}$ et $\mathbb{W}_n(B)$ est une $\mathbb{Z}_{(p)}$-algèbre.

Pour montrer que cela définit bien une structure à puissances divisées et que celle-ci est unique, considérons l'homomorphisme

$\phi : \mathbb{W}_n \to \mathbb{O}^n$ qui a servi à définir la structure d'anneau de $\mathbb{W}_n$(I.1). On a

$$\phi V = p V' \phi$$

où V' est l'endomorphisme $(x_1,\ldots,x_n) \longmapsto (0,x_1,\ldots,x_{n-1})$ dans $\mathbb{O}^n$. Cet homomorphisme est multiplicatif et on peut donc écrire

$$\phi\gamma_N V(x) = \phi p^{N-1}/N!\ V(x^N) = p^{N-1}/N!\ \phi V(x^N)$$

$$= p^{N-1}/N!\ pV'\phi(x^N) = p^N/N!\ [V'\phi(x)]^N$$

$$= 1/N!\ [pV'\phi(x)]^N = 1/N!\ [\phi V(x)]^n$$

d'où, posant $y = V(x)$,

$$(*) \qquad \phi\gamma_N(y) = 1/N!\ \phi(y^N) \ .$$

Comme $\mathbb{Z}_p$ est intègre, cette égalité détermine uniquement

$$\gamma_N(y) = (0,g_1,\ldots,g_N) \in \mathbb{W}_n(B)$$

où les g_i sont des polynômes à coefficients dans $\mathbb{Z}_p$ (et pas seulement dans $\mathbb{Q}$). Le fait que γ_N soit bien une puissance divisée résulte clairement de (*) et l'unicité provient de ce que de l'égalité $N!\gamma_N(y) = y^N$ on tire que l'on a nécessairement (*) .

Il résulte de ceci que si X est un schéma de caractéristique p, on peut considérer X_{W_n} = Spec $W_n(\mathcal{O}_X)$ = $(X, W_n(\mathcal{O}_X))$ (schéma ayant même espace topologique que X mais ayant $W_n(\mathcal{O}_X)$ comme faisceau structural) comme épaississement de X muni de puissances divisées compatibles avec celles de Λ_n. En particulier, si X est un ouvert de S, X_{W_n} est un objet du site cristallin de S au-dessus de Λ_n. Donc, tout cristal en quelque chose (module, algèbre...) sur S définit un objet avec le même type de structure sur S_{W_n}.

3.2 Définition de $\Psi_n : S_{n\text{-Witt}} \longrightarrow S_{n\text{-cris}}$.

Par définition,

$$\Psi_n^* : S_n\text{-cris} \longrightarrow S_{n\text{-Witt}}$$

est le foncteur

$$\{F : (U,U') \longmapsto F(U,U')\} \longmapsto \{\Psi_n^* F : U \longmapsto F(U,U_{W_n})\}$$

où (U, U_{W_n}) est l'épaississement naturel défini précédemment. On a alors

$$\Psi_n^* \mathcal{O}_{S_{n\text{-cris}}} : U \longmapsto W_n(\Gamma(U,\mathcal{O}_U))$$

et on prend pour homomorphisme d'anneaux

$$\Psi_n^* \mathcal{O}_{\mathcal{S}_{n\text{-cris}}} \longrightarrow W_n(\mathcal{O}_S)$$

l'homomorphisme identité.

3.3 Définition de φ_n .

Soit A une Λ_n-algèbre et soit $A \to A_0$ un homomorphisme surjectif d'anneaux dont le noyau J vérifie la condition suivante:

(*) pour tout $x \in J$ et tout $i, 0 \leq i \leq n$, on a $p^i x^{p^{n-i}} = 0$.

Par exemple, cette condition est vérifiée si J est un idéal à puissances divisées. En effet, si on a $p^n x = 0 \quad \forall x \in J$, on a aussi $p^i x^{p^{n-i}} = p^i p^{n-i}! \, x^{(p^{n-i})} = p^n y = 0$.

Considérons alors l'homomorphisme d'anneaux

$$\Phi_{n+1} : W_{n+1}(A) \longrightarrow A$$

$$\Phi_{n+1}(x_1, x_2, \ldots, x_{n+1}) = x_1^{p^n} + p x_2^{p^{n-1}} + \ldots + p^{n-1} x_n^p + p^n x_{n+1} .$$

Cet homomorphisme est nul sur $V^n W_{n+1}(A) = \ker\{R_n : W_{n+1}(A) \to W_n(A)\}$ et définit donc par passage au quotient un homomorphisme d'anneaux

$$\phi' = \phi_n F : W_n(A) \longrightarrow A$$

$$\phi'(x_1, \ldots, x_n) = x_1^{p^n} + p x_2^{p^{n-1}} + \ldots + p^{n-1} x_n^p .$$

D'après la condition (*), ϕ' est nul sur

$$W_n(J) = \ker\{W_n(A) \longrightarrow W_n(A_0)\}$$

et se factorise donc à son tour en un homomorphisme

$$\xi_{nA} : W_n(A_0) \longrightarrow A .$$

Cet homomorphisme est fonctoriel en A.

On définit alors $\varphi_n : S_{n\text{-cris}} \longrightarrow S_{n\text{-Witt}}$ comme suit: Le morphisme de topos sous-jacent

$$\varphi_n^* : S_{n\text{-Witt}} \longrightarrow S_{n\text{-cris}}$$

est le foncteur

$$\{F : U \longmapsto F(U)\} \longmapsto \{ \varphi_n^*F : (U,U') \longmapsto F(U) \} .$$

En d'autres termes (avec les notations de 2.5), on a $\varphi_n^*F_{(U,U')} = i_*F/U$ (où i désigne la nil-immersion $u \hookrightarrow U'$). On a alors $\varphi_n^* W_n(\underline{0}_S) : (U,U') \longmapsto W_n(\Gamma(U,0_U))$ et on prend pour homomorphisme d'anneaux $\xi : \varphi_n^* W_n(\underline{0}_S) \longrightarrow \underline{0}_{S_{n\text{-cris}}}$ l'homomorphisme

$$(U,U') \longmapsto \xi_{n\Gamma(U',0_{U'})} : W_n(\Gamma(U,0_U)) \longrightarrow \Gamma(U',0_{U'}) .$$

3.4 Etude du composé $\varphi_n \Psi_n : S_{n\text{-Witt}} \longrightarrow S_{n\text{-Witt}}$

Il est clair que le morphisme de topos sous-jacent $\Psi_n^* \varphi_n^*$ est l'identité. Il reste à montrer que l'homomorphisme d'anneaux

$$\Psi_n^* \xi : W_n(\underline{O}_S) = \Psi_n^* \varphi_n^* W_n(\underline{O}_S) \longrightarrow \Psi_n^* O_{S_{n\text{-cris}}} \xrightarrow{\text{identité}} W_n(\underline{O}_S)$$

n'est autre que

$$U \longmapsto \{ F^n : W_n(\Gamma(U,O_U)) \longrightarrow W_n(\Gamma(U,O_U)) \} .$$

On doit utiliser la construction de ξ_{nA} dans le cas où A_0 est une $\mathbb{F}_p$-algèbre, $A = W_n(A_0)$ et J est l'idéal d'augmentation. Soit

$$\varepsilon : A_0 \longrightarrow A = W_n(A_0) , \quad \varepsilon(x) = (x,0,\ldots,0)$$

un système de représentants multiplicatifs. Si $(x_1,x_2,\ldots,x_n) \in W_n(A_0)$, on le relève en $(\varepsilon(x_1), \varepsilon(x_2),\ldots, \varepsilon(x_n)) \in W_n(A)$ et on a

$$\xi_{nA}(x_1,\ldots,x_n) = \sum_{i=0}^{n-1} p^i \varepsilon(x_{i+1}^{p^{n-i}}) = (x_1^{p^n},\ldots,x_n^{p^n})$$

puisqu'en effet on a (I.2.3) :

$$\sum_{i=0}^{n-1} p^i \varepsilon(y_{i+1}) = (y_1, y_2^p, \ldots, y_n^{p^{n-1}}) .$$

L'étude du composé $\Psi_n \varphi_n$ sur $S_{n\text{-cris}}$ est laissée en exercice.

4. Cas d'un schéma parfait.

On suppose toujours S de caractéristique p et on considère maintenant le topos $S_{cris} = (S|\mathbb{Z}_{(p)}, p\mathbb{Z}_{(p)})$ de S au-dessus de $\mathbb{Z}_{(p)}$. Comme tout épaississement (U,U') est une nilimmersion, p est localement nilpotent sur U', de sorte que si U est quasi compact, (U,U') est en fait un objet du site cristallin de S sur Λ_n pour n suffisamment grand. Il en résulte en particulier que les sites cristallins de S au-dessus de $\mathbb{Z}_{(p)}$ et de S au-dessus de $\hat{\mathbb{Z}}_{(p)} = \mathbb{Z}_p$ sont identiques.

4.1. Notations

Soit A un anneau et I un idéal de A. Pour tout entier $n \geq 1$, on désigne par I_n l'idéal engendré par les éléments $p^{i-1} x^{p^{n-i}}$, $x \in I$, $1 \leq i \leq n$.

Les I_n forment une suite décroissante d'idéaux et on a $I_1 = I$, $p^{n-1} I \subset I_n$. Si I est muni de puissances divisées, on a alors l'égalité $p^{n-1} I = I_n$ car

$$p^{i-1} x^{p^{n-i}} = p^{i-1} p^{n-i}! \, x^{(p^{n-i})} = p^{n-1} y, \quad \text{avec} \quad y \in I .$$

Si l'on suppose de plus que $p \in I$ (et donc $p^n \in I_n$), on a alors les inclusions

$$p^n A \subset I_n = p^{n-1} I \subset p^{n-1} A .$$

4.2 Théorème. Soit A un anneau et $I \subset A$ un idéal. Supposons

(i) $A_1 = A/I$ de caractéristique $p > 0$ et parfait

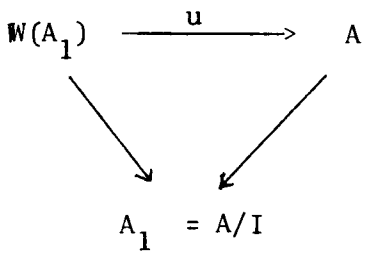
(ii) A séparé et complet pour la topologie définie par les I_n (c'est-à-dire $A \simeq \varprojlim A/I_n$).

La condition ii) est vérifiée par exemple si I est nilpotent, ou encore, si I est à puissances divisées et si A est séparé et complet pour la topologie p-adique.

Alors il existe un et un seul homomorphisme

$$u : \mathbb{W}(A_1) \longrightarrow A$$

compatible avec les augmentations de A et $\mathbb{W}(A_1)$, c'est-à-dire rendant le diagramme suivant commutatif.



De plus, l'homomorphisme u possède les propriétés suivantes:

a) Pour tout n, on a

$$u^{-1}(I_n) \supset V^n \mathbb{W}(A_1) = \ker\{\mathbb{W}(A_1) \longrightarrow \mathbb{W}_n(A_1)\}$$

et, en particulier, u est continu.

b) Si $\varepsilon: A_1 \longrightarrow W(A_1)$ est un système de "représentants multiplicatifs" de A_1, soit $R \subset A$ l'image de $u\varepsilon$. Alors R est l'ensemble des $x \in A$ tels que pour tout n il existe $y \in A$ tel que $y^{p^n} = x$. R est stable par multiplication et l'application $R \to A_1$ induite par l'augmentation $A \to A_1$ est bijective, donc admet une application inverse $\alpha: A_1 \to R \subset A$ qui est multiplicative.

c) Si $x = (x_1, x_2, \ldots, x_i, \ldots) \in W(A_1)$, on a

$$u(x) = \sum_{i \geq 0} p^i \alpha(x_{i+1}^{p^{-i}}) \qquad \text{(série convergente dans A).}$$

Démonstration. Montrons d'abord que tout homomorphisme $u : W(A_1) \to A$ compatible avec les augmentations possède les propriétés a) b) c).

a) Comme A_1 est de caractéristique p, on a $p^n \in I_n$ de sorte que u envoie $p^n W(A_1) = V^n W(A_1)$ dans I_n.

b) Il est clair que l'homomorphisme multiplicatif

$$u\varepsilon : A_1 \longrightarrow R$$

est injectif (donc bijectif) car son composé avec l'augmentation $R \subset A \to A_1$ est l'identité (on a donc $u\varepsilon = \alpha$). Montrons que

$$R = \{x \in A \mid \forall n, \ \exists y \in A \mid y^{p^n} = x \} \ .$$

Comme A_1 est parfait et isomorphe à R par l'homomorphisme multiplicatif α, on a évidemment $R = R^{p^n}$ pour tout n. Réciproquement, soit $x \in A$ pour lequel il existe pour tout n un y_n tel que $y_n^{p^n} = x$. Soient $\bar{x}$ et $\bar{y}_n$ les classes de x et de y_n dans A_1. On a $\bar{y}_n^{p^n} = \bar{x}$, d'où $\bar{y}_n = \bar{x}^{p^{-n}} = \alpha(\bar{x})^{p^{-n}}$ et donc $v = y_n - \alpha(\bar{x})^{p^{-n}} \in I$. On en déduit que l'on a

$$x = y_n^{p^n} = (\alpha(\bar{x})^{p^{-n}} + v)^{p^n} = \alpha(\bar{x}) + v' ,$$

où $v' = p^n v + \ldots$ appartient à $p^n I \subset I_{n+1}$. Comme A est séparé, on en conclut que $x = \alpha(\bar{x})$.

c) Comme on a $\alpha = u\varepsilon$ et que d'après I.2.3 on a

$$x = (x_1, x_2, \ldots, x_i, \ldots) = \sum_{i \geq 0} p^i \varepsilon(x_{i+1})^{p^i} ,$$

on a nécessairement

$$u(x) = \sum_{i \geq 0} p^i \alpha(x_i^{p^{-i}}) .$$

L'unicité de u résulte clairement de b) qui définit α de manière unique et de la formule c). Il reste à construire un homomorphisme u, et il suffit pour cela de définir une famille de morphismes

$$u_n : W_n(A_1) \longrightarrow A/I_n$$

compatibles aux morphismes de transition et telle que $u_1 = \mathrm{Id}(A_1)$. Comme le noyau I/I_n de $A/I_n \longrightarrow A/I = A_1$ satisfait à la condition (*) de 3.3, on dispose d'un homomorphisme

$$\xi_{n\ A/I_n} : \quad W_n(A_1) \longrightarrow A/I_n$$

obtenu (cf.3.3) par passage au quotient du morphisme

$$\phi_n F = \phi' : W_n(A/I_n) \longrightarrow A/I_n$$

$$\phi'(x_1,\ldots,x_n) = x_1^{p^n} + px_2^{p^{n-1}} + \ldots + p^{n-1}x_n^p \quad .$$

Les morphisme $\xi_{n\ A/I_n}$ ne commutent pas avec les homomorphismes de transition, mais on vérifie que l'on a des diagrammes commutatifs

$$\begin{array}{ccccc} W_{n+1}(A_1) & & \xrightarrow{\qquad\qquad\xi_{n+1\ A/I_{n+1}}\qquad\qquad} & & A/I_{n+1} \\ \Big\downarrow R & & & & \Big\downarrow \\ W_n(A_1) & \xrightarrow{F} & W_n(A_1) & \xrightarrow{\xi_{n\ A/I_n}} & A/I_n \end{array} \quad .$$

Comme A_1 est parfait, l'endomorphisme de Frobénius F est inversible et on construit donc des homomorphismes

$$u_n : W_n(A_1) \longrightarrow A/I_n$$

compatibles aux morphismes de transition en posant

$$u_n = \xi_{n\ A/I_n} \circ F^{-n} \quad ,$$

le nombre d'itérations de F^{-1} étant choisi de façon à ce que pour $n = 1$ on ait $u_1 = Id(A_1)$.

4.3 Proposition. Si on ne suppose plus nécessairement que A_1 est parfait mais que l'on a seulement la condition ii) du théorème 4.2, alors pour tout anneau parfait B_1 de caractéristique $p > 0$ et pour tout homomorphisme

$$v_1 : B_1 \longrightarrow A_1 ,$$

il existe un et un seul homomorphisme

$$v : \mathbb{W}(B_1) \longrightarrow A$$

qui soit compatible avec v_1 sur les anneaux d'augmentation. L'homomorphisme v est alors continu, et on a même

$$v^{-1}(I_n) \supset V^n \mathbb{W}(B_1) = \ker \{\mathbb{W}(B_1) \longrightarrow \mathbb{W}_n(B_1)\} .$$

La démonstration de cette proposition est calquée sur la précédente en remplaçant l'homomorphisme u_n par l'homomorphisme

$$v_n = \xi_{n\, A/I_n} \circ \mathbb{W}_n(v_1) \circ F^{-n} : \mathbb{W}_n(B_1) \longrightarrow A/I_n .$$

4.4 Corollaire. Soit S un schéma de caractéristique p parfait. Alors pour tout objet (U, U') du site cristallin de S au-dessus de Λ_n, il existe un unique homomorphisme (dans le site)

$$f : (U, U') \longrightarrow (S, S_{\mathbb{W}_n})$$

où $S_{\mathbb{W}_n}$ = Spec $(\mathbb{W}_n(\underline{O}_S))$ désigne l'épaississement défini en 3.1. En d'autres termes, $(S, S_{\mathbb{W}_n})$ est un objet final du site.

Démonstration. On déduit aussitôt du théorème 4.2 que pour tout ouvert affine $V' = \operatorname{Spec} A$ de U', on a, posant $V = V' \times_{U'} U = \operatorname{Spec} A_1$, un unique homomorphisme

$$U : W_n(\Gamma(V, \mathcal{O}_V)) \longrightarrow \Gamma(V', \mathcal{O}_{V'})$$

compatible avec les augmentations. Ces homomorphismes se recollent nécessairement et définissent un unique homomorphisme

$$u : f^* W_n(\underline{\mathcal{O}}_S) = W_n(\underline{\mathcal{O}}_u) \longrightarrow \underline{\mathcal{O}}_{U'}$$

compatible avec les augmentations.

4.5 Proposition. Soit S un schéma de caractéristique p parfait. Alors la catégorie des cristaux en modules quasi cohérents (resp. localement libres) du site cristallin de S au-dessus de Λ_n est équivalente à la catégorie des faisceaux de $W_n(\underline{\mathcal{O}}_S)$ - modules quasi cohérents (resp.localement libres).

Plus généralement, si F est une catégorie fibrée sur $\underline{\mathrm{Sch}}/\Lambda_n$, la catégorie des F-cristaux sur S est équivalente à la fibre $F(S_{W_n})$.

Au cristal F on fait correspondre l'objet $F_{(S,S_{W_n})} \in F(F_{W_n})$ et inversement, à l'objet G de $F(S_{W_n})$ on associe le cristal défini sur tout épaississement (U,U') par

$$G'_{(U,U')} = f^*G$$

où $f : (U,U') \to (S,S_{W_n})$ est le morphisme canonique. Le cas particulier des modules quasi cohérents (resp. localement libres) résulte de la proposition du §2.7.

4.6 Proposition. Soit S un schéma de caractéristique p parfait, et soit F une catégorie fibrée sur $\underline{Sch}/\mathbb{Z}_{(p)}$, "recollable pour la topologie de Zariski" (c'est-à-dire que pour tout schéma X la restriction de F au site des ouverts de Zariski de X est un champ - cf. Giraud, "cohomologie non abélienne"). Alors la catégorie des F-cristaux sur S est équivalente à la catégorie

$$\lim_{\leftarrow} \quad F(S_{W_n})$$

des systèmes d'objets $G_n \in \mathrm{Ob}\, F(S_{W_n})$ qui vérifient

$$G_n = i^* G_{n+1} \ ,$$

i désignant l'immersion canonique $S_{W_n} \hookrightarrow S_{W_{n+1}}$.

Exemple. La catégorie des cristaux en modules localement libres de type fini est équivalente à la catégorie des $W(\underline{O}_S)$-modules projectifs de type fini.

Démonstration. Au F-cristal F on associe le système des $G_n = F_{(S,S_{W_n})} \in F(S_{W_n})$. Inversement, si $(G_n) \in \lim_{\leftarrow} F(S_{W_n})$ et si (U,U') est un épaississement du site, on définit un objet $F_{(U,U')} \in F(U')$ obtenu par recollement des objets

$$F_{(V,V')} = f^* G_n$$

où V' est un ouvert quasi compact de V' (donc tel que $p^n = 0$ pour un certain n) et où f désigne le morphisme canonique

$$f : (V,V') \longrightarrow (S,S_{W_n}) \quad .$$

4.7. On ne suppose plus maintenant que S est parfait, mais on suppose que S est un schéma sur un corps k de caractéristique p parfait. On note alors $W = W(k)$, $W_n = W_n(k)$.

Proposition. Si (U,U') est un épaississement du site cristallin de S au-dessus de Λ_n, il existe un et un seul homomorphisme

$$g : (U, U') \longrightarrow (\mathrm{Speck}, \mathrm{Spec}\ W_n)$$

et cet homomorphisme est compatible avec les structures à puissances divisées.

La démonstration est une conséquence immédiate de la proposition 4.3 et est d'ailleurs analogue à celle de 4.4.

Corollaire. Si S est un schéma sur un corps parfait k, les sites cristallins de S au-dessus de $\mathbb{Z}_{(p)}$ (resp. de S au-dessus de Λ_n) et de S au-dessus de W (resp. de S au-dessus de W_n) sont isomorphes.

5. Cas d'un schéma relatif lisse.

Soient (S, I, γ) comme au paragraphe 2, X un S-schéma et F un module spécial sur le site Nil-Cris $(X/S, I, \gamma)$. Soit $\Delta^1(X)$ le premier voisinage infinitésimal de X dans $X \times_S X$. Sur l'idéal définissant X dans $\Delta^1(X)$, on définit des puissances divisées par $\gamma_1 =$ identité, et $\gamma_n = 0$ pour $n \geq 2$. On obtient donc un objet $X \subset \Delta^1(X)$ du site cristallin nilpotent. Considérons d'autre part le diagramme suivant:

$$\begin{array}{ccc} X & \xrightarrow{id_X} & X \\ & \searrow^{pr_1} \quad \nearrow_{pr^2} & \\ & \Delta^1(X) & \end{array}$$

Si F est un module spécial, on a des isomorphismes canoniques

$$pr_1^*(F_{X\subset X}) \xrightarrow{\sim} F_{X\subset\Delta^1 X} \xleftarrow{\sim} pr_2^*(F_{X\subset X}) \quad .$$

Mais rappelons la définition d'une connexion:

Définition (5.1). Une connexion sur un O_X-module M consiste en une donnée de descente infinitésimale

$$\phi : pr_1^*(M) \xrightarrow{\sim} pr_2^*(M)$$

satisfaisant la condition habituelle des cocycles pour le diagramme

$$\Delta_2^1(X) \;\substack{\rightarrow\\ \rightarrow\\ \rightarrow}\; \Delta^1(X) \;\substack{\rightarrow\\ \rightarrow}\; X \ ,$$

où Δ_2^1 est le premier voisinage infinitésimal de X dans $X \times_S X \times_S X$.

Une telle donnée est équivalente à la donnée d'un morphisme S-linéaire

$$\nabla : M \longrightarrow \Omega^1_{X/S} \otimes_{O_X} M$$

qui satisfait à la condition

$$\nabla(am) = da \otimes m + a \nabla m ,$$

pour toute section locale a de O_X et pour toute section locale m de M.

Définition (5.2). On appelle morphisme horizontal entre deux modules F et G, munis de connexions ϕ_F et ϕ_G, un morphisme $u : F \longrightarrow G$ qui rend commutatif le diagramme

$$\begin{array}{ccc} pr_1^*(F) & \xrightarrow{\phi_F} & pr_2^*(F) \\ {\scriptstyle pr_1^*(u)}\downarrow & & \downarrow{\scriptstyle pr_2^*(u)} \\ pr_1^*(G) & \xrightarrow[\phi_G]{} & pr_2^*(G) \end{array}$$

Les remarques précédentes permettent donc de définir un foncteur

(5.3)(Cris.Mod quasicoh (X/S)) ——> (Mod. avec connexion sur X).

On a alors les résultats:

Proposition (5.4) Si X est lisse sur S, le foncteur (5.3) induit une équivalence de la catégorie des modules spéciaux quasi cohérents sur le site Nil-Cris (X/S) sur la catégorie des O_X-modules quasi cohérents munis d'une connexion à courbure nulle.

Rappelons que dire qu'une connexion est à courbure nulle, signifie que le morphisme O_X-linéaire composé de

$$\nabla : \quad M \longrightarrow \quad \Omega^1_{X/S} \otimes_{O_X} M$$

et de l'homomorphisme

$$\Omega^1_{X/S} \otimes M \longrightarrow \Omega^2_{X/S} \otimes M$$

$$\omega \otimes f \longmapsto d\omega \otimes f - \omega \otimes \nabla f \quad ,$$

est nul.

Proposition (5.5). Si X est lisse sur S et si p est nilpotent sur S, le foncteur analogue à (5.3) induit une équivalence de la catégorie des modules spéciaux sur le site cristallin de Berthelot sur la catégorie des O_X-modules munis d'une connexion à courbure nulle et nilpotents.

Rappelons ici ce que signifie la nilpotence: soient S_0 le sous-schéma fermé de S défini par l'idéal pO_S, $X_0 = X \times_S S_0$ et F un O_X-module muni d'une connexion ∇ de courbure nulle. Sur l'image inverse F_0 de F sur X_0, on a une connexion ∇_0 "induite" par ∇, qui est à courbure nulle. On associe à ∇ (et de même à ∇_0) un morphisme

$$\bar{\nabla} : \underline{\mathrm{Der}}_S (O_X, O_X) \longrightarrow \underline{\mathrm{End}}_{O_S} (F,F)$$

par la règle: $\bar{\nabla}(D)$ est le composé de

$$\nabla : F \longrightarrow \Omega^1_{X/S} \otimes F$$

et de

$$D \otimes 1 \ ; \ \Omega^1_{X/S} \otimes F \longrightarrow F$$

L'application $\bar{\nabla}$ a les propriétés suivantes

1) $\bar{\nabla}(D_1 + D_2) = \bar{\nabla}(D_1) + \bar{\nabla}(D_2)$

2) $\bar{\nabla}(aD) = a\bar{\nabla}(D)$

3) $\bar{\nabla}(D)(af) = D(a) \cdot f + a\bar{\nabla}(D)(f)$.

Si X est lisse sur S, la donnée de $\bar{\nabla}$ vérifiant 1) 2) et 3) équivaut à celle d'une connexion. Dire que la courbure est nulle signifie qu'on a la relation

$$\bar{\nabla}([D_1, D_2]) = [\bar{\nabla}(D_1), \bar{\nabla}(D_2)] \quad .$$

Au-dessus de S_0, on définit une application dite <u>la p-courbure</u>,

$$\Psi : \underline{\mathrm{Der}}_{S_0}(O_{X_0}, O_{X_0}) \longrightarrow \underline{\mathrm{End}}_{S_0}(F_0, F_0)$$

par la règle: $\Psi(D) = \bar{\nabla}_0(D^p) - (\bar{\nabla}_0(D))^p$. L'application Ψ possède les propriétés suivantes

1) pour tout D, $\Psi(D)$ est O_{X_0} - linéaire

2) Ψ est additif

3) $\Psi(aD) = a^p \Psi(D)$

4) $\Psi(D)$, $\bar{\nabla}_0(D)$ et $\bar{\nabla}_0(D^p)$ commutent entre eux.

5) Tous les $\Psi(D)$, quand D varie, commutent entre eux.

Définition (5.6). On dit que le module F est nilpotent si les conditions suivantes équivalentes sont vraies: localement pour la topologie de Zariski,

(i) les $\bar{\nabla}_0(D_i)$ sont nilpotents pour une base convenable $\{D_i\}$ de $\underline{\mathrm{Der}}_S(O_X, O_X)$.

(ii) pour tous les D, $\Psi(D)$ est nilpotent.

(iii) pour tous les D nilpotents, $\bar{\nabla}(D)$ est nilpotent.

Les assertions de ce numéro sont dues à Berthelot, sauf l'assertion sur la p-courbure qui est due à Katz.

6. Cristaux sur un schéma sur un corps parfait de caractéristique p.

Soit k un corps parfait de caractéristique p et soit X_0 un k-schéma. La catégorie $\mathrm{Cris}(X_0/W(k))$ est alors équivalente au site $\mathrm{Cris}(X_0/\mathbb{Z}_p)$ (4.8). De plus pour une catégorie fibrée F au-dessus de $\underline{\mathrm{Sch}}$, on a une équivalence de catégories

$$F\text{-cris}(X_0/W(k)) \xrightarrow{\sim} \varprojlim F\text{-cris}(X_0/W_n(k)) \quad .$$

Supposons que X_0 est lisse sur k et que pour tout n, X_0 se relève en un schéma lisse X_n sur $W_n(k)$ tel que $X_n \simeq X_{n+1} \otimes W_n$.

$$\begin{array}{ccccc} \longrightarrow & X_n & \longrightarrow & X_{n+1} & \longrightarrow \\ & \downarrow & & \downarrow & \\ \longrightarrow & \mathrm{Spec}\, W_n(k) & \longrightarrow & \mathrm{Spec}\, W_n(k) & \longrightarrow \end{array}$$

(ce sera le cas par exemple si X_0 est affine et lisse sur k). Alors la catégorie des modules spéciaux sur $Cris(X_0/W(k))$ est équivalente à la catégorie des systèmes de modules F_n sur X_n, munis d'une connexion à courbure nulle, qui se recollent. Par un passage à la limite, on en déduit une équivalence avec la catégorie des modules F sur le schéma formel $\mathcal{X}$ sur $W(k)$ associé aux X_n, munis d'une connexion "formelle" à courbure nulle.

Supposons de plus que X_0 soit propre sur k et se relève en un schéma propre et lisse X sur $W(k)$. Alors, la catégorie des modules spéciaux sur $Cris(X_0/W(k))$ est équivalente à la catégorie des O_X-modules munis d'une connexion à courbure nulle. Soit K le corps des fractions de $W(k)$ et donnons-nous un plongement $K \subset \mathbb{C}$. La donnée d'un O_X-module avec une connexion de courbure nulle définit un objet de même type sur X_K. Mais par GAGA, il est équivalent de se donner un module avec le même type de structure sur la variété complexe $X(\mathbb{C})$. Ceci est encore équivalent à la donnée d'un système de coefficients locaux.

Dans le cas où $\mathcal{X}$ n'est pas algébrissable, on peut encore regarder l'espace rigide analytique (au sens de Tate) associé à $\mathcal{X}$. Dans ce cas, il résulte des travaux de Khiel [P.M. #33] que la cohomologie cristalline de X_0 est essentiellement la même que la cohomologie de De Rham de l'espace rigide analytique associé à $\mathcal{X}$.

7. Indications sur la cohomologie cristalline

Revenons aux conditions générales du paragraphe 2 en supposant que l'idéal I sur S satisfait à la condition de Berthelot. On s'intéresse aux groupes de cohomologie

$$H^*_{cris}(X/S) = H^*_{cris}(X/S, I, \gamma) \overset{\text{déf}}{=} H^*((X/S, I, \gamma)_{cris}, \underline{O}_{X/S}) .$$

Notons aussi par $\underline{H}_{cris}(X/S) = \underline{H}_{cris}(X/S, I, \gamma)$ le complexe de faisceaux de cohomologie cristalline $\mathbb{R} f_{cris*}(\underline{O}_{X/S})$, où $f_{cris} : X_{cris} \longrightarrow S_{cris}$ est le morphisme de topos induit par f, dont les objets de cohomologie seront notés $\underline{H}^*_{cris}(X/S)$; les $\underline{H}^i_{cris}(X/S)$ sont donc des cristaux en modules sur le topos annelé S_{cris}. (On peut aussi prendre la cohomologie à coefficients plus généraux, par exemple à coefficients dans un cristal de modules quasi cohérent...) On a de nombreuses indications que ceci est une "bonne" cohomologie, surtout lorsque $X_0 = X \times_S S_0$ est propre et lisse sur $S_0 = \mathrm{Var}(I)$. Notons les propriétés:

a) Invariance. On a des isomorphismes canoniques (X_0 étant le schéma défini ci-dessus)

$$H^*_{cris}(X/S) \xrightarrow{\sim} H^*_{cris}(X_0/S) \; ; \; \underline{H}_{cris}(X/S) \xrightarrow{\sim} \underline{H}_{cris}(X_0/S).$$

b) Lien avec de Rham. Si X est lisse sur S, on a

$$H^*_{cris}(X/S) \simeq H^*_{DR}(X/S) \overset{\text{déf}}{=} H^*(X, \underline{\Omega}^*_{X/S}) ,$$

$$\underline{H}^*_{cris}(X/S)_S \simeq \underline{H}^*_{DR}(X/S) \overset{\text{déf}}{=} \mathbb{R}^* f_* (\underline{\Omega}^*_{X/S}) ,$$

où $\underline{\Omega}^*_{X/S}$ est le complexe de de Rham de X relativement à S, et $\underline{H}^*_{cris}(X/S)_S = \mathbb{R}^*f_{cris*}(\underline{O}_{X/S})_S$ est la restriction du complexe de faisceaux cristallins $\mathbb{R}^*f_{cris*}(\underline{O}_{X/S})$ au site Zariskien sous-jacent. La connexion de $\mathbb{R}^*f_{cris*}(\underline{O}_{X/S})_S$ donne une connexion sur $\underline{H}^*_{DR}(X/S)$ qui n'est autre que la connexion de Gauss-Manin .

Ces théorèmes de comparaison prouvent en particulier que si S est le spectre d'un corps de caractéristique nulle, alors la cohomologie cristalline de X donne les "bons" nombres de Betti (car on est ramené au cas où $k = \mathbb{C}$, et on procède alors par voie transcendante, en utilisant un théorème de [15])

c) Résultats de Deligne en caractéristique 0. Signalons seulement le suivant: si S est le spectre du corps des complexes, et si X est localement de type fini sur S, alors on a des isomorphismes canoniques

$$H^*_{cris}(X/S) = H^*(X(\mathbb{C}), \mathbb{C}) \quad .$$

d) Changement de base (au niveau de la catégorie dérivée). Supposons qu'on ait un morphisme de changement de base $u : (S', I', \gamma') \longrightarrow (S,I,\gamma)$. On a alors pour X_0 lisse et cohérent sur S_0:

$$u^*(\mathbb{R} f_{cris*}(\underline{O}_{X/S})) \simeq \mathbb{R}f'_{cris*}(\underline{O}_{X'/S'})$$

où $f' : X' \longrightarrow S'$ est le morphisme déduit de $f : X \longrightarrow S$ par extension de base de S à S'.

e) Formule de Künneth. Pour deux schémas relatifs X, X' cohérents sur S, avec X_0, X'_0 lisses, on a

$$\mathbb{R}(fx_S f')_{cris*}(\underline{O}_{Xx_SX'/S}) \simeq \mathbb{R}f_{cris*}(\underline{O}_{X/S}) \overset{L}{\otimes} \mathbb{R}f'_{cris*}(\underline{O}_{X'/S}) \quad .$$

f) Finitude. Si X_0 est propre et lisse sur S_0, le complexe $\mathbb{R}f_{cris*}(\underline{O}_{X/S})$ est parfait, i.e., isomorphe localement (pour la topologie de Zariski) à un complexe L^* tel que tous les L^i sont localement libres de type fini et $L^i = 0$ sauf pour un nombre fini de i.

g) Il existe une théorie des classes de Chern cristalline (Berthelot-Illusie [5]).

h) Cas d'un schéma sur un corps k de caractéristique p. Soit X_0 un schéma au-dessus de k, et soit $\Lambda_n = \mathbb{Z}/p^n\mathbb{Z}$. Alors, en passant à la limite dans les cohomologies cristallines relativement aux Λ_n, on obtient des groupes (et faisceaux) de cohomologie

$$H^*_{cris}(X_0) \overset{dfn}{=} \lim_{\leftarrow n} H^*_{cris}(X_0/\Lambda_n)$$

$$\underline{H}_{cris}(X_0) \overset{dfn}{=} \lim_{\leftarrow n} \underline{H}_{cris}(X_0/\Lambda_n) \quad .$$

Supposons maintenant que k soit parfait, et que X_0 soit propre et lisse sur k. Alors dans ce cas, $\underline{H}_{cris}(X_0)$ est un complexe parfait de $W = W(k)$ - modules (voir SGA XV (Houzel), p. 31-39), dont les objets de

cohomologie sont les $H^i_{cris}(X_0)$. Cette cohomologie est fonctorielle, commute aux changements de base, et satisfait à Künneth. Donc, modulo torsion sur W, on a

$$H^*_{cris}(X_0) \otimes H^*_{cris}(Y_0) \xrightarrow{\sim} H^*_{cris}(X_0 \times_k Y_0) .$$

Si $f_0 : X_0 \to k$ se relève à $f : X \to W$ avec f propre et lisse, et si on pose $X_n = X \times_W W_n$, on a des isomorphismes

$$H^*_{cris}(X_0) = \varprojlim_n H^*_{cris}(X_n/W_n) \xrightarrow{\sim} \varprojlim H^*_{DR}(X_n/W_n) \xrightarrow{\sim} H^*_{DR}(X/W) ,$$

et on retrouve l'invariance de la cohomologie de de Rham pour différents relèvements de X_0 dans le cas propre. Il peut arriver que l'on ait un relèvement non pas à W mais à un anneau de valuation complet V d'inégale caractéristique à corps résiduel k. Alors on a $W \subset V$, et, si L est le corps des fractions de V,

$$H^*_{DR}(X_L) \simeq H^*_{cris}(X_0) \otimes_W L .$$

Or $H^*_{DR}(X_L)$ est muni d'une filtration naturelle (provenant de l'hypercohomologie), d'où le relèvement s'exprime par le fait que sur $H^*_{cris}(X_0) \otimes_W L$ apparait une filtration.

Remarques: Lacunes de la théorie. Elles sont immenses, déjà au niveau de la théorie pour des schémas de type fini sur un corps k, notamment pour k de caractéristique p. En effet:

1) Si X_0 est lisse sur k (car k = p), mais si X_0 n'est pas propre sur k (où si X_0 est propre, mais non lisse), on trouve des invariants pathologiques (ne satisfaisant pas à un théorème de finitude). Il faut sans doute faire appel aux constructions de Monsky-Washnitzer, et définir un site M-W-cristallin. Il est à craindre que dans ce processus, on soit amené à perdre les phénomènes de torsion.

2) Sauf en caractéristique nulle (cas traîté par Deligne), on ne sait pas quelles doivent être les bonnes conditions de finitude sur des coefficients plus généraux que le faisceau structural, qui joueraient le rôle de faisceaux de $\mathbb{C}$-vectoriels transcendants algébriquement constructibles, et seraient stables par les opérations habituelles (telles que les $R^i f_*(\underline{O}_{X/S})$). D'ailleurs, même sur le corps $\mathbb{C}$, la théorie des $R^i f_*$ dans le cadre des coefficients de Deligne n'a pas été développée de façon purement algébrique.

3) Même dans le cas propre et lisse sur k parfait de caractéristique p, on n'a pas mis au point un théorème de dualité (avec Gysin).

CHAPITRE V

PROGRAMME

1. Foncteur de Dieudonné.

Soit S un schéma où p est localement nilpotent et soit S_{cris} le topos cristallin de S relativement à $\mathbb{Z}_{(p)}$. On définit un foncteur additif

$$\mathbb{D}^* : BT(S)^o \to \text{Crisloclib } (S)$$

compatible aux images inverses (donc foncteur cartésien sur la catégorie fibrée des groupes de BT sur des bases où p est localement nilpotent). Si $S_0 = \text{Var}(p)$, on a une équivalence de catégories

$$\text{Crisloclib } (S) \xrightarrow{\sim} \text{Crisloclib } (S_0)$$

de sorte que la donnée de $\mathbb{D}^*$ équivaut à la donnée de

$$\mathbb{D}^* : BT(S_0)^o \longrightarrow \text{Crisloclib } (S_0) ,$$

i.e., on est ramené au cas S de caractéristique p. Dans le cas général, $\mathbb{D}^*(G)$ ne dépend que de $G_0 = G \times_S S_0$.

Plaçons-nous sur S_0 de caractéristique p. Utilisant F_{G_0} et V_{G_0} et la compatibilité de $\mathbb{D}^*$ aux images inverses, on voit que $M = \mathbb{D}^*(G_0)$ est naturellement muni de morphismes F_M, V_M

$$M^{(p)} = \mathfrak{C}^*_S(M) \underset{V_M}{\overset{F_M}{\rightleftarrows}} M$$

satisfaisant

$$V_M F_M = p\, id_{M^{(p)}}, F_M V_M = p\, id_M \quad .$$

On appelle un tel triple (M, F_M, V_M) un F-V-cristal ou cristal de Dieudonné, et on a donc un foncteur

$$\mathbb{D}^* : BT(S_0)^o \longrightarrow F\text{-}V\text{-}Cris(S_0) \ .$$

C'est ce foncteur qui mérite le nom de foncteur de Dieudonné. On voit que sa formation commute à tout changement de base. De plus, on prouve que pour S_0 spectre d'un corps parfait, il coïncide à isomorphisme canonique près avec le foncteur de Dieudonné habituel, qui est alors une équivalence de catégories, de sorte que dans ce cas la connaissance de $\mathbb{D}^*(G_0)$ permet de reconstituer G_0. Ainsi, dans le cas général, la connaissance de $M = \mathbb{D}^*(G_0)$ comme F-V-cristal sur S_0 permet de retrouver les fibres de G_0 en des corps parfaits au-dessus de S_0; cela justifie donc le sentiment que pour l'essentiel, on a saisi avec le cristal $M = \mathbb{D}^*(G_0)$ la famille des $G_{0\bar{s}}$. Une question importante que je n'ai pas résolue est:

Problème 1: Le foncteur de Dieudonné sur une base S_0 de caractéristique p est-il pleinement fidèle? Son image essentielle est-elle formée des F-V-cristaux "admissibles" définis plus bas?

Pour résoudre cette question, il me semble qu'il faudrait arriver à formuler une théorie de Dieudonné sur S_0 pour des schémas en p-groupes finis localement libres sur S_0 quelconques, ou du moins pour ceux plats sur un $\Lambda_n = \mathbb{Z}/p^n\mathbb{Z}$ en trouvant une équivalence entre la catégorie de ces groupes sur S_0, et une catégorie de F-V-cristaux sur S_0 muni de structures supplémentaires (sans doute inutile si S_0 est parfait) que je n'ai pas réussi à dégager encore, et qui très probablement impliqueront la donnée d'une filtration sur un objet convenable d'une catégorie dérivée...

Problème 2. Développer une telle théorie de Dieudonné pour des p-groupes finis localement libres sur une base S_0 de caractéristique $p > 0$. Si S_0 est parfait, établir une anti-équivalence entre la catégorie des p-groupes finis localement libres sur S_0 qui sont plats sur Λ_n, et la catégorie des $W_n(\underline{O}_S)$ - Modules localement libres M, muni de F_M et V_M satisfaisant les conditions habituelles.

Une solution affirmative à ce dernier problème devrait évidemment impliquer une solution affirmative au problème 1 dans le cas où S_0 est un schéma parfait (cf. IV 4.5).

2. Filtrations associées aux cristaux de Dieudonné. Revenons au cas d'un S général (sur lequel p est localement nilpotent). On définit alors, pour tout $G \in \mathrm{Ob}\ BT(S)$, une filtration du Module localement libre $\mathbb{D}^*(G)_S$ sur S par un sous-Module localement facteur direct (donc localement libre de type fini) $\mathrm{Fil}^1 = \underline{\omega}_G$, donnant lieu à une suite exacte

$$(*) \qquad 0 \longrightarrow \underline{\omega}_G \longrightarrow \mathbb{D}^*(G)_S \longrightarrow \underline{t}_{G^*} \longrightarrow 0 \ ,$$

où en fait $\underline{\omega}_G$ est le module des différentielles invariantes sur le groupe formel $\bar{G}$ associé à G (qui sera construit plus loin), et $\underline{t}_G = \underline{\check{\omega}}_{G^*}$ est l'Algèbre de Lie associée au groupe de BT dual G^* de G. Cette suite exacte est fonctorielle en G et compatible aux images inverses par un $S' \to S$.

Appelons F-V-<u>cristal filtré sur</u> S (par abus de langage) un F-V-cristal en Modules localement libres M sur S muni de la donnée d'une filtration de M_S par un sous-module localement facteur direct.

On trouve donc en fait un foncteur

$$BT(S) \longrightarrow \text{F-V-crisfil}(S) \ ,$$

compatible aux images inverses.

<u>Remarque</u>. La filtration (*) doit être considérée comme étant l'équivalent d'une filtration "de Hodge" sur une cohomologie de De Rham relative en dimension 1. Ce point sera explicité plus bas.

Soit maintenant S' un épaississement à puissances divisées de S. On se propose de trouver tous les prolongements possibles (à isomorphisme près) du groupe de Barsotti-Tate G donné sur S en un groupe de Barsotti-Tate G' sur S' tel que $G' \times S = G$. On prouvera que si à tout tel G' on associe la filtration correspondante sur $\mathbb{D}^*(G')_{S'} = \mathbb{D}^*(G)_{S'}$

$= \mathbb{D}^*(G_o)_{S'}$ (en effet S' peut être considéré comme épaississement de S_o), filtration qui prolonge celle que l'on a sur $\mathbb{D}^*(G)_S = \mathbb{D}^*(G_o)_S$, on trouve une bijection entre l'ensemble des classes d'isomorphie cherchées et l'ensemble des filtrations qui prolongent. De façon plus précise, on a

Théorème de déformation pour les groupes de Barsotti-Tate.

Soient S un schéma où p est localement nilpotent, S' un épaississement à puissances divisées de S, et considérons le foncteur canonique

$BT(S') \rightarrow$ catégorie des paires d'un groupe de Barsotti-Tate G' et d'un sous-module localement facteur direct de $\mathbb{D}^*(G)_S$, qui prolonge le sous-module $\mathrm{Fil}^1 \mathbb{D}^*(G)_S = \underline{\omega}_G$ de $D^*(G)_S$.

Alors, ce foncteur est une équivalence de catégories si S' est à puissances divisées nilpotentes ou si on se borne à des groupes G, G' qui sont infinitésimaux ou ind-unipotents.

Remarque. Si le problème 1 avait une réponse affirmative, on en conclurait une description de la catégorie des groupes de Barsotti-Tate sur S en termes de cristaux de Dieudonné filtrés sur S, en appliquant le théorème de déformation aux cas du couple (S_o, S), notant que l'idéal $p\,\underline{O}_S$ est bien un idéal à puissances divisées. On notera d'ailleurs que le théorème de déformation dans le cas général (S, S') est en fait

équivalent au cas particulier d'un couple (S_o, S), car il est formel via Crisloclib $(S) \xrightarrow{\sim}$ Crisloclib (S_o).

Problème 3. Trouver une variante du théorème de déformation pour les p-groupes finis localement libres.

3. F-V-cristaux admissibles en caractéristique p.

Revenons au cas d'un schéma de caractéristique p. Le cristal de Dieudonné $\mathbb{D}^*(G_o)$ étant muni d'une filtration canonique (de $\mathbb{D}^*(G_o)_{S_o}$), on pourrait craindre que le problème 1 est mal posé, et qu'il faudrait envisager le foncteur comme étant à valeurs dans des cristaux de Dieudonné filtrés. En fait, dans le cas envisagé ici, il se trouve que la filtration est uniquement déterminée en termes de la structure de cristal de Dieudonné, comme on va l'expliquer maintenant.

Considérons le morphisme de topos annelés (qui a été défini déjà précédemment, dans le paragraphe d'exemples de cristaux, pour les relations entre cristaux et vecteurs de Witt)

$$\varphi : (S_o \mid \mathbf{F}_p)_{cris} = (S_o)_{1\text{-}cris} \rightleftarrows (S_o)_{Zar} = (S_o)_{1\text{-}Witt}.$$

Soit $M = \mathbb{D}^*(G_o)$, et soit M_o sa restriction au site cristallin relatif à $\mathbb{F}_p$. Il se trouve que d'après $FV = p$, $VF = p$, les composés dans la suite

$$M_o^{(p)} \xrightarrow{F_{M_o}} M_o \xrightarrow{V_{M_o}} M_o^{(p)} \xrightarrow{F_{M_o}} M_o$$

sont nuls; en fait, on prouvera mieux, à savoir que pour tout cristal de Dieudonné M, la suite précédente est exacte (terme à terme sur tout épaississement à puissances divisées de caractéristique p de S_o) et on obtient ainsi des sous-cristaux en modules localement libres

$$\text{Ker } V_{M_o} = \text{Im } F_{M_o} \subset M_o \ , \quad \text{Ker } F_{M_o} = \text{Im } V_{M_o} \subset M_o^{(p)} \ .$$

Ceci dit, notons que $M_{S_o} = \underset{\sim}{\Psi}^*(M_o)$, donc (III.3)

$$\varphi^*(M_{S_o}) \simeq M_o^{(p)} \ ,$$

et donc on a

$$\varphi^* \ (\text{Fil}^1(M_{S_o})) \subset M_o^{(p)} \ .$$

Ceci posé, on montre qu'on a

$$\varphi^*(\text{Fil}^1(M_{S_o})) = \text{Ker } F_{M_o} \quad (= \text{Im } V_{M_o}) \subset M_o^{(p)} \ .$$

D'autre part, on montre que φ a des propriétés de fidélité telles que la relation précédente détermine sans ambiguité le sous-Module localement facteur direct Fil^1 de M_{S_o}.

On dira qu'un F-V-cristal en modules localement libres M_o sur le site cristallin de S_o au-dessus de $\mathbb{F}_p$ est <u>admissible</u> s'il existe une sous-module localement facteur direct Fil^1 de $(M_o)_{S_o}$ tel que l'on ait la relation précédente; ce Fil^1 est unique et détermine une filtration qu'on appellera la <u>filtration canonique.</u> On dit de même qu'un cristal de

Dieudonné M sur S_o est admissible si la restriction M_o au site cristallin relatif à $\mathbb{F}_p$ est admissible. On voit donc que si M est le cristal de Dieudonné associé à un groupe de BT sur S_o, M est admissible, et la filtration de M_{S_o} envisagée dans §2 est la filtration canonique définie précédemment.

4. La théorie de déformation pour les schémas abéliens.

Dans cette théorie, il n'y a plus de nombre premier privilégié, par contre il faut travailler avec le site cristallin nilpotent. On trouve un foncteur contravariant de la catégorie des schémas abéliens sur le schéma S vers les cristaux sur le site cristallin nilpotent de S.

$$(*) \qquad \text{Schémab}\,(S) \longrightarrow \text{Crisloclib}_{nilp}(S) \ ,$$

qui peut être défini par exemple comme

$$\mathbb{D}^* : A \longmapsto R^1 f_{cris*}(\underline{\mathcal{O}}_{A_{cris}})$$

où on considère

$$f_{cris} : A_{crisnilp} \longrightarrow S_{crisnilp}$$

induit par $f : A \to S$. Par une variante du théorème de changement de base, on voit que

$$\mathbb{D}^*(A)_S = \underline{H}^1_{DR}(A/S) \overset{dfn}{=} R^1 f_*(\Omega^\bullet_{A/S}) \ .$$

Pour calculer $\mathbb{D}^*(A)_{S'}$, S' épaississement à puissances divisées localement nilpotentes de S, on aura pour tout prolongement de A en un schéma abélien A' sur S'

$$\mathbb{D}^*(A)_{S'} = \underline{H}^1_{DR}(A'/S') \quad .$$

On notera que d'après un théorème connu (cf. livre de Mumford: Geometric Invariant Theory) il existe toujours un A' pour S affine; le fait que $\underline{H}^1(A'/S')$ ne dépende, à isomorphisme près, pas du prolongement choisi de A, peut être considéré ici comme conséquence du tapis de la cohomologie cristalline.

En fait, utilisant la filtration de Hodge sur la cohomologie de De Rham, on trouve une filtration sur $\mathbb{D}^*(A)_S$, savoir

$$0 \to R^0f_*(\Omega^1_{A/S}) \to \underline{H}^1_{DR}(A/S) \to R^1f_*(\underline{O}_S) \to 0$$

qu'on peut interpréter comme

$$(**) \qquad 0 \to \underset{\underline{\omega}_A}{\overset{\vee}{\underline{t}_A}} \to \mathbb{D}^*(A)_S \to \underline{t}_{A^*} \to 0 \quad .$$

Le foncteur (*) et la suite exacte (**) sont fonctoriels en A et compatibles avec image inverse. On peut considérer que le foncteur (*) se factorise

$$\mathbb{D}^* : \text{Schémab}(S) \longrightarrow \text{Crisloclib}_{\text{nilp}}\ \text{fil}(S)$$

vers les cristaux en modules localement libres "filtrés" (en deux crans localement libres). Utilisant cette factorisation, on trouve que pour un objet S' du site cristallin nilpotent de S, la donnée d'un prolongement de A en un schéma abélien A' sur S' revient à la donnée d'un prolongement de la filtration canonique (**) de $\mathbb{D}^*(A)_S$ en une filtration (à quotients localement libres) de $\mathbb{D}^*(A)_{S'}$. Plus précisément, on a le

Théorème de déformation pour les schémas abéliens.

Soient S un schéma, S' un voisinage à puissances divisées localement nilpotentes de S, alors le foncteur naturel

$$\text{Schémab}(S') \to \text{catégorie des couples } (A, \text{Fil}^1) \text{ d'un schéma abélien A sur S et d'un sous-module localement facteur direct } \text{Fil}^1 \text{ de } \mathbb{D}^*(A)_{S'} \text{ prolongeant } \text{Fil}^1 \mathbb{D}^*(A)_S \simeq \underline{\omega}_A$$

est une équivalence de catégories.

On peut donner une deuxième interprétation du foncteur $\mathbb{D}^*$ sur les schémas abéliens permettant de définir un foncteur quasi inverse du foncteur du théorème. Pour ceci, on considère pour tout schéma abélien A sur S son extension vectorielle universelle, qui est une extension

$$\mathbb{D}^* : \text{Schémab}(S) \longrightarrow \text{Crisloclib}_{\text{nilp}}\ \text{fil}(S)$$

vers les cristaux en modules localement libres "filtrés" (en deux crans localement libres). Utilisant cette factorisation, on trouve que pour un objet S' du site cristallin nilpotent de S, la donnée d'un prolongement de A en un schéma abélien A' sur S' revient à la donnée d'un prolongement de la filtration canonique (**) de $\mathbb{D}^*(A)_S$ en une filtration (à quotients localement libres) de $\mathbb{D}^*(A)_{S'}$. Plus précisément, on a le

Théorème de déformation pour les schémas abéliens.

Soient S un schéma, S' un voisinage à puissances divisées localement nilpotentes de S, alors le foncteur naturel

Schémab (S') → catégorie des couples (A, Fil^1) d'un schéma abélien A sur S et d'un sous-module localement facteur direct Fil^1 de $\mathbb{D}^*(A)_{S'}$, prolongeant $\text{Fil}^1 \mathbb{D}^*(A)_S \simeq \underline{\omega}_A$

est une équivalence de catégories.

On peut donner une deuxième interprétation du foncteur $\mathbb{D}^*$ sur les schémas abéliens permettant de définir un foncteur quasi inverse du foncteur du théorème. Pour ceci, on considère pour tout schéma abélien A sur S son extension vectorielle universelle, qui est une extension

$$0 \to \underline{t}_{A^*}^{v} \to E(A) \to A \to 0 \ .$$

Il se trouve qu'on peut trouver un cristal en groupes lisses canonique sur S, soit $\mathbb{E}(A)$, tel que l'on ait $E(A) \simeq \mathbb{E}(A)_S$. La définition est telle que $\mathbb{E}(A)$ définisse un foncteur

$$\text{Schémab}(S) \to \text{Cris Groupes lisses}_{nilp}(S)$$

compatible aux changements de base, l'isomorphisme précédent étant également fonctoriel et compatible aux changements de base. Il s'ensuit donc que l'on peut définir $\mathbb{E}(A)$ comme $S' \mapsto \mathbb{E}(A)_{S'}$, avec $\mathbb{E}(A)_{S'} = E(A')$, A' désignant un schéma abélien qui prolonge A sur S', à charge de définir un système transitif d'isomorphismes canoniques entre les groupes obtenus pour des prolongements différents. Dans le cas où S est de caractéristique nulle (donc plus question de puissances divisées!) cela est particulièrement simple : on prouve qu'il existe à isomorphisme unique près un seul schéma en groupes lisses E' sur l'épaississement S' de S qui prolonge E (NB: il suffirait même d'un nilépaississement, comme on voit par passage à la limite à partir du cas noethérian): c'est le résultat déjà signalé dans une vieille lettre à Tate. Dans le cas général, c'est plus délicat, et peut se faire par "la méthode de l'exponentielle", qui sera exposée dans le contexte analogue des groupes de Barsotti-Tate dans la suite du séminaire. On peut ainsi définir $\mathbb{E}(A^*)$ par

$$\mathbb{E}(A^*) = \mathbb{R}^1 f_{cris^*} (\mathbb{G}_{mA_{cris}}) \ ,$$

où A_{cris} désigne le topos cristallin nilpotent absolu (relativement à $\mathbb{Z}$): cette méthode peut également s'adapter au cas des groupes de Barsotti-Tate.

Quoiqu'il en soit de la méthode utilisée pour définir $\mathbb{E}(A)$, on peut énoncer qu'il y a un isomorphisme canonique (fonctoriel, compatible aux extensions de la base)

$$\mathbb{D}^*(A) = \underline{\mathrm{Lie}}(\mathbb{E}(A^*)) ,$$

la structure d'extension de $\mathbb{D}^*(A)$ n'étant autre que la structure sur $\underline{\mathrm{Lie}}$ déduite de la structure d'extension de $\mathbb{E}(A)_S = E(A)$.

Ceci posé, revenant aux conditions du théorème de déformation, on voit, par un sorite sur l'exponentielle sur lequel nous reviendrons, que la donnée d'un prolongement $\mathrm{Fil}^1 \subset \mathbb{D}^*(A)_{S'} = \underline{\mathrm{Lie}}(\mathbb{E}(A^*)_{S'})$ localement facteur direct prolongeant $\mathrm{Lie}(\underline{t}_A) = \underline{t}_A \subset \mathbb{D}^*(A)_S = \mathrm{Lie}(\mathbb{E}(A^*)_{S'|S})$ équivaut à la donnée d'un sous-groupe lisse à structure vectorielle de $\mathbb{E}(A^*)_{S'}$, qui prolonge le sous-groupe $\underline{t}_A^\vee$ de $\mathbb{E}(A^*)_S$. Si L est ce sous-groupe, alors il est immédiat que $\mathbb{E}(A^*)_{S'}/L$ est un schéma abélien sur S', dont le schéma abélien dual est le A' cherché. (NB : il serait plus naturel ici de travailler avec

$$\mathbb{D}^*(A) = \underline{\mathrm{Lie}}\,(\mathbb{E}(A)) \xrightarrow{\text{isom can}} \mathbb{D}^*(A^*)$$

plutôt qu'avec $\mathbb{D}^*(A)$ pour énoncer le théorème de déformations; l'équivalence des deux points de vue provient de l'accouplement parfait

$$\mathbb{D}^*(A) \otimes \mathbb{D}^*(A^*) \longrightarrow \underline{O}_S \quad \text{crisnilp}$$

compatible avec les filtrations.)

Remarque. En théorie des groupes de Barsotti-Tate, nous donnerons deux constructions de $\mathbb{D}^*(G)$, inspirées de deux constructions indiquées dans le cas des schémas abéliens: l'une "cohomologique", l'autre via une "extension vectorielle universelle" $\mathbb{E}(G)$. La construction de $\mathbb{E}(G)$ peut aussi s'obtenir par deux méthodes, l'une cohomologique, l'autre par l'exponentielle étant directement adaptée à la démonstration du théorème de déformations.

5. Relations entre les deux théories (pour schémas abéliens et pour groupes de Barsotti-Tate).

Supposons que p soit localement nilpotent sur S. Travaillons à nouveau avec le site cristallin de Berthelot (pas le nilpotent). Le résultat essentiel sera, pour un schéma abélien variable A sur S, un isomorphisme fonctoriel compatible aux changements de base

$$\mathbb{D}^*(A(\infty)) \simeq \mathbb{R}^1 f_{cris*}(\underline{O}_{A_{cris}}) ,$$

cet isomorphisme induisant, pour les valeurs des deux membres sur S, un isomorphisme compatible aux filtrations $\underline{\overset{v}{t}}_A$ et $\underline{\overset{v}{t}}_{A^*}$ (compte tenu des isomorphismes $\underline{t}_{A(\infty)} \simeq \underline{t}_A$ et idem pour A*). C'est en fait en postulant un tel isomorphisme qu'on arrive par voie heuristique à une définition de $\mathbb{D}^*(G)$ pour un groupe de Barsotti-Tate G quelconque.

Ceci impliquera en particulier le fait que, pour un épaississement à puissances divisées localement nilpotentes S' de S, il y a identité de la théorie des prolongements infinitésimaux de A, et de $A(\infty)$. De ceci, par devissage sur l'ordre de nilpotence, on peut déduire par exemple immédiatement le théorème de Serre-Tate déjà annoncé plus haut.

[On peut aussi définir une extension vectorielle universelle E(G) d'un groupe de Barsotti-Tate, et on trouvera un isomorphisme canonique

$$E(A(\infty)) \simeq E(A)(\infty)$$

donnant naissance, par le procédé habituel, à un isomorphisme plus général de cristaux en groupes

$$\mathbb{E}(A(\infty)) \simeq \mathbb{E}(A)(\infty) \ .\ ]$$

CHAPITRE VI

PROPRIETES INFINITESIMALES DES GROUPES DE BARSOTTI-TATE.
DEFORMATION DE GROUPES DE BARSOTTI-TATE.

1. Voisinages infinitésimaux. Groupes de Lie formels.

1.1. Soient S un schéma et $i : Y \to X$ un monomorphisme de faisceaux Y sur S. (où S est muni de n'importe quelle topologie entre la topologie de Zariski et la topologie fpqc). On appelle $k^{ème}$ voisinage infinitésimal de Y dans X et on note $\mathrm{Inf}_Y^k(X)$, le sous-faisceau de X engendré par les images des morphismes $X' \to X$, relatifs à des diagrammes commutatifs

$$\begin{array}{ccc} Y' & \xrightarrow{i'} & X' \\ \downarrow & & \downarrow \\ Y & \xrightarrow{i} & X \end{array}$$

où $i' : Y' \to X'$ est une immersion nilpotente d'ordre k de schémas sur S.

Lorsque X est représentable et que Y est un sous-schéma fermé défini par l'idéal I de O_X, on retrouve la notion de voisinage infinitésimal défini dans EGA IV, et on a

$$\mathrm{Inf}_Y^k(X) = V(I^{k+1}) \quad .$$

Les Inf^k définissent une suite de sous-foncteurs croissants avec k

$$\mathrm{Inf}_Y^k(X) \to \mathrm{Inf}_Y^{k+1}(X) \to \ldots \to \mathrm{Inf}_Y^{\infty}(X) = \varinjlim_k \mathrm{Inf}_Y^k(X),$$

et on a fonctorialité en (X, Y, S).

Un cas particulier important est celui où X est "ponctué" sur S, c'est-à-dire où X est muni d'une section e_X sur S et où $Y = e_X(S)$. On note alors $\mathrm{Inf}^k(X)$ en omettant Y dans la notation et on note

$$\bar{X} = \mathrm{Inf}^{\infty}(X) \quad .$$

Si $X = \bar{X}$, on dit que X est <u>ind-infinitésimal</u>. On utilisera ceci par exemple dans le cas où X est un groupe et où e_X est la section unité.

<u>Définition</u> (1.2). Un schéma localement de présentation finie G sur S, ponctué sur S par e est dit "lisse à l'ordre k" s'il satisfait aux conditions suivantes, qui sont équivalentes:

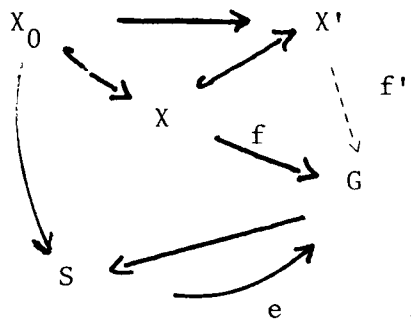
(i) $\mathrm{Inf}^k(G)$ est localement (**Zar**) sur S isomorphe à un schéma de la forme $\mathrm{Spec}\ \underline{O}_S\ [T_1, T_2, \ldots, T_n]/(T_1, \ldots, T_n)^{k+1}$

(i bis) $\underline{\omega}_{G,e} \overset{\text{dfn}}{=} e^*(\underline{\Omega}^1_{G/S})$ (faisceau conormal le long de la section unité) est localement libre de type fini et

$$\mathrm{Sym}^i(\underline{\omega}_{G,e}) \longrightarrow \underline{\mathrm{Gr}}^i_e(\underline{O}_X)$$

est un isomorphisme pour $i \leq k$.

(ii) Pour tout S-schéma affine X_0, tout voisinage infinitésimal X' d'ordre k de X_0, tout sous-schéma X de X' contenant X_0, et tout S-morphisme $f : X \to G$ tel que $f|X_0$ soit le morphisme unité



il existe un S-morphisme $f' : X' \longrightarrow G$ qui prolonge f.

ii bis) Pour tout diagramme commutatif cartésien de S-schémas

$$\begin{array}{ccc} X & \xhookrightarrow{i} & X' \\ \uparrow & & \uparrow \\ X_0 & \longrightarrow & X'_0 \end{array} \quad , \qquad (X_0 = X \cap X'_0) \ ,$$

avec i une immersion nilpotente d'ordre k, et tout S-morphisme $f : X \to G$ tel que $f_0 = f|X_0$ soit le morphisme unité, il existe un S-morphisme $f' : X' \to G$ qui prolonge f.

(ii ter) Comme (ii) avec X' un voisinage d'ordre k de X.

Définition (1.3). Un faisceau X sur S ponctué sur S par e est dit une variété formelle ponctuée sur S si elle satisfait aux conditions suivantes:

a) $X = \bar{X} \overset{dfn}{=} \mathrm{Inf}^{\infty}(X)$ (X est ind-infinitésimal),

b) chaque $\mathrm{Inf}^{k}(X)$ est lisse à l'ordre k.

On note que cette notion ne dépend pas de la topologie choisie sur (Sch)/S pourvu que celle-ci soit comprise entre (Zar) et (fpqc). On peut définir les variétés formelles sur S (pas nécessairement ponctuées) comme les faisceaux X sur S qui localement pour (fpqc) sont isomorphes au faisceau sous-jacent à une variété formelle ponctuée (la section n'est alors pas uniquement déterminée par cette condition), mais on n'aura pas besoin ici de cette variante.

Un groupe de Lie formel sur S est un faisceau en groupe G sur S tel que le faisceau ponctué sous-jacent soit une variété formelle ponctuée sur S. On peut l'interpréter aussi comme un groupe dans la catégorie des variétés formelles ponctuées sur S (laquelle admet en effet des produits finis); il s'ensuit que cette notion encore ne dépend pas de la topologie.

Par la suite, nous nous limitons aux groupes de Lie formels commutatifs.

Proposition (1.4). Supposons que p soit localement nilpotent sur S. Si G est un groupe commutatif ind-infinitésimal sur S tel que les $\mathrm{Inf}^k(G)$ soient représentables (par exemple si G est un groupe de Lie formel sur S), alors G est de p-torsion.

2. Résultats spéciaux à la caractéristique p.

Dans tout ce paragraphe, on suppose S de caractéristique $p > 0$.

Pour tout schéma en groupes (commutatif) G sur S et pour tout entier $i \geq 0$, on pose

$$G[i] = \mathrm{Ker}\{f^i_{G/S} : G \longrightarrow G^{(p^i)}\}$$

On a évidemment $G^{(p^n)}[i] \simeq (G[i])^{(p^n)}$ pour tout n, et on vérifie que $\mathrm{Inf}^i G \subset G[i]$. Enfin, si G est plat sur S, on a $G[i] \subset G(i)$ car $p^i = v^i_{G^o} f^i_{G/S}$.

Pour tout k, $0 \leq k \leq i$, $f^k_{G/S}$ induit un morphisme

$$\tilde{f}^k : G[i] \longrightarrow G[i-k]^{(p^k)} \quad ,$$

et on dira qu'un schéma en groupes G est <u>à filtration $\tilde{f}$-régulière d'échelon n</u> si $G = G[n]$ et si pour tout i, $0 \leq i \leq n$,

$$\tilde{f}^i : G[n] = G \longrightarrow G[n-i]^{(p^i)}$$

est un épimorphisme de τ-faisceaux (où τ désigne une topologie sur Sch/S intermédiaire entre f.p.p.f et f.p.q.c.)

Proposition (2.1) Soit G un groupe fini localement libre sur S et tel que $G = G[n]$. Les assertions suivantes sont alors équivalentes:

(i) G est à filtration $\mathfrak{f}$-régulière d'échelon n.

(i bis) Les morphismes $\mathfrak{f}^i : G[n] \to G[n-i]^{(p^i)}$ sont plats (et donc fidèlement plats) pour $0 \leq i \leq n$.

(ii) $\exists i$, $1 \leq i \leq n-1$ tel que $\mathfrak{f}^i$ est un épimorphisme

(ii bis) $\exists i$, $1 \leq i \leq n-1$ tel que $\mathfrak{f}^i$ est plat

(iii) Posant (en tant que τ-faisceaux)

$$Gr_i^{\mathfrak{f}}(G) = G[i]/G[i-1] \quad , \qquad 1 \leq i \leq n,$$

les homomorphismes

$$\theta_i : Gr_n^{\mathfrak{f}}(G) \longrightarrow [Gr_{n-i}^{\mathfrak{f}}(G)]^{(p^i)}$$

induits par $\mathfrak{f}^i$ sont des isomorphismes pour $0 \leq i \leq n-1$.

(iv) Les groupes $G[i]$ sont finis localement libres et, définissant $Gr_i^{\mathfrak{f}}(G)$ dans la catégorie des schémas en groupes plats sur S, les homomorphismes θ_i sont des isomorphismes.

(v) Localement pour (Zar), l'algèbre augmentée A de G est isomorphe à $O_S[T_1,\ldots,T_d]/(T_1^{p^n}, T_2^{p^n},\ldots, T_n^{p^n})$.

(vi) Localement pour (Zar), A est isomorphe, en tant qu'algèbre augmentée, à $\mathrm{Sym}_{O_S}(\underline{\omega})/(\underline{\omega}^{(p^n)})$, où $\underline{\omega}$ est un module localement

libre de type fini sur S et $(\underline{\omega}^{(p^n)})$ désigne l'idéal engendré par les éléments homogènes de degré p^n ($\underline{\omega}$ sera le module conormal de G le long de sa section unité).

(vi) bis La condition (vi) est satisfaite par les fibres géométriques de G.

Démonstration

(i) => (i bis) ; (ii) => (ii bis) résultent du critère de platitude fibre à fibre (E.G.A. IV_3 11.3.10)

(i bis) => (i) (ii bis) => (ii) résultent immédiatement de ce que $\mathfrak{f}^i$ est un morphisme de présentation finie.

(i) <=> (ii) <=> (iii) se prouve par un raisonnement analogue à celui utilisé en (III. 2.2) ; On montre d'abord que si f^i, $i \geq 1$, est un épimorphisme, il en est de même de $\mathfrak{f}^{i+1}$. Remarquant alors que θ_{n-1} se factorise par $n-1$ monomorphismes

$$\alpha : G[i]/_{G[i-1]}(p^{n-i}) \longrightarrow G[i-1]/_{G[i-2]}(p^{n-i+1}) ,$$

on voit qu'il suffit que $\mathfrak{f}^{n-1}$ soit un épimorphisme pour que tous les morphismes α soient des isomorphismes, ce qui équivaut à (iii). Enfin, si tous les α sont des isomorphismes, il en résulte par récurrence sur i que les morphismes $\mathfrak{f} : G[i]^{(p^{n-i})} \longrightarrow G[i-1]^{(p^{n-i+1})}$ sont des épimorphismes pour tout i.

(iii) => (iv) Par le critère de platitude fibre à fibre, $G[i]$ est plat sur S, donc fini localement libre. Il en est de même de $Gr_i^f(G) \approx Gr_1^f(G) = G[1]$, qui sont donc quotients dans la catégorie des groupes plats sur S.

(iv) => (iii) Trivialement.

Pour prouver l'équivalence de ces assertions avec les assertions (v) à $(vi)^{bis}$, on peut évidemment supposer S affine.

(vi) => (v) est clair.

(v) => (vi) Soit $\underline{\omega}$ le module conormal de G le long de sa section unité. S étant affine et l'hypothèse (v) impliquant que $\underline{\omega}$ est localement libre, on peut choisir un relèvement $\underline{\omega} \longrightarrow J$ de l'homomorphisme canonique $J \longrightarrow \underline{\omega} = J/J^2$, d'où l'on tire un homomorphisme surjectif d'algèbres augmentées

$$(*) \qquad \mathrm{Sym}(\underline{\omega})/_{(\underline{\omega}(p^n))} \longrightarrow A \ ,$$

et il résulte de (v) que c'est un isomorphisme.

(v) => (ii^{bis}). Si l'on note $J^{[p]}$ l'idéal engendré dans A par les puissances p-èmes des sections locales de J, l'homomorphisme

$$(A/J^{[p]})(p^{n-1}) \longrightarrow A$$

déduit par passage au quotient de l'homomorphisme $x \longmapsto x^{p^{n-1}}$ (le fait que $G[n] = G$ équivaut à ce que $x^{p^n} = 0$ pour toute section

locale de J) fait de A une algèbre plate sur $(A/J[p])^{(p^{n-1})}$ si A est de la forme envisagée dans (v). Or cela signifie exactement que f^{n-1} est plat.

Pour achever la démonstration, il suffit de prouver que (ii^{bis}) implique (vi). En effet l'équivalence avec (vi^{bis}) en résultera, car la condition (ii^{bis}) est équivalente à la même condition sur les fibres géométriques.

Supposons d'abord que S soit le spectre d'un corps parfait k. On sait alors, par le théorème de Hopf-Borel-Dieudonné (SGA_3 VII_B 5.4) que l'algèbre affine du groupe infinitésimal $G = G[n]$ est de la forme

$$A \simeq k[T_1,\ldots,T_d]/(T_1^{p^{n_1}}, T_2^{p^{n_2}},\ldots,T_d^{p^{n_d}}),$$

avec $n_i \geq 1$. Comme $J^{[p^n]} = 0$, on a $n_i \leq n$ pour tout i, $1 \leq i \leq d$, et il reste à prouver que $n_i = n$ pour tout i. Si pour un i on avait $n_i < n$, il en résulterait que l'homomorphisme (*) ne serait pas injectif, contrairement à l'hypothèse de fidèle platitude faite.

Dans le cas général, on se ramène immédiatement au cas où $S = \operatorname{Spec} B$, B local de corps résiduel k. Soit ω le module conormal et soit $d = \operatorname{rang}_k \omega \otimes k$. Choisissons une suite $(T_1,\ldots,T_d)$ de d éléments de J dont les images dans $\omega \otimes k$ forment une base et considérons l'homomorphisme correspondant

$$B[T_1,\ldots,T_d]/(T_1^{p^n},\ldots,T_d^{p^n}) \longrightarrow A .$$

C'est un homomorphisme surjectif de B-modules libres et il suffit de prouver que ces deux B-modules ont même rang pour prouver que c'est un isomorphisme. Or il suffit de faire un changement de base de S vers une clôture parfaite de k pour voir, d'après ce que l'on sait si la base est un corps parfait, que le rang de A est p^{nd} comme le rang du premier membre.

c.q.f.d.

Corollaire (2.2) Si G est un groupe fini localement libre à filtration f-régulière d'échelon n, G est lisse à l'ordre p^n-1 le long de sa section unité

Cela est clair d'après l'écriture explicite de G.

Proposition (2.3). Soit $G = G(n)$, $n \geq 1$, un groupe de B.-T. Tronqué d'échelon n sur S. Alors

a) $G[n] \subset G$ est à filtration f-régulière d'échelon n

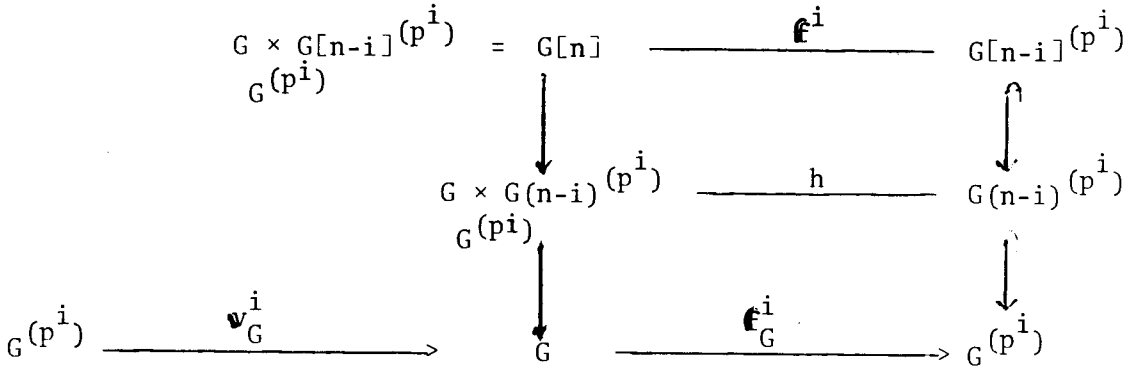
b) $$G[n] = \operatorname{Ker} f_G^n = \operatorname{Im} v_G^n$$

et $$\operatorname{Ker} v_G^n = \operatorname{Im} f_G^n$$

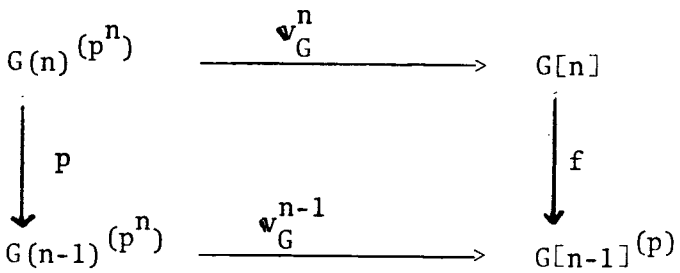
c) $G[n]$ est plat (donc fini localement libre) sur S. Il en résulte que $G[n]$ vérifie les conditions équivalentes de la proposition (2.1).

Démonstration

a) Par hypothèse, $\mathbf{f}_G^i \circ \mathbf{v}_G^i = p^i$ a pour image $G(n-i)^{(p^i)}$. Il en résulte que h est un épimorphisme, d'où l'on déduit qu'il en est de même de $\mathbf{f}^i : G[n] \longrightarrow G[n-i]^{(p^i)}$.



b) Pour $n = 1$, cela n'est autre que la définition même d'un groupe de B.-T. tronqué d'échelon 1. Pour $n \geq 2$, on a vu (III.3.3) que $G(1) \subset G(n) = G$ vérifiait (b), et l'on va raisonner par récurrence sur les $G(i) \subset G$. Puisque $\mathbf{f}_G^n \circ \mathbf{v}_G^n = p^n \, \mathrm{Id}_{G(n)} = 0$, on a $\mathrm{Im}\, v_G^n \subset G[n]$ et l'on a un diagramme commutatif



Si l'on suppose que $G(n-1)$ vérifie (b) il en résulte que $\mathbf{v}_G^n$ est un épimorphisme modulo $\mathrm{Ker}\, \mathbf{f} = G[1]$, et il suffit de prouver que $G[1]$ est contenu dans l'image de $\mathbf{v}_G^n$. Or on a

$$G[1] = w(G(1)^{(p)}) = w(p^{n-1}G(n)^{(p)}) = w^n[F^{n-1}G(n)^{(p)}] \subset w^n[G(n)^{(p^n)}]$$

On prouve de même que $\operatorname{Ker} w_G^n = \operatorname{Im} F_G^n$.

c) Puisque l'on a $G[n] = \operatorname{Im} w_G^n$, $G[n]$ est plat d'après le critère de platitude fibre à fibre.

Si G est un groupe de B.-T. sur S, on pose par définition

$$G[n] = G(n)[n]$$

et l'on a alors $G(i)[n] = G[n]$ si $i \geq n$.

Corollaire (2.4). Soit G un groupe de B.-T. sur S. Alors, pour tout $n \geq 1$, $G(n)$ est lisse à l'ordre p^n-1 sur S, et on a

$$\operatorname{Inf}^k G \subset G[n] \quad \text{si} \quad k \leq p^n-1 \ .$$

Démontrons cette dernière inclusion. On a

$$\operatorname{Inf}^k(G) = \varinjlim_n \operatorname{Inf}^k(G(n))$$

et, pour $n \geq k$,

$$\operatorname{Inf}^k((G(n)) \subset G(n)[k] = G[k] \ .$$

Donc, pour $k \leq p^n-1$, $\operatorname{Inf}^k G \subset G[p^n-1]$ et, appliquant la proposition (2.1), on voit, d'après la structure explicite de $G[p^n-1]$, que

$$\operatorname{Inf}^k G \subset G[p^n-1][n] = G[n] \ .$$

2.5 Groupes de Lie formels en caractéristique p.

Soit $G = \varinjlim_k \mathrm{Inf}^k(G)$ un groupe de Lie formel sur S. On a alors

$$G[n] = \varinjlim (\mathrm{Inf}^k(G))[n] \quad ,$$

et les $\mathrm{Inf}^k G$ étant lisses à l'ordre k, on voit d'après leur structure explicite (1.2), que, pour k suffisamment grand, $(\mathrm{Inf}^k G)[n]$ est fini localement libre à filtration $\mathfrak{f}$-régulière d'échelon n. En effet, localement (Zar) sur S, pour $k \geq dp^n$, on a

$$G[n] = (\mathrm{Inf}^k G)[n] \approx \underline{\mathrm{Spec}}\ \underline{O}_S[T_1,\ldots,T_d]/(T_1{}^{p^n},\ldots,T_d{}^{p^n}) \quad ,$$

d désignant le rand du module conormal $\underline{\omega}$ de G (d est une fonction localement constante de $s \in S$).

Comme par ailleurs $\mathrm{Inf}^k G \subset G[k]$, on a

$$G = \varinjlim_n G[n] \quad ,$$

d'où il résulte que $\mathfrak{f}_{G/S}: G \to G^{(p)}$ est un épimorphisme.

On a donc associé au groupe de Lie formel G le système

$$G[n] \hookrightarrow G[n+1] \hookrightarrow \ldots .$$

de groupes finis localement libres à filtration $\mathfrak{f}$-régulière d'échelon n. Par analogie avec les systèmes p-coadiques, un tel système sera dit $\mathfrak{f}$-coadique.

Inversement, à un tel système $\mathfrak{f}$-coadique de groupes finis localement libres $G[n]$ annulés par $\mathfrak{f}^n$ (et donc à filtration $\mathfrak{f}$-régulière d'échelon n) on associe sa limite inductive dont on vérifie que c'est un groupe de Lie formel. On a donc:

Proposition (2.6). La catégorie des groupes de Lie formels (commutatifs) G sur S de caractéristique p est équivalente à la catégorie des systèmes $\mathfrak{f}$-coadiques de schémas en groupes finis localement libres $G[n]$ à filtration $\mathfrak{f}$-régulière d'échelon n.

Regroupant ce qui précède, on a le résultat suivant:

Théorème (2.7). (Construction du groupe de Lie formel associé à un groupe de B.-T. en caractéristique p). Soit G un groupe de B.-T, sur S. Si l'on pose

$$\bar{G} = \mathrm{Inf}^{\infty}G = \varinjlim_{k} \mathrm{Inf}^{k}(G) \quad ,$$

on a aussi

$$\bar{G} = \varinjlim G[n], \qquad \text{avec} \quad G[n] = G(n)[n] \quad ,$$

et $\bar{G}$ est un groupe de Lie formel. De plus, on a

$$\bar{G}[n] = G[n] \quad ,$$

et, pour $k \leq p^n-1$,

$$\mathrm{Inf}^{k}G = \mathrm{Inf}^{k}\bar{G} = \mathrm{Inf}^{k}G(n) \subset G[n] \subset G(n) \quad .$$

3. Groupe de Lie formel associé à un groupe de B.-T sur une base non nécessairement de caractéristique p.

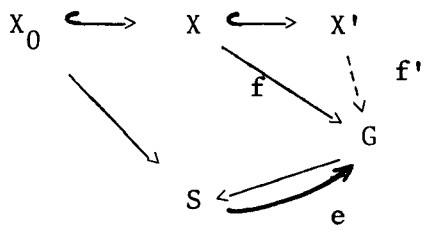
Le théorème (2.7) se généralise au cas où p est localement nilpotent sur S:

Théorème (3.1) Soit G un groupe de B.-T. sur S, avec p localement nilpotent sur S. Alors

a) $\bar{G} = \varinjlim_{k} \mathrm{Inf}^{k}(G) \subset G$ est un groupe de Lie formel sur S.

On dira que $\bar{G}$ est le groupe de Lie formel associé à G; sa formation est fonctorielle en G et commute aux changements de base.

b) G est formellement lisse sur S pour les nil-immersions (et pas seulement pour les immersions nilpotentes), c'est-à-dire que pour toute nil-immersion $X_0 \hookrightarrow X'$ et tout S-morphisme $f : X \longrightarrow G$ tel que $X_0 \hookrightarrow X \hookrightarrow X'$ et $f|X_0$ soit le morphisme unité; il existe un prolongement $f' : X' \longrightarrow G$ de f au-dessus de S.



La démonstration de ce théorème se fait par dévissage à partir du cas où la base est de caractéristique p, et il est nécessaire d'utiliser le formalisme du complexe cotangent relatif. Celui-ci est aussi utilisé dans la théorie des déformations, dont on va énoncer le principal résultat avant de donner quelques indications sur le formalisme du complexe cotangent relatif.

4. Déformations infinitésimales des groupes de Barsotti-Tate (énoncé).

On a le résultat suivant, qui sera essentiel pour la théorie de Dieudonné:

Théorème (4.1). Soit $i : S_0 \hookrightarrow S$ une nil-immersion, avec S affine et soit G_0 un groupe de B.-T. sur S_0. Alors:

a) Il existe un groupe de B.-T. G sur S qui prolonge G_0.

b) Si l'on note $E(G_0,S)$ (resp. $E(G_0(n), S)$) l'ensemble des prolongements, à isomorphisme près de G_0 en un groupe de B.-T. sur S (resp. de $G_0(n)$ en un groupe de B.-T. tronqué d'échelon n sur S), l'application naturelle

$$(*) \qquad E(G_0, S) \longrightarrow E(G_0(n), S)$$

est surjective.

c) Si l'immersion i est nilpotente d'ordre k et si $p^N 1_{S_0} = 0$, alors l'application (*) est bijective pour $n \geq kN$.

d) Si S est un voisinage infinitésimal du premier ordre de S_0 ($k = 1$), et si p est nilpotent sur S_0, alors $E(G_0, S)$ est un torseur sous $\underline{t}_{G_0^*} \otimes \underline{t}_{G_0}$, où $\underline{t}_{G_0}$ désigne l'algèbre de Lie du groupe de Lie formel $\bar{G}_0$ associé à G_0.

(Dans le cas où G_0 est un groupe de Lie formel, le théorème de prolongement est dû à Lazard qui a déterminé l'espace modulaire des lois de groupe de Lie formel.)

5. Complexe cotangent relatif

Le but de ce paragraphe est de décrire brièvement certaines propriétés du complexe cotangent relatif et d'expliquer comment la théorie du complexe cotangent relatif permet d'étudier quelques problèmes de déformation; on l'utilisera en particulier pour étudier les problèmes de déformation des schémas en groupes et des groupes de Barsotti-Tate.

La définition locale du complexe cotangent relatif est due à M.André et D. Quillen (cf. M.André. Méthode simpliciale en algèbre homologique et algèbre commutative. [1] et D.Quillen Homotopical algebra. [30]) et la définition globale à L. Illusie [19], qui l'applique à toutes sortes de problèmes de déformation. L'étude de la déformation des schémas en groupes plats sur S est due à P. Deligne et L. Illusie.

Soit X un S-schéma, le complexe cotangent relatif de X sur S $L_\cdot^{X/S}$ est un objet de la catégorie dérivée $D^-(O_X)$. En particulier, on

peut le représenter par un complexe de O_X-modules du type

$$L_\bullet^{X/S} = \{\ldots \to L_2 \to L_1 \to L_0 \to 0\} \quad .$$

La fonctorialité s'exprime de la façon suivante: Pour tout diagramme cartésien

$$\begin{array}{ccc} X' & \xrightarrow{f} & X \\ \downarrow & & \downarrow \\ S' & \longrightarrow & S \end{array}$$

on a un morphisme naturel de $D^-(O_{X'})$

$$\mathbb{L}f^* (L_\bullet^{X/S}) \longrightarrow L_\bullet^{X'/S'}$$

Complexe cotangent tronqué.

Si on remplace le complexe $\{\ \to\ldots\to L_2 \to L_1 \to L_0 \to 0\}$ définissant $L_\bullet^{X/S}$ par le complexe tronqué à l'ordre 1

$$\tau\leq 1 (L_\bullet^{X/S}) = \{0 \to L'_1 \to L_0 \to 0\}$$

obtenu en remplaçant L_1 par $L'_1 = \mathrm{im}L_2$, on obtient un complexe qui a mêmes objets de cohomologie de $L_\bullet^{X/S}$ à l'ordre 0 et 1, qui a été étudié par A.Grothencieck (Catégories cofiltrées additives et complexe cotangent relatif. [16]) . Ce complexe a des propriétés intéressantes et on peut en donner une construction directe chaque fois qu'on sait plonger X dans un S-schéma X' formellement lisse sur S (ce qui est toujours vrai localement.) Soit I l'idéal de O_X, définissant l'immersion $X \subset X'$, on a alors

$$\tau\leq 1(L_{\cdot}^{X/S}) \quad \approx \quad \{\ 0 \to I/I^2 \to \Omega^1_{X'/S} \otimes_{\underline{O}_{X'}} \underline{O}_X \to 0\ \}$$

et dans ce cas

$$L_0 = \Omega^1_{X'/S} \otimes_{\underline{O}_{X'}} \underline{O}_X \quad \text{est un } \underline{O}_X\text{-module}$$

localement libre de type fini.

On voit alors dans ce cas que les faisceaux $H^i(L_{\cdot}^{X/S})$, $i = 0, 1$, sont quasi cohérents. Cette propriété est encore vraie pour i quelconque.

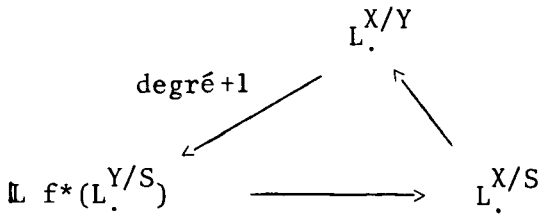
De même si S est noethérien et si X est localement de type fini, $H^i(L_{\cdot}^{X/S})$ est cohérent pour $i = 0, 1$. Cette propriété est aussi vraie pour i quelconque.

Si X est une <u>intersection complète relative,</u> c'est-à-dire si X est de présentation finie sur S et s'il existe une immersion <u>régulière</u> de X dans un X' formellement lisse sur S, on montre alors que $H^i(L_{\cdot}^{X/S}) = 0$ pour $i \geq 2$, par conséquent le complexe $L_{\cdot}^{X/S}$ est isomorphe au complexe tronqué à l'ordre 1 dans la catégorie dérivée. Dans ce cas d'ailleurs, comme l'immersion $X \subset X'$ est régulière, I/I^2 est un O_X-module localement libre. Le complexe cotangent est donc alors un <u>complexe parfait d'amplitude parfaite</u> $\subset [-1, 0]$.

Dans ces conditions, on peut se demander pourquoi utiliser le gros complexe $L_{\cdot}^{X/S}$. C'est parce que c'est vraiment le gros complexe qui a les meilleurs propriétés du point de vue de la fonctorialité et de

la transitivité. En particulier, soit $f : X \to Y$ et $g : Y \to S$ deux morphismes de schémas, on démontre qu'on a un triangle exact

(*)



qui généralise la suite exacte des différentielles

$$f^* \ \Omega^1_{Y/S} \longrightarrow \Omega^1_{X/S} \longrightarrow \Omega^1_{X/Y} \longrightarrow 0 \quad .$$

On a en effet $H^o(L^{X/S}_{\cdot}) \simeq \Omega^1_{X/S}$, ce qu'on peut vérifier dans la situation décrite plus haut grâce à la suite exacte

$$I/I^2 \to \Omega^1_{X'/S} \underset{\underline{O}_{X'}}{\otimes} \underline{O}_X \to \Omega^1_{X/S} \to 0 \quad .$$

De même si on définit dans ce cas

$$N_{X/S} = \mathrm{Ker}(I/I^2 \to \Omega^1_{X'/S} \underset{\underline{O}_{X'}}{\otimes} \underline{O}_X) \quad ,$$

le triangle exact (*) donne lieu à la suite exacte longue de cohomologie

$$f^* N_{Y/S} \to N_{X/S} \to N_{X/Y} \to f^* \Omega^1_{Y/S} \to \Omega^1_{X/S} \to \Omega^1_{X/Y} \to 0 \quad .$$

Dans le cas où X est une intersection complète relative sur Y, on a une suite exacte à six termes.

En ce qui concerne le changement de base on a le résultat

Proposition. Soit

$$\begin{array}{ccc} X' & \xrightarrow{f} & X \\ \downarrow & & \downarrow \\ S' & \longrightarrow & S \end{array}$$

un diagramme cartésien de schémas, alors le morphisme

$$\mathbb{L}f^*(L_\cdot^{X/S}) \longrightarrow L_\cdot^{X'/S'}$$

est un isomorphisme si X et S' sont tor-indépendants, c'est-à-dire si, pour tout $i > 0$, on a $\underline{\mathrm{Tor}}_i^{\underline{O}_S}(\underline{O}_X, \underline{O}_{S'}) = 0$. C'est le cas en particulier si X et S-plat ou si S' est S-plat.

Problèmes de déformation typiques.

1°) Classification des voisinages infinitésimaux du premier ordre.

Soient X un S-schéma, J un $\underline{O}_X$-module quasi cohérent, on cherche à classifier les voisinages infinitésimaux au-dessus de S

$$X \subset X'$$

tel que X soit défini par l'idéal J de $O_{X'}$, considéré comme idéal de carré nul. C'est-à-dire qu'on a la suite exacte

$$0 \to J \to O_{X'} \to O_X \to 0 \quad .$$

De tels voisinages sont donc classifiés par $\underline{\mathrm{Ext}}^1_{\underline{O}_S}(\underline{O}_X, J)$ et on démontre qu'on a un isomorphisme

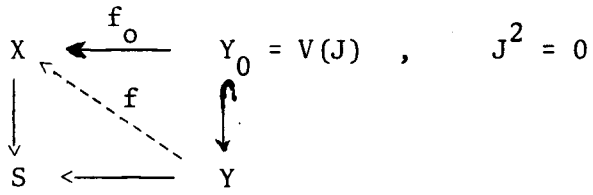
$$\underline{\mathrm{Ext}}^1_{\underline{O}_S}(\underline{O}_X, J) \simeq \mathrm{Ext}^1_{\underline{O}_X}(L_\cdot^{X/S}, J) \simeq \mathrm{Hom}_{D(\underline{O}_X)}(L_\cdot^{X/S}, J[1]) .$$

L'ensemble des solutions est alors un torseur sous

$$\mathrm{Ext}^0_{\underline{O}_X}(L_\cdot^{X/S}, J) \simeq \mathrm{Hom}(\Omega^1_{X/S}, J) .$$

2°) Déformation de morphismes de schémas.

Problème. Soient X et Y deux S-schémas et soit Y_0 le sous-schéma de Y défini par un idéal J de carré nul de $\underline{O}_Y$. Soit $f_0 : Y_0 \to X$ un S-morphisme. Trouver tous les morphismes $f : Y \to X$ qui prolongent f_0.



On démontre que l'obstruction à un tel prolongement

$$\partial f_o \in \mathrm{Ext}^1_{\underline{O}_Y}(\mathbb{L}f_o^* (L_\cdot^{X/S}), J)$$

et que l'ensemble des solutions si $\partial f_o = 0$ est un torseur sous $\mathrm{Ext}^0_{\underline{O}_Y}(\mathbb{L}f_o^* L_\cdot^{X/S}, J) \simeq \mathrm{Hom}(f_o^* \Omega^1_{X/S}, J)$.

3°) Déformation des schémas plats.

Problème. Soient S un schéma, S_0 un sous-schéma de S défini par un idéal de carré nul J et X_0 un S_0-schéma plat. Trouver tous les S-schémas plats X qui prolongent X, c'est-à-dire tels qu'il existe un diagramme cartésien

$$\begin{array}{ccc} X_0 & \hookrightarrow & X \\ \downarrow & & \downarrow \\ S_0 & \hookrightarrow & S \end{array}$$

On démontre que l'obstruction à l'existence d'un tel schéma est

$$\partial (X_0, S) \in \operatorname{Ext}^2_{\underline{O}_{X_0}} (L^{X_0/S_0}_{\cdot}, J \otimes_{\underline{O}_{S_0}} \underline{O}_{X_0}) \quad .$$

Si cette classe est nulle, l'ensemble des solutions est alors un torseur sous $\operatorname{Ext}^1_{\underline{O}_{X_0}} (L^{X_0/S_0}_{\cdot}, J \otimes_{\underline{O}_{S_0}} \underline{O}_{X_0})$ groupe des automorphismes d'une solution est isomorphe à

$$\underline{\operatorname{Ext}}^0_{\underline{O}_{X_0}} (L^{X_0/S_0}_{\cdot}, J \otimes_{\underline{O}_{S_0}} \underline{O}_{X_0}) \simeq \operatorname{Hom} (\Omega^1_{X_0/S_0}, J) \quad .$$

Références pour ces résultats:

A. Grothendieck [16]

L. Illusie ([17], [18], [19]).

APPENDICE

Une lettre
de M.A. Grothendieck
à Barsotti

Dear Barsotti,

I would like to tell you about a result on specialization of Barsotti-Tate groups (the so-called p-divisible groups on Tate's terminology) in char.p, which perhaps you know for a long time, and a corresponding conjecture or rather question, whose answer may equally be known to you.

First some terminology. Let k a perfect field of char $p > 0$, W the ring of Witt vectors over k, K its field of fractions. An F-cristal over k will mean here a free module of finite type M over W, together with a σ-linear endomorphism $F_M : M \to M$ (where $\sigma : W \to W$ is the Frobenius automorphism) such that F_M is injective i.e. F(M) contains $p^n M$ for some $n \geq 0$. I am rather interested in F-iso-cristals, namely F-cristals up to isogeny, which can be interpreted as finite dimensional vector spaces E over K, together with a σ-linear automorphism $F_E : E \to E$, such that there exists a "lattice" $M \subset E$ mapped into itself by F_E ; I will rather call such objects effective F-isocristals (and drop the suffix "iso" (and even F) when the context allows it), and consider the larger category of (E,F_E), with no assumption of existence of stable lattice M made, as the category of F-isocristals. It is obtained from the category of effective F-isocristals and its natural internal tensor product, by "inverting" formally the "Tate cristal" $K(-1) = (K, F_{K(-1)} = p\sigma)$: the isocristals (E,F_E) such that $(E, p^n F_E)$ is effective (i.e. the set of iterates of $(p^n F_E)$ is bounded for the natural norm structure) can be viewed as those of the form $E_0(n) = E_0 \otimes K(-1)^{\otimes(-n)}$, with E_0 an effective F-(iso)-cristal.

Assume now k alg.closed. Then by Dieudonné's classification theorem as reported on in Manin's report, the category of F-(iso)cristals over k is semi-simple, and the isomorphism classes of simple elements of this category can be indexed by $\underline{Q}$ (the group of rational numbers), or what amounts to the same, by pairs of relatively prime integers

$$r,s \in \underline{Z} \ , \ r \geq 1, \quad (s,r) = 1$$

to such a pair corresponding the simple object

$$E_{s/r} = E_{r,s}$$

whose rank is r, and which for $s \geq 0$ can be described by the cristal over the prime field $\underline{F}_p$ as

$$E_{s/r} = \underline{Q}_p[T]/(T^r - p^s) \ , \ F_{s/r} = \text{multiplication by } T \ .$$

For $s \leq 0$, we get $E_{s/r}$ by the formula

$$E_{-\lambda} = (E_\lambda)^\vee \ ,$$

where $^\vee$ denotes ordinary dual endowed with the contragredient F automorphism. In Manin's report, only effective F-cristals are considered, with the extra restriction that F_E is topologically nilpotent, but by Tate twist this implies the result as I state it now. Indexing by $\underline{Q}$ rather than by pairs (s,r) has the advantage that we have the simple formula

$$E_\lambda \otimes E_{\lambda'} \simeq \text{sum of cristals } E_{\lambda+\lambda'} \ .$$

In other words, if we decompose each cristals in its isotypic component corresponding to the various "slopes" $\lambda \in \underline{Q}$, so that we get a natural

graduation on it with group $\underline{Q}$, we see that this graduation is compatible with the tensor product structure:

$$E(\lambda) \otimes E'(\lambda') \subset (E \otimes E')(\lambda + \lambda') .$$

The terminology of "slope" of an isotypic cristal, and of the sequence of slopes occuring in any cristal (when decomposing it into its isotypic- - components) is due, I believe, to you, as discussed on formal groups in Pisa about three years ago ; but I did not appreciate then the full appropriateness of the notion and of the terminology. Let's define the sequence of slopes of a cristal (E, F_E) by its isotypic decomposition, repeating each λ a number of times equal to rank $E(\lambda)$ (bearing in mind that if $\lambda = s/r$ with $(s,r) = 1$, then the multiplicity of λ in E i.e. rank $E(\lambda)$ is a multiple of r) ; moreover it is convenient to order this sequence in increasing order. This definition makes still a good sense if k is not algebraically closed, by passing over to the algebraic closure of k ; in fact, the isotypic decomposition over $\bar{k}$ <u>descends</u> to k, so we get much better than just a pale sequence of slopes, but even a canonical "iso-slope" ("isopentique" in french) decomposition over k

$$E = \bigoplus_{\lambda \in Q} E(\lambda) .$$

(NB This is true only because we assumed k perfect ; there is a reasonable notion of F-cristal also if k is not perfect, but then we should get only a <u>filtration</u> of a cristal by increasing slopes...). Now if k is a finite field with q elements, of rank a over the prime field, and if (E, F_E) is a cristal over k, then F_E^a is a linear endomorphism of E over K, and it turns out that the slopes of the cristal are just the valuations of the

proper values of F_E^a , for a valuation of $\bar{\mathbb{Q}}_p$ normalised in such a way that

$$v(q) = 1 \text{ , i.e. } v(p) = 1/a \text{ .}$$

(This is essentially the "technical lemma" in Manin's report, the restrictive conditions in Manin being in fact not necessary.) Thus, the sequence of slopes of the cristal, as defined above, is just the sequence of slopes of the Newton polygon of the characteristic polynomial of the arithmetic Frobenius endomorphism F_E^a, and their knowledge is equivalent to the knowledge of the p-adic valuations of the proper values of this Frobenius !

Lets come back to a general perfect k. Then the cristals which are effective are those whose slopes are > 0 ; those which are Dieudonné modules, i.e. which correspond to Barsotti-Tate groups over k (not necessarily connected) are those whose slopes are in the closed interval $[0,1]$: slope zero corresponds to ind-étale groups, slope one to multiplicative groups. Moreover, an arbitrary cristal decomposes canonically into a direct sum

$$E = \bigoplus_{i \in Z} E_i(-i) \quad ,$$

where (-i) are Tate twists (corresponding to multiplying the F endomorphism by p^i), and the E_i have slopes $0 \leq \lambda < 1$ (or, if we prefer, $0 < \lambda \leq 1$), and hence correspond to Barsotti-Tate groups up to isogeny over k, without multiplicative component (resp. which are connected). The interest of this remark comes from the fact that if X is a proper and smooth scheme over k,

then the cristallin cohomology groups $H^i(X)$ can be viewed as F-cristals, H^i with slopes between 0 and i (*) and define in this way a whole avalanche of Barsotti-Tate groups over k (up to isogeny), which are quite remarkable invariants whose knowledge should be thought as essentially equivalent with the knowledge of the characteristic polynomials of the "arithmetic" Frobenius acting on (any reasonable) cohomology of X (although the arithmetic Frobenius is not really defined, unless k is finite !).

Now the result about specialization of Barsotti-Tate groups. This is as follows : assume the BT groups G, G' are such that G' is a specialization of G. Let $\lambda_1,\ldots,\lambda_h$ (h = "height") be the slopes of G, and $\lambda'_1,\ldots,\lambda'_h$ the ones for G'. Then we have the equality

$$(1) \qquad \sum \lambda'_i = \sum \lambda'_i \qquad (= \dim G = \dim G')$$

and the inequalities

$$(2) \qquad \lambda_1 \leq \lambda'_1 \ , \ \lambda_1 + \lambda_2 \leq \lambda'_1 + \lambda'_2 \ ,\ldots, \ \sum_{i=1}^{j} \lambda_j \leq \sum_{i=1}^{j} \lambda'_j \ \ldots \ .$$

In other words, the "Newton polygon" of G (i.e. of the polynomial $\prod_i (1 + (p^{\lambda_i})T)$) lies below the one of G', and they have the same endpoints (0,0) and (h,N).

I get this result through a generalized Dieudonné theory for BT

(*) This is not proved now in complete generality, but is proved if X lifts formally to char. zero, and is certainly true in general.

groups over an arbitrary base S of char.p, which allows to associate to such an object an F-cristal over S, which heuristically may be thought of as a family of F-cristals in the sense outlined above, parametrized by S. Using this theory, the result just stated is but a particular case of the analogous statement about specialization of arbitrary cristals. Now this latter statement is not hard to prove at all: passing to $\wedge^h E$ and $\wedge^h E'$, the equality (1) is reduced to the case of a family of rank one cristals, and to the statement that such a family is just a twist of some fixed power of the (constant) Tate cristal. And the general equality (2) is reduced, passing to $\wedge^j E$ and $\wedge^j E'$, to the first inequality $\lambda_1 \leq \lambda'_1$. Raising both E and E' to a tensor-power r.th such that $r\lambda_1$ is an integer, we may assume that λ_1 is an integer, and a Tate twist allows us to assume that $\lambda_1 = 0$, so the statement boils down to the following : if the general member of the family is an effective cristal, so are all others. This is readily checked in terms of the explicit definition of "cristal over S".

The wishful conjecture I have in mind now is the following : the necessary conditions (1) (2) that G' be a specialization of G are also sufficient. In other words, starting with a BT group $G_o = G'$, and taking its formal modular deformation in char. p (over a modular formal variety S of dimension dd^*, $d = \dim G_0$, $d^* = \dim G_0^*$), and the BT group G over S thus obtained, we want to know if for every sequence of rational numbers λ_i between 0 and 1, satisfying (1) and (2), these numbers occur as the sequence of slopes of a fiber of G at some point of S. This does not seem too unreasonable, in view of the fact that the set of all (λ_i)[satisfying

the conditions just stated is indeed finite, as is of course the set of slope-types of all possible fibers of G over S.

I should mention that the inequalities (2) were suggested to me by a beautiful conjecture of Katz, which says the following : if X is smooth and proper over a finite field k, and has in dimension i Hodge numbers $h^0 = h^{0,i}$, $h^1 = h^{1,i-1}$, ... , $h^i = h^{i,0}$, and if we consider the caracteristic polynomial of the arithmetic frobenius F^a operating on some reasonable cohomology group of X (say ℓ-adic for $\ell \neq p$, or cristallin), then the Newton polygon of this polynomial should be <u>above</u> the one of the polynomial $\prod (1+p^iT)^{h_i}$, In a very heuristic and also very suggestive way, this could now be interpreted by stating (without any longer assuming k finite) that the cristallin H^i of X is a specialization of a cristal whose sequence of slopes is : 0 h^0 times, 1 h^1 times,..., i h^i times. If X lifts formally to char zero, then we can introduce also the Hodge numbers of the lifted variety, which are numbers satisfying

$$h'^0 \leq h^0 \ , \ \ldots \ , \ h'^i \leq h^i \quad ,$$

and one should expect a strengthening of Katz's conjecture to hold, with the h'^j replaced by the h^j. Thus the transcendental analogon of a char.p F-cristal seems to be something like a Hodge structure or a Hodge filtration, and the sequence of slopes of such a structure should be defined as the sequence in which j enters with multiplicity $h'^j = \text{rank } Gr^j$. (NB. Katz made his conjecture only for global complete intersections, however I would not be as cautious as he !). I have some idea how Katz's conjecture with the h^i's (not the h'^i's for the time being) may be attacked by the machinery of

cristallin cohomology, at least the first inequality among (2) ; on the other hand, the formal argument involving exterior powers, outlined after (2), gives the feeling that it is really the first inequality $\lambda_1 \leq \lambda_1'$ which is essential, the other should follow once we have a good general framework.

I would very much appreciate your comments to this general nonsense, most of which is certainly quite familiar to you under a different terminology.

Very sincerely yours,

A. Grothendieck

Bures May 11, 1970

BIBLIOGRAPHIE

[1] André, M. : Méthode simpliciale en algèbre homotopique et algèbre commutative, Lecture Notes in Mathematics, Vol. 32, Springer-Verlag, 1967.

[2] Barsotti, I.: Analytical Methods for Abelian Varieties in Positive Characteristic, Coll. théorie des groupes algébriques, C.B.R.M., Bruxelles, 1962.

[3] Berthelot, P. : Cohomologie p-cristalline des schémas, C.R.Acad.Sci. Paris t.269 (1969), A297-300, A357-360, A397-400; t.272 (1971) A42-45, A141-144, A254-257, A1314-1317, A1397-1400.

[4] Berthelot, P. : thèse (à paraître)

[5] Berthelot, P. et Illusie, L. : Classes de Chern en cohomologie cristalline

[6] Deligne, P. : Cohomologie cristalline en caractéristique 0, Séminaire IHES, à paraître aux Lectures Notes (?).

[7] Demazure, M. : Lectures on p-divisible groups, Lectures Notes in Mathematics, Vol.302, Springer-Verlag, 1972.

[8] Demazure, M. et Gabriel, P. : Groupes Algébriques, North Holland, Amsterdam, 1970.

[9] Demazure, M. et Grothendieck, A. : Schémas en groupes, Lectures Notes in Mathematics, Vol. 151-153, Springer-Verlag, 1970 (cité SGA 3 dans le texte).

[10] Giraud, J. : Cohomologie non abélienne, Springer-Verlag, 1971.

[12] Grothendieck, A. et Dieudonné, J. : Eléments de géométrie algébrique, Publ. Math. IHES, Vol.4, 8, 11, 17, 20, 24, 28, 32.

[13] Grothendieck, A. et al. : Séminaire de géométrie algébrique du Bois-Marie. Lectures notes in Mathematics, Vol.224, 269, 270, 305, Springer, 1971-1972.

[14] Grothendieck, A. : Crystals and the De Rham cohomology of schemes. (notes de I.Coates et O.Jussila), in "Dix exposés sur la cohomologie des schémas", North Holland, 1968.

[15] Grothendieck, A. : On the De Rham cohomology of algebraic varieties, Publ. Math. IHES Vol.29, 1966.

[16] Grothendieck, A. : Catégories cofibrées et complexe cotangent relatif. Lecture Notes in Mathematics, vol.79, Springer-Verlag,1968.

[17] Illusie, L. : Algèbre homotopique relative, C.R.Acad.Sci.Paris,t.268 (1969), A11-14, A206-209.

[18] Illusie, L. : Complexe cotangent relatif d'un faisceau d'algèbres, C.R.Acad.Sci.Paris, t.268 (1969), A278-281, A323-326.

[19] Illusie, L. : Complexe cotangent et déformations I et II, Lecture Notes in Mathematics, vol.239 et 283, Springer, 1971-1972.

[20] Katz, N. : On the differential equations satisfied by period matrices, Publ. Math. IHES, vol,35, 1968.

[21] Kiehl, R. : Die De Rham Kohomologie Algebraischer Mannigfaltigkeiten über einen Bewerteten Körper. Publ. Math. IHES, vol.33, 1967.

[22] Manin, Yu.: The Theory of Commutative Formal Groups over Fields of Finite Characteristic, traduction anglaise, Russian Math. Surv. Vol.18 (1963).

[23] Mazur, B. : Frobenius and the Hodge Filtration. Bull. Amer.Math.Sco. 78 (1972) 653-667 et Ann.of Math.98(1973) 58-95 .

[23a] Mazur, B. et Messing, W. Universal extensions and one-dimensional crystallin cohomology. A paraître. Lect. Notes in Math. 370

[24] Messing, W. : The Crystals Associated to Barsotti-Tate Groups, with Applications to Abelian Schemes, Lecture Notes in Math. Vol.264, 1972.

[25] Monsky et Washnitzer.: The Construction of Formal Cohomology Sheaves Proc. Nat. Acad. Sci. U.S.A. 52 (1964) 1511-1514.

[26] Mumford, D. : Geometric Invariant Theory, Ergebrisse Math, Springer-Verlag, 1965.

[27] Mumford, D. : Abelian Varieties, Oxford, 1970.

[28] Oda, T. : The First De Rham Cohomology Group and Dieudonné Modules, Ann. Sci. Ecole Norm. Sup., 1969.

[29] Oort, F. : Commutative Group Schemes, Lecture Notes in Mathematics, Vol.15, Springer-Verlag, 1966.

[30] Quillen, D. : Homotopical Algebra, Lecture Notes in Mathematics, Vol. 43, Springer-Verlag, 1967.

[31] Roby, N. : Les algèbres à puissances divisées, Bull. Sci. Math., 1965.

[32] Serre, J.-P.: Corps locaux, Hermann, Paris, 1962.

[33] Serre, J.-P.: Groupes p-divisibles (d'après J.Tate), Séminaire Bourbaki, exposé 318, 1967.

[34] Tate, J. : p-Divisible Groups, Proceedings of a Conference on Local Fields, Nuffic Summer School at Driebergen, Springer-Verlag, 1967.