Périodique mensuel

de la

SOCIÉTÉ MATHÉMATIQUE DE FRANCE

11, rue Pierre et Marie-Curie - 75005 PARIS

Publié avec le concours du CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

Abonnement : 300 F par an

Chez OFFILIB, 48, rue Gay-Lussac, 75005 PARIS

astérisque
47-48

1977

groupes p-divisibles sur les corps locaux

Jean-Marc FONTAINE

Institut Fourier
Université Scientifique et Médicale de Grenoble

société mathématique de france

Je voudrais remercier le département de mathématiques de Queen's University, Kingston, Ontario, en particulier P. Ribenboim, de m'avoir donné l'occasion d'éclaircir mes idées sur les schémas en groupes finis et plats lors d'un cours que j'y fis à l'automne 1974.

Les résultats annoncés dans [20], [21] et [22] (dont les démonstrations constituent une partie du chapitre III et du § 1 du chapitre IV du présent mémoire, ainsi qu'une partie de [23]) ont été exposés lors d'un cours au Collège de France (Fondation Peccot) au printemps 1975. Les démonstrations étaient différentes car on utilisait au maximum les résultats connus. Je voudrais remercier la fondation Peccot de son hospitalité et les auditeurs de ce cours de leur patience et de leurs interventions.

Je voudrais aussi remercier tous ceux qui m'ont aidé aux différents stades de ce travail. Tout particulièrement P. Berthelot et W. Messing, mais aussi P. Cartier, P. Deligne, L. Illusie, N. Katz, M. Lazard, B. Mazur, M. Raynaud. Et enfin et surtout J.-P. Serre sans lequel ce travail n'aurait jamais vu le jour.

Ces remerciements seraient incomplets si je n'exprimais ici ma reconnaissance à Mme Guttin-Lombard et à Mlle Marchand qui ont réalisé la frappe du manuscrit.

TABLE DES MATIÈRES

INTRODUCTION

0.1. Soit p un nombre premier, soit k un corps parfait de caractéristique p, soit $A = W(k)$ l'anneau des vecteurs de Witt à coefficients dans k, soit A' l'anneau des entiers d'une extension finie totalement ramifiée du corps des fractions de A et soit e le degré de cette extension.

Le présent mémoire a pour objet

- la classification, à isomorphisme près, des (schémas en) groupes formels commutatifs sur k ;
- la classification, à isomorphisme près, des (schémas en) groupes formels, lisses et de dimension finie, sur A et sur A' si $e \leq p-1$;
- la classification, à isogénie près, des groupes de Barsotti-Tate (ou groupes p-divisibles) sur A'.

0.2. Ce mémoire a été conçu pour pouvoir être lu par les non-spécialistes : il suffit, en principe, de connaître un peu d'algèbre commutative (par exemple celle de Bourbaki) et les rudiments du langage des catégories (par exemple, [40]). On a essayé d'être aussi "élémentaire" que possible. On a systématiquement négligé le point de vue "géométrique" au profit du point de vue "fonctoriel" (et on a escamoté les difficultés d'ordre logique : les "catégories" de foncteurs que l'on considère ne sont de "vraies" catégories qu'à condition de se restreindre à un univers convenable, ce qui est implicitement supposé). Dans cet esprit, donnons, dès maintenant, quelques définitions (nous les reprendrons dans un cadre plus général au chapitre I) : soit B un anneau qui est soit k, soit A, soit A' :

- on appelle B-anneau fini toute B-algèbre associative, commutative et unitaire qui est un B-module de longueur finie ;
- un B-foncteur formel est un foncteur covariant de la catégorie des B-anneaux finis dans celle des ensembles ; on dit que c'est un schéma fini sur B s'il est représentable, que c'est un schéma formel sur B si c'est une limite inductive de schémas finis ;
- un B-foncteur en groupes formels (commutatifs) est un objet en groupes (commutatifs) dans la catégorie des B-foncteurs formels ; autrement dit c'est un foncteur covariant de la catégorie des B-anneaux finis dans celle des groupes (commutatifs) ; un groupe formel sur B (resp. un groupe fini sur k) est un foncteur en groupes formels dont le foncteur formel sous-jacent est un schéma formel (resp. fini) ;
- un groupe formel G sur B est lisse si, pour tout B-anneau fini R et tout idéal I de R de carré nul, l'homomorphisme canonique de $G(R)$ dans $G(R/I)$ est surjectif ;
- un p-groupe formel G sur B est un groupe formel commutatif de p-torsion (i.e. G s'identifie à $\varinjlim \operatorname{Ker} p^n|G$) ;
- un p-groupe fini sur k est un p-groupe formel qui est un groupe fini ;
- un groupe p-divisible, ou de Barsotti-Tate, sur k est un p-groupe formel tel que la multiplication par p est un épimorphisme, à noyau fini ; un groupe p-divisible, ou de Barsotti-Tate sur A ou A' est un p-groupe formel lisse qui, par restriction aux k-anneaux finis, définit un groupe p-divisible sur k (en fait, il y a seulement équivalence entre la catégorie des groupes formels que l'on vient de définir et celle des groupes p-divisibles).

0.3. Il nous a semblé utile de rassembler dans un chapitre préliminaire (chap. I) les résultats classiques et élémentaires sur les groupes formels qui sont utilisés dans la suite. Il ne contient aucune idée vraiment nouvelle, tout au plus quelques variantes de résultats bien connus ([13], [14], [15], [27], [28], [36]). Sa lecture est vivement déconseillée aux spécialistes qui l'utiliseront comme un chapitre de références.

0.4. Les quatre premiers paragraphes du chapitre II ont pour objet l'étude et la construction des covecteurs de Witt.

Soit m un entier ≥ 1. On sait ce que c'est que le schéma en anneaux commutatifs W_m des vecteurs de Witt : pour tout anneau commutatif R,

$W_m(R)$ est formé des éléments de la forme $(a_0, a_1, \dots, a_{m-1})$, avec les a_i dans R ; l'addition et la multiplication sont données par des polynômes convenables à coefficients entiers rationnels (cf. n° II.1).

Le morphisme de schémas $V_m : W_m \to W_{m+1}$, qui, à $(a_0, \dots, a_{m-1}) \in W_m(R)$, associe $(0, a_0, \dots, a_{m-1}) \in W_{m+1}(R)$, est compatible avec l'addition. Par passage à la limite, il nous permet de définir le $\mathbb{Z}$-foncteur en groupes commutatifs $CW^u = \varinjlim W_m$, que nous appelons le <u>groupe des covecteurs de Witt unipotents</u>.

Pour tout anneau commutatif R , on peut munir le groupe $CW^u(R)$ d'une structure de groupe topologique (telle que si $\varphi : R \to S$, l'homomorphisme $CW^u(\varphi)$ est continu). On note $CW(R)$ le complété séparé de $CW^u(R)$ pour cette topologie. En tant qu'ensemble, $CW(R)$ s'identifie à l'ensemble des covecteurs de Witt

$$\underline{a} = (\dots, a_{-n}, \dots, a_{-1}, a_0) ,$$

où les a_{-n} sont des éléments de R vérifiant la condition

(ψ) $\begin{cases} \text{\underline{il existe un entier} } r \geq 0 \text{ \underline{tel que l'idéal de} } R \text{ \underline{engendré par les} } a_{-n} , \\ \text{\underline{pour} } n \geq r , \text{ \underline{est nilpotent}}. \end{cases}$

Le groupe $CW^u(R)$ s'identifie au sous-groupe de $CW(R)$ formé des $\underline{a}$ tels que les a_{-n} sont presque tous nuls ; c'est un sous-groupe dense de $CW(R)$.

Cette construction est faite au § 1 . Les endomorphismes du groupe CW sont étudiés au § 2 . Par restriction à la catégorie des k-anneaux finis, CW définit un p-groupe formel lisse $\widehat{CW}_k$ sur k qui est introduit au § 4. Le § 3 a pour but de donner une description de l'algèbre affine de $\widehat{CW}_k$ et de certain de ses sous-groupes et ne joue qu'un rôle tout à fait secondaire.

0.5. Soit σ le Frobenius absolu sur A (i.e. l'unique automorphisme continu de A tel que $\sigma(a) \equiv a^p \pmod{pA}$, pour tout $a \in A$) et soit $D_k = A[\underline{F}, \underline{V}]$ l'anneau (non commutatif si $k \neq \mathbb{F}_p$) engendré par A et deux éléments $\underline{F}$ et $\underline{V}$ soumis aux relations $\underline{F}\,\underline{V} = \underline{V}\,\underline{F} = p$, $\underline{F}a = \sigma(a)\underline{F}$ et $a\underline{V} = \underline{V}\sigma(a)$, pour tout $a \in A$.

Appelons D_k-<u>module</u> $A[\underline{F}]$-<u>profini</u> tout D_k-module à gauche qui est un

$A[\underline{F}]$-module profini sur lequel $\underline{V}$ opère continûment. On montre que, si G est un p-groupe formel sur k , le groupe $\mathrm{Hom}(G, \widehat{CW}_k)$ des morphismes (dans la catégorie des groupes formels sur k) de G dans $\widehat{CW}_k$ a une structure naturelle de D_k-module $A[\underline{F}]$-profini ; on le note $\underline{M}(G)$ et on l'appelle le <u>module de Dieudonné</u> de G . Il est clair que $\underline{M}$ peut être considéré comme un foncteur contravariant additif de la catégorie des p-groupes formels sur k dans celle des D_k-modules $A[\underline{F}]$-profinis. Les quatre premiers paragraphes du chapitre III ont pour objet la démonstration des deux théorèmes suivants :

THÉORÈME 1.- <u>Le foncteur</u> $\underline{M}$ <u>est pleinement fidèle et induit une anti-équivalence entre la catégorie des</u> p-<u>groupes formels sur</u> k <u>et celle des</u> D_k-<u>modules</u> $A[\underline{F}]$-<u>profinis</u>.

THÉORÈME 2.- <u>Le groupe</u> $\widehat{CW}_k$ <u>est un objet injectif de la catégorie des groupes formels commutatifs sur</u> k .

On construit, en outre, un foncteur quasi-inverse $\underline{G}$ du foncteur $\underline{M}$: si M est un D_k-module $A[\underline{F}]$-profini

- pour tout k-anneau fini R , le groupe $\underline{G}(M)(R)$ est le groupe $\mathrm{Hom}^{\mathrm{cont}}_{D_k}(M, \widehat{CW}_k(R))$ des applications D_k-linéaires continues de M dans $\widehat{CW}_k(R)$,
- si $\varphi : R \to S$ est un morphisme de k-anneaux finis, l'application $\underline{G}(M)(\varphi)$ est la flèche évidente.

0.6. Appelons D_k-<u>module fini</u> tout D_k-module à gauche qui est de longueur finie en tant que A-module. On a une notion de dualité dans la catégorie des D_k-modules finis (cf. n° III.5) et nous notons M' le dual d'un D_k-module fini M .

Si G est un p-groupe fini sur k , notons $\mathbb{D}(G)$ son dual de Cartier ; c'est un p-groupe fini sur k et $\underline{M}(G)$ et $\underline{M}(\mathbb{D}(G))$ sont des D_k-modules finis. L'objet du § 5 du chapitre III est de montrer que les foncteurs $G \mapsto \underline{M}(\mathbb{D}(G))$ et $G \mapsto (\underline{M}(G))'$ sont naturellement équivalents. On y utilise, de façon essentielle, le § 6 du chapitre II qui a pour objet l'étude de l'exponentielle d'Artin-Hasse, la construction d'un anneau un peu compliqué, noté $C\Lambda(k) = \mathbb{C}_k$, et l'étude des covecteurs de Witt à coefficients dans $\mathbb{C}_k$.

On déduit facilement de ce résultat le fait que le foncteur "module de Dieudonné des p-groupes finis sur k" construit dans ce mémoire est naturellement équivalent au foncteur "module de Dieudonné traditionnel" (qui nécessite la décomposition du groupe considéré en le produit d'un groupe unipotent par un groupe de type multiplicatif).

La construction de l'équivalence naturelle entre $G \mapsto \underline{M}(\mathbb{D}(G))$ et $G \mapsto (\underline{M}(G))'$ utilise un intermédiaire : la construction d'un foncteur covariant $\underline{M}'$ de la catégorie des p-groupes finis sur k dans celle des D_k-modules finis, qui est l'analogue, pour ces groupes, du module des courbes typiques de Cartier pour les groupes formels lisses et connexes sur k : en tant que groupe $\underline{M}'(G)$ est le sous-groupe de $G(\mathcal{C}_k)$ formé des α tels que $u_\ell(\alpha) = 0$, pour tout nombre premier $\ell \neq p$ (où u_ℓ est l'analogue de l'opérateur $F_\ell \circ V_\ell$ de Cartier). Si G est un groupe connexe tel que $F_G^m = 0$, on a $G(\mathcal{C}_k) = G(k[T]/T^{p^m})$ et la construction de $\underline{M}'(G)$ se simplifie considérablement.

0.7. Le § 6 du chapitre III a pour objet de donner une autre description du module de Dieudonné d'un p-groupe formel sur k lorsque celui-ci est lisse. C'est en fait le point de départ du chapitre IV et on y utilise de façon essentielle l'étude du "relèvement des covecteurs" faite au § 5 du chapitre II.

0.8. Le but du chapitre IV est la classification des p-groupes formels lisses sur A', à isomorphisme près, lorsque $e \leq p-1$ et des groupes p-divisibles sur A', à isogénie près, pour e quelconque.

Le § 1 correspond au cas $e = 1$, autrement dit $A = A'$, que nous avons préféré traiter séparément afin de ne pas mélanger les difficultés.

Soit G un p-groupe formel lisse de dimension finie sur A et soit $\mathfrak{R}$ son algèbre affine. Par extension des scalaires, G définit un p-groupe formel lisse G_k sur k dont l'algèbre affine est $\mathfrak{R}_k = \mathfrak{R} \otimes_A k = \mathfrak{R}/p\mathfrak{R}$. Soit K le corps des fractions de A et soit $\mathfrak{R}_K = \mathfrak{R} \otimes_A K$. Avec des notations évidentes, soit $P^u(\mathfrak{R})$ le sous-A-module de $\mathfrak{R}_K$ formé des α tels que $d\alpha \in \Omega_A(\mathfrak{R})$, module des A-différentielles continues de l'anneau $\mathfrak{R}$, identifié à un sous-module de $\Omega_K(\mathfrak{R}_K)$. On munit $P^u(\mathfrak{R})$ d'une topologie A-linéaire convenable et on note $P(\mathfrak{R})$ le séparé complété de $P^u(\mathfrak{R})$ pour cette topologie (si G est connexe et si $(X_1, X_2, \dots, X_d)$ est un système de coordonnées pour $\mathfrak{R}$, i.e. si $\mathfrak{R} = A[[X_1, X_2, \dots, X_d]]$, $P(\mathfrak{R})$ s'identifie au module des séries formelles en les X_j, à coefficients dans K, qui vérifient $\frac{\partial\alpha}{\partial X_j} \in \mathfrak{R}$, pour tout j). On construit au § 5 du chapitre II une application A-linéaire continue $w_{\mathfrak{R}} : \widehat{CW}_k(\mathfrak{R}_k) \to P(\mathfrak{R})/p\mathfrak{R}$ qui est, en fait, un isomorphisme.

Soit $\Delta : \mathfrak{R} \to \mathfrak{R} \hat{\otimes}_A \mathfrak{R}$ le coproduit. Cette application se prolonge en une application, encore notée Δ, de $P(\mathfrak{R})$ dans $P(\mathfrak{R} \hat{\otimes}_A \mathfrak{R})$. Soit

$$\mathcal{MH}(G) = \{\alpha \in P(R) \mid \Delta\alpha - \alpha \hat{\otimes} 1 - 1 \hat{\otimes} \alpha \in p\mathfrak{R} \hat{\otimes}_A \mathfrak{R}\} .$$

On démontre au § 6 du chapitre III que $w_{\mathfrak{R}}$ induit un isomorphisme de $\underline{M}(G_k)$ sur $MH(G) = \mathcal{MH}(G)/p\mathfrak{R}$.

Notons $\mathfrak{L}(G)$ le sous-A-module de $P(R)$ formé des α tels que $\Delta\alpha = \alpha \hat{\otimes} 1 + 1 \hat{\otimes} \alpha$. Soit $\rho(G)$ l'application A-linéaire composée

$$\mathfrak{L}(G) \xrightarrow{\text{incl.can.}} \mathcal{MH}(G) \xrightarrow{\text{proj.can.}} MH(G) \xrightarrow{\text{iso.can.}} \underline{M}(G_k) ;$$

on démontre que l'application $\tilde{\rho}(G) : \mathfrak{L}(G)/p\mathfrak{L}(G) \to \underline{M}(G_k)/\underline{F}\,\underline{M}(G_k)$, induite par passage aux quotients, est un isomorphisme.

Soit Λ_A^ℓ la catégorie dont les objets sont les triplets $(\mathfrak{L}, M, \rho)$

- où M est un D_k-module profini, tel que l'action de $\underline{F}$ sur M est injective et $M/\underline{F}M$ est un espace vectoriel sur k de dimension finie,
- où $\mathfrak{L}$ est un A-module libre de rang fini,
- où $\rho : \mathfrak{L} \to M$ est une application A-linéaire qui induit, par passage aux quotients, un isomorphisme $\tilde{\rho} : \mathfrak{L}/p\mathfrak{L} \to M/\underline{F}M$;

et dont les flèches sont évidentes.

On voit que l'on peut considérer la correspondance

$$G \mapsto \mathfrak{L}M(G) = (\mathfrak{L}(G), \underline{M}(G_k), \rho(G))$$

comme un foncteur contravariant additif $\mathfrak{L}M$ de la catégorie des p-groupes formels lisses sur A dans Λ_A^ℓ. Le but du § 1 du chapitre IV est de montrer que, si $p \neq 2$, ce foncteur est pleinement fidèle et induit une anti-équivalence entre les deux catégories. On a des résultats analogues pour $p = 2$ à condition de se restreindre soit aux groupes "unipotents" soit aux groupes connexes.

Soit G un p-groupe formel lisse et de dimension finie sur A et soit $\mathcal{S}$ un A-anneau qui est un A-module libre de rang fini. On donne aussi une description du groupe $G(\mathcal{S})$ à l'aide du triplet $(\mathcal{L},M,\rho) = \mathcal{L}M(G)$: soit $\mathcal{S}_k = \mathcal{S}\otimes_A k$, $\mathcal{S}_K = \mathcal{S}\otimes_A K$, soit $N_{\mathcal{L}}(\mathcal{S})$ le groupe des applications A-linéaires de $\mathcal{L}$ dans $\mathcal{S}$ et soit $G_M(\mathcal{S})$ le groupe des applications D_k-linéaires continues de M dans $\widehat{CW}_k(\mathcal{S}_k)$; si $p \neq 2$ ou si G est unipotent le groupe $G(\mathcal{S})$ s'identifie canoniquement, et fonctoriellement en $\mathcal{S}$, au sous-groupe de $N_{\mathcal{L}}(\mathcal{S}) \times G_M(\mathcal{S})$ formé des $(x_{\mathcal{L}},x_M)$ tels que le diagramme

$$\begin{tikzcd}
\mathcal{L} \arrow[r, "x_{\mathcal{L}}"] \arrow[dd, "\rho"'] & \mathcal{S}_K \arrow[dr, "\text{proj.}"] & \\
 & & \mathcal{S}_K/p\mathcal{S} \\
M \arrow[r, "x_M"] & \widehat{CW}_k(\mathcal{S}_k) \arrow[ur, "w_{\mathcal{S}}"'] &
\end{tikzcd}$$

(où $w_{\mathcal{S}}$ est une application A-linéaire construite au § 5 du chapitre II) est commutatif.

Dans le cas des groupes p-divisibles, l'application $\rho(G)$ est injective ; soit $L(G)$ l'image de $\mathcal{L}(G)$ par $\rho(G)$. En associant à G le couple $(L(G),\underline{M}(G_k))$, on obtient une anti-équivalence entre la catégorie des groupes p-divisibles sur A et une catégorie H_A^d dont les objets sont des couples (L,M), où M est un D_k-module et L un sous-A-module de M, avec des propriétés convenables.

0.9. Pour pouvoir obtenir, sur A', des résultats analogues à ceux que l'on a sur A, on est conduit à introduire un foncteur $M \mapsto M_{A'}$ de la catégorie des D_k-modules dans celle des A'-modules, et c'est l'objet du § 2 du chapitre IV.

Soit M un D_k-module. Pour tout entier j, soit $M^{(j)}$ le D_k-module déduit de M par l'extension des scalaires σ^j (où σ est le Frobenius absolu). Le décalage (resp. le Frobenius) induit une application D_k-linéaire $v_j : M^{(j)} \to M^{(j+1)}$ (resp. $f_j : M^{(j)} \to M^{(j-1)}$). Soit $\mathfrak{m}$ l'idéal maximal de A'. Alors $M_{A'}$ est la limite inductive d'un diagramme (assez compliqué) dont les objets sont certains des $\mathfrak{m}^i \otimes_A M^{(j)}$ et les flèches sont construites à partir des v_j et des f_j. Lorsque $e \leq p-1$, $M_{A'}$ est la limite inductive du diagramme

$$\begin{tikzcd}
 & \mathfrak{m}\otimes_A M \arrow[dl, "\psi_0"'] \arrow[dr, "\chi_0"] & \\
A'\otimes_A M & & p^{-1}\mathfrak{m}\otimes_A M^{(1)} \\
 & A'\otimes_A M^{(1)} \arrow[ul, "\varphi_0"] \arrow[ur, "\psi'_0"'] &
\end{tikzcd}$$

où $\psi_0(\lambda\otimes\underline{a}) = \lambda\otimes\underline{a}$, $\chi_0(\lambda\otimes\underline{a}) = p^{-1}\lambda\otimes v_0(\underline{a})$, $\psi'_0(\lambda\otimes\underline{a}) = \lambda\otimes\underline{a}$, $\varphi_0(\lambda\otimes\underline{a}) = \lambda\otimes f_1(\underline{a})$.

Dans le cas particulier où M est un A-module libre de type fini (i.e. où $M = \underline{M}(G_k)$, avec G_k un groupe p-divisible sur k), on a une application A'-linéaire de $M_{A'}$ sur un réseau de $M_{K'} = M\otimes_A K'$ (où $K' = \mathrm{Frac}(A')$) que l'on peut décrire très simplement. Le noyau de cette application est la partie de torsion $(M_{A'})_{tor}$ de $M_{A'}$; celle-ci est nulle si $e \leq p-1$, mais est un A'-module fini, non nul, en général, si $e \geq p$.

0.10. Dans le § 3 du chapitre IV, on utilise les constructions du § 2 pour étendre aux A'-algèbres les résultats sur les relèvements des covecteurs dans les A-algèbres obtenus au § 5 du chapitre II :

- soit G un p-groupe formel lisse et de dimension finie sur A' et soit $\mathcal{R}$ son algèbre affine. On définit, comme dans le cas $e = 1$ (n° 0.8) un A'-module topologique $P(\mathcal{R})$. On note $P'(\mathcal{R})$ l'adhérence du sous-A'-module de $P(\mathcal{R})$ engendré par les éléments de la forme $p^{-n}\alpha^{p^n}$, avec $\alpha \in \mathfrak{m}\mathcal{R}$ et $n \in \mathbb{N}$ (si $e \leq p-1$, on a $P'(\mathcal{R}) = \mathfrak{m}\mathcal{R}$). Soit $\mathcal{R}_k = \mathcal{R}\otimes_{A'} k$. On construit un isomorphisme $w_{\mathcal{R}}$ du A'-module $\widehat{CW}_{k,A'}(\mathcal{R}_k) = (\widehat{CW}_k(\mathcal{R}_k))_{A'}$ sur $P(\mathcal{R})/P'(\mathcal{R})$.

- soit $\mathcal{S}$ un A'-anneau qui est un A'-module libre de rang fini. Soit $\mathcal{S}_K = \mathcal{S}\otimes_A K = \mathcal{S}\otimes_{A'} K'$, $\mathcal{S}_k = \mathcal{S}\otimes_{A'} k = \mathcal{S}/\mathfrak{m}\mathcal{S}$. On définit, comme pour $\mathcal{R}$, un sous-A'-module $P'(\mathcal{S})$ de $\mathcal{S}_K$. On construit alors une application A'-linéaire $w_{\mathcal{S}}$ de $\widehat{CW}_{k,A'}(\mathcal{S}_k) = (\widehat{CW}_k(\mathcal{S}_k))_{A'}$ dans $\mathcal{S}_K/P'(\mathcal{S})$.

0.11. Conservons les hypothèses et les notations du n° précédent pour décrire les résultats du § 4 du chapitre IV.

Le coproduit $\Delta : \mathcal{R} \to \mathcal{R}\hat{\otimes}_A\mathcal{R}$ se prolonge en une application encore notée Δ de $P(\mathcal{R})$ dans $P(\mathcal{R}\hat{\otimes}_A\mathcal{R})$. Nous notons $\mathcal{M}\mathcal{H}_{A'}(G)$ le sous-A'-module fermé de $P(\mathfrak{R})$ formé des α tels que $\Delta\alpha - \alpha\hat{\otimes}1 - 1\hat{\otimes}\alpha \in P'(\mathfrak{R}\hat{\otimes}_A\mathfrak{R})$ et $MH_{A'}(G) = \mathcal{M}\mathcal{H}_{A'}(G)/P'(\mathfrak{R})$. On démontre que l'application $w_{\mathfrak{R}}$ induit un isomorphisme canonique de $M_{A'}(G_k) = (\underline{M}(G_k))_{A'}$ sur $MH_{A'}(G)$.

Soit $\mathcal{L}_{A'}(G) = \{\alpha \in P(\mathfrak{R}) \mid \Delta\alpha = \alpha\hat{\otimes}1 + 1\hat{\otimes}\alpha\}$ et soit $\rho_{A'}(G)$ l'application A'-linéaire composée

$$\mathcal{L}_{A'}(G) \xrightarrow{\text{incl.}} \mathcal{M}\mathcal{H}_{A'}(G) \xrightarrow{\text{proj. can.}} MH_{A'}(G) \xrightarrow{\text{iso.can.}} M_{A'}(G_k) .$$

On définit alors une catégorie $\Lambda^{\ell}_{A'}$, dont les objets sont des triplets $(\mathcal{L},M,\rho)$ où M est un D_k-module, $\mathcal{L}$ un A'-module et ρ une application A'-linéaire de $\mathcal{L}$ dans $M_{A'}$ vérifiant des propriétés convenables. La correspondance $G \to (\mathcal{L}_{A'}(G), \underline{M}(G_k), \rho_{A'}(G))$ définit un foncteur contravariant additif $\mathcal{L}M_{A'}$ de la catégorie des p-groupes formels lisses et de dimension finie sur A' dans $\Lambda^{\ell}_{A'}$.

On montre que, si $e < p-1$, le foncteur $\mathcal{L}M_{A'}$ induit une anti-équivalence entre ces deux catégories. Pour tout G et pour tout A'-anneau $\mathcal{S}$ qui est un A'-module libre de rang fini, on peut donner une description du groupe $G(\mathcal{S})$, à l'aide du triplet $\mathcal{L}M_{A'}(G)$ et de l'application $w_{\mathcal{S}}$, qui est du même genre que ce qui a été fait pour $e = 1$.

Si $e = p-1$, on a des résultats analogues, à condition de se restreindre soit aux groupes unipotents, soit aux groupes connexes.

Lorsque e est quelconque, $\mathcal{L}M_{A'}$ n'est pas pleinement fidèle (du moins si $e \geq 2p-1$) et je ne sais pas décrire l'image essentielle. Toutefois, à tout objet $(\mathcal{L},M,\rho)$ de la catégorie $\Lambda^{\ell}_{A'}$, on peut associer un foncteur en groupes $G_{(\mathcal{L},M,\rho)}$ sur la catégorie des A'-anneaux qui sont des A'-modules libres de rang fini. Si $(\mathcal{L},M,\rho) = \mathcal{L}M_{A'}(G)$, où G est un p-groupe formel lisse et de dimension finie sur A' , on peut construire deux morphismes de foncteurs en groupes $\varphi_G : G \to G_{(\mathcal{L},M,\rho)}$ et $\psi_G : G_{(\mathcal{L},M,\rho)} \to G$ vérifiant $\psi_G \circ \varphi_G = p^t.\mathrm{id}_G$ et $\varphi_G \circ \psi_G = p^t.\mathrm{id}_{G_{(\mathcal{L},M,\rho)}}$ (où t est un entier qui ne dépend que de e : c'est le plus grand entier tel que $p^t - te \leq p^n - ne$, pour tout entier $n \geq 0$).

0.12. Dans le § 5 du chapitre IV, on applique les résultats du § 4 aux groupes p-divisibles : si G est un groupe p-divisible sur A' , l'application $\rho(G)$

est injective et on note $L_{A'}(G)$ son image. En associant à G le couple $(L_{A'}(G), \underline{M}(G_k))$, on obtient un foncteur contravariant additif $LM_{A'}$ de la catégorie des groupes p-divisibles sur A' dans une catégorie, notée $H^d_{A'}$ dont les objets sont formés de couples (L,M) , avec M un D_k-module et L un sous-A'-module de $M_{A'}$, jouissant de propriétés convenables.

Si $e < p-1$, ce foncteur induit une anti-équivalence.

Si $e \geq p-1$, il n'en est plus de même. Cependant, si G est un groupe p-divisible sur A' , notons G_m le plus petit sous-schéma en groupes fermé de G tel que, pour tout A'-anneau $\mathcal{S}$ qui est un A'-module libre de rang fini, $G_m(\mathcal{S})$ soit le noyau de la flèche canonique de $G(\mathcal{S})$ dans $G(\mathcal{S}/m\mathcal{S}) = G_k(\mathcal{S}_k)$. On constate que G_m est un schéma en groupes fini et plat sur A' annulé par p^t et que le quotient G/G_m est un groupe p-divisible sur A' , isogène à G . On peut donner une description de G/G_m , considéré comme foncteur en groupes sur la catégorie des A'-anneaux qui sont des A'-modules libres de rang fini, à l'aide du couple $LM_{A'}(G)$.

Ceci implique aussi une classification à isogénie près des groupes p-divisibles sur A' : notons $H^d_{K'}$ la catégorie dont les objets sont les couples (L,M) , avec M un $(D_k \otimes_A K)$-module et L un sous-K'-espace vectoriel de $M_{K'} = M \otimes_K K'$, avec une définition évidente pour les flèches.

En associant à G le couple $LM_{K'}(G) = (L_{K'}(G), M_K(G_k))$, avec $M_K(G_k) = \underline{M}(G_k) \otimes_A K$ et $L_{K'}(G) = L_{A'}(G) \otimes_{A'} K'$, on obtient un foncteur contravariant additif pleinement fidèle $LM_{K'}$ de la catégorie "des groupes p-divisibles sur A' , à isogénie près" dans $H^d_{K'}$.

0.13. Soit G un groupe p-divisible sur A' et soit $\mathcal{S}$ un A'-anneau qui est un A'-module libre de rang fini. Les méthodes développées au chapitre IV permettent de décrire le groupe $G(\mathcal{S})$ (où, du moins, si $e \geq p-1$, le groupe $(G/G_m)(\mathcal{S})$) à l'aide du couple $(L,M) = LM_{A'}(G)$. On doit donc pouvoir décrire les modules galoisiens $T_p(G)$, module de Tate de G (ou $T_p(G/G_m)$ si $e \geq p-1$) et, pour e quelconque, $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_p(G)$. C'est ce que l'on fait au § 1 du chapitre V .

Cette description est assez compliquée : soit A_C l'anneau des entiers du complété C d'une clôture algébrique $\overline{K}'$ de K' . Soit $\mathrm{Res}(A_C) = \varprojlim_{n \in \mathbb{N}} R_n$, où $R_n = A_C/pA_C$, l'application de transition de R_{n+1} dans R_n étant la flèche $x \mapsto x^p$. On définit le groupe $BW(Res(A_C))$ des "bivecteurs de Witt à coefficients dans $Res(A_C)$" ; si $\mathcal{G} = Gal(\bar{K}'/K')$, on montre que l'on peut considérer $BW(Res(A_C))$ aussi bien comme un D_k-module à gauche que comme un $K[\mathcal{G}]$-module à gauche ; on peut en outre définir une application $K[\mathcal{G}]$-linéaire $bw_{A_C} : BW(Res(A_C)) \to C$ et on note $bw_{A_C,K'} : K' \otimes_K BW(Res(A_C)) \to C$ l'application K'-linéaire déduite de bw_{A_C} par extension des scalaires.

Soit G un groupe p-divisible sur A' et soit $(L_{K'}, M_K) = LM_{K'}(G)$. Pour tout $u \in Hom_{D_k}(M_K, BW(Res(A_C)))$, notons $u_{K'} : K' \otimes_K M_K \to K' \otimes_K BW(Res(A_C))$ l'application K'-linéaire déduite de u par extension des scalaires. Alors $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_p(G)$ s'identifie au sous-$\mathbb{Q}_p[\mathcal{G}]$-module de $Hom_{D_k}(M_K, BW(Res(A_C)))$ formé des u tels que $u_{K'}(L_{K'}) \subset \ker bw_{A_C,K'}$.

Nous étudierons ailleurs ([24]) le D_k-module $Hom_{\mathbb{Q}_p[\mathcal{G}]}(U, BW(Res(A_C)))$ lorsque U est un $\mathbb{Q}_p[\mathcal{G}]$-module admettant une décomposition de Hodge-Tate. Cela devrait nous permettre en particulier de montrer que, réciproquement, on peut reconstruire le couple $(L_{K'}, M_K)$ associé à un groupe p-divisible G sur A' à partir de la seule connaissance du $\mathbb{Q}_p[\mathcal{G}]$-module $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_p(G)$ (par exemple, M_K devrait s'identifier à $Hom_{\mathbb{Q}_p[\mathcal{G}]}(\mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_p(G), BW(Res(A_C)))$).

0.14. Dans le § 3 du chapitre V, on explique comment on peut retrouver les résultats de Cartier sur la classification des groupes formels lisses et connexes, de dimension finie sur k au moyen de courbes typiques ([7]).

Dans le § 2 , on explique comment on retrouve les résultats de Honda ([32]) sur les mêmes groupes et sur leurs relèvements sur $W(k)$.

0.15. On a compris que ce mémoire repose sur la construction des covecteurs de Witt. C'est Barsotti ([1], [2], [3]) qui en a entrepris le premier une étude systématique (pour classifier les groupes formels commutatifs, lisses et connexes, de dimension finie sur k , et, au moins lorsque k est algébriquement clos, les groupes p-divisibles sur k). Notre construction est différente de celle de Barsotti et nous semble plus commode (Barsotti défini les covecteurs à coefficients dans un anneau qui est une algèbre sur $\mathbb{F}_p$ ou sur $\mathbb{Q}$

et dont le groupe additif est muni d'une topologie $\mathbb{Z}_{(p)}$-linéaire ; la somme de deux covecteurs n'est alors pas partout définie et, pour obtenir un groupe additif, il faut se restreindre à une partie convenable de l'ensemble des covecteurs, qu'il faut préciser à chaque fois).

0.16. On a vu que beaucoup des résultats contenus dans ce mémoire se rapprochent de résultats connus et que nous expliquons (not. au chap. V) les rapports avec certains d'entre eux. L'avantage le plus net de nos méthodes nous semble être qu'à chaque fois on obtient une description du groupe formel étudié, <u>considéré comme foncteur en groupes commutatifs</u> sur une catégorie convenable, à l'aide de l'objet qui le classifie (à ma connaissance, le seul cas où ceci avait pu être fait est celui des p-groupes finis unipotents sur k , Grothendieck [30]).

Je voudrais maintenant dire quelques mots sur la construction "traditionnelle" du module de Dieudonné.

C'est Dieudonné qui, le premier, a montré que l'on pouvait classifier certains groupes formels commutatifs sur k , à l'aide de D_k-modules à gauche. Au langage près, il obtient ([16], voir surtout IV) une équivalence entre la catégorie des groupes formels commutatifs, lisses et connexes, de dimension finie sur k et celle des D_k-modules d'un type particulier. Il utilise pour cela le "groupe hyperexponentiel" dont il démontre [17] qu'il est isomorphe au groupe additif des vecteurs de Witt.

Les idées de Dieudonné ont été reprises par de nombreux auteurs (Cartier, Gabriel, Barsotti, Manin,...). Soit Fcu_k la catégorie des p-groupes finis connexes uipotents sur k ; Gabriel [27] a utilisé ses propres travaux sur les catégories pro-artiniennes [26] pour construire une anti-équivalence entre cette catégorie et celle des D_k-modules finis, sur lesquels l'action de $\underline{F}$ et celle de $\underline{V}$ sont nilpotentes : la catégorie Fcu_k a un seul objet simple, le groupe α_p (d'algèbre affine $k[X]/X^p$, avec $\Delta X = X \otimes 1 + 1 \otimes X$, $\epsilon X = 0$) ; on construit son enveloppe injective dans la catégorie $\underrightarrow{\lim}\, Fcu_k$ (qui se trouve être le groupe formel que nous notons $\widehat{CW}_k^{u,c}$ au § 4 du chapitre II) et on montre que l'anneau des endomorphismes de $\widehat{CW}_k^{u,c}$ est, à peu de chose près, l'anneau D_k .

Il est alors facile d'en déduire une classification complète des p-groupes finis sur k : un peu de cohomologie galoisienne permet de se débarrasser des groupes étales, et les groupes de type multiplicatif se ramènent aux groupes étales par la dualité de Cartier (voir, entre autres, [37], chap. I, [15], chap. III, [14], chap. V). Cette classification se trouve être naturellement équivalente à la nôtre (cf. cor. 3 à la prop. 5.3 du chap. III) et s'étend, bien sûr, par passage à la limite, aux groupes formels qui sont limite inductive de p-groupes finis. Outre le fait d'être un peu plus générale, notre classification présente l'avantage de ne pas recourir à la dualité de Cartier pour la partie de type multiplicatif. C'est très commode, aussi bien pour décrire le groupe des points d'un groupe formel à l'aide de son module de Dieudonné que pour l'étude des relèvements en caractéristique 0 .

Signalons en passant, bien que ce type de problèmes ne soit pas du tout étudié dans ce mémoire que divers auteurs ont tenté, à juste titre, de rendre cette classification plus précise en étudiant les D_k-modules eux-mêmes (cf. Dieudonné ([16], VII) pour les groupes formels lisses et connexes, de dim. finie, à isogénie près, Manin [37] pour les mêmes groupes, à isomorphisme près lorsque k est algébriquement clos, Kraft [33], pour les groupes finis tués par p).

0.17. C'est Grothendieck qui, le premier, a pensé que l'on devait pouvoir classifier les groupes p-divisibles sur A' (à isomorphisme près si $e < p-1$, à isogénie près pour e quelconque) au moyen d'un couple formé du module de Dieudonné M de la fibre spéciale et d'un sous-module d'une extension des scalaires convenable de M . Les premiers résultats ont été annoncés par Cartier ([8], via l'étude des courbes typiques) et Grothendieck ([29], [30], via la construction des cristaux de Dieudonné). Les travaux de Grothendieck ont été repris systématiquement par Messing ([39]) qui obtient une classification complète pour $e < p-1$ ([39], chap. V, th. 1.6), puis par Mazur et Messing ([38]) avec une étude détaillée des extensions universelles des groupes p-divisibles et des schémas abéliens. Le lecteur regrettera, à juste titre, que ne soit pas explicité ici comment ces résultats se relient aux nôtres. Cela nous aurait emmené trop loin.

Nous indiquons toutefois brièvement et sans démonstration (chap. V,

n° 3.7, rem. 2) comment on peut construire l'extension universelle d'un groupe p-divisible G sur k (resp. sur A), connaissant son module de Dieudonné (resp. le module de Dieudonné de la fibre spéciale), à l'aide du groupe des covecteurs de Witt. Nous espérons pouvoir généraliser cette construction.

0.18. A l'origine de ce travail, il y a une question que m'avait posée Serre : déterminer l'image de Galois dans la représentation p-adique définie par une courbe elliptique sur K = Frac(A) , avec bonne réduction supersingulière. J'avais fait les calculs "à la main" en me servant des travaux de Hazewinkel [31]. Le contraste entre la simplicité du résultat [19] et la complexité des calculs donnait envie de comprendre ce qui était caché derrière. Dans un premier temps, cela m'a conduit à interpréter les résultats de Honda [32] en termes de modules de Dieudonné "à la Gabriel". D'où ce mémoire qui contient finalement un peu plus que cela.

Dans un deuxième temps, cela m'a conduit à donner une classification des schémas en groupes finis et plats sur A , du même type que celle qui est donnée ici pour les groupes p-divisibles. Les résultats ont été annoncés dans [22] et seront démontrés dans [23] . [23] contiendra aussi les résultats sur les courbes elliptiques et une classification, au moins partielle, des schémas en groupes finis et plats sur A' lorsque $e \leq p-1$.