GROUPES p-DIVISIBLES

par

Joël Riou

Id: tate.tex,v 1.25 2003/05/05 08:38:45 cvs Exp

Table des matières

1. Définition et premières propriétés

1.1. Définition. — Soit p un nombre premier et S un schéma quelconque.

Définition 1.1. — Un groupe p-divisible de hauteur h sur un schéma S est la donnée d'un système inductif de S-schémas en groupes commutatifs de présentation finie $\mathscr{G} = (\mathscr{G}_\nu)_{\nu\in\mathbb{N}}$, où l'on note $i_\nu \colon \mathscr{G}_\nu \to \mathscr{G}_{\nu+1}$ les morphismes de transition, tel que :

(i) pour tout $\nu \in \mathbb{N}$, $\mathscr{G}_\nu$ est fini et plat sur S, d'ordre $p^{\nu h}$;

(ii) pour tout $\nu \in \mathbb{N}$, la suite suivante est exacte :

$$0 \to \mathscr{G}_\nu \xrightarrow{i_\nu} \mathscr{G}_{\nu+1} \xrightarrow{[p^\nu]} \mathscr{G}_{\nu+1}$$

où l'on note $[n]$ la multiplication par n sur un groupe commutatif.

En particulier, les morphismes de transitions sont des immersions fermées.

Les exemples les plus simples sont les suivants :

1. le système inductif évident $(\frac{1}{p^\nu}\mathbb{Z}_p/\mathbb{Z}_p)_{\nu\in\mathbb{N}}$, où on n'a pas indiqué le foncteur « groupe constant », définit un groupe p-divisible sur S de hauteur 1 que l'on note $\mathbb{Q}_p/\mathbb{Z}_p$;
2. le système inductif évident $(\boldsymbol{\mu}_{p^\nu})_{\nu\in\mathbb{N}}$ définit un groupe p-divisible sur S de hauteur 1 que l'on note $\mathbb{G}_m(p)$;

3. si $\mathscr{A}$ est un S-schéma abélien de dimension g, le morphisme $[n]\colon \mathscr{A} \to \mathscr{A}$ est fini et plat[(1)] de degré n^{2g}, de sorte que le noyau $\mathscr{A}[n]$ de $[n]$ est un S-schéma en groupes fini et plat (et de présentation finie). On peut ainsi considérer le groupe p-divisible $\mathscr{A}(p) = (\mathscr{A}[p^\nu])_{\nu\in\mathbb{N}}$, qui est de hauteur $2g$.

Lemme 1.2. — *Soit $\mathscr{G}$ un groupe p-divisible sur S, alors on a des suites exactes de S-schémas en groupes finis et plats, pour tous $\mu, \nu \geq 0$:*

$$0 \to \mathscr{G}_\mu \overset{i_{\mu,\nu}}{\to} \mathscr{G}_{\mu+\nu} \overset{p_{\mu,\nu}}{\to} \mathscr{G}_\nu \to 0$$

Démonstration. — Le morphisme $i_{\mu,\nu}$ est simplement le composé des morphismes de transition. La multiplication par p^μ sur $\mathscr{G}_{\mu+\nu}$ se factorise évidemment par $\mathscr{G}_\nu$, ce qui définit $p_{\mu,\nu}$. L'exactitude de la suite en $\mathscr{G}_\mu$ et en $\mathscr{G}_{\mu+\nu}$ est évidente. Il reste à montrer que $p_{\mu,\nu}$ est fidèlement plat. D'après un théorème de Grothendieck, le quotient $\mathscr{G}_{\mu+\nu}$ par l'action de $\mathscr{G}_\mu$ par translation existe et définit un S-schéma en groupes de présentation finie C qui est fini et plat. On sait que $\mathscr{G}_{\mu+\nu} \to C$ est fidèlement plat. On obtient facilement un monomorphisme de S-schémas en groupes $C \to \mathscr{G}_\nu$ qui est une immersion fermée car c'est un monomorphisme propre (puisque fini). C et $\mathscr{G}_\nu$ ayant le même ordre, $C = \mathscr{G}_\nu$. □

Définition 1.3. — Soit $\mathscr{G}$ un groupe p-divisible. On note $\mathscr{G}'$ le groupe p-divisible dual. Si $\mathbb{D}$ désigne la dualité de Cartier, on a $\mathscr{G}'_\nu = \mathbb{D}\mathscr{G}_\nu$, le morphisme de transition $\mathscr{G}'_\nu \to \mathscr{G}'_{\nu+1}$ est le dual de Cartier du morphisme $p_{1,\nu}\colon \mathscr{G}_{\nu+1} \to \mathscr{G}_\nu$. Le lemme précédent permet de s'assurer que $\mathscr{G}'$ est bien un groupe p-divisible (de même hauteur).

Il est clair que le bidual d'un groupe p-divisible lui est canoniquement isomorphe.

1.2. Groupes étales, groupes connexes. — On suppose ici que S est le spectre d'un *anneau local hensélien* R à corps résiduel de caractéristique p[(2)].

Lemme 1.4. — *Soit G un S-schéma en groupes commutatif fini et plat. Alors, il existe une suite exacte fonctorielle de S-schémas en groupes de présentation finie, finis et plats :*

$$0 \to G^0 \overset{i}{\to} G \overset{j}{\to} G^{\text{ét}} \to 0$$

où G^0 est connexe et $G^{\text{ét}}$ étale.

Démonstration. — Soit k_s une clôture séparable du corps résiduel k de R. Notons G le groupe de Galois de l'extension k_s/k et $\tilde{R}$ l'hensélisé strict de R correspondant au choix de la clôture séparable que l'on vient de faire. Le groupe G agit R-linéairement sur $\tilde{R}$ de façon compatible avec son action résiduelle.

Soit A la R-algèbre de G. Notons $\tilde{A} = A \otimes_R \tilde{R}$. On définit $\tilde{A}^{\text{ét}}$ comme étant la sous-$\tilde{R}$-algèbre de $\tilde{A}$ engendrée par les idempotents de $\tilde{A}$. Cette algèbre $\tilde{A}^{\text{ét}}$ s'identifie évidemment à l'algèbre des fonctions localement constantes sur l'espace topologique de G à valeurs dans $\tilde{A}$, ce qui montre bien que $\tilde{A}^{\text{ét}}$ est une R-algèbre localement libre et étale. Cela permet aussi de voir que $\operatorname{Spec}\tilde{A}^{\text{ét}}$ est un $\tilde{R}$-schéma en groupes commutatif que l'on note $\tilde{G}^{\text{ét}}$. Le fait que ce schéma en groupes soit un revêtement fini étale de $\operatorname{Spec} R$ permet d'obtenir que le morphisme $\tilde{G} \to \tilde{G}^{\text{ét}}$ est fidèlement plat. On voit aussitôt que le noyau du morphisme $\tilde{G} \to \tilde{G}^{\text{ét}}$ est la composante neutre de $\tilde{G}$, ce qui montre le lemme pour $\tilde{G}$.

On passe au cas général par descente étale. En effet, l'ensemble des idempotents de $\tilde{A}$ est stable par l'action du groupe fondamental G, de sorte qu'il existe une unique sous-R-algèbre $A^{\text{ét}}$ de A

(1) Tout d'abord, il est assez clair que $[n]$ est quasi-fini et propre, donc fini. Pour montrer que $[n]$ est plat, on peut supposer que S est affine, puis par approximation noethérienne qu'il est noethérien. La question étant de nature locale sur S, on peut ainsi supposer que S est local noethérien. $\mathscr{A}$ étant plat sur S, le critère de platitude fibre à fibre [**EGA IV 11.3.10**] permet de supposer que S est le spectre d'un corps k. On peut noter $A = \mathscr{A}$. Comme A est réduit, on peut conclure que $[n]^\star\colon A \to A$ est plat en utilisant qu'un module de présentation finie M sur un anneau réduit est libre si et seulement si les dimensions des espaces vectoriels $M \otimes k(x)$ forment une fonction localement constant sur le spectre de l'anneau.

(2) En caractéristique 0, tous les schémas en groupes sont lisses, donc les notions qui suivent y sont vides de sens.

telle que $A^{\text{ét}} \otimes_R \tilde{R}$ soit $\tilde{A}^{\text{ét}}$. Les constructions qui s'ensuivent et les propriétés des morphismes étudiées sont stables par descente étale, ce qui permet de conclure. □

Remarque 1.5. — R étant hensélien, la formation de cette suite exacte est compatible au changement de base $\operatorname{Spec} k \to \operatorname{Spec} R$.

Remarque 1.6. — Si $R = k$ est un corps *parfait*, la suite exacte ci-dessus est canoniquement scindée. En effet, un produit de k-algèbres (finies) réduites est réduite, ainsi G_{red} est un sous-schéma en groupes fermé (réduit donc étale) de G, et on voit aussitôt que le morphisme composé $G_{\text{red}} \to G \to G^{\text{ét}}$ est un isomorphisme.

Corollaire 1.7. — *Soit $\mathscr{G}$ un groupe p-divisible sur un anneau hensélien R. Alors, il existe une suite exacte canonique :*

$$0 \to \mathscr{G}^0 \to \mathscr{G} \to \mathscr{G}^{\text{ét}} \to 0$$

où $\mathscr{G}^0$ est connexe et $\mathscr{G}^{\text{ét}}$ est étale (ce qui signifie que les groupes finis qui les composent sont itou).

Démonstration. — Les foncteurs $G \longmapsto G^0$ et $G \longmapsto G^{\text{ét}}$ sur les schémas en groupes de présentation finie, finis et plats sont exacts[3]. En utilisant le lemme 1.2, on obtient aisément que le système (G^0_ν) est un groupe p-divisible connexe et que $(G^{\text{ét}}_\nu)$ est un groupe p-divisible étale. □

Définition 1.8. — On dit d'un k-schéma en groupes fini commutatif qu'il est bi-infinitésimal s'il est connexe et que son dual de Cartier aussi (itou pour les schémas en groupes sur un anneau local hensélien). On dit d'un k-schéma en groupes fini commutatif qu'il est unipotent si son dual de Cartier est connexe. On dit d'un k-schéma en groupes fini commutatif qu'il est de type multiplicatif si son dual de Cartier est étale.

Corollaire 1.9. — *Soit $\mathscr{G}$ un schéma en groupes de présentation finie, fini et plat (resp. un groupe p-divisible) sur un anneau hensélien R. Alors, il existe sur $\mathscr{G}$ une filtration canonique par des sous-schémas en groupes finis et plats (resp. des sous-groupes-p-divisibles) :*

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

où $\mathscr{G}^{mult}$ de type multiplicatif, $\mathscr{G}^0/\mathscr{G}^{mult} = \mathscr{G}^{bi}$ bi-infinitésimal et $\mathscr{G}/\mathscr{G}^0 = \mathscr{G}^{\text{ét}}$ est étale.

Si R est un corps parfait de caractéristique p, on a une décomposition canonique :

$$\mathscr{G} = \mathscr{G}^{mult} \times \mathscr{G}^{bi} \times \mathscr{G}^{\text{ét}}$$

2. Modules de Dieudonné

Dans cette partie, k sera un corps parfait de caractéristique p.

2.1. Frobeniuseries. — Si X est un $\mathbb{Z}/p\mathbb{Z}$-schéma, on note $f : X \to X$ le morphisme de Frobenius, qui vaut l'identité sur l'espace topologique sous-jacent et l'élévation à la puissance p-ième sur le faisceau structural. Maintenant, si $X \xrightarrow{q} \operatorname{Spec} k$ est un k-schéma, on pose $X^{(p)} = X \times_{q, \operatorname{Spec} k, f} \operatorname{Spec} k$ et on note $F \colon X \to X^{(p)}$ le morphisme faisant commuter le diagramme suivant :

$$\begin{tikzcd}
X \arrow[dr, "F"] \arrow[drr, bend left, "f"] \arrow[ddr, bend right, "q"'] & & \\
& X^{(p)} \arrow[r] \arrow[d] & X \arrow[d, "q"] \\
& \operatorname{Spec} k \arrow[r, "f"] & \operatorname{Spec} k
\end{tikzcd}$$

[3] La preuve de ce résultat est laissée en exercice au lecteur...

Cette construction est suffisamment fonctorielle pour que si G est un k-schéma en groupes, alors $F : G \to G^{(p)}$ est un morphisme de k-schémas en groupes. Le morphisme F s'appelle le *Frobenius.* Construisons le *Verschiebung* comme dans [**SGA 3**, $\mathrm{VII_A}$ 4.2-3].

Le groupe symétrique Σ_p agit sur G^p par permutation des coordonnées. On note $\Sigma^p G$ le quotient de G^p par l'action de ce groupe fini. Si $G = \operatorname{Spec} A$, $G^p = \operatorname{Spec} A^{\otimes p}$ et $\Sigma^p G = \operatorname{Spec} B$ où $B = (A^{\otimes p})^{\Sigma_p}$, c'est l'algèbre des tenseurs symétriques. On vérifie aussitôt que le morphisme d'addition $G^p \to G$ passe au quotient par l'action de Σ^p pour définir un morphisme $+ \colon \Sigma^p G \to G$. Notons N l'ensemble des tenseurs *symétrisés* dans $A^{\otimes p}$. N est évidemment un idéal de B. On note $G^{[p]} = \operatorname{Spec} B/N$ et i l'immersion fermée $G^{[p]} \to \Sigma^p G$. Comme $p! = 0$ dans k, on voit que le morphisme composé $G \xrightarrow{\Delta} G^p \to \Sigma^p G$ se factorise par $G^{[p]}$. On dispose d'un morphisme mirifique $G^{[p]} \to G^{(p)}$ qui au niveau des algèbres est le morphisme $A \otimes_{k,f} k \to B$ qui envoie $x \otimes y$ sur $yx \otimes x \otimes \cdots \otimes x$. Il est évident que le composé $G \to G^{[p]} \xrightarrow{\varphi} G^{(p)}$ est le Frobenius.

Lemme 2.1. — *Le morphisme mirifique $G^{[p]} \to G^{(p)}$ est un isomorphisme.*

Démonstration. — Plus généralement, si M est un k-vectoriel, on a un morphisme(4) fonctoriel de k-espaces vectoriels $M \otimes_{k,f} k \to (M^{\otimes p})^{\Sigma_p}/N$ qui envoie $x \otimes y$ sur $yx \otimes x \otimes \cdots \otimes x$, N désignant les tenseurs symétrisés.

Si M est de dimension 0 ou 1, l'énoncé est trivial. Pour conclure, on voit qu'il suffit de montrer que le foncteur « tenseurs symétriques modulo tenseurs symétrisés » est additif sur les k-vectoriels, ce qui n'est pas difficile. □

On obtient ainsi un diagramme commutatif qui permet de définir le *Verschiebung* V :

$$\begin{tikzcd}
G^{(p)} \arrow[r, "V"] & G \\
G^{[p]} \arrow[u, "\varphi"] \arrow[r, "i"] & \Sigma^p G \arrow[u, "+"'] \\
G \arrow[u] \arrow[r, "\Delta"] \arrow[uu, bend left=60, "F"] & G^p \arrow[u] \arrow[uu, bend right=60, "+"']
\end{tikzcd}$$

Remarque 2.2. — La formation de $G^{(p)}$ et des morphismes F et V commute à toute extension des scalaires.

Il résulte du diagramme précédent que $FV = p$. On peut aussi en déduire que $VF = p$, ce qui donne le diagramme suivant :

$$\begin{tikzcd}
\mathscr{G} \arrow[r, "{[p]}"] \arrow[d, "F"'] & \mathscr{G} \arrow[d, "F"] \\
\mathscr{G}^{(p)} \arrow[r, "{[p]}"'] \arrow[ur, "V"] & \mathscr{G}^{(p)}
\end{tikzcd}$$

Par ailleurs, on peut montrer que pour les k-schémas en groupes finis, *Frobenius* et *Verschiebung* se correspondent par dualité de Cartier, ce qui rend le lemme suivant absolument trivial :

Lemme 2.3. — *Soit G un k-schéma en groupes fini.*

(i) G est étale si et seulement si F est un isomorphisme ;

(ii) G est de type multiplicatif si et seulement si V est un isomorphisme ;

(iii) G est connexe si et seulement si F est nilpotent ;

(iv) G est unipotent si et seulement si V est nilpotent ;

(v) G est bi-infinitésimal si et seulement si F et V sont nilpotents.

(4) Il faut vérifier que si x et y sont deux éléments de M, alors $(x+y)^{\otimes p} - x^{\otimes p} - y^{\otimes p}$ est un tenseur symétrisé, ce qui n'est pas difficile.

On rappelle que la catégorie des k-schémas en groupes finis est abélienne.

Corollaire 2.4. — *Soit G un k-schéma en groupes finis connexe. Alors, G est d'ordre une puissance de p.*

Idée de preuve. — Par dévissage, on peut supposer que $F = 0$. Notons I l'idéal d'augmentation de l'algèbre A de G. Il existe une bijection naturelle entre l'ensemble des k-dérivations de A dans A et $\mathrm{Hom}_k(I/I^2, A)$ qui est telle que si on note δ la k-dérivation associée à un élément f de $\mathrm{Hom}_k(I/I^2, A)$, alors pour $y \in I$, $\delta(y) \equiv f(y)\,[I]$. Il existe ainsi des k-dérivations $D_1, \ldots, D_n \colon A \to A$ et des éléments $y_1, \ldots, y_n \in I$ tels que $\mathbb{D}_i(y_j) \equiv \delta_{ij}\,[I]$. On peut faire passer cette situation au gradué de A pour les puissances de I, de sorte que l'on ait cette fois $D_i(y_j) = \delta_{ij}$ dans le gradué. On peut conclure en utilisant un développement de Taylor à l'ordre $p-1$ (en effet, $(p-1)!$ est inversible dans k !) que la dimension du gradué est p^n.

Grâce à un calcul de dimensions, on en déduit que A est isomorphe à $k[Y_1, \ldots, Y^n]/(Y_1^p, \ldots, Y_n^p)$. □

2.2. Modules de Dieudonné. —

2.2.1. Le théorème de Dieudonné. — On rapelle que k est un corps parfait de caractéristique p. On note $\mathbb{W}(k)$ l'anneau des vecteurs de Witt sur k, $\sigma \colon \mathbb{W}(k) \to \mathbb{W}(k)$ le Frobenius.

Définition 2.5. — On appelle module de Dieudonné sur k la donnée d'un $\mathbb{W}(k)$-module de type fini M muni de deux applications $\mathbb{Z}$-linéaires $F \colon M \to M$ et $V \colon M \to M$ telles que pour tout $\lambda \in \mathbb{W}(k)$ on ait les égalités suivantes dans $\mathrm{End}_{\mathbb{Z}}(M)$:

$$F.\lambda = \sigma(\lambda).F \qquad \lambda.V = V.\sigma(\lambda) \qquad F.V = V.F = p$$

***Théorème 2.6* (Dieudonné).** — *Il existe une équivalence de catégories $\mathcal{D}$ de la catégorie opposée de celle des k-schémas en groupes d'ordre une puissance de p vers celle des modules de Dieudonné sur k de longueur finie (comme $\mathbb{W}(k)$-modules).*

Pour construire le foncteur de Dieudonné $\mathcal{D}$, dans [**G**], on utilise un découpage des co-vecteurs de Witt et des p-groupes finis sur k en partie unipotente et en partie de type multiplicatif. On peut alors séparer les cas. Le cas difficile est celui des groupes unipotents où l'on a besoin des co-vecteurs de Witt (unipotents).

Définition 2.7. — Dans la suite du paragraphe, on appelera par abus p-groupe formel sur k la donnée d'un système inductif $(G_\nu)_{\nu\in\mathbb{N}}$ de k-schémas en groupes finis commutatifs tel que pour tout $\nu \in \mathbb{N}$, la suite suivante est exacte :

$$0 \to G_\nu \to G_{\nu+1} \overset{[p^\nu]}{\to} G_{\nu+1}$$

On peut montrer[5] que la catégorie des p-groupes formels est abélienne et que les p-groupes divisibles sont les objets de cette catégorie dans lesquels la multiplication par p est un épimorphisme. Le théorème de Dieudonné passe à la limite pour donner le théorème suivant :

***Théorème 2.8* (Dieudonné).** — *Il existe une équivalence de catégories $\mathcal{D}$ de la catégorie opposée de celle des k-groupes formels sur k vers celle des modules de Dieudonné sur k.*

Dans cette équivalence de catégories, les groupes p-divisibles correspondent aux modules de Dieudonnés libres sur $\mathbb{W}(k)$.

Lemme 2.9. — *Si G est un p-groupe formel sur k correspondant à un module de Dieudonné M, on a le dictionnaire suivant, où F et V sont les Frobenius et Verschiebung sur M :*

(i) G est étale si et seulement si F est bijectif ;

(ii) G est de type multiplicatif si et seulement si V est bijectif ;

(iii) G est connexe si et seulement si F est nilpotent ;

[5] C'est un excellent exercice.

(iv) G est unipotent si et seulement si V est nilpotent ;

(v) G est bi-infinitésimal si et seulement si F et V sont nilpotents.

2.2.2. Cristaux et groupes p-divisibles à isogénie près. — On peut raisonner à isogénie près s'intéresser à la catégorie des groupes p-divisibles sur k à isogénie près. D'un autre côté, on peut considérer la catégorie des F-isocristaux :

Définition 2.10. — On appelle F-cristal sur k la donnée d'un $\mathbb{W}(k)$-module D muni d'un $\mathbb{Z}$-endomorphisme $F\colon E \to E$ injectif tel que pour tout $\lambda \in \mathbb{W}(k)$, on ait $F.\lambda = \sigma(\lambda).F$.

Définition 2.11. — Notons K la corps des fractions de $\mathbb{W}(k)$. On appelle F-isocristal sur k la donnée d'un K-espace vectoriel E muni d'un $\mathbb{Q}$-endomorphisme $F\colon E \to E$ injectif tel que pour tout $\lambda \in K$, on ait $F.\lambda = \sigma(\lambda).F$. F est donc bijectif.

Définition 2.12. — Pour tout nombre rationnel $\alpha = \frac{r}{h}$ avec $r \in \mathbb{Z}$, $h \in \mathbb{N}^\star$ premiers entre eux, on note $E_{[\alpha]}$ le F-isocristal $\mathbb{Z}_p[T]/(T^h - p^r) \otimes_{\mathbb{Z}_p} K$ où $F = \lambda_T \otimes \sigma$ où λ_T est la multiplication par T sur $\mathbb{Z}_p[T]/(T^h - p^r)$. On dit que $E_{[\alpha]}$ est de pente α.

***Théorème 2.13* (Dieudonné-Manin).** — *Si k est un corps algébriquement clos de caractéristique p, la catégorie des F-isocristaux sur k est semi-simple et un ensemble représentatif de ses objets simples est $(E_{[\alpha]})_{\alpha\in\mathbb{Q}}$.*

On montre facilement que la décomposition isocline (*i.e.* selon les pentes) d'un F-isocristal sur la clôture algébrique k_s d'un corps parfait k de caractéristique p provenant par extension des scalaires à k_s d'un F-isocristal sur k est en fait « défini » sur k. Ainsi, tout F-isocristal sur un corps parfait k arbitraire est somme directe de F-isocristaux n'ayant qu'une pente.

Le lemme suivant n'est pas difficile :

Lemme 2.14. — *Soit (E, F) un F-isocristal.*

(i) il existe un F-cristal D tel que $E = D\left[\frac{1}{p}\right]$ si et seulement si les pentes de E sont ≥ 0 ;

(ii) il existe un module de Dieudonné (M, F, V) tel que $(M, F) = (E, F)$ si et seulement si les pentes α de E vérifient $0 \leq \alpha \leq 1$.

Corollaire 2.15. — *Soit k un corps parfait de caractéristique p. La catégorie des groupes p-divisibles sur k est équivalente à la catégorie opposée de celle des F-cristaux dont les pentes sont comprises, au sens large, entre 0 et 1.*

3. Groupes de Lie formels

3.1. Définition. —

Définition 3.1. — Soit R un anneau. Un groupe de Lie formel (commutatif) Γ sur R est la donnée d'une R-algèbre augmentée $\mathscr{A}$, *isomorphe* à $R[[X_1, \ldots, X_n]]$ pour un certain n que l'on appelle la dimension de R, et d'un homomorphisme $\varphi\colon \mathscr{A} \to \mathscr{A}\hat{\otimes}\mathscr{A}$ qui définisse *formellement* une loi de groupe commutative. Plus précisément, si on identifie $\mathscr{A}$ à $R[[X_1, \ldots, X_n]]$, que l'on désigne par $Y = (Y_1, \ldots, Y_n)$ et $Z = (Z_1, \ldots, Z_n)$ les paquets de variables intervenant dans $\mathscr{A}\hat{\otimes}\mathscr{A}$, que l'on note $F = (F_1, \ldots, F_n)$ les images des X_i par φ, alors on demande que les formules suivantes soient vérifiées :

(i) $X = F(X, 0) = F(0, X)$;

(ii) $F(X, F(Y, Z)) = F(F(X, Y), Z)$;

(iii) $F(X, Y) = F(Y, X)$.

On remarquera que l'existence de l'inversion est automatique[(6)].

[(6)] Cela résulte de variantes formelles du théorème des fonctions implicites ou du théorème d'inversion locale.

Notons I l'idéal d'augmentation de $\mathscr{A}$. L'axiome (i) implique que $F(X,Y) \equiv X + Y\,(I^2)$. L'espace tangent du groupe de Lie formel est le R-module dual de I/I^2.

Pour tout entier $m \in \mathbb{Z}$, notons $\varphi_m \colon \mathscr{A} \to \mathscr{A}$ le morphisme d'anneaux correspondant à la multiplication par m sur le groupe formel. Posons $f_m(X) = (\varphi_m(X_1), \dots, \varphi_m(X_n))$. On obtient aisément que $f_m(X) \equiv mX(I^2)$. La formule du binôme se généralise ainsi :

***Théorème 3.2* (Lazard)**. — *Il existe une unique famille $(\psi_i(X))_{i\geq 1}$ telle que pour tout $i \geq 1$, $\psi_i(X)$ soit une famille $(\psi_i^{(1)}(X), \dots, \psi_i^{(n)}(X))$ d'éléments de $R[[X_1, \dots, X_n]]$ et que*
(i) $\psi_1(X) = X$;
(ii) $\psi_i(X) \in I^i$ (c'est-à-dire que $\psi_i(X)$ est d'ordre $\geq i$) ;
(iii) pour tout $m \in \mathbb{Z}$, $f_m(X) = \sum_{i=1}^{\infty} \binom{m}{i} \psi_i(X)$

Notons que la formule (iii) est vraie même pour $i \in \mathbb{Z}$ en donnant le sens habituel à $\binom{m}{i}$ dans ce cas.

Preuve du théorème. — Si la famille ψ_i existe, elle est clairement unique. Pour tout $m \in \mathbb{Z}$, on peut décomposer $f_m(X)$ en :

$$f_m(X) = \sum_{\alpha} a_\alpha(m) X^\alpha$$

où α parcourt les multi-indices. On obtient ainsi des applications $a_\alpha \colon \mathbb{Z} \to R^n$. Il s'agit de montrer par récurrence sur le degré $|\alpha|$ de α que pour tout multi-indice α, la fonction a_α est une fonction binômiale de degré $\leq |\alpha|$.

Une fonction $a \colon \mathbb{Z} \to R$ est dite binômiale de degré $\leq n$ s'il existe des éléments (nécessairement uniques) $(a^0, \dots, a^n) \in R^{n+1}$ tels que

$$\forall m \in \mathbb{Z} \quad a(m) = \sum_{i=0}^{n} a^i \binom{m}{i}$$

Si les coefficients a_α sont bien des fonctions binômiales de degré $\leq |\alpha|$, on pourra poser

$$\psi_i = \sum_{|\alpha| \geq i} a_\alpha^i \binom{m}{i}$$

ce qui donnera que pour tout $m \in \mathbb{Z}$, $f_m(X) = \sum_{i\geq 0} \binom{m}{i} \psi_i(X)$. Le terme constant étant nul, on aura $\psi_0 = 0$, ce qui donnera le résultat.

Faisons la récurrence annoncée plus haut sur $|\alpha|$. Pour $|\alpha| \leq 1$, c'est clair vu que $f_m(X) \equiv X\,(I^2)$. On suppose maintenant que $|\alpha| \geq 2$ et que pour tout multi-indice β de degré $< |\alpha|$, a_β est une fonction binômiale de degré $\leq |\beta|$. D'après les formules de récurrences sur les coefficients binômiaux, il suffit de montrer que Δa_α est une fonction binômiale de degré $< |\alpha|$ où $(\Delta a_\alpha)(m) = a_\alpha(m+1) - a_\alpha(m)$. Considérons les coefficients de F :

$$F(X,Y) = X + Y + \sum_{\gamma,\delta} c_{\gamma\delta} X^\gamma Y^\delta$$

où γ et δ parcourent les multi-indices de degré ≥ 1.

En remplaçant Y par f_m, on obtient donc :

$$f_{m+1}(X) = X + f_m(X) + \sum_{\gamma,\delta} c_{\gamma,\delta} X^\gamma f_m(X)^\delta$$

Comme $|\alpha| \geq 2$, on obtient que $\Delta a_\alpha(m)$ s'écrit comme la somme des coefficients du monôme X^α apparaissant dans chaque expression $c_{\gamma,\delta} X^\gamma f_m(X)^\delta$. Il s'agit de regarder ce qui se passe pour chaque expression $X^\gamma f_m(X)^\delta$ pouvant contribuer, ce qui, compte tenu du fait que $|\gamma| \geq 1$, impose que $|\delta| < |\alpha|$. Il s'agit ainsi d'étudier dans ce cas les coefficients de $X^{\alpha-\gamma}$ dans $f_m(X)^\delta$. En développant $f_m(X)^\delta$, on voit que ces coefficients sont des sommes de produits des coefficients $b_{i_\nu}(m)$ de X^{i_ν} dans $f_m(X)$ où $\sum i_\nu = \alpha - \gamma$. Par hypothèse de récurrence, les fonctions b_{i_ν} sont binômiales de degré $\leq |i_\nu|$, ce qui permet de conclure en utilisant le fait que le produit de deux fonctions binômiales est une fonction binômiale de degré inférieur ou égal à la somme des degrés. $\square$

3.2. L'équivalence de catégories. — Dans cette partie, on suppose que R est un anneau local noethérien complet de corps résiduel k de caractéristique p

Soit Γ un groupe de Lie formel sur R d'algèbre $\mathscr{A}$. Notons $\psi\colon \mathscr{A} \to \mathscr{A}$ le morphisme d'algèbres correspondant à la multiplication par p sur Γ. On dit que Γ est divisible si $\psi\colon \mathscr{A} \to \mathscr{A}$ fait de $\mathscr{A}$ un $\mathscr{A}$-module libre de rang fini. On définit alors un groupe p-divisible $\Gamma(p)$ sur R de la façon suivante. Pour tout $\nu \in \mathbb{N}$, on note Γ_{p^ν} le noyau[7] de $p^\nu\colon \Gamma \to \Gamma$. On voit aisément que A_ν est une R-algèbre locale, ainsi Γ_{p^ν} est un R-schémas en groupes fini et plat *connexe*, donc son ordre est une puissance de p (*cf.* corollaire 2.4). Si Γ_p est d'ordre p^h, alors on a bien construit un groupe p-divisible $\Gamma_p = (\Gamma_{p^\nu})_\nu$ de hauteur h.

Théorème 3.3. — *Soit R un anneau local noethérien complet de corps résiduel de caractéristique p. Alors, le foncteur $\Gamma \longmapsto \Gamma(p)$ induit une équivalence de catégories de la catégorie des groupes de Lie formels divisibles sur R vers la catégorie des groupes p-divisibles connexes sur R.*

Démonstration. — Soit Γ un groupe de Lie formel divisible. Norons I l'idéal d'augmentation de son algèbre $\mathscr{A}$, $\mathfrak{m}$ l'idéal maximal de R et $M = \mathfrak{m}\mathscr{A} + I$ l'idéal maximal de $\mathscr{A}$.

Tout d'abord, on note que les idéaux $\mathfrak{m}^\nu\mathscr{A} + J_\nu$ forment un système fondamental de voisinages de 0 pour la topologie M-adique sur $\mathscr{A}$. En effet, comme les anneaux $\mathscr{A}/(\mathfrak{m}^\nu A + J_\nu)$ sont artiniens et que $\mathscr{A}$ est local, les idéaux $\mathfrak{m}^\nu\mathscr{A} + J_\nu$ contiennent des puissances de $\mathfrak{m}$, donc sont ouverts. Or, $\psi(I) \subset pI + I^2 \subset MI$, d'où par récurrence, $J_\nu = \psi^{\circ\nu}(I)\mathscr{A} \subset M^\nu I$, ce qui prouve l'assertion.

Comme $\mathscr{A}$ est complet pour la topologie M-adique, on obtient que $\mathscr{A} = \lim_\nu \mathscr{A}_\nu$. On en déduit aisément la pleine fidélité du foncteur $\Gamma \longmapsto \Gamma(p)$.

Pour conclure, donnons-nous un groupe p-divisible connexe $\mathscr{G}$ sur R. Notons A_ν l'algèbre de $\mathscr{G}_\nu$ et considérons les morphismes (surjectifs) $A_{\nu+1} \to A_\nu$ induit par les immersions fermées $\mathscr{G}_\nu \to \mathscr{G}_{\nu+1}$. On note $\mathscr{A}$ la limite projective du système $(A_\nu)_\nu$. $\mathscr{A}$ vient naturellement avec une comultiplication $\mathscr{A} \to \mathscr{A}\hat{\otimes}\mathscr{A}$.

Il reste à montrer que $\mathscr{A}$ est isomorphe à une algèbre de séries formelles et que le groupe de Lie formel associé est divisible. La deuxième assertion est assez claire (on peut lui donner un sens avant de savoir la première assertion...). Le R-module $\mathscr{A}$ étant isomorphe à un produit (dénombrable) de copies de R et R étant noethérien[8], $\mathscr{A}$ est une R-algèbre plate. Grâce à cette platitude, on peut suppposer que R est un corps.

Pour tout entier $\nu \in \mathbb{N}$, on note H_ν le noyau de $F^\nu\colon G \to G^{(p^\nu)}$. On a évidemment $H_\nu \subset G_\nu$ et puis pour tout ν il existe un entier N tel que $G_\nu \subset H_N$ (F est nilpotent sur G_ν car il s'agit d'un k-schéma en groupes fini connexe.). Par conséquent, si $H_\nu = \operatorname{Spec} B_\nu$, $A = \lim \mathscr{A}_\nu = \lim B_\nu$. Notons I_ν l'idéal d'augmentation de B_ν et $I = \lim I_\nu$ celui de A. On choisit des éléments $x_1, \ldots, x_n \in I$ dont les images dans I_1/I_1^2 en forme une k-base. Comme H_1 est le noyau de F dans H_ν, le noyau de $I_\nu \to I_1$ est engendré par les puissances p-ièmes d'éléments de I_ν, on en déduit aisément un isomorphisme $I_\nu/I_\nu^2 \to I_1/I_1^2$ de telle sorte que les images des éléments $x_1, \ldots, x_n$ engendrent I_ν par Nakayama.

Grâce au fait que F est surjectif, l'« additivité des indices » donne que l'ordre de H_ν est celui de H_1 à la puissance ν. On peut considérer le morphisme d'anneaux $k[X_1, \ldots, X_n]/(X_1^{p^\nu}, \ldots, X_n^{p^\nu}) \to B_\nu$ qui envoie X_i sur x_i. Ce morphisme d'anneaux est tautologiquement surjectif, donc injectif pour des raisons de dimensions : il suffit de savoir que $\dim B_1 = p^n$ ce qui résulte de la démonstration du corollaire 2.4. On passant à la limite projective, on obtient bien que $A = k[[X_1, \ldots, X_n]]$. □

3.3. Dimensions. —

Définition 3.4. — Si $\mathscr{G}$ est un groupe p-divisible sur un anneau local noethérien complet R de corps résiduel parfait de caractéristique p, on note $\dim \mathscr{G}$ la dimension du groupe de Lie formel associé à $\mathscr{G}^0$.

(7) C'est-à-dire que $\Gamma_{p^\nu} = \operatorname{Spec} A_\nu$ où $A_\nu = \mathscr{A}/J_\nu$ et $J_\nu = \psi^{\circ\nu}(I).\mathscr{A}$, I étant l'idéal d'augmentation de $\mathscr{A}$.

(8) En effet, on peut montrer que si $(A_i)_{i\in I}$ est une famille de R-modules et M un R-module de type fini, alors le morphisme évident $\operatorname{Tor}_q^A(M, \prod_i A_i) \to \prod_i \operatorname{Tor}_q^A(M, A_i)$ est un isomorphisme si R est noethérien,.

Lemme 3.5. — *Soit $\mathscr{G}$ un groupe p-divisible sur R de hauteur h. Notons $n = \dim \mathscr{G}$ et $n' = \dim \mathscr{G}'$. On a l'égalité*

$$n + n' = h$$

Démonstration. — Il suffit de traiter le cas où k est un corps parfait. À la fois, p, F et V sont surjectifs sur $\mathscr{G}$ de sorte que l'égalité $VF = p$ donne naissance à une suite exacte

$$0 \to \ker F \to \ker p \to \ker V \to 0$$

Le rang de $\ker F$ est p^n d'après la preuve du théorème 3.3, celui de $\ker p$ est p^h et par dualité de Cartier, celui de $\ker V$ est $p^{n'}$, ce qui permet de conclure. $\square$

3.4. Le logarithme. — Dans cette partie, on suppose que R est un anneau de valuation discrète complet de corps résiduel parfait $k = R/\mathfrak{m}$ de caractéristique p et de corps des fractions K de caractéristique 0.

Soit L le complété d'une extension *algébrique* de K et $\mathscr{O}_L$ son anneau d'entiers.

Définition 3.6. — Soit $\mathscr{G}$ un groupe p-divisible sur R. On définit les $\mathbb{Z}_p$-modules :

$$\mathscr{G}(\mathscr{O}_L/\mathfrak{m}^i\mathscr{O}_L) = \operatorname{colim}_\nu \mathscr{G}_\nu(\mathscr{O}_L/\mathfrak{m}^i\mathscr{O}_L) \quad \mathscr{G}(\mathscr{O}_L) = \lim_i \mathscr{G}(\mathscr{O}_L/\mathfrak{m}^i\mathscr{O}_L)$$

Exemple 3.7. — si $G = \mathbb{G}_m(p)$, $G(\mathscr{O}_L) = U$, où U désigne l'ensemble des unités de $\mathscr{O}_L$ congrues à 1 modulo l'idéal maximal.

On note que si $\mathscr{G}$ est étale, $\mathscr{G}(\mathscr{O}_L)$ est de torsion. Si $\mathscr{G}$ est connexe et qu'on note $\mathscr{A}$ l'algèbre de son groupe de Lie formel, on voit que $\mathscr{G}(\mathscr{O}_L)$ s'identifie à l'ensemble des morphismes de R-algèbres $\mathscr{A} \to \mathscr{O}_L$ continus pour la topologie $M = (I + \mathfrak{m})$-adique sur $\mathscr{A}$ et la topologie de la valuation sur $\mathscr{O}_L$. En particulier, si $\mathscr{A} = R[[X_1, \ldots, X_n]]$, $\mathscr{G}(\mathscr{O}_L)$ s'identifie ensemblistement à un produit de n copies de l'idéal maximal de $\mathscr{O}_L$.

Lemme 3.8. — *Soit $\mathscr{G}$ un groupe p-divisible sur R. Alors, on a une suite exacte :*

$$0 \to \mathscr{G}^0(\mathscr{O}_L) \to \mathscr{G}(\mathscr{O}_L) \to \mathscr{G}^{\text{ét}}(\mathscr{O}_L) \to 0$$

Notons $t_\mathscr{G}$ l'espace tangent de $\mathscr{G}$ (autrement dit celui de $\mathscr{G}^0$), c'est un R-module libre de type fini. On note $t_\mathscr{G}(L) = t_\mathscr{G} \otimes_R L$.

Définition 3.9. — On définit l'application logarithme $\log\colon \mathscr{G}(\mathscr{O}_L) \to t_\mathscr{G}(L)$ par la formule[9]

$$(\log x)(\varphi) = \lim_{\nu\to\infty} \frac{\varphi(p^\nu x) - \varphi(0)}{p^\nu}$$

pour tout $\varphi \in \mathscr{A}$ où $\mathscr{A}$ est l'algèbre du groupe de Lie formel associé à $\mathscr{G}^0$. On notera que l'expression $f(p^\nu x)$ à un sens, pour un x donné, dès que ν est assez grand puisqu'alors $p^\nu x \in \mathscr{G}^0(\mathscr{O}_L)$.

Proposition 3.10. — *La suite définissant le logarithme est convergente. On obtient bien un morphisme de groupes abéliens.*

Démonstration. — On utilise le théorème de Lazard pour obtenir l'égalité

$$f_{p^\nu}(X) = \sum_{i=1}^{m} \binom{p^\nu}{i} \psi_i(X)$$

où f_{p^ν} est induit par $[p^\nu]$. Si $y \in L^n$, on note $v(y)$ l'inf des valuations des coordonnées de x. Soit $x \in \mathscr{G}^0(\mathscr{O}_L)$, on a

$$v\left(\frac{\binom{p^\nu}{i}\psi_i(x)}{p^\nu}\right) \geq -v(i) + i\,v(x)$$

[9] Cette formule est à rapprocher de celle qui dit que si $x \in \mathbb{R}_+^\star$, alors $\ln x$ est la limite de la suite $nx^{\frac{1}{n}}$.

On en déduit aisément que $\frac{f_{p^\nu}(x)}{p^\nu}$ converge vers

$$\log(x) = \sum_{i=1}^{\infty} \frac{(-1)^{i-1}}{i} \psi_i(X)$$

Le fait que la formule de la définition donne bien une dérivation et donc un élément de l'espace tangent est clair.

Pour montrer que le logarithme est un morphisme de groupes, il s'agit essentiellement d'utiliser les formules $F(f_m(X), f_m(Y)) = f_m(F(X,Y))$ pour $m = p^\nu$ et de passer à la limite. □

En utilisant une variante du théorème d'inversion locale, on obtient l'existence d'une application exponentielle qui est seulement un isomorphisme local inverse de log. De cela, on déduit notamment que le noyau du logarithme est un sous-groupe de torsion.

4. Représentations galoisiennes

Soit K une extension finie de $\mathbb{Q}_p$. On note R (ou $\mathscr{O}_K$) l'anneau des entiers de K. On choisit une clôture algébrique $\overline{K}$ de K, on note $\mathbb{C}_p$ le complété de $\overline{K}$ et $\mathscr{O}_{\mathbb{C}_p}$ l'anneau des entiers de $\mathbb{C}_p$.

Définition 4.1. — Soit G un groupe p-divisible sur K. On définit des modules avec action de $\mathrm{Gal}(\overline{K}/K)$:

$$\Phi(G) = \mathrm{colim}_{\nu,i}\, G_\nu(\overline{K}) \qquad T(G) = \lim_{\nu,[p]} G_\nu(\overline{K})$$

On remarque que $\Phi(G) = T(G) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p$ et que $T(G) = \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p/\mathbb{Z}_p, \Phi(G))$.

Lemme 4.2. — *Le foncteur qui à un groupe p-divisible G sur K associe $\Phi(G)$ (resp. $T(G)$) vu comme $\mathbb{Z}_p$-module avec action de $\mathrm{Gal}(\overline{K}/K)$ isomorphe comme module à $(\mathbb{Q}_p/\mathbb{Z}_p)^h$ (resp. $\mathbb{Z}_p^h$) est une équivalence de catégories.*

Démonstration. — En effet, K étant de caractéristique 0, tout schéma en groupes de type fini sur K est lisse (Cartier), donc tout groupe p-divisible sur K est étale. □

Si $\mathscr{G}$ est un groupe p-divisible sur $\mathscr{O}_K$, on note $T(\mathscr{G}) = T(G)$ (resp. $\Phi(\mathscr{G}) = \Phi(G)$) où G est la fibre générique de $\mathscr{G}$. Notons $\mathscr{G}'$ le dual de Cartier de $\mathscr{G}$. Pour tout $\nu \in \mathbb{N}$, comme $\mathscr{G}'_\nu$ est fini, $\mathscr{G}'_\nu(\mathscr{O}_{\mathbb{C}_p}) \xrightarrow{\sim} \mathscr{G}'_\nu(\mathbb{C}_p)$. En utilisant la dualité de Cartier, on obtient $\mathscr{G}'_\nu(\mathbb{C}_p) = \mathrm{Hom}_{\mathscr{O}_{C_p}}(\mathscr{G}_{\nu,\mathscr{O}_{C_p}}, \mathbb{G}_m(p))$, et finalement

$$T(\mathscr{G}') = \mathrm{Hom}_{\mathscr{O}_{\mathbb{C}_p}}(\mathscr{G}_{\mathscr{O}_{C_p}}, \mathbb{G}_m(p))$$

En passant aux $\mathscr{O}_{\mathbb{C}_p}$-points ou à l'espace tangent, on obtient des accouplements compatibles au logarithme :

$$\begin{tikzcd}
T(\mathscr{G}') \times \mathscr{G}(\mathscr{O}_{C_p}) \arrow[r] \arrow[d, "\mathrm{Id} \times \log"'] & U \arrow[d, "\log"] \\
T(\mathscr{G}') \times t_{\mathscr{G}}(\mathbb{C}_p) \arrow[r] & \mathbb{C}_p
\end{tikzcd}$$

Les logarithmes sont surjectifs. On obtient ainsi des suites exactes où l'on note $T' = T(\mathscr{G}')$:

(1)
$$\begin{tikzcd}
0 \arrow[r] & \Phi(G) \arrow[r] \arrow[d, "\alpha_0"] & \mathscr{G}(\mathscr{O}_{\mathbb{C}_p}) \arrow[r, "\log"] \arrow[d, "\alpha"] & t_{\mathscr{G}}(\mathbb{C}_p) \arrow[r] \arrow[d, "d\alpha"] & 0 \\
0 \arrow[r] & \mathbf{Hom}(T', U_{tors}) \arrow[r] & \mathbf{Hom}(T', U) \arrow[r, "\log"] & \mathbf{Hom}(T', \mathbb{C}_p) \arrow[r] & 0
\end{tikzcd}$$

Les Hom sur la deuxième ligne sont simplement des morphismes de $\mathbb{Z}_p$-modules, on passera aux points fixes sous $\mathrm{Gal}(\overline{K}/K)$ plus bas.

Proposition 4.3. — *α_0 est bijective ; α et $d\alpha$ sont injectives.*

Démonstration. — Premièrement, α_0 est bijective : cela résulte du fait que la fibre générique de $\mathscr{G}$ est étale et de propriétés élémentaires de la dualité de Cartier. Notons au passage que $T(\mathscr{G}) = \mathbf{Hom}(T(\mathscr{G}'), \mathbb{Z}_p(1))$ où $\mathbb{Z}_p(1) = T(\mathbb{G}_m(p))$.

Deuxièmement, $\ker\alpha$ et $\operatorname{coker}\alpha$ sont des $\mathbb{Q}_p$-espaces vectoriels. D'après le lemme du serpent, cela résulte du fait que $\ker d\alpha$ et $\operatorname{coker} d\alpha$ sont des $\mathbb{Q}_p$-espaces vectoriels.

Troisièmement, $\mathscr{G}(\mathscr{O}_K) = \mathscr{G}(\mathscr{O}_{\mathbb{C}_p})^{\mathrm{Gal}(\overline{K}/K)}$ et $t_G(K) = t_G(\mathbb{C}_p)^{\mathrm{Gal}(\overline{K}/K)}$. C'est une conséquence formelle du fait que $\mathbb{C}_p^{\mathrm{Gal}(\overline{K}/K)} = K$.

Quatrièmement, α est injective sur $\mathscr{G}(\mathscr{O}_K)$. Par dévissage, on peut supposer que $\mathscr{G}$ est soit étale soit connexe. S'il est étale, cela résulte des étapes 1 et 3. Supposons $\mathscr{G}$ connexe, comme $(\ker\alpha)^{\mathrm{Gal}(\overline{K}/K)}$ est un $\mathbb{Q}_p$-espace vectoriel, pour montrer qu'il est nul, il suffit de montrer qu'il n'existe pas d'élément infiniment p-divisible dans $\mathscr{G}(\mathscr{O}_K)$, ce qui résulte du fait que dans un groupe de Lie formel $\operatorname{Spec}\mathscr{O}_K[[X_1, ..., X_n]]$ sur un anneau de valuation *discrète*, si les coordonnées d'un point $x = (x_1, \dots, x_n) \in \mathfrak{m}^n$ sont dans $\mathfrak{m}^i$ alors celles de $[p]x$ sont dans $\mathfrak{m}^{i+1}$.

Cinquièmement, $d\alpha$ est injective sur $t_G(K)$. D'après le lemme du serpent, $\ker\alpha = \ker d\alpha$, on peut passer aux points fixes et utiliser l'étape précédente.

Sixièmement, $d\alpha$ est injective (et donc α aussi). On peut factoriser $d\alpha$ en

$$t_G(\mathbb{C}_p) = t_G(K) \otimes_K \mathbb{C}_p \to \mathrm{Hom}_{\mathrm{Gal}(\overline{K}/K)}(T', \mathbb{C}_p) \otimes_K \mathbb{C}_p \to \mathrm{Hom}(T', \mathbb{C}_p)$$

La première flèche est injective d'après l'étape précédente, et la deuxième par un lemme de « descente » :

Septièmement, soit k un corps et K une extension de k telle que $K^{\mathrm{Aut}(K/k)} = k$. Pour tout K-espace vectoriel W sur lequel $\mathrm{Aut}(K/k)$ agit semi-linéairement, l'application K-linéaire $W^{\mathrm{Aut}(K/k)} \otimes_k K \to W$ est injective. $\square$

Théorème 4.4. — *Les morphismes verticaux dans le diagramme suivant sont bijectifs :*

$$\begin{tikzcd}
\mathscr{G}(\mathscr{O}_K) \arrow[r, "\log"] \arrow[d, "\alpha_K"] & t_{\mathscr{G}}(K) \arrow[d, "d\alpha_K"] \\
\mathrm{Hom}_{\mathrm{Gal}(\overline{K}/K)}(T(\mathscr{G}), U) \arrow[r, "\log"] & \mathrm{Hom}_{\mathrm{Gal}(\overline{K}/K)}(T(\mathscr{G}'), \mathbb{C}_p)
\end{tikzcd}$$

Démonstration. — Commençons par noter que si $A' \xrightarrow{\varphi} A$ est un monomorphisme de $\mathrm{Gal}(\overline{K}/K)$-modules, l'application évidente $\operatorname{coker}(\varphi^{\mathrm{Gal}(\overline{K}/K)}) \to (\operatorname{coker}\varphi)^{\mathrm{Gal}(\overline{K}/K)}$ est injective. Comme les conoyaux des deux morphismes verticaux (injectifs d'après la proposition 4.3) du milieu et de droite dans le diagramme (1) sont isomorphes d'après le lemme du serpent, on se ramène à montrer que la flèche $d\alpha_K$ est surjective, ce qui va se faire par un calcul de dimensions puisqu'il s'agit d'une application linéaire entre K-espaces vectoriels de dimension finie.

Posons $W' = \mathbf{Hom}_{\mathbb{Z}_p}(T(\mathscr{G}'), \mathbb{C}_p)$ et $W = \mathbf{Hom}_{\mathbb{Z}_p}(T(\mathscr{G}), \mathbb{C}_p)$. Ce sont des $\mathbb{C}_p$-espaces vectoriels de dimension h muni d'une action semi-linéaire de $\mathrm{Gal}(\overline{K}/K)$. Notons $d' = \dim_K W'^{\mathrm{Gal}(\overline{K}/K)}$, $d = \dim_K W^{\mathrm{Gal}(\overline{K}/K)}$, $n = \dim G$, $n' = \dim G'$. L'injectivité de $d\alpha_K$ pour $\mathscr{G}$ et $\mathscr{G}'$ implique que les inégalités $n \le d'$ et $n' \le d$. Comme $n + n' = h$ (*cf.* lemme 3.5), il suffit de prouver que $d + d' \le h$.

On a vu pendant la preuve de la proposition 4.3 que l'on avait un accouplement parfait $T(\mathscr{G}) \times T(\mathscr{G}') \to \mathbb{Z}_p(1)$ dont on déduit un accouplement $\mathrm{Gal}(\overline{K}/K)$-équivariant non dégénéré :

$$W \times W' \to \mathbb{C}_p(-1)$$

Or, $\mathbb{C}_p(-1)^{\mathrm{Gal}(\overline{K}/K)} = 0$, donc $W^{\mathrm{Gal}(\overline{K}/K)}\mathbb{C}_p$ et $W'^{\mathrm{Gal}(\overline{K}/K)}\mathbb{C}_p$ sont orthogonaux pour cet accouplement, ce qui implique que $d + d \le h$.

$\square$

Corollaire 4.5. — *Il existe un $\mathbb{C}_p$-isomorphisme* $\mathrm{Gal}(\overline{K}/K)$*-équivariant*

$$(\det T(\mathscr{G})) \otimes_{\mathbb{Z}_p} \mathbb{C}_p \xrightarrow{\sim} \mathbb{C}_p(n)$$

où $n = \dim\mathscr{G} = \dim\mathscr{G}^0$.

Démonstration. — Dans la preuve du théorème, on a vu que dans l'accouplement liant W et W', chacun des espaces $t_{\mathscr{G}}(\mathbb{C}_p)$ et $t_{\mathscr{G}'}(\mathbb{C}_p)$ est l'orthogonal de l'autre. On a ainsi une suite exacte canonique :

$$0 \to t_{\mathscr{G}}(\mathbb{C}_p)(1) \to T(\mathscr{G}) \otimes_{\mathbb{Z}_p} \mathbb{C}_p \to t^{\vee}_{\mathscr{G}'}(\mathbb{C}_p) \to 0$$

Pour conclure, il suffit de passer au det et de choisir des bases des K-vectoriels $t_{\mathscr{G}}(K)$ et $t_{\mathscr{G}'}(K)$. □

Corollaire 4.6. — *Il existe un isomorphisme canonique de $\mathbb{C}_p$-espaces vectoriels avec action semi-linéaire de* $\mathrm{Gal}(\overline{K}/K)$ *:*

$$T(\mathscr{G}) \otimes_{\mathbb{Z}_p} \mathbb{C}_p = t^{\vee}_{\mathscr{G}'}(\mathbb{C}_p) \oplus t_{\mathscr{G}}(\mathbb{C}_p)(1)$$

Démonstration. — Il suffit de voir que la suite exacte de représentations galoisiennes intervenue dans la preuve du corollaire précédent se scinde de manière unique. Le $\mathrm{Gal}(\overline{K}/K)$-module continu des Endomorphismes de cette extension est isomorphe à une somme de copies de $\mathbb{C}_p(1)$. On peut conclure en utilisant le fait que $\mathbf{H}^i(\mathrm{Gal}(\overline{K}/K), \mathbb{C}_p(1)) = 0$ pour $i = 0$ ou $i = 1$. □

Cela implique que $T(\mathscr{G})$ est une représentation de Hodge-Tate.

Bibliographie

[EGA] **Alexander Grothendieck**, **Jean Dieudonné**. Éléments de géométrie algébrique. *Publications Mathématiques de l'I.H.E.S.*, **4** (1960), **8** (1961), **11** (1961), **17** (1963), **20** (1964), **24** (1965), **28** (1966), **32** (1967).

[SGA 3] **Alexander Grothendieck**, **Michel Demazure**. Propriétés générales des schémas en groupes. Groupes de type multiplicatif et structure des schémas en groupes généraux. Structure des schémas en groupes réductifs. *Séminaire de géométrie algébrique du Bois-Marie*, (1962-1964). *Lecture Notes in Mathematics*, **151** (1970), **153** (1970), **153** (1970). *Springer.*

[G] **Alexander Grothendieck**. Groupes de Barsotti-Tate et cristaux de Dieudonné. *Séminaire de mathématiques supérieures*, été 1970. *Les presses de l'université de Montréal*, (1974).

[Se1] **Jean-Pierre Serre**. Corps locaux. *Troisième édition. Actualités scientifiques et industrielles*, **1296** (1968). Publications de l'institut mathématique de l'université de Nancago. *Hermann.*

[Se2] **Jean-Pierre Serre**. Lie Algebras and Lie Groups. *Lecture Notes in Mathematics*, **1500** (1992). Deuxième édition. *Springer-Verlag.*

[Tate] **John Tate**. p-divisible groups *in Proceedings of a conference on local fields* (Driebergen, 1966), pages 158-183. *Springer*, (1967).

Le lecteur est aussi invité à consulter les notes du groupe de travail sur les variétés abéliennes organisé par Jérôme Plût à l'ENS Ulm en 2001-2002. Il y fut abondamment question des cristaux de Dieudonné. Les notes de la plupart des exposés sont disponibles à l'adresse suivante : `http://www.eleves.ens.fr/home/plut/var-ab.html`.

5 mai 2003

Joël Riou, 45 rue d'Ulm, 75005 Paris • *Url :* `http://www.eleves.ens.fr:8080/home/jriou/`
• *Url :* `http://www.math.jussieu.fr/~riou/`
• *E-mail :* `joel.riou@normalesup.org`