Inventiones math. 35, 273 – 284 (1976)

Inventiones mathematicae

Groupes de Lubin-Tate généralisés

Pierre Cartier* (Bures-sur-Yvette)

A Jean-Pierre Serre, en témoignage de 25 ans d'amitié et d'échanges confiants

Introduction

On doit à Lubin et Tate [8] la construction d'une famille de groupes formels à un paramètre associés aux corps locaux, groupes qui jouent un rôle important dans les exposés les plus récents du corps de classes local (voir par exemple, l'exposé de Serre dans le livre de Cassels et Fröhlich [4]).

Dans le présent travail, nous entreprenons de généraliser la construction de Lubin et Tate aux groupes formels de dimension >1. Pour notre construction, on part d'un anneau local A, que nous supposons intègre pour simplifier, dont le corps des fractions est de caractéristique 0, et le corps résiduel de caractéristique $p>0$. On suppose de plus qu'on a relevé en un automorphisme σ de A une puissance de l'opérateur de Frobenius $x \mapsto x^p$ du corps résiduel de A. A chaque paire formée d'un A-module libre de type fini M et d'un opérateur σ-semi-linéaire η dans M satisfaisant à $\eta(\mathfrak{m} \cdot M) \subset p \cdot M$ (on note $\mathfrak{m}$ l'idéal maximal de A), on peut alors associer un groupe formel $LT(M, \eta)$; l'algèbre de Lie de $LT(M, \eta)$ est égale à M. De plus, il existe dans $LT(M, \eta)$ un opérateur dont l'action sur l'algèbre de Lie est égale à η, et qui relève l'opérateur de décalage du groupe formel obtenu par réduction de $LT(M, \eta)$ modulo $\mathfrak{m}$. Ces propriétés généralisent des propriétés bien connues des groupes de Lubin-Tate ordinaires, et montrent que ces derniers s'obtiennent par spécialisation convenable de A, M et η. Cette approche produit au moins un résultat «concret» nouveau, à savoir que la série logarithme du groupe de Lubin-Tate est donnée par $l(X) = \sum_{n=0}^{\infty} \frac{X^{q^n}}{\pi^n}$.

Les démonstrations s'appuient de manière essentielle sur ma théorie des courbes typiques dans les groupes formels, résumée dans [1] et [2] (voir aussi l'exposé de Lazard dans [7]). Pour la commodité des références, on trouvera ci-après un rappel de quelques définitions essentielles. Le lecteur pourra juger de l'aisance avec laquelle on peut raisonner, une fois admis les théorèmes fonda-

* Directeur de Recherches au Centre National de la Recherche Scientifique. L'auteur remercie cette institution pour le soutien financier qu'elle lui fournit

mentaux sur les courbes typiques, en faisant la comparaison avec les calculs de Honda [6] ou de Hazewinkel [5].

Ce travail a été élaboré pour l'essentiel en 1966/67. En fait, c'est en essayant de comprendre et de généraliser la construction de Lubin-Tate que j'ai été amené progressivement à élaborer la théorie des courbes typiques. La dédicace à Serre me semble d'autant plus justifiée qu'il a suivi mes efforts avec beaucoup d'attention et d'intérêt, et m'a laissé exposer leurs résultats dans son Séminaire du Collège de France.

Conventions

Par groupe formel sur un anneau K, on entend un groupe formel G *lisse et commutatif*. Comme schéma formel[1], G est donc de la forme $Spf\mathcal{O}$, avec $\mathcal{O}$ isomorphe à un anneau de séries formelles $K[[X_1, \ldots, X_d]]$. Le choix d'un isomorphisme de $\mathcal{O}$ avec $K[[X_1, \ldots, X_d]]$ définit un *système de coordonnées* $x_1, \ldots, x_d$ dans G, et l'entier $d \geqq 0$ s'appelle la *dimension* de G.

La *droite formelle* est le schéma formel $\mathbf{D} = Spf\, K[[t]]$. Une *courbe* dans G est un morphisme de schémas formels $\gamma: \mathbf{D} \to G$ tel que $\gamma(0) = 0$. Une fois choisi un système de coordonnées $(x_1, \ldots, x_d)$ dans G, une courbe γ est définie par une suite de séries formelles $\gamma_1(t), \ldots, \gamma_d(t)$ sans terme constant. L'addition des courbes se définit au moyen de la loi de groupe de G, d'où un groupe commutatif $C(G)$. Pour tout nombre premier l, on définit un endomorphisme F_l du groupe $C(G)$ caractérisé par la formule

$$F_l\, \gamma(t^l) = \sum_{i=0}^{l-1} \gamma(\zeta^i t),$$

où ζ est un élément d'un sur-anneau de K, satisfaisant à l'équation $\sum_{i=0}^{l-1} \zeta^i = 0$ (il est toujours possible de trouver un tel élément ζ).

Soit p un nombre premier. On dit qu'une courbe γ est *typique* (pour p) si l'on a $F_l\, \gamma = 0$ pour tout nombre premier $l \neq p$; ces courbes forment un sous-groupe $CT(G)$ de $C(G)$. Le groupe $CT(G)$ est muni des opérateurs $F = F_p$, V et $[a]$ définis par

$$[a]\, \gamma(t) = \gamma(at), \qquad V\gamma(t) = \gamma(t^p).$$

On appelle *opérateurs d'homothétie* les opérateurs $[a]$ (pour a dans K). On renvoie à [2] pour une liste complète des relations entre ces opérateurs.

Enfin, si L est une K-algèbre, on note G/L le groupe formel sur L déduit de G par extension des scalaires.

1. Notations

On note A un anneau local, $\mathfrak{m}$ son idéal maximal et $k = A/\mathfrak{m}$ le corps résiduel. On note aussi σ un automorphisme de A et $q = p^f$ (avec $f \geqq 1$) une puissance d'un

[1] On pourra consulter ma Note [2] (ou l'exposé plus développé de Lazard [7]) pour connaître une manière de s'exprimer commode dans la théorie des schémas formels lisses

nombre premier p. On fera les hypothèses suivantes:

a) *Le corps k est de caractéristique p.*

b) *On a $\sigma(a) \equiv a^q \bmod \mathfrak{m}$ pour tout $a \in A$.*

c) *Pour tout $a \neq 0$ dans A, on a $p \cdot a \neq 0$.*

Il est clair que σ conserve l'idéal maximal $\mathfrak{m}$ de A; d'après a), σ définit par passage au quotient l'automorphisme $x \mapsto x^q$ de k, donc k est parfait. D'après c), l'anneau A se plonge dans l'anneau de fractions $K = A\left[\frac{1}{p}\right]$. On a $K = \bigcup_{i \geq 0} p^{-i} A$ et K est une algèbre sur $\mathbb{Q}$. L'automorphisme σ de A se prolonge de manière unique en un automorphisme (noté encore σ) de K.

On suppose par ailleurs donnés un module libre M de type fini sur l'anneau A, et une application η de M dans M qui remplit les conditions suivantes:

d) *Semi-linéarité: Quels que soient x, y dans M et a dans A, on a*

$$\eta(x+y) = \eta(x) + \eta(y), \qquad \eta(a\,x) = \sigma(a) \cdot \eta(x). \tag{1}$$

e) *On a $\eta(\mathfrak{m} \cdot M) \subset p \cdot M$.*

La seconde hypothèse est superflue lorsque $\mathfrak{m} = p \cdot A$ (cas non ramifié). Comme M est un module libre sur le sous-anneau A de K, on peut identifier M à son image dans le K-module $N = K \underset{A}{\otimes} M$ par l'application $x \mapsto 1 \otimes x$. On a alors $N = \bigcup_{i \geq 0} p^{-i} M$ et N est un espace vectoriel sur $\mathbb{Q}$. On prolongera η à N par $\eta(p^{-i} x) = p^{-i} \eta(x)$ (ce qui est sans ambiguïté); les relations (1) sont encore satisfaites.

2. Caractérisation de certains groupes formels

Comme K est une algèbre sur $\mathbb{Q}$, tout groupe formel (commutatif) sur K, d'algèbre de Lie N, est isomorphe au groupe additif N^+. On peut décrire comme suit le module $D = CT(N^+)$ des courbes typiques (pour p) de N: les éléments de D sont les séries formelles de la forme

$$\gamma(t) = \sum_{n=0}^{\infty} x_n\, t^{p^n} \tag{2}$$

avec $x_n \in N$ pour tout $n \geqq 0$. L'addition est définie de manière évidente; quant aux opérateurs V, F et $[c]$ (pour $c \in K$), ils sont définis par les règles suivantes:

$$V\gamma(t) = \sum_{n=1}^{\infty} x_{n-1}\, t^{p^n}, \tag{3}$$

$$F\,\gamma(t) = \sum_{n=0}^{\infty} p\, x_{n+1}\, t^{p^n}, \tag{4}$$

$$[c]\,\gamma(t) = \sum_{n=0}^{\infty} c^{p^n} x_n\, t^{p^n}. \tag{5}$$

Le module N étant muni de la topologie discrète, on munit $D \approx N^{\mathbf{N}}$ de la topologie produit; c'est la topologie associée à la filtration par les sous-modules $V^n D$.

Soit G un groupe formel sur l'anneau A, d'algèbre de Lie M. Soit $G_{/K}$ le groupe formel sur K obtenu par extension des scalaires de A à K. L'algèbre de Lie de $G_{/K}$ est $N = K \underset{A}{\otimes} M$, et d'après ce qui précède, on peut identifier $G_{/K}$ à N^+. Comme A est un sous-anneau de K, on peut identifier $C = CT(G)$ à un sous-groupe de $D = CT(G_{/K})$. On a les propriétés suivantes:

1) *Soit $\gamma \in D$. On a $V\gamma \in C$ si et seulement si $\gamma \in C$.*

2) *Pour tout $\gamma \in C$ et tout $a \in A$, les courbes $F\gamma$ et $[c]\gamma$ appartiennent à C.*

3) *Le module M est égal à l'ensemble des coefficients de t dans les courbes γ appartenant à C.*

4) *Le sous-groupe C de D est fermé.*

Réciproquement, on déduit facilement du théorème fondamental des groupes formels que tout sous-groupe C de D satisfaisant aux propriétés 1) à 4) correspond à un groupe formel G sur A, d'algèbre de Lie M, et que ce groupe formel G est défini à un isomorphisme unique près. Autrement dit, nous avons résolu le problème des «formes sur l'anneau A du groupe additif N^+ sur K».

3. Construction de certains *VF*-modules

Nous mettons maintenant η en jeu. Nous définissons C comme le sous-ensemble de D formé des courbes $\gamma(t) = \sum_{n=0}^{\infty} x_n t^{p^n}$ satisfaisant aux relations

$$x_n \in M \qquad \text{pour } 0 \leqq n \leqq f-1, \tag{6}$$

$$x_n - \eta(x_{n-f})/p \in M \qquad \text{pour } n \geqq f. \tag{7}$$

Il est clair que C est un sous-groupe fermé de D. Par ailleurs, le coefficient x_0 de t dans $\gamma(t) \in C$ est dans M par hypothèse; réciproquement, pour tout $x \in M$, la courbe

$$g_x(t) = \sum_{n=0}^{\infty} \eta^n(x)\, t^{q^n}/p^n \tag{8}$$

appartient à C et le coefficient de t dans $g_x(t)$ est égal à x.

Lemme 1. *Soit $\gamma \in D$. On a $V\gamma \in C$ si et seulement si $\gamma \in C$.*

Posons $\gamma(t) = \sum_{n=0}^{\infty} x_n t^{p^n}$ avec $x_n \in N$ pour tout $n \geqq 0$. D'après l'expression (3) de $V\gamma$, la relation $V\gamma \in C$ équivaut aux relations

$$x_{n-1} \in M \qquad \text{pour } 1 \leqq n \leqq f-1,$$

$$x_{f-1} - \eta(0)/p \in M,$$

$$x_{n-1} - \eta(x_{n-1-f})/p \in M \qquad \text{pour } n \geqq f+1.$$

Ces relations signifient visiblement que γ appartient à C.

Lemme 2. *Pour tout $\gamma \in C$, on a $F\gamma \in C$.*

Avec les notations précédentes, on a $F\gamma(t) = \sum_{n=0}^{\infty} y_n t^{p^n}$ avec $y_n = p\, x_{n+1}$ pour tout $n \geqq 0$. En particulier, on a

$$y_0 = p\, x_1, \quad y_1 = p\, x_2, \ldots, y_{f-2} = p\, x_{f-1}$$

donc $y_0, y_1, \ldots, y_{f-2}$ appartiennent à M. Comme γ appartient à C, l'élément $z = x_f - \eta(x_0)/p$ appartient à M, et comme x_0 appartient aussi à M, il en est de même de $y_{f-1} = p\, x_f = p\, z + \eta(x_0)$. Enfin, pour $n \geqq f$, on a

$$y_n - \eta(y_{n-f})/p = p \cdot [x_{n+1} - \eta(x_{n+1-f})/p],$$

donc y_n appartient à M. On a bien prouvé que $F\gamma$ appartient à C.

On peut établir les lemmes 1 et 2 par une autre méthode, peut-être plus instructive. Tout d'abord, la formule (8) conserve un sens pour tout x dans N et définit un élément g_x de D. D'autre part, les formules

$$y_n = x_n \quad \text{pour } 0 \leqq n \leqq f-1, \qquad y_n = x_n - \eta(x_{n-f})/p \quad \text{pour } n \geqq f \tag{9}$$

définissent une permutation $(x_n)_{n \geqq 0} \mapsto (y_n)_{n \geqq 0}$ de l'ensemble $N^{\mathbb{N}}$ des suites d'éléments de N. Les formules (9) s'inversent comme suit

$$x_n = \sum_{i=0}^{[n/f]} \eta^i(y_{n-fi})/p^i; \tag{10}$$

on a alors

$$\sum_{n=0}^{\infty} x_n t^{p^n} = \sum_{n=0}^{\infty} \sum_{i=0}^{[n/f]} t^{p^n} \eta^i(y_{n-fi})/p^i$$
$$= \sum_{i,j=0}^{\infty} t^{p^{fi+j}} \eta^i(y_j)/p^i = \sum_{j=0}^{\infty} g_{y_j}(t^{p^j})$$

par application de la formule de sommation

$$\sum_{n=0}^{\infty} \sum_{i=0}^{[n/f]} u(n,i) = \sum_{i,j=0}^{\infty} u(fi+j, i).$$

Autrement dit, toute courbe $\gamma \in D$ s'écrit de manière unique sous la forme

$$\gamma = \sum_{j=0}^{\infty} V^j g_{y(j)} \tag{11}$$

pour une suite d'éléments $y(0), y(1), y(2), \ldots$ de N et γ appartient à C si et seulement si chacun des $y(j)$ appartient à M. Il est alors clair que C est stable par V; qu'il soit stable par F résulte de la formule suivante, facile à établir

$$F\, g_x = V^{f-1} g_{\eta(x)} \quad (x \in M), \tag{12}$$

et qui entraîne (par la relation $FV\gamma = p\gamma$)

$$F\gamma = V^{f-1} g_{\eta(y(0))} + \sum_{j=1}^{\infty} p \cdot V^{j-1} g_{y(j)}, \tag{13}$$

lorsque γ est donnée par la formule (11).

4. Opérateurs d'homothétie

Pour montrer que le groupe C de courbes correspond à un groupe formel sur A, il reste à prouver que C est stable par les opérateurs d'homothétie $[a]$. Nous procéderons par étapes.

Lemme 3. *Soient a, b des éléments de A et $i \geqq 1$ un entier. La congruence $a \equiv b \bmod \mathfrak{m}^i$ entraîne la congruence $a^p \equiv b^p \bmod \mathfrak{m}^{i+1}$.*

Ce résultat bien connu peut se démontrer comme suit. On écrit

$$a^p - b^p = (a-b) \cdot c \quad \text{avec } c = \sum_{i=0}^{p-1} a^i b^{p-1-i}.$$

Or, on a $a \equiv b \bmod \mathfrak{m}$, d'où $c \equiv p\, a^{p-1} \bmod \mathfrak{m}$, et comme p appartient à $\mathfrak{m}$, il en est de même de c; par suite, $a^p - b^p = (a-b) \cdot c$ appartient à $\mathfrak{m}^i \cdot \mathfrak{m} = \mathfrak{m}^{i+1}$.

Lemme 4. *Si la courbe $\gamma(t) = \sum_{n=0}^{\infty} x_n t^{p^n}$ appartient à C, on a $a \cdot x_n \in M$ pour tout entier $n \geqq 0$ et tout élément a de $\mathfrak{m}^{[n/f]}$.*

Démonstration par récurrence sur n, le cas $0 \leqq n \leqq f-1$ résultant de l'hypothèse (6). Supposons donc $n \geqq f$; il existe $y \in M$ tel que $x_n = y + \eta(x_{n-f})/p$. Soit a un élément de $\mathfrak{m}^{[n/f]}$; il existe des éléments b_i de $\mathfrak{m}$ et c_i de $\mathfrak{m}^{[n/f]-1}$ tels que $a = b_1 c_1 + \cdots + b_s c_s$. On a alors

$$a \cdot x_n = a \cdot y + \sum_{i=1}^{s} \eta(\sigma^{-1}(b_i)\, \sigma^{-1}(c_i) \cdot x_{n-f})/p;$$

or $\mathfrak{m}$ est stable par σ, d'où $\sigma^{-1}(c_i) \in \mathfrak{m}^{[n/f]-1}$, et par l'hypothèse de récurrence, $z_i = \sigma^{-1}(c_i) \cdot x_{n-f}$ appartient à M. Or l'hypothèse e) du n° 1 entraîne

$$\eta(\sigma^{-1}(b_i) \cdot z_i) \in p \cdot M;$$

comme on a $a \in A$ et $y \in M$, on a aussi $a \cdot y \in M$, d'où finalement $a \cdot x_n \in M$.

Lemme 5. *Le sous-groupe C de D est stable par $[a]$ pour tout $a \in A$.*

Soit $\gamma(t) = \sum_{n=0}^{\infty} x_n t^{p^n}$ un élément de C et soit $a \in A$. Nous avons à prouver que, pour tout entier $n \geqq f$, l'élément

$$y_n = a^{p^n} \cdot x_n - \eta(a^{p^{n-f}} \cdot x_{n-f})/p \tag{14}$$

de N appartient à M. Par hypothèse, on a $a^{p^f} \equiv \sigma(a) \bmod \mathfrak{m}$; en élevant $n-f$ fois cette congruence à la puissance p-ième, on trouve

$$a^{p^n} \equiv \sigma(a^{p^{n-f}}) \mod \mathfrak{m}^{n-f+1} \tag{15}$$

par application du lemme 3. Or, on peut écrire

$$y_n = (a^{p^n} - \sigma(a^{p^{n-f}})) \cdot x_n + \sigma(a^{p^{n-f}}) \cdot (x_n - \eta(x_{n-f})/p) \tag{16}$$

d'après la semi-linéarité de η. On a $n \geqq f \geqq 1$, d'où $n-f+1 \geqq n/f \geqq [n/f]$, et par suite, l'élément $a^{p^n} - \sigma(a^{p^{n-f}})$ appartient à $\mathfrak{m}^{[n/f]}$. D'après le lemme 4, le premier

terme du second membre de (16) appartient à M; il en est de même du second terme puisque $\sigma(a^{p^{n-f}})$ appartient à A et $x_n - \eta(x_{n-f})/p$ à M par définition de C. On a donc $y_n \in M$.

5. Groupes de Lubin-Tate généralisés

D'après les résultats généraux rappelés au n° 2 et les lemmes 1, 2 et 5, on voit que C est l'ensemble des courbes typiques d'un groupe formel G sur l'anneau A, d'algèbre de Lie M. On dit que c'est le *groupe de Lubin-Tate* associé à (M, η); on le note $LT(M, \eta)$.

Pour décrire ce groupe formel de manière plus explicite, introduisons une base $(e_1, \ldots, e_d)$ du A-module M. Soit $\mathbf{D}$ la droite formelle et g le morphisme de schémas formels de $\mathbf{D}^d$ dans G associé aux courbes $g_{e_i} = \gamma_i$ $(1 \leqq i \leqq d)$ par la formule

$$g(t_1, \ldots, t_d) = \gamma_1(t_1) + \cdots + \gamma_d(t_d). \tag{17}$$

L'application linéaire tangente à g à l'origine est donnée par

$$g'(u_1, \ldots, u_d) = u_1 \cdot e_1 + \cdots + u_d \cdot e_d; \tag{18}$$

elle est donc bijective, et le théorème des fonctions implicites montre que g est un isomorphisme de schémas formels. L'isomorphisme réciproque $g^{-1}: G \to \mathbf{D}^d$ définit un système de coordonnées $(x_1, \ldots, x_d)$ sur G.

Par ailleurs, notant selon l'usage $\mathbf{G}_a$ le groupe formel additif à un paramètre (dont le schéma formel sous-jacent est $\mathbf{D}$), on définit un isomorphisme h de $(\mathbf{G}_a)^d$ sur M^+ par $h(t_1, \ldots, t_d) = t_1 \cdot e_1 + \cdots + t_d \cdot e_d$. Comme on a $G_{/K} = M^+_{/K}$ par construction, on voit que $l = (h_{/K})^{-1}$ est un isomorphisme de groupes formels de $G_{/K}$ sur $(\mathbf{G}_{a/K})^d$. Le morphisme l s'exprime dans le système de coordonnées $(x_1, \ldots, x_d)$ de G par des séries formelles $l_i(X_1, \ldots, X_d)$ qui constituent la *loi logarithme* du groupe formel G dans le système de coordonnées $(x_1, \ldots, x_d)$. On explicite facilement ces séries:

$$l_i(X_1, \ldots, X_d) = \sum_{n=0}^{\infty} \sum_{j=1}^{d} b(n)_{ij} X_j^{q^n}/p^n. \tag{19}$$

La matrice $\mathbf{B}(n)$ d'éléments $b(n)_{ij}$ (pour $1 \leqq i, j \leqq d$) se calcule par les formules

$$\eta(e_j) = \sum_{i=1}^{d} a_{ij} \cdot e_i \quad \text{pour } 1 \leqq j \leqq d, \tag{19a}$$

$$\mathbf{A} = (a_{ij})_{1 \leqq i, j \leqq d}, \tag{19b}$$

$$\mathbf{B}(n) = \mathbf{A} \cdot \sigma(\mathbf{A}) \cdot \sigma^2(\mathbf{A}) \ldots \sigma^{n-1}(\mathbf{A}) \quad \text{pour } n \geqq 1, \quad \mathbf{B}(0) = I. \tag{19c}$$

Dans ces formules, la matrice $\sigma^n(\mathbf{A})$ s'obtient en appliquant l'automorphisme σ^n de l'anneau A à chacun des éléments de la matrice $\mathbf{A}$.

Une fois connue la loi logarithme de G, on peut déterminer en principe les séries formelles $F_i(X_1, \ldots, X_d; Y_1, \ldots, Y_d) = F_i$ traduisant la loi de groupe de G dans le système de coordonnées $(x_1, \ldots, x_d)$. On a en effet

$$l_i(F_1, \ldots, F_d) = l_i(X_1, \ldots, X_d) + l_i(Y_1, \ldots, Y_d) \quad (1 \leqq i \leqq d) \tag{20}$$

et comme l'ensemble des termes linéaires de la série l_i est égal à X_i, le système précédent a une unique solution $(F_1, \ldots, F_d)$.

Il est clair *a priori* que les formules (19) et (20) définissent une loi de groupe formel $(F_1, \ldots, F_d)$ à coefficients dans K; le point non trivial est que ces séries aient *leurs coefficients dans l'anneau A*. Pour autant que je puisse voir, les calculs de Honda [6] et Hazewinkel [5] pourraient servir à établir ce point directement.

6. Caractère fonctoriel

Soit $\mathscr{M}$ la catégorie dont les objets sont les paires (M, η) formées d'un A-module M libre de type fini, et d'un opérateur semi-linéaire η dans M tel que $\eta(\mathfrak{m} \cdot M) \subset p \cdot M$. Un morphisme de (M, η) dans (M', η') est une application linéaire u de M dans M' telle que $\eta' u = u \eta$; la composition des morphismes est celle des applications.

Lemme 6. *Soient (M, η) et (M', η') deux objets de la catégorie $\mathscr{M}$ et u un morphisme de (M, η) dans (M', η'). Il existe un morphisme de groupes formels $LT(u)$ de $LT(M, \eta)$ dans $LT(M', \eta')$ et un seul qui induise u sur les algèbres de Lie* [rappelons que M est l'algèbre de Lie de $LT(M, \eta)$ et M' celle de $LT(M', \eta')$].

Posons $N = K \underset{A}{\otimes} M$ et $N' = K \underset{A}{\otimes} M'$, et étendons u en une application K-linéaire v de N dans N'. Posons aussi $G = LT(M, \eta)$ et $G' = LT(M', \eta')$. On peut considérer u comme un morphisme du groupe formel additif M^+ dans le groupe additif M'^+ et v comme un morphisme de $N^+ = (M^+)_{/K}$ dans $N'^+ = (M'^+)_{/K}$. Il s'agit de montrer qu'il existe un morphisme $w = LT(u)$ de G dans G' tel que $w_{/K} = v$, autrement dit que «*le morphisme v est défini sur l'anneau A*». Pour cela, d'après les théorèmes généraux sur les groupes formels, il suffit de prouver que v applique le sous-groupe $CT(G)$ de $CT(N^+)$ dans le sous-groupe $CT(G')$ de $CT(N'^+)$.

Soit donc $\gamma(t) = \sum_{n=0}^{\infty} x_n t^{p^n}$ un élément de $CT(G)$; on a par hypothèse

$x_n \in M$ pour $0 \leqq n \leqq f-1$

$x_n - \eta(x_{n-f})/p \in M$ pour $n \geqq f$.

Or on a $v(M) \subset M'$ et $v\,\gamma(t) = \sum_{n=0}^{\infty} v(x_n)\, t^{p^n}$; de $v\,\eta' = \eta'\, v$, on déduit alors que

$$v(x_n) - \eta'(v(x_{n-f})/p) = v(x_n - \eta(x_{n-f})/p)$$

est un élément de M' pour tout $n \geqq f$, d'où $v\,\gamma \in CT(G')$.

Si u et u' sont deux morphismes composables dans la catégorie $\mathscr{M}$, les morphismes de groupes formels $LT(u'\,u)$ et $LT(u') \cdot LT(u)$ induisent tous deux l'application linéaire $u'\,u$ sur les algèbres de Lie, donc coïncident d'après le lemme 6.

On a donc défini un foncteur LT de la catégorie $\mathscr{M}$ dans celle des groupes formels (commutatifs et lisses) sur l'anneau A.

7. Réduction modulo m

Soit $G = LT(M, \eta)$ et soit $\Gamma = G_{/k}$ le groupe formel sur le corps $k = A/\mathfrak{m}$ déduit de G par réduction modulo $\mathfrak{m}$. Soit G^σ le groupe formel sur A obtenu en tordant G par l'automorphisme σ de A. Il est immédiat qu'on a $G^\sigma = LT(M^\sigma, \eta)$, où M^σ est le A-module déduit de M en modifiant les homothéties par

$$a * x = \sigma^{-1}(a) \cdot x \quad \text{pour } a \in A \text{ et } x \in M. \tag{21}$$

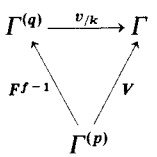
Comme on a $\sigma(a) \equiv a^q \bmod \mathfrak{m}$ pour tout $a \in A$, le groupe formel $(G^\sigma)_{/k}$ déduit de G^σ par réduction modulo $\mathfrak{m}$ n'est autre que le groupe formel $\Gamma^{(q)}$ obtenu en tordant Γ par l'automorphisme $x \mapsto x^q$ du corps k de caractéristique p.

L'hypothèse que η est semi-linéaire signifie que c'est une application A-linéaire de M^σ dans M, donc un morphisme de (M^σ, η) dans (M, η) au sens de la catégorie $\mathscr{M}$. On peut donc définir le morphisme $v = LT(\eta)$ de G^σ dans G, et par réduction modulo $\mathfrak{m}$, le morphisme $v_{/k}$ de $\Gamma^{(q)}$ dans Γ. Comme Γ est un groupe formel commutatif sur le corps k qui est parfait de caractéristique $p > 0$, on définit [2] pour tout entier n des opérateurs de Frobenius $F: \Gamma^{(p^n)} \to \Gamma^{(p^{n+1})}$ et de décalage $V: \Gamma^{(p^n)} \to \Gamma^{(p^{n-1})}$.

Lemme 7. *Le morphisme v de G^σ dans G a les propriétés suivantes:*

a) *L'action de v sur les algèbres de Lie coïncide avec η.*

b) *En réduction modulo* $\mathfrak{m}$, *on a le diagramme commutatif*



L'assertion a) résulte de la définition de $v = LT(\eta)$.

Prouvons b). Pour tout $x \in M$, on a défini au n° 3 une courbe typique g_x dans G (voir formule (8)); par réduction modulo $\mathfrak{m}$, on déduit de g_x une courbe typique γ_x dans Γ. D'après la formule (12), on a $F\, g_x(t) = g_{\eta(x)}(t^{p^{f-1}})$; comme l'opérateur F sur les courbes typiques commute à la réduction modulo $\mathfrak{m}$, on a donc

$$F\, \gamma_x(t) = \gamma_{\eta(x)}(t^{p^{f-1}}). \tag{22}$$

Soit γ une courbe dans Γ; pour tout entier n, on note $\gamma^{(p^n)}$ la courbe dans $\Gamma^{(p^n)}$ obtenue en appliquant à γ l'automorphisme $x \mapsto x^{p^n}$ du corps k. L'opérateur F^{f-1} de $\Gamma^{(p)}$ dans $\Gamma^{(q)}$ transforme la courbe $\gamma_x^{(p)}(t)$ en $\gamma_x^{(q)}(t^{p^{f-1}})$ et comme v transforme la courbe g_y^σ en $g_{\eta(y)}$, on voit que $v_{/k}$ transforme la courbe $\gamma_y^{(q)}$ en la courbe $\gamma_{\eta(y)}$. Compte tenu de la formule (22), on voit que le morphisme $v_{/k}\, F^{f-1}$ de $\Gamma^{(p)}$ dans Γ transforme la courbe $\gamma_x^{(p)}$ en la courbe $F\, \gamma_x$.

Le composé VF des morphismes $F: \Gamma \to \Gamma^{(p)}$ et $V: \Gamma^{(p)} \to \Gamma$ est égal à la multiplication par p dans le groupe formel Γ. Si $\gamma(t)$ est une courbe typique dans Γ, F la transforme en la courbe $\gamma^{(p)}(t^p)$ dans $\Gamma^{(p)}$, et V transforme donc cette dernière en la courbe $p \cdot \gamma(t)$ dans Γ. Or, sur le corps k de caractéristique p, on a l'égalité [3] $p \cdot \gamma(t) = F\, \gamma(t^p)$. Autrement dit, le morphisme $V: \Gamma^{(p)} \to \Gamma$ transforme une courbe $\gamma^{(p)}$ en $F\, \gamma$, i.e. on a $V \circ \gamma^{(p)} = F\, \gamma$. En particulier, V transforme la courbe $\gamma_x^{(p)}$ en la courbe $F\, \gamma_x$.

On a donc établi la formule

$$v_{/k}\, F^{f-1} \circ \gamma_x^{(p)} = V \circ \gamma_x^{(p)} \quad \text{pour tout } x \in M. \tag{23}$$

---

[2] Pour la théorie des groupes formels sur un corps de caractéristique $p > 0$, on pourra se reporter par exemple à mon exposé de Bruxelles [3]

[3] Le lecteur devra distinguer l'opérateur F sur les courbes de Γ de l'application $\gamma \mapsto F \circ \gamma$ de $CT(\Gamma)$ dans $CT(\Gamma^{(p)})$; de même pour V

Soit alors $(e_1, \ldots, e_d)$ une base du A-module M. L'application

$$\Phi: (t_1, \ldots, t_d) \mapsto \gamma_{e_1}^{(p)}(t_1) + \cdots + \gamma_{e_d}^{(p)}(t_d)$$

est donc un isomorphisme de schémas formels de $(\mathbf{D}_{/k})^d$ sur $\Gamma^{(p)}$; la formule (23) montre que l'on a $v_{/k} F^{f-1} \Phi = V\Phi$, d'où la relation cherchée $v_{/k} F^{f-1} = V$.

8. Groupes de Lubin-Tate «classiques»

Soient p un nombre premier, $\mathbb{Q}_p$ le corps des nombres p-adiques, et K une extension de degré fini de $\mathbb{Q}_p$. Notons A l'anneau des éléments de K entiers sur l'anneau $\mathbb{Z}_p$ des entiers p-adiques, $\mathfrak{m}$ l'idéal maximal de A et $k = A/\mathfrak{m}$ le corps résiduel. Le corps k est fini de caractéristique p; notons $q = p^f$ le nombre de ses éléments; on a donc $f = [k: \mathbb{F}_p]$ où $\mathbb{F}_p$ est le corps fini à p éléments. Pour tout a dans A, on a $a^q \equiv a \bmod \mathfrak{m}$, de sorte que la théorie précédente s'applique en prenant pour σ l'automorphisme identique de A. Enfin, on note π une uniformisante, c'est-à-dire un élément de A tel que $\mathfrak{m} = \pi A$.

On pose $M = A$, considéré comme A-module, et l'on note η la multiplication par p/π dans A. On a $\mathfrak{m} \cdot M = \pi \cdot A$, d'où $\eta(\mathfrak{m} \cdot M) = p \cdot M$. Notons G_π le groupe formel $LT(M, \eta)$ correspondant. Dans G_π, il existe une coordonnée x telle que $x(g_1(t)) = t$, où la courbe $g_1 \in CT(G_\pi)$ est donnée par un cas particulier de la formule (8), à savoir

$$g_1(t) = \sum_{n=0}^{\infty} t^{q^n}/\pi^n. \tag{24}$$

Il est immédiat que g_1 est la loi logarithme du groupe formel G_π dans la coordonnée x; par suite, dans la coordonnée x, la loi de groupe de G_π correspond à une série formelle $L(X, Y)$ définie par

$$\sum_{n=0}^{\infty} L(X, Y)^{q^n}/\pi^n = \sum_{n=0}^{\infty} (X^{q^n} + Y^{q^n})/\pi^n. \tag{25}$$

Ici encore, il est clair que cette formule définit une loi de groupe à coefficients dans le corps K; le grand miracle est que les coefficients de la série $L(X, Y)$ appartiennent à l'anneau A.

Pour tout $a \in A$, la multiplication par a est un endomorphisme de (M, η) dans la catégorie $\mathcal{M}$. Comme nous avons pris soin de prouver le caractère fonctoriel de notre construction[4], on peut donc associer à a un endomorphisme $[a]_\pi$ de G_π. Dans la coordonnée x, l'endomorphisme $[a]_\pi$ correspond à une série formelle $[a]_\pi(X)$ caractérisée par la relation

$$\sum_{n=0}^{\infty} [a]_\pi(X)^{q^n}/\pi^n = a \cdot \sum_{n=0}^{\infty} X^{q^n}/\pi^n. \tag{26}$$

En particulier, le terme linéaire de $[a]_\pi(X)$ est égal à $a \cdot X$, d'où l'on déduit aussitôt que $a \mapsto [a]_\pi$ *est un isomorphisme de A sur l'anneau des endomorphismes de G_π.*

[4] Ce travail a été écrit en 1967. Vu les fluctuations rapides de la mode, je ne sais si j'oserais encore invoquer aujourd'hui la Trinité Fonctorielle

Lemme 8. *Posons* $u=[\pi]_\pi$. *En réduction modulo* m, *l'endomorphisme* $u_{/k}$ *de* $\Gamma=(G_\pi)_{/k}$ *coïncide avec l'opérateur de Frobenius* F^f.

Notons tout d'abord que le corps k est fini à $q=p^f$ éléments, donc l'opérateur de Frobenius F^f existe en tant qu'endomorphisme de Γ.

Posons $v=[p/\pi]_\pi$. On a $vu=p$, d'où $v_{/k}u_{/k}=p$ par réduction modulo m. Par ailleurs, d'après le lemme 7, on a $v_{/k}F^{f-1}=V$ puisque η est la multiplication par p/π dans A. Comme on a aussi $VF=p$, on en conclut

$$v_{/k}u_{/k}=v_{/k}F^f. \tag{27}$$

Comme Γ est un groupe formel de dimension 1 sur le corps k, l'égalité cherchée résultera de (27) pourvu que l'on prouve que $v_{/k}$ n'est pas nul.

Soit θ la série formelle exprimant $[\pi]_\pi$ dans la coordonnée x. On a donc (formule (26))

$$\sum_{n=0}^{\infty}\theta(X)^{q^n}/\pi^n=\pi X+\sum_{n=1}^{\infty}X^{q^n}/\pi^{n-1}. \tag{28}$$

On en déduit

$$\theta+\theta^q/\pi\equiv\pi X+X^q \mod X^{q+1} \tag{29}$$

et donc

$$\theta\equiv\pi X+X^q(1-\pi^{q-1}) \mod X^{q+1}. \tag{30}$$

Cette série n'est évidemment pas nulle modulo π, d'où $u_{/k}\neq 0$. Comme π est une uniformisante, il existe un entier $h\geqq 1$ et un élément inversible a de A tels que $p=a\cdot\pi^h$, d'où $v=[a]_\pi\cdot u^{h-1}$. Comme $[a]_\pi$ est un automorphisme de G^π, et que $u_{/k}\neq 0$, on a finalement $v_{/k}\neq 0$.

Lemme 9. *Soit* θ *la série formelle exprimant l'endomorphisme* $[\pi]_\pi$ *de* G_π *dans la coordonnée* x. *On a les propriétés suivantes:*

a) *On a* $\theta(L(X,Y))=L(\theta(X),\theta(Y))$.

b) *Le coefficient de* X *dans* $\theta(X)$ *est égal à* π.

c) *On a* $\theta(X)\equiv X^q \bmod \pi$.

L'assertion a) signifie que $[\pi]_\pi$ est un endomorphisme de G_π. On sait qu'en général $[a]_\pi$ induit la multiplication par a sur l'espace tangent à G_π à l'origine, d'où b) en particulier. Enfin, l'assertion c) ne fait que traduire le lemme 8.

On a reconnu dans le lemme 9 la description donnée par Lubin et Tate de leur groupe formel. Nous avons ici fait un choix canonique de la série formelle $\theta(X)\in A[[X]]$, caractérisé par la formule (28), et correspondant à la série logarithme $\sum_{n=0}^{\infty}X^{q^n}/\pi^n$. En conclusion, le groupe formel G_π construit dans ce n° n'est autre que le groupe de Lubin-Tate «classique».

9. Dernières remarques

a) Soit (M,η) un objet de la catégorie $\mathcal{M}$ tel que $\eta(M)\subset p\cdot M$. Avec les notations du n° 3, le groupe C se compose de toutes les séries formelles $\sum_{n=0}^{\infty}x_n t^{p^n}$ à coefficients

dans M, d'où $LT(M,\eta)=M^+$. Prenons en particulier $A=\mathbb{Z}_p$, $\sigma=1$, $f=1$ et $\eta(x)=p^i x$ avec $i\geqq 1$. Le *groupe formel* $LT(\mathbb{Z}_p, p^i)$ *n'est autre que le groupe additif* $\mathbf{G}_a$ à un paramètre.

b) Prenons cette fois $A=\mathbb{Z}_p$, $\sigma=1, f=1$, mais $\eta(x)=x$. La série $g_1(t)$ est égale à $\sum_{n=0}^{\infty} t^{p^n}/p^n$; il est bien connu (Artin-Hasse) que la série $u(t)=\exp g_1(t)$ a ses coefficients dans l'anneau $\mathbb{Z}_p$ des entiers p-adiques, et l'on a évidemment $u(t)\equiv 1+t \bmod t^2$. Par construction, u est un morphisme du groupe $G=LT(\mathbb{Z}_p, 1)$ dans le groupe multiplicatif à un paramètre $\mathbf{G}_m$. Autrement dit, *le groupe* $LT(\mathbb{Z}_p, 1)$ *est isomorphe au groupe multiplicatif* $\mathbf{G}_m$.

c) Plus généralement, lorsque A est non-ramifié (i.e. $\mathfrak{m}=pA$) et que η est bijectif, le groupe de Lubin-Tate $LT(M,\eta)$ est un relèvement à A d'un tore formel T sur le corps k. Autrement dit, après extension des scalaires de k à une extension algébriquement close de k, le groupe formel T devient isomorphe à un produit $(\mathbf{G}_m)^d$ de groupes multiplicatifs.

d) Nous avons supposé tout au long que p n'est pas diviseur de 0 dans l'anneau A. Ceci simplifie l'exposition de la théorie, mais n'est pas indispensable. Nous exposerons ultérieurement en détail une telle extension de la théorie lorsque A est non-ramifié et complet pour la topologie $\mathfrak{m}$-adique. Ceci permet en particulier de retrouver les groupes de Lubin-Tate attachés aux corps locaux de caractéristique non nulle, que nous avons laissés de côté ici.

Références

1. Cartier, P.: Groupes formels associés aux anneaux de Witt généralisés. C.R. Acad. Sci. Paris **265**, 50–52 (1967)
2. Cartier, P.: Modules associés à un groupe formel commutatif. Courbes typiques. C.R. Acad. Sci. Paris **265**, 129–132 (1967)
3. Cartier, P.: Groupes algébriques et groupes formels. In: Colloque sur la théorie des groupes algébriques, Bruxelles 1962
4. Cassels, J.L.W. et Fröhlich A. (edit.): Algebraic number theory. London-New York: Academic Press 1967
5. Hazewinkel, M.: Constructing formal groups, I, II, III, IV (Reports 7119+Appendice, 7201, 7207, 7322, Econometric Institute, Université Erasme, Rotterdam)
6. Honda, T.: Formal groups and zeta functions. Osaka Journ. Math. **5**, 199–213 (1968)
7. Lazard, M.: Commutative formal groups. Lecture Notes in Math. **443**. Berlin-Heidelberg-New York: Springer 1975
8. Lubin, J., Tate, J.: Formal complex multiplication in local fields. Ann. of Maths. **81**, 380–387 (1965)

Received April 23, 1976

Pierre Cartier
Institut des Hautes Etudes Scientifiques
35 route de Chartres
F-91440 Bures-sur-Yvette
France