UNIVERSITÉ SCIENTIFIQUE ET MÉDICALE DE GRENOBLE
Laboratoire de Mathématiques Pures associé au C.N.R.S.

Jean-Marc Fontaine
INSTITUT
DE MATHÉMATIQUES PURES
Boîte Postale 116
38402 SAINT-MARTIN-D'HÈRES

Téléphone (76) 87-45-61 à 64

le 22 février 1974

Cher Serre,

Voici donc une première lettre consacrée à quelques réflexions sur les groupes formels. Mon but aujourd'hui c'est de te convaincre que, pour un groupe formel lisse, mon module des "presque-logarithmes" c'est la même chose que le module de Dieudonné du groupe, ce dernier terme étant pris au sens de Manin. Malheureusement la construction de Manin, bien que très élégante, n'est pas du tout adaptée à ma description : chez moi le groupe multiplicatif ne joue aucun rôle particulier et, surtout, je ne peux absolument pas me permettre de procéder par passage à la limite à partir du cas des groupes finis car j'utilise de façon essentielle l'injectivité du Frobenius.

Je vais donc utiliser un intermédiaire entre Manin et moi (sans me fatiguer à chercher ce qui, dans cette construction, revient à Barsotti) Cela va consister à associer à tout groupe formel un module de Dieudonné, et ceci d'une manière qui, en un certain sens est la meilleure possible. Je n'aurai alors aucune difficulté à montrer que dans le cas où Manin sait faire (resp. dans le cas d'un groupe lisse) on retrouve son module (resp. mes "presque-logarithmes"). Cette construction est devenue récemment, pour moi, tout à fait claire, ce qui va me permettre d'éviter d'avoir à t'écrire une partie des choses désagréables que j'avais essayé de te raconter. En fait il s'agit de construire un vrai groupe formel, que je note CW_1, et le module de Dieudonné d'un groupe G sera défini comme le module des morphismes de G dans CW_1. C'est donc de la construction de CW_1 qu'il va surtout être question dans cette lettre.

1 - Tout d'abord quelques notations et conventions.

Je note k un corps parfait de caractéristique p, non nulle, fixé une fois pour toutes. Ce que j'appelle une algèbre profinie c'est une algèbre sur k, associative, commutative, avec un élément-unité, qui est limite projective d'algèbres finies (i.e. de dimension finie sur k). Un morphisme d'algèbres profinies c'est un homomorphisme continu qui envoie l'élément-unité sur l'élément-unité.

Un groupe formel (sous-entendu commutatif) c'est un foncteur en groupes abéliens sur la catégorie des algèbres profinies, qui est représentable. Un groupe formel G, à isomorphisme près, ça s'écrit donc $G = \mathrm{Spf}\, A$, où A est une bigèbre formelle, i.e. une algèbre profinie avec des morphismes

$$\Delta : A \longrightarrow A \hat{\otimes} A \quad , \quad \varepsilon : A \longrightarrow k \quad , \quad \sigma : A \longrightarrow A$$

qui ont les propriétés qu'il faut. Le foncteur Spf est une antiéquivalence entre la catégorie des bigèbres formelles et celle des groupes formels, merci Yoneda.

2 - Les anneaux (de Barsotti, si tu veux).

Je note B_o (avec B comme Barsotti) l'anneau des polynômes

$$B_o = k[X_{-1}, X_{-2}, \ldots, X_{-n}, \ldots] \quad \text{(en abrégé } B_o = k[X]\text{)}.$$

J'appelle $\underline{m}$ l'idéal maximal de B_o et, pour r et $s \geqslant 0$, je définis les idéaux $\underline{f}^r = (X_{-n}^{p^r})_{n \in \mathbb{N}^*}$, $\underline{v}^s = (X_{-n})_{n > s}$ de B_o.

Je note $B_4 = k[[X]]$ l'anneau des "vraies" séries formelles en les X_{-n}, i.e. le complété de B_o pour la topologie définie par les idéaux de la forme $\underline{m}^r + \underline{v}^s$ (note, c'est très important, que B_4, qui est profini, est aussi le complété de B_o pour la topologie obtenue en prenant comme idéaux ouverts les idéaux de codimension finie qui contiennent un idéal de la forme $\underline{f}^r + \underline{v}^s$).

Maintenant, je vais te vendre trois autres algèbres profinies comprises entre B_o et B_4. Si tu en veux bien, la suite devrait aller toute seule.

Pour $i = 1,2,3,4$, l'algèbre B_i est le complété de B_o pour la topologie obtenue en prenant comme idéaux ouverts les idéaux de codimension finie qui contiennent un idéal de la forme

$$\underline{f}^r \cap \underline{v}^s \quad \text{pour} \quad i = 1 ,$$
$$\underline{f}^r \quad \text{pour} \quad i = 2 ,$$
$$\underline{v}^s \quad \text{pour} \quad i = 3 ,$$
$$\underline{f}^r + \underline{v}^s \quad \text{pour} \quad i = 4 \text{ (je me répète)} .$$

Remarque : l'hypothèse de cod. finie permet de remplacer, si on veut, les $\underline{f}^r$ par les puissances de $\underline{m}$.

Les algèbres B_i , pour $i = 1,2,3$, paraissent bien peu maniables. Il ne faut pas en avoir peur. En particulier, après identifications canoniques, on a le diagramme suivant (dans lequel les flèches sont des inclusions)

$$k[X] = B_o \longrightarrow B_1 \begin{array}{l} \nearrow B_2 \searrow \\ \searrow B_3 \nearrow \end{array} B_4 = k[[X]] \quad .$$

3 - Les covecteurs.

Si, avec des notations évidentes, j'identifie $B_o \otimes B_o$ à $k[X,Y]$ et $B_4 \hat{\otimes} B_4$ à $k[[X,Y]]$, les $B_i \hat{\otimes} B_i$ s'identifient à des sous-algèbres de $k[[X,Y]]$.

Je note $S_o, S_1, \ldots, S_m, \ldots$ les polynômes qui définissent l'addition dans les vecteurs de Witt. Ce n'est pas difficile de voir que, pour n fixé, la suite des $S_m(X_{-n-m}, X_{-n-m+1}, \ldots, X_{-n}, Y_{-n-m}, Y_{-n-m+1}, \ldots, Y_{-n})$ converge, non seulement dans $k[[X,Y]]$, mais encore dans $B_1 \hat{\otimes} B_1$. Ceci me définit un homomorphisme Δ de B_o dans $B_1 \hat{\otimes} B_1$:

$$\Delta(X_{-n}) = \lim_{m \to +\infty} S_m(X_{-n-m}, X_{-n-m+1}, \ldots, X_{-n}, Y_{-n-m}, \ldots, Y_{-n}) .$$

Maintenant Δ est continu pour la topologie $B_o \to B_1$, donc a fortiori pour les autres, et se prolonge donc, pour $i = 1,2,3,4$, en un morphisme, que je note encore Δ , de B_i dans $B_i \hat{\otimes} B_i$. J'ai donc ainsi défini quatre bigèbres formelles, donc aussi quatre groupes formels

$$CW_i = \mathrm{Spf}\, B_i .$$

4 - Le module de Dieudonné.

Soit G un groupe formel. J'appelle module de Dieudonné de G, et je note $M(G)$ le module des morphismes de G dans CW_1 :

$$M(G) = \mathrm{Mor}(G, CW_1) .$$

C'est un module à gauche sur l'anneau $\mathrm{End}(CW_1)$ des endomorphismes du groupe CW_1. Si je note W_k l'anneau des vecteurs de Witt à coeff. dans k et $D_k = W_k[F,V]$ l'anneau (de Dieudonné) non commutatif usuel il se trouve, miracle, que $\mathrm{End}(CW_1)$ s'identifie à D_k.

Exemples:

a) si G est un groupe du type de ceux regardés par Manin, $M(G)$ s'identifie au module de Dieudonné défini par Manin (cf plus loin).

b) $M(CW_1) = W_k[F,V]$, $M(CW_2) = W_k[[F]][V]$, $M(CW_3) = W_k[F][[V]]$, $M(CW_4) = W_k[[F,V]]$.

Remarques:

a) En fait $M(G)$ est non seulement un D_k-module mais aussi un W_k-module topologique, séparé et complet (pour la topologie de la convergence simple). Si on est courageux, on peut refaire toute la théorie avec le foncteur contravariant M. Si on est un tout petit peu optimiste, on peut se dire que M est une antiéquivalence entre la catégorie des groupes formels dont la partie étale est comme on pense (pas de $\mathbb{Z}/l\mathbb{Z}$, avec $l \neq p$) et celle des D_k-modules, W_k-topologiques, qui...

b) Mais on peut aussi dire qu'on s'en fout et, par exemple, se contenter des groupes qui sont limite inductive de groupes finis : on obtient alors les D_k-modules, W_k-profinis (i.e. limite projective de D_k-modules qui sont de longueur finie sur W_k).

c) Par exemple, CW_4 est bien lim. ind. de groupes formels finis : c'est la lim. des vecteurs de Witt de longueur finie. Si j'avais travaillé avec CW_4 j'aurais perdu à la fois la partie étale et la partie multiplicative.

d) Le groupe CW_3 s'interprète bien : c'est la limite inductive des complétés formels des vecteurs de Witt de longueur finie. Moralement, c'est avec CW_3 que Manin travaille, ce qui revient à éliminer la partie multiplicative.

e) Si j'ai bien compris, moralement, Barsotti travaille avec CW_2 . S' en est bien ainsi, il doit perdre la partie étale.

Peut-être vas-tu me dire que c'est bien joli mais que CW_1 n'est pas très maniable parce que l'algèbre B_1 ne s'écrit pas de manière agréable. A cela deux réponses :

La première (c'est comme cela que je faisais avant) : Soit B_1' le complété de B_0 pour la topologie définie par les idéaux $\underline{m}^r \cap \underline{v}^s$. C'est une sous-algèbre de B_1 qui n'est pas profinie mais qui se décri commodément comme sous-algèbre de B_4 : avec des notations évidentes, un élément $\lambda = \sum_{i \in \mathbb{N}(-\mathbb{N})} a_i X^i$ est dans B_1' si et seulement s'il vérifie les deux conditions suivantes :

- pour tout entier s , on a $a_i = 0$ pour presque tout i avec $|i| \leq$
- pour tout entier s , λ mod. $\underline{v}^s$ (que je peut considérer comme un élément de $k[[X_{-1}, X_{-2}, .., X_{-s}]]$) est un polynôme.

Alors $B_1' \hat{\otimes} B_1'$ s'identifie à une sous-algèbre de $B_1 \hat{\otimes} B_1$ qui se trouve contenir les $\Delta(X_{-n})$. Ce qui fait qu'on peut dire que B_1' est une "bi gèbre topologique" , d'où un foncteur en groupes (sur les algèbres topologiques) CW_1' et je peux remplacer CW_1 par CW_1' (autrement dit un morphisme continu de B_1 dans A , si A est une algèbre profinie, c'est la même chose qu'un morphisme continu de B_1' dans A).

OK ! Je ne suis pas convaincu que ce que je viens de raconter éclaire la situation. Cela doit plutôt expliquer pourquoi ce que je racontai avant était épouvantable !

La deuxième est l'objet du numéro suivant :

5 - Le module de Dieudonné: traduction terre à terre.

Soit $A = \varprojlim A_i$ (avec les A_i finis (et les applications de transition surjective, ce qui est toujours possible)) une algèbre profinie. A quoi ressemble le groupe abélien $CW_1(A)$, qui est en fait un D_k-module ? Traduisons :

- comme ensemble, c'est l'ensemble des suites d'éléments de A

$$(\ldots, x_{-n}, \ldots, x_{-2}, x_{-1})$$

qui vérifient la condition :

" pour tout i , les images des x_{-n} dans A_i sont presque toutes dans le radical de Jacobson " .

Si la partie étale de G est finie, la condition se simplifie :

" presque tous les x_{-n} sont dans le radical de Jacobson de A " .

- comme groupe, l'addition de (x_{-n}) avec (y_{-n}) est (z_{-n}) donnée par

$$z_{-n} = \lim S_m(x_{-n-m},..,x_{-n},y_{-n-m},..,y_{-n}) \ .$$

- pour la structure de D_k-module, il suffit de savoir que

$$V((x_{-n})) = (x_{-n-1}) \quad , \quad F((x_{-n})) = (x^p_{-n}) \quad ; \text{ si } \hat{a} \text{ est le}$$

représentant multiplicatif dans W_k de l'élément a de k on a

$$\hat{a}((x_{-n})) = (a^{p^{-n}} x_{-n})$$

(on peut s'amuser à écrire la formule de la multiplication par un élément quelconque de W_k en utilisant les polynômes qui définissent la multiplication dans les vecteurs de Witt).

Enfin si $G = \mathrm{Spf}\, A$ est un groupe formel, $M(G)$ apparaît comme un sous-D_k-module de $CW_1(A)$

$$M(G) = \{ (..,x_{-n},..,x_{-1}) \in CW_1(A) \mid (\Delta(x_{-n})) = (x_{-n} \hat{\otimes} 1) + (1 \hat{\otimes} x$$

(où Δ désigne le coproduit $A \to A \hat{\otimes} A$).

6 - La construction de Manin (de préférence racontée par Demazure).

Il est à peu près immédiat que si $G = \varinjlim G_i$ alors $M(G) = \varprojlim M(G_i)$ et que $M(G \times H) = M(G) \oplus M(H)$. Si on a montré que, pour un groupe fini, le module du dual c'est le dual du module, et si on regarde toutes les constructions de modules de Dieudonné données par Demazure dans son petit "lecture notes", on voit qu'on est ramené à montrer que

si G est un groupe fini unipotent, $M(G)$ s'identifie au module construit par Manin.

Ce n'est pas malin : on voit que ce que fait Manin revient à travailler dans CW_3 , i.e. a se limiter aux covecteurs dont les composantes sont nulles à partir d'un certain rang : comme pour un groupe uni-

potent fini $V^s = 0$, pour s assez grand, on ne rajoute rien en travaillant avec CW_1 .

La seule chose qui n'est pas tout à fait triviale est de montrer que si G est un groupe fini, alors $M(D(G)) = M(G)^*$ (notations de Demazure!). Je connais une démonstration dégueulasse que je vais t'épargner, mais c'est clair que cela doit pouvoir se faire sans se salir les mains : une autre fois! (mais le point essentiel pour une telle démonstration me semble être que le module de Dieudonné du complété formel de $\underline{Z}$, dual du groupe multiplicatif est K/W_k (si K est le corps des fractions de W_k).

7 - Le module des "presque-logarithmes".

Aujourd'hui je vais me limiter au cas d'un groupe formel connexe et lisse. Soit $G = \mathrm{Spf} A$. Je choisis des coordonnées et j'ai

$$A = k[[(X_i)_{i\in I}]] \quad \text{(en abrégé } k[[X]]\text{)},$$

et le coproduit Δ est donné par une famille de séries formelles $\Gamma(X,Y) = (\Gamma_i(X,Y))_{i\in I}$.

Soit K le corps des fractions de W_k . L'anneau $K[[X]]$ n'a pas de mal à être un module sur W_k . Je fais opérer F dessus par (notation évidentes)

$$F(\sum\nolimits' a_i X^i) = \sum\nolimits' \sigma(a_i) X^{ip} \quad \text{(où } \sigma \text{ est le Frobenius abs.)}$$

Je pose

$$\mathcal{W}(A) = \{ \varphi \in K[[X]] \mid \partial\varphi/\partial X_i \in W_k[[X]] \text{ , pour tout } i \} .$$

C'est un sous-$W_k[F]$-module de $K[[X]]$ qui contient $W_k[[X]]$. Je note $N(A)$ le $W_k[F]$-module quotient $\mathcal{W}(A)/W_k[[X]]$.

Théorème : Le quotient $N(A)$ est canoniquement isomorphe à $CW_{\hat{}}(A)$.

(Remarque: on a $pN(A) \subset FN(A)$ et F est injectif sur $N(A)$, donc V opère bien sur $N(A)$).

La démonstration consiste à construire un homomorphisme Θ de $CW_{\hat{}}(A)$ dans $K[[X]]/W_k[[X]]$, puis à vérifier que Θ est injectif et d'image $N(A)$. Voici comment Θ se construit : soit

$x = (\ldots, x_{-n}, \ldots, x_{-2}, x_{-1})$ un élément de $N(A)$.

Pour chaque n , je choisis un relèvement $\hat{x}_{-n}$ de x_{-n} dans $W_k[[X]]$

La série

$$p^{-1}x_{-1}^{p} + p^{-2}x_{-2}^{p^2} + \ldots + p^{-n}x_{-n}^{p^n} + \ldots$$

converge dans $K[[X]]$. Alors $\Theta(x)$ est tout simplement sa réduction modulo $W_k[[X]]$, qui se trouve ne pas dépendre des choix des relèvements.

Maintenant soit $\mathcal{B} = k[[(Z_j)_{j\in J}]]$ (en abrégé $k[[Z]]$) un autre anneau de séries formellles à coefficients dans k . Soit $\varphi \in N(A)$ et soit $f = (f_i)_{i\in I}$ une famille de séries formelles, sans termes constan en les Z_j . Soit $\hat{\varphi}$ un relèvement de φ dans $\mathcal{W}(A)$ et soit $\hat{f}$ un relèvement de f dans $W_k[[Z]]$. Il est immédiat que $\hat{\varphi}(\hat{f})$ est dans $\mathcal{W}(\mathcal{B})$ et que sa réduction modulo $W_k[[Z]]$ est un élément $\varphi(f)$ de $N(\mathcal{B})$ qui ne dépend pas du choix des relèvements de φ et de f .

Avec ces notations, $M(G)$ se caractérise comme le sous-D_k-module de $N(A)$

$$M(G) = \{ \varphi \in N(A) \mid \varphi(\Gamma(X,Y)) = \varphi(X) + \varphi(Y) \} .$$

Si tu préfères, tu peux dire que, si $\hat{\Gamma}(X,Y)$ désigne une famille de séries formelles à coefficients dans W_k qui relève la famille $\Gamma(X,Y)$, alors $M(G)$ est le quotient de

$$\mathcal{M}(G) = \{ \psi \in K[[X]] \mid \psi(\Gamma(X,Y)) - \psi(X) - \psi(Y) \in W_k[[X,Y]] , \ \partial\psi/\partial X_i \in W_k[[X]] \text{ , pour tout } i \}$$

par $W_k[[X]]$.

Remarque : Comme ici le groupe formel est connexe, je peux considérer $M(G)$ comme un module sur $W_k[[F]][V]$. D'ailleurs j'aurais pu travailler avec CW_2 dont l'anneau des endomorphismes est $W_k[[F]]\{V\}$. Cela aurait donné le même $M(G)$ et aurait changé légèrement $N(A)$ (il faut se limiter aux séries formelles à coeff. dans K sans termes constants ce qui permet de considérer déjà $N(A)$ comme un $W_k[[F]]\{V\}$ -module).

8 - Compléments.

Je t'écrirai bientôt (?) une autre lettre pour te raconter les chose suivantes :

- En quel sens le module de Dieudonné des "presque-logarithmes" est le

dual du module des courbes p-typiques de Cartier.

- Comment la construction du module des "presque-logarithmes" si on n suppose plus G connexe (i.e. si $G = \mathrm{Spf}\, A_{et}[[(X_i)_{i\in I}]]$, avec A_{et} algèbre étale) : ce n'est pas très malin : si $A_{et} = \prod k_j$ (les k_j de corps) et si, pour tout j , K_j est le corps des fractions de W_{k_j} , il suffit de remplacer K dans ce qui précède par le produit des K_j Ce n'est pas une construction "gratuite" : cela permet de faire rentre dans les groupes étudiés les groupes p-divisibles et, en particulier, d'avoir une notion de dualité.

- Comment on peut, à partir du module des "presque-logarithmes", clas sifier et construire explicitement les différents relèvements sur W_k d'un groupe formel (comp. connexe lisse) sur k donné par son module de Dieudonné (dans le cas connexe, au langage près, cela revien à faire ce que fait Honda).

- Comment certains des résultats de Tate s'interprètent dans le langa ge des "presque-logarithmes".

ò o ò

Et puis, si tu n'en as pas marre, je t'écrirais aussi une lettre où je te raconterai les points d'ordre fini pour un groupe connexe de dimension 1 et hauteur 2 , avecaapplications aux courbes elliptiques (mais je pense t'écrire celle-ci avant l'autre !).

Je te renvois en même temps le preprint de Cox sur les groupes for- mels. Je n'ai pas regardé de près. Je crois que les groupes qu'il cons truit l'ont aussi été par Honda (J.Math.Soc.Japan,22,1970,p.213-246), et d'ailleurs en dimension quelconque alors que Cox le fait en dimen- sion un . Ce qu'il semble faire en plus c'est dire exactement quels so les groupes qu'on obtient par ce procédé : ainsi c'est plus clair que dans Honda, et je ne sais pas pourquoi Honda ne l'a pas présenté comme cela.

Nous avons retenu l'appartement à Val-d'Isère (La Daille) du 4 au 15 avril . Je crois que tu devrais repousser de quelques jours ton o- pération ! En principe Hyman Bass doit venir au début (i.e. jusqu'à

Bourbaki). Il y aura peut-être Michèle Lynch et un ou deux Raynaud (une partie du temps). je ferai l'aller et retour de Paris les 8 et 9 pour le comité con ; mais Laurence restera certainement fidèle au poste !

En tout cas, on t'attend à Grenoble le 19 mars au soir (je ferai peut-être un saut à Paris d'ici là pour une thèse de 3° cycle) en espérant que la neige voudra bien te faire honneur.

Amitiés à ta femme et à Claudine,

Salut

Jean-Marc Fontaine