

COMPOSITIO MATHEMATICA

GUY LAFFAILLE

Groupes p -divisibles et corps gauches

Compositio Mathematica, tome 56, n° 2 (1985), p. 221-232

<http://www.numdam.org/item?id=CM_1985__56_2_221_0>

© Foundation Compositio Mathematica, 1985, tous droits réservés.

L'accès aux archives de la revue « Compositio Mathematica » (<http://http://www.compositio.nl/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

GROUPES p -DIVISIBLES ET CORPS GAUCHES

Guy Laffaille

1. Introduction

1.1. Soit E une extension finie de Q_p . Soit $q = p^r$ le cardinal du corps résiduel \tilde{O} de E . Soit K un corps local contenant E , à corps résiduel parfait k et tel que E contienne une uniformisante de K . Soit \bar{K} une clôture algébrique de K et soit $G = \text{Gal}(\bar{K}/K)$.

Le but de ce travail est de généraliser la construction des groupes formels de Lubin-Tate. Un groupe de Lubin-Tate est un groupe formel de dimension 1 défini sur l'anneau des entiers A de K et tel que le module galoisien obtenu à partir du module de Tate par extension des scalaires à Q_p soit un espace vectoriel de dimension 1 sur E .

Soit D un corps gauche de centre E' , isomorphe à E , de dimension n^2 sur E' et d'invariant t/n .

1.2. Le résultat principal est le suivant:

THÉORÈME: *Il existe des groupes formels de dimension n tels que le module galoisien associé soit un espace vectoriel à droite de dimension 1 sur D . L'enveloppe algébrique de l'image de G dans le groupe des Q_p -automorphismes du module galoisien de ces groupes formels est isomorphe au groupe multiplicatif D^* de D .*

Avant d'énoncer le résultat de façon plus précise, nous avons besoin de quelques notations.

Soit E_0 (resp. K_0) le corps des fractions de l'anneau des vecteurs de Witt à coefficients dans \tilde{O} (resp. k).

Comme E contient une uniformisante de K , on a un isomorphisme canonique de $E \otimes_{E_0} K_0$ sur K . Soient σ le Frobenius absolu agissant sur k et K_0 et τ l'automorphisme de K défini par:

$$\tau(x \otimes a) = x \otimes \sigma^r(a) \quad \text{pour } x \in E \text{ et } a \in K_0.$$

Soit s un entier tel que $st \equiv -1$ modulo n . Si m est un entier, on note \bar{m} l'entier tel que $0 \leq \bar{m} < n$ et $m \equiv \bar{m}$ modulo n .

On note \underline{X} le n -uplet (X_1, \dots, X_n) et $\underline{X}^{q'} = (X_1^{q'}, \dots, X_n^{q'})$.

Enfin on note Ω la matrice carrée d'ordre n de $M_n(E)$ telle que

$$\Omega = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ 0 & 0 & 0 & \dots & 1 \\ \pi & 0 & 0 & \dots & 0 \end{bmatrix}$$

1.3. THÉORÈME: Soit $l(\underline{X})$ un n -uplet de séries formelles en les n variables X_1, \dots, X_n à coefficients dans K . Soient a_1, \dots, a_n des éléments de A tels que a_n soit une unité. Si $l(\underline{X}) \equiv \underline{X}$ modulo degré 2 et si les conditions suivantes sont réalisées:

(i) $l(\underline{X}) + \sum_{i=1}^{n-1} a_i \Omega^{i-n} l^{\tau^{-i}}(\underline{X}^{q^{-i}}) + (a_n/\pi) l^{\tau^n}(\underline{X}^{q^n}) \in (A[[\underline{X}]])^n$;

(ii) le PGCD des entiers i tels que $a_i \neq 0$ est premier à n ;

alors $l(\underline{X})$ est le logarithme d'un groupe p -divisible connexe Γ défini sur A de dimension n et de hauteur $[D:Q_p]$. Soit V le module galoisien associé à Γ , alors $\text{End}_G(V)$ est isomorphe à D^0 , le corps opposé à D .

Si k est algébriquement clos, tout groupe p -divisible défini sur A tel que $\text{End}_G(V)$ soit isomorphe à D^0 , de dimension n et de hauteur $[D:Q_p]$ est isogène à un groupe p -divisible dont le logarithme vérifie une congruence de la forme (i) avec des a_i qui vérifient (ii). Le choix d'une base du D -espace vectoriel à droite V définit un isomorphisme de l'enveloppe algébrique de Galois sur D^* .

1.4. REMARQUE: Quel que soit le n -uplet $g(\underline{X}) \in (A[[\underline{X}]])^n$, il existe un et un seul n -uplet $l(\underline{X})$ de séries formelles à coefficients dans K tel que $l(\underline{X}) + \sum_{i=1}^{n-1} a_i \Omega^{i-n} l^{\tau^{-i}}(\underline{X}^{q^{-i}}) + (a_n/\pi) l^{\tau^n}(\underline{X}^{q^n}) = g(\underline{X})$ et $l(\underline{X}) \equiv \underline{X}$ modulo degré 2 (cf. [H1] p. 9 et p. 59).

1.5. Au $n^{\circ}2$, on construit le corps D pour pouvoir faire des calculs explicites dans la suite.

Au $n^{\circ}3$, on utilise les résultats de [F-L] pour construire des représentations p -adiques cristallines, au sens de [F3], de G telles que le $Q_p[G]$ -module correspondant soit un D -espace vectoriel à droite de dimension 1 et soit de Hodge-Tate de poids 0 et 1, la multiplicité de 1 étant égale à n . D'après une conjecture de Fontaine [F2], cette représentation doit provenir d'un groupe p -divisible; les résultats de [F1] permettent de déterminer l' "équation fonctionnelle" que doit vérifier le logarithme du groupe p -divisible. Il ne reste plus à vérifier qu'il existe un tel groupe p -divisible ce que permet de faire le résultat de Hazewinkel [H1,H2].

Au $n^{\circ}4$, on montre que les modules de Dieudonné de ces groupes p -divisibles ont pour anneau d'endomorphismes le corps D et on classeifie à isogénies près les groupes p -divisibles obtenus.

Au $n^{\circ}5$, on montre que l'enveloppe algébrique de Galois est bien isomorphe à D^* et on montre les théorèmes.

Dans le cas où D est commutatif, on retrouve évidemment certains des résultats de Lubin et Tate. Comme dans [L-T], les résultats obtenus sont indépendants du choix de π et du choix des séries à coefficients entiers dans le (i) du théorème. On ne retrouve pas les autres résultats d'unicité: il y a beaucoup de classes d'isogénies et deux groupes isogènes ne sont pas forcément isomorphes.

2. Construction des corps gauches de centre E

2.1. Soit ω la matrice carrée d'ordre n égale à la transposée de Ω . On a $\omega^n = \pi \text{id}$ où id est la matrice unité d'ordre n .

Soit L l'extension non ramifiée de E de degré n contenue dans \bar{K} .

Si $\lambda \in L$, on note $D(\lambda)$ la matrice diagonale de $M_n(L)$ telle que

$$D(\lambda)_{ii} = \tau^{s(i-1)}(\lambda).$$

2.2. PROPOSITION: Soit D le sous-anneau de $M_n(L)$ engendré par ω et les $D(\lambda)$ avec $\lambda \in L$. Alors D est un corps gauche de centre E et d'invariant t/n .

Démonstration. (Sans doute bien connue) On a :

$$\begin{aligned} & \omega D(\tau^s(\lambda)) \\ &= \begin{pmatrix} 0 & 0 & \dots & 0 & 0 & \pi \\ 1 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & \dots & 1 & 0 & 0 \\ 0 & 0 & \dots & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} \tau^s(\lambda) & & & & & \\ & \tau^{2s}(\lambda) & & & & 0 \\ & 0 & \ddots & & & \\ & & & \ddots & & \\ & & & & \tau^{(n-1)s}(\lambda) & \\ & & & & & \lambda \end{pmatrix} \\ &= \begin{pmatrix} \lambda & & & & & \\ & \tau^s(\lambda) & & & & \\ & & \ddots & & & \\ & & & \tau^{(n-1)s}(\lambda) & & \\ 0 & & & & & \end{pmatrix} \begin{pmatrix} 0 & 0 & \dots & 0 & 0 & \pi \\ 1 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & \dots & 1 & 0 & 0 \\ 0 & 0 & \dots & 0 & 1 & 0 \end{pmatrix} \\ &= D(\lambda) \omega. \end{aligned}$$

L'anneau D est donc l'ensemble des combinaisons linéaires $\sum_{i=0}^{n-1} D(\lambda_i) \omega^i$. C'est donc un L -espace vectoriel de dimension n . Tout élément non nul s'écrit $(\sum_{i=0}^{n-1} D(\lambda_i) \omega^i) \omega^m$ avec les λ_i entiers dans L et λ_0 une unité, $m \in \mathbb{Z}$. Modulo π , la matrice $\sum_{i=0}^{n-1} D(\lambda_i) \omega^i$ est triangulaire inférieure avec les $\tau^{s(i-1)}(\lambda_0)$ sur la diagonale, donc elle est inversible. Donc tout

élément non nul de D est inversible dans $M_n(L)$ et il est clair que son inverse est dans D .

On a :

$$D(\tau^s(\lambda)) = \omega^{-1}D(\lambda)\omega,$$

d'où :

$$D(\tau^{sm}(\lambda)) = \omega^{-m}D(\lambda)\omega^m,$$

pour tout entier m . L'invariant de D est alors l'image dans Q/Z de t/n (cf. Cassels-Frölich p. 138). La proposition est donc démontrée.

On obtient ainsi tous les invariants possibles, donc ce procédé permet de construire tous les corps gauches de centre E et de dimension finie sur E .

3. L'équation fonctionnelle

3.1. Soient Γ un groupe p -divisible défini sur A et V le module galoisien obtenu à partir du module de Tate de Γ par extension des scalaires à Q_p . Le but de ce paragraphe est de montrer que si Γ est de dimension n et si l'anneau des endomorphismes de V est isomorphe à D^0 le corps gauche opposé à D alors le logarithme de Γ vérifie une équation fonctionnelle de la forme (i) du théorème 1.3. On va d'abord utiliser les modules de Dieudonné filtrés et on traduira ensuite les résultats en termes de logarithmes.

Soit C le complété de \bar{K} . Soit $V_C\{i\} = \{x \in C \otimes_{Q_p} V \mid g(x) = \chi'(g)x \text{ pour tout } g \in G\}$ où χ est le caractère cyclotomique de G donnant l'action de G sur les racines de l'unité d'ordre une puissance de p . Le module V est de Hodge-Tate de poids 0 et 1, donc si $V_C(i) = C \otimes_K V_C\{i\}$, on a $V_C = C \otimes_{Q_p} V = V_C(0) \oplus V_C(1)$.

3.2. Le groupe de Galois agit semi-linéairement sur V_C , donc $K \otimes_{Q_p} D^0$ agit naturellement sur les $V_C\{i\}$. Donc $C \otimes_K K \otimes_{Q_p} D^0 = C \otimes_{Q_p} D^0$ agit sur $V_C(1)$. Puisque C neutralise D , l'anneau $C \otimes_{Q_p} D^0$ est un produit d'anneaux de matrices $M_n(C)$. Donc $V_C(1)$ est un idéal de cet anneau; sa dimension sur C est égale à celle de Γ donc à n . Donc $V_C(1)$ est un $C \otimes_{Q_p} D^0$ -module simple. Pour tout Q_p -plongement γ de E' dans C , soit V_γ le C -espace vectoriel déduit du E' -espace vectoriel V par le changement de corps de base γ ; on a $V_C = \oplus V_\gamma$. Comme $V_C(1)$ est simple, $V_C(1)$ est contenu dans un V_γ . Ce γ définit un isomorphisme de E' sur E et nous l'utilisons pour identifier E' et E . On peut donc supposer que $V_C(1)$ est contenu dans la composante associée à l'identité.

3.3. Rappelons que V est une représentation cristalline au sens de [F3]. On peut donc lui associer un module de Dieudonné filtré M qui est un K_0 -espace vectoriel de dimension $[D:Q_p]$, muni d'un automorphisme

σ -semilinéaire F , obtenu par extension des scalaires à partir du module de Dieudonné usuel de la fibre spéciale de Γ . La filtration de $M_K = K \otimes_{K_0} M$ vérifie $M_K^0 = M_K$, $M_K^2 = 0$ et M_K^1 est un K -espace vectoriel de dimension n .

D'après le $n^\circ 3.2$, le module galoisien V vérifie les conditions du $n^\circ 8.13$ de [F-L]. Par suite on peut lui associer un autre module de Dieudonné filtré Δ qui est un objet de la catégorie $MF_{K/E}$ de [F-L]. Comme E est plongé dans le centre de l'anneau des endomorphismes de V , on peut aussi calculer les endomorphismes dans la catégorie $MF_{K/E}$. Donc Δ est un K -espace vectoriel de dimension n^2 muni d'un automorphisme τ -semi-linéaire ϕ ; la filtration de Δ vérifie $\Delta^0 = \Delta$, $\Delta^2 = 0$ et Δ^1 est un K -espace vectoriel de dimension n . On retrouve M en considérant $Q_p[F] \otimes_{Q_p} \Delta$ avec $F^r = \phi$ (cf. [F-L] $n^\circ 8.6$ à 8.9).

3.4. Comme au $n^\circ 2$, on identifie D au sous-anneau de $M_n(L)$ engendré par ω et les $D(\lambda)$ avec $\lambda \in L$.

Soit K' le complété de l'extension non ramifiée maximale de K contenue dans \bar{K} et soit A' l'anneau des entiers de K' . On prolonge τ à K' de manière évidente.

Soit Δ' le module de Dieudonné filtré obtenu à partir de Δ par extension des scalaires de K à K' . On a $\Delta^1 = K' \otimes_K \Delta^1$. Le corps gauche D opère sur Δ' ; si $h \in D$ et $x \in \Delta'$, on note $h * x$ le résultat de l'action de h sur x .

PROPOSITION: Avec les notations qui précèdent, il existe $x \in \Delta^1$ tel que:

- Δ^1 a pour base les $\omega^i * x$ pour $0 \leq i < n$;
- Δ' a pour base les $\phi^j(\omega^i * x)$ pour $0 \leq i, j < n$;
- il existe des $a_i \in A'$, avec $1 \leq i \leq n$, tels que a_n soit une unité et que $\phi^n(x) = \sum_{i=1}^n a_i \phi^{-is}(\omega^i * x)$.

DÉMONSTRATION: Soit ϵ un générateur de L/E ; comme L est un corps, on a une action semi-simple et même diagonalisable de $D(\epsilon)$ sur Δ^1 , puisque les valeurs propres de $D(\epsilon)$ appartiennent à K' , ces valeurs propres étant des conjugués de ϵ pour l'action du groupe de Galois de L/K .

Soit y un vecteur propre de $D(\epsilon)$ pour la valeur propre $\tau^i(\epsilon)$. On a alors $D(\lambda) * y = \tau^i(\lambda)y$ pour tout $\lambda \in L$.

On a

$$\omega D(\tau^s(\epsilon)) = D(\epsilon) \omega.$$

D'où:

$$\begin{aligned} D(\epsilon) * (\omega * y) &= (D(\epsilon) \omega) * y = (\omega D(\tau^s(\epsilon))) * y \\ &= \omega * (D(\tau^s(\epsilon)) * y) = \omega * (\tau^{i+s}(\epsilon) y) \\ &= \tau^{i-s}(\epsilon) (\omega * y). \end{aligned}$$

Donc $\omega * y$ est vecteur propre de $D(\epsilon)$ pour la valeur propre $\tau^{i+s}(\epsilon)$. Comme s est premier à n , on en déduit que les $\omega^i * y$, pour $0 \leq i \leq n-1$, sont propres pour $D(\epsilon)$ avec des valeurs propres distinctes, ces vecteurs sont donc indépendants. En particulier, ϵ est valeur propre de $D(\epsilon)$. Comme Δ^1 est stable pour l'action de D , il existe $x \in \Delta^1$ vecteur propre de $D(\epsilon)$ pour la valeur propre ϵ ; les $\omega^i * x$, pour $0 \leq i \leq n-1$, forment une base de Δ^1 .

Comme ω permute les espaces propres de $D(\epsilon)$, ils ont tous la même dimension qui est donc égale à n .

Comme ϕ commute à l'action de D , on a :

$$\begin{aligned} D(\epsilon) * (\phi^j(\omega^i * x)) &= \phi^j((D(\epsilon)\omega^i) * x) \\ &= \phi^j(\tau^{is}(\epsilon)(\omega^i * x)) = \tau^{is+j}(\epsilon)\phi^j(\omega^i * x). \end{aligned}$$

Donc $\phi^j(\omega^i * x)$ est propre pour $D(\epsilon)$ pour la valeur propre $\tau^{is+j}(\epsilon)$. Les $\phi^j(\omega^i * x)$, pour $0 \leq i, j$, engendrent un module filtré Δ'' tel que $\Delta''^1 = \Delta^1$. Le quotient Δ'/Δ'' a donc une filtration nulle; comme Δ' est faiblement admissible, [F-L] $n^\circ 7.4$, Δ'/Δ'' n'admet que la pente 0. Comme Γ est connexe, Δ' n'a que des pentes > 0 , donc $\Delta' = \Delta''$. Les vecteurs $\phi^{-is}(\omega^i * x)$ pour $1 \leq i \leq n$ avec $\phi^n(x)$ forment un système de $n+1$ vecteurs propres de $D(\epsilon)$ pour la valeur propre ϵ , ils sont donc liés. Le coefficient de $\phi^n(x)$ est non nul, sinon l'espace propre de $D(\epsilon)$ pour la valeur propre ϵ est de dimension $< n$.

Il existe donc des $a_i \in K'$ tels que :

$$\phi^n(x) = \sum_{i=1}^n a_i \phi^{-is}(\omega^i * x).$$

Cette relation en donne d'autres en appliquant $\omega, \omega^2, \dots, \omega^{n-1}$.

Pour achever la démonstration de la proposition, il suffit de démontrer le lemme suivant.

3.5. LEMME: *Les a_i sont entiers et a_n est une unité.*

DÉMONSTRATION: Comme Δ' est faiblement admissible, si M est un réseau Δ' , [L]1.2, stable par ϕ , la longueur de $M/\phi M$ est égale à la dimension de Δ^1 . Autrement dit la valuation du déterminant de ϕ calculé sur n'importe quelle base de Δ' est égale à $n.v(\pi)$. En prenant pour base les $\phi^j(\omega^i * x)$, on voit que la valuation du déterminant de ϕ est égale à $n(v(a_n) + v(\pi))$. Donc a_n est une unité.

Puisque Δ' provient d'un groupe p -divisible, ses pentes sont comprises entre 0 et 1. La relation $\phi^n(x) = \sum_{i=1}^n a_i \phi^{-is}(\omega^i * x)$ permet de calculer les pentes de Δ' .

On prend pour base de Δ' sur K' les $\phi^j(\omega' * x)$ avec $0 \leq j \leq n - 1$, en munissant les couples (i, j) de l'ordre lexicographique. Sur cette base, la matrice de ϕ qui est d'ordre n^2 se décompose en blocs d'ordre n . Les $n - 1$ premières colonnes de blocs comportent $n - 1$ blocs nuls, l'autre étant un bloc identité. La dernière colonne de blocs est formée de matrices de la forme $a_i \omega'$.

Pour trouver les pentes de Δ' , il faut trouver les vecteurs propres des puissances de ϕ . Si on calcule ces puissances par blocs, on voit que tout se passe comme si on travaillait avec une matrice d'ordre n à coefficients dans le corps commutatif $K'' = K'(\omega)$ avec $\omega^n = \pi$. On est donc ramené à un corps de base commutatif K'' et à un espace de dimension n engendré par x comme K'' $[\phi]$ -module. On peut alors appliquer la technique de Manin, [M] p. 29: la plus petite pente de Δ' est l'opposé de la plus grande pente du polygone de Newton du polynôme à coefficients dans K'' :

$$X^n - \sum_{i=1}^n a_i \omega' X^{-is},$$

en prenant $v(\pi) = 1$.

Les pentes de Δ' sont donc positives si et seulement si les a_i sont entiers. Le lemme est donc démontré.

3.6. PROPOSITION: *Soit $l(\underline{X})$ un n -uplet de séries formelles en les n variables X_1, \dots, X_n . Supposons qu'il existe des éléments $b_1, \dots, b_n \in A$ tels que b_n soit une unité et que:*

$$l(\underline{X}) + \sum_{i=1}^{n-1} b_i \Omega^{i-n} l^{\tau^{-is}}(\underline{X}^{q^{-is}}) + (b_n/\pi) l^{\tau^n}(\underline{X}^{q^n}) \in (A[[\underline{X}]])^n.$$

Si $l(\underline{X}) \equiv \underline{X}$ modulo degré 2, alors $l(\underline{X})$ est le logarithme d'un groupe formel Γ défini sur A . Le module de Dieudonné filtré de Γ vérifie les hypothèses de la proposition 3.4.

DÉMONSTRATION: On utilise les résultats de Hazewinkel [H1] p. 59, [H2] p. 74. Le n -uplet $l(\underline{X})$ vérifie les hypothèses du lemme de l'équation fonctionnelle. On en déduit que $l^{-1}(l(\underline{X}) + l(\underline{Y}))$ est à coefficients dans A , donc c'est une loi de groupe formel.

A partir du logarithme, on sait construire le module de Dieudonné filtré (cf Fontaine Groupes p -divisibles p. 202).

Soit x_i l'image de la $(i + 1)$ -ième ligne de $l(\underline{X})$ dans Δ . Alors Δ^1 a pour base les x_i pour $0 \leq i \leq n - 1$ et Δ est engendré par les $\phi^j(x_i)$.

L'équation fonctionnelle que vérifie $l(\underline{X})$ entraîne que l'on a la relation suivante:

$$x_0 + \sum_{i=1}^{n-1} (b_i/\pi) \phi^{-is}(x_i) + (b_n/\pi) \phi^n(x_0) = 0.$$

Il suffit de poser $a_n = -\pi/b_n$ et $a_i = -b_i/b_n$ pour retrouver les conditions de la proposition 3.4.

L'équation fonctionnelle donne pour les autres lignes d'autres relations. Il est clair que ces relations s'obtiennent en remplaçant x_i par x_{i+1} , pour $0 \leq i \leq n-2$, et x_{n-1} par πx_0 . Il y a donc un endomorphisme u de Δ qui vérifie $u^n = \pi \text{id}$. On fait alors agir $\omega \in D$ par l'intermédiaire de u et on vérifie immédiatement que D se plonge dans $\text{End } \Delta$.

4. Les endomorphismes et la classification à isogénies près

4.1. Dans ce paragraphe, on suppose que k est algébriquement clos.

PROPOSITION: *Soit Δ un module filtré sur K qui vérifie les conditions a), b), c) de la proposition 3.4. Alors l'anneau des endomorphismes de Δ est isomorphe au corps gauche D si et seulement si le PGCD des i tels que $a_i \neq 0$ est premier à n .*

DÉMONSTRATION. Soit $u \in \text{End } \Delta$. Comme u conserve la filtration, on a:

$$u(\omega^m * x) = \sum_j b_{j,m} \omega^j * x \text{ avec } b_{j,m} \in K'.$$

Alors:

$$\begin{aligned} u(\phi^n(\omega^m * x)) &= \sum_i a_i \sum_l \tau^{-is}(b_{l,i+m}) \phi^{-is}(\omega^l * x) \\ &= \sum_j \tau^n(b_{j,m}) \phi^n(\omega^j * x) \\ &= \sum_j \tau^n(b_{j,m}) \sum_i a_i \phi^{-is}(\omega^{i+j} * x). \end{aligned}$$

Donc u est un endomorphisme si et seulement si, pour tous i, j, m , on a:

$$\tau^n(b_{j,m}) a_i \omega^{i+j-i+j} = \tau^{-is}(b_{i+j,i+m}) a_i.$$

Pour $i = 0$, on a $\tau^n(b_{j,m}) = b_{j,m}$. Donc les $b_{j,m}$ sont dans L .

Ces égalités permettent de calculer $b_{\overline{i+j, i+m}}$ en fonction de $b_{j,m}$ si $a_i \neq 0$. Fixons j et m . On peut donc calculer tous les éléments de la forme $b_{\overline{i+j, i+m}}$ en fonction de $b_{j,m}$ si et seulement si le PGCD des i tels que $a_i \neq 0$ est premier à n .

Si c'est le cas, la dimension de $\text{End}(\Delta)$ sur L est égale à n ; comme D est contenu dans $\text{End}(\Delta)$ par construction, on a bien $\text{End}(\Delta) = D$. Si ce n'est pas le cas, la dimension de $\text{End}(\Delta)$ sur L est $> n$ et on vérifie facilement que c'est un anneau de matrices à coefficients dans un corps gauche contenu dans D .

4.2. PROPOSITION: *Soient Γ_1 et Γ_2 deux groupes p-divisibles de dimension n , de hauteur $[D:Q_p]$, définis sur A , tels que l'anneau des endomorphismes de leur modules galoisiens soit isomorphe à D^0 . Soit Δ_1 (resp. Δ_2) le module de Dieudonné filtré de Γ_1 (resp. Γ_2). Soit x_1 (resp. x_2) un élément de Δ_1^1 (resp. Δ_2^1) non nul tel que*

$$\phi^n(x_1) = \sum a_{i,1} \phi^{-is}(\omega^i * x_1)$$

(resp. $\phi^n(x_2) = \sum a_{i,2} \phi^{-is}(\omega^i * x_2)$).

Alors Γ_1 et Γ_2 sont isogènes si et seulement si il existe $\delta \in K$ tel que pour tout i : $a_{i,2} \tau^n(\delta) = a_{i,1} \tau^{-is}(\delta)$.

DÉMONSTRATION: On sait que Γ_1 et Γ_2 sont isogènes si et seulement si leurs modules de Dieudonné filtrés sont isomorphes, [F1] prop. 5.2. Supposons que Δ_1 et Δ_2 sont isomorphes. Un isomorphisme de Δ_1 sur Δ_2 est une application linéaire u qui envoie Δ_1^1 sur Δ_2^1 ; on a donc $u(\omega^i * x_1) = \sum_j b_{i,j} \omega^j * x_2$; u doit aussi commuter à ϕ . Le calcul fait à la proposition précédente montre que l'on a les relations:

$$\tau^n(b_{j,m}) a_{i,2} \omega^{i+j-\overline{i+j}} = \tau^{-is}(b_{\overline{i+j, i+m}}) a_{i,1}.$$

Il y a n^3 égalités. En fait on a n fois le même système dont les inconnues sont les $b_{j,m}$ avec $\overline{j-m}$ fixé. On a donc n^2 équations à n inconnues et $2n$ paramètres (les $a_{i,1}$ et les $a_{i,2}$). Comme le PGCD des i tels que $a_{i,1} \neq 0$ est premier à n on peut calculer les $b_{\overline{i+j, i+m}}$ en fonction de $b_{j,m}$; les solutions forment donc un espace vectoriel de dimension 1 ou 0 sur L . Soit $(b_{\overline{i+j, i+m}})_{1 \leq i \leq n}$ une solution, les autres sont alors de la forme $(\tau^{-is}(\lambda) b_{\overline{i+j, i+m}})_{1 \leq i \leq n}$ avec $\lambda \in L$. D'après le théorème de Dedekind, on voit que l'on peut supposer que $\sum_i b_{\overline{i+j, i+m}}$ est non nul. Posons $\delta = \sum_i b_{\overline{i+j, i+m}}$; en faisant la somme des n équations comportant $a_{i,1}$ on obtient $a_{i,2} \tau^n(\delta) = a_{i,1} \tau^{-is}(\delta)$. Réciproquement si ces conditions sont vérifiées, il suffit d'envoyer x_1 sur δx_2 pour obtenir un isomorphisme entre Δ_1 et Δ_2 .

5. L'enveloppe algébrique de Galois

5.1. PROPOSITION: *Soit Γ un groupe p -divisible défini sur A de dimension n et de hauteur $[D:Q_p]$. Soit Δ le module de Dieudonné filtré de Γ . Supposons que $\text{End } \Delta = D$. Alors la puissance extérieure d'ordre n^2 de Δ dans $\underline{M}_{K/E}$ est isomorphe à la puissance tensorielle d'ordre n du module de Dieudonné du groupe de Lubin-Tate associé à E .*

DÉMONSTRATION: La dimension du K -espace vectoriel $\Lambda^{n^2}\Delta$ est égale à 1. La filtration vérifie $(\Lambda^{n^2}\Delta)^n = \Lambda^{n^2}\Delta$ et $(\Lambda^{n^2}\Delta)^{n+1} = 0$; ce module filtré est admissible [F2] p. 37, donc si M est un réseau stable par la longueur de $M/\phi M$ est égale à n ; donc après extension des scalaires à K' , il existe une base telle que $\phi(x) = \pi^n x$.

Le module galoisien du Lubin-Tate associé à E et π est bien connu [S] 2.1; son module de Dieudonné filtré N est donc de dimension 1 sur K , la filtration vérifie $N^1 = N$ et $N^2 = 0$ et l'admissibilité entraîne l'existence d'une base y telle que $\phi(y) = \pi y$. Il est alors clair que la puissance tensorielle d'ordre n de N est isomorphe à la puissance extérieure n^2 -ième de Δ .

5.2. COROLLAIRE: *L'enveloppe algébrique de l'image de Galois a un quotient isomorphe à E^* .*

DÉMONSTRATION: L'énoncé est vrai pour le Lubin-Tate associé à E et π ; donc il est vrai pour ses puissances tensorielles et donc pour $\Lambda_E^{n^2}V$ d'après la proposition précédente.

5.3. PROPOSITION: *Avec les hypothèses précédentes, l'enveloppe algébrique de Galois est isomorphe à D^* .*

DÉMONSTRATION: Le module de Tate de Γ admet D^0 , le corps opposé à D , comme anneau d'endomorphismes. Donc l'image de G est contenue dans le commutant de D^0 , donc dans D^* . Soit H l'enveloppe algébrique de G , comme G est contenu dans D^* , on a $H \subset D^*$. Donc tous les éléments de H sont semi-simples, donc H ne contient pas d'éléments unipotents, donc H est réductif.

On a donc une représentation irréductible du groupe réductif H de dimension n^2 .

D'après Tits, [T] théo 7.2, cette représentation provient d'un poids dominant λ et l'image de λ dans le groupe de Brauer est d'ordre n .

D'après Serre, [S] Prop. 7 ou 1, les composantes irréductibles de H sont de type A, B, C ou D.

Soient $(R_i)_{i \in I}$ les composantes irréductibles du système de racines R de H . Reprenons les notations de Serre, [S] p. 183. Ici le centre E_1 est égal à E donc $r = 1$ et $m = n$. On a donc $n = \pi d(\omega_i)$. Les ω_i , non nuls sont minuscules.

Calculons $d(\omega_i)$ dans les 4 cas a priori possibles, (cf. [5] p. 186).

Pour A_l , on a $d(\omega_i) = \binom{l+1}{i}$ avec $l \geq 1$.

Pour B_l , on a $d(\omega_i) = 2^l$ avec $l \geq 2$, donc $d(\omega_i) \geq 4$.

Pour C_l , on a $d(\omega_i) = 2l$ avec $l \geq 2$, donc $d(\omega_i) \geq 4$.

Pour D_l , on a $d(\omega_i) = 2^{l-1}$ avec $l \geq 4$, donc $d(\omega_i) \geq 8$.

On a aussi $\text{ordre}(\omega) = \text{PPCM}(\text{ordre}(\omega_i)) \leq \Pi \text{ordre}(\omega_i)$. D'où $n \leq \Pi \text{ordre}(\omega_i)$.

Or [B] p. 250 pour A_l , on a $\text{ordre}(\omega_i) \leq l+1 \leq d(\omega_i)$; pour B_l , on a $\text{ordre}(\omega_i) \leq 2 \leq d(\omega_i)$; pour C_l , on a $\text{ordre}(\omega_i) \leq 2 \leq d(\omega_i)$; pour D_l , on a $\text{ordre}(\omega_i) \leq 4 \leq d(\omega_i)$.

On en déduit l'inégalité:

$$\Pi d(\omega_i) \leq n \leq \Pi \text{ordre}(\omega_i) \leq \pi d(\omega_i).$$

Donc pour tout i , on a $d(\omega_i) = \text{ordre}(\omega_i)$; donc toutes les composantes irréductibles de R sont de type A_l . On a $n = \pi l_i$ et les l_i sont premiers entre eux puisque $\pi l_i = \text{PPCM}(l_i)$. D'après Serre p. 184, les R_i sont conjugués par un certain groupe de Galois, ce qui est impossible si les l_i sont premiers entre eux. Donc l'ensemble I ne contient qu'un seul élément et R est de type A_{n-1} . D'après le corollaire 5.2, H a un quotient abélien isomorphe à E^* , donc $H = D^*$.

La proposition est donc démontrée.

5.4. DÉMONSTRATION DES THÉORÈMES: D'après la proposition 3.6, $l(\underline{X})$ est le logarithme d'un groupe p -divisible Γ défini sur A . D'après la proposition 4.1, l'anneau des endomorphismes de Γ est isomorphe au corps gauche D . D'après la proposition 5.3, l'enveloppe algébrique de Galois est isomorphe à D^* . Enfin la proposition 3.4 entraîne la dernière assertion du théorème 1.3. Le théorème 1.2 se déduit du théorème 1.3. 5.5 Pour terminer, nous donnons un résultat qui précise l'image de Galois:

PROPOSITION: *Supposons k algébriquement clos. Dans chaque classe d'isogénies, on peut choisir un groupe p -divisible Γ tel que l'anneau des endomorphismes de Γ soit isomorphe à l'ordre maximal de D . L'action de Galois sur le noyau de la multiplication par ω de Γ est donné par le caractère fondamental de niveau n .*

DÉMONSTRATION: Utilisons la proposition 3.4. Soit M le sous A -module de Δ ayant pour base les $\gamma^j(\omega^i * x)$; c'est un réseau fortement divisible de Δ (cf. F-L n°7-8). Le module $M/\omega * M$ est associé à un groupe fini, le noyau de la multiplication par ω du groupe p -divisible Γ associé à M . D'après le théorème 5.3 de [F-L], le module galoisien associé est obtenu en faisant agir le groupe de Galois sur les racines de $\pi^{-1}X^{p^n} = a_n X$. Le groupe d'inertie modérée a donc au moins $q^n - 1$ éléments. D'autre part le groupe d'inertie s'envoie dans le groupe des unités de l'ordre maximal

de D formé des matrices à coefficients entiers dans le plongement de D dans $M_n(L)$ donné au $n^{\circ}2$. Le plus grand quotient d'ordre premier à p de ce groupe est d'ordre $q^n - 1$. Le groupe d'inertie modérée est donc d'ordre $q^n - 1$ et le groupe de Galois agit bien sur le noyau de la multiplication par ω par le caractère fondamental de niveau n . Enfin il est clair par construction de M que l'anneau des endomorphismes de Γ est isomorphe à l'ordre maximal de D . La proposition est donc démontrée.

Bibliographie

- [B] N. BOURBAKI: *Groupes et Algèbres de Lie*. Chapitres 4, 5, 6. Hermann, Paris (1968).
- [CF] J.W.S. CASSELS et A. FROHLICH: *Algebraic Number Theory*. Academic Press: London and New York (1967).
- [F1] J.-M. FONTAINE: Groupes p -divisibles sur les corps locaux. *Astérisque*, p. 47–48. Soc. Math. de France, Paris (1977).
- [F2] J.-M. FONTAINE: Modules galoisiens, modules filtrés et anneaux de Barsotti-Tate. In: *Journées de Géométrie Algébrique de Rennes; Astérisque*, Vol. 65 p. 3–80. Soc. math. de France Paris (1979).
- [F3] J.-M. FONTAINE: Sur certains types de représentations p -adiques du groupe de Galois d'un corps local; construction d'un anneau de Barsotti-Tate, *Ann. of Math.* 115 (1982) 529–577.
- [F-L] J.-M. FONTAINE et G. LAFFAILLE: Constructions de représentations p -adiques. *Annales de l'E.N.S.*, Paris.
- [H1] M. HAZEWINKEL: *Formal Groups and Applications*. Academic Press: New York, San Francisco, London (1978).
- [H2] M. HAZEWINKEL: On formal groups: The functional equation lemma and some of its applications. In: *Journées de Géométrie Algébrique de Rennes; Astérisque*, Vol. 63, p. 73–82. Soc. Math. de France, Paris (1979).
- [L] G. LAFFAILLE: Construction de groupes p -divisibles: Le cas de dimension 1. In: *Journées de Géométrie Algébrique de Rennes; Astérisque*, No1. 65, Soc. Math. de France (1978).
- [LT] J. LUBIN et J. TATE: Formal complex multiplication in local fields. *Ann. of Math.* 81 (1965) 380–387.
- [M] I. MANIN: The theory of commutative formal groups over fields of finite characteristic. *Russian math. Surveys* 18 (1963) 1–83.
- [S] J.-P. SERRE: Groupes algébriques associés aux modules de Hodge-Tate. In: *Journées de Géométrie Algébrique de Rennes; Astérisque*, Vol. 65, p. 155–187. Soc. Math. de France, Paris (1979).
- [Ti] J. TITS: Représentations linéaires irréductibles d'un groupe réductif sur un corps quelconque. *J. reine ang. Math.* 247 (1971) 196–220.

(Oblatum 24-I-1984)

Laboratoire de Mathématiques Pures - Institut Fourier dépendant de l'Université Scientifique et Médicale de Grenoble associé au C.N.R.S.

B.P. 74

38402 ST MARTIN D'HERES

France