Jean-Marc Fontaine
Department of Mathematics
Jeffery Hall

QUEEN'S UNIVERSITY
KINGSTON, ONTARIO
CANADA

Algebra Group
Secretary: A. Geramita

Le 29 novembre 1974

Cher Serre,

Je n'ai pas de machine à écrire ici. En plus j'ai l'impression de ne pa
avoir appris l'anglais, mais d'avoir oublié le français. Aussi j'espère que je ne
pas trop te faire souffrir.

Nous partons le 7 décembre pour Princeton où nous arriverons sans doute a
tard parce que la <<mise en route>> risque d'être assez longue et qu'on fer
peut-être une halte chez Bass pour laisser une partie des bagages. On reste à
Princeton les 8, 9 et 10 et on rentre à New-York le 11. On compte rester tra
quatre jours chez Bass et rentrer à Paris (mais pour le moment on a des pl
retenues pour le 19).

Je crois que je n'aurai pas le courage de faire un crochet harvardien au
la VW de Lichtenbaum qui ne marche pas trop bien et toute la petite fam
qui est un vrai déménagement! D'ailleurs, si je comprend bien, le 7 tu [redacted]
seras plutôt du côté de Princeton ou New-York. Nous nous verrons peut-ê
quelque part par là, et rien à Paris (où nous resterons jusqu'au 26).

Laurence commence à en avoir ras le bol du plat pays ontarien. En
plus, on a fait une virée à Montréal qui a plutôt foiré : on était chez
Wilber Jonsson (*) (copain de Bill + Michel) qui est très gentil mais qui venait
d'emménager : a big mess, avec toute sorte de peintures et de produits qui pue
et l'impossibilité pour Isabelle de poser le pied par terre. Au bout de deux jou
Laurence a décidé de ramener le bébé <<malade>>. Bien lui en a pris

(*) tu logeas chez lui naguère, paraît-il : mais c'était un autre appartement et il n'y était pas.

d'ailleurs, car le lendemain il y a eu un "big snow storm" : je n'avais jamais vu un truc pareil et Montréal était à peu près paraly J'avais réussi à aller jusqu'à Mac Gill le matin et j'ai passé la jo dans une espèce de forteresse d'où on ne pouvait pratiquement ni entrer n sortir. J'ai pu me traîner péniblement jusqu'à la gare, le soir, escorté par Labute : le train avait trois heures de retard. Mais j'ai été content de faire la connaissance de Labute ... Et la veille au soir on avait quand même dîné dans un très bon restaurant (mais sans Lauren

Quand à moi, je ne suis vraiment remis au boulot (ça a été long, mais maintenant ça y est). J'ai des grands morceaux de rédaction d'un machin bien au point et j'aurai bien aimé avoir un mois de plus pour porter avec une rédaction complète.

En tout cas, j'ai l'impression d'avoir la matière d'un cours relativ consistant, avec comme plan :

1) Classification des groupes formels en car. p (ie des schéma en groupes finis d'ordre une puissance de p, des groupes de Lie formel et des groupes p-divisibles) : construction du module de Dieudonné avec des correcteurs.

2) Classification des groupes de Lie formels et des groupes p-divisibl sur les vecteurs de Witt (ie. traduction des résultats de Honda dans le langage des modules de Dieudonné + petite généralisation).

3) Classification des p-groupes finis (ie des schémas en groupes commutatifs affine dont l'algèbre affine est libre de rang une puissance de sur les vecteurs de Witt : cf explications plus loin

4) Application de 2) et 3) à l'action de Verlois sur les points d'un p-divisible connexe de dim. 1 sur les vecteurs de Witt.

5) (Si on n'en a pas marre avant) : application aux courbes elliptiques

A propos des cours Reeot, j'ai reçu juste avant la grande grève d la poste en France, une lettre de Mademoiselle Baladi (du collège) m demandant quand je comptais parler et un tas d'autres renseignements. La datait du 1er octobre mais avait été transité par Grenoble et cela avait pris du tem et la demoiselle disait que c'était urgent! Mais je ne vois guère d'autre solut que de prendre contact avec elle dès mon retour à Paris. Et j'aimerais bien fixer dates et horaires en accord avec d'éventuels auditeurs (sinon ce groupes comm tifs sur les vecteurs de Witt >> ne paraît un titre possible).

+

Je voudrais maintenant te parler un peu des ces p-groupes finis sur les vecteurs de Witt. Tu te souviens que je t'avais dit que je pensais que tout homomorphisme sur les fibres génériques provenait d'un homomorphisme sur les groupes (si $p \neq 2$; si $p=2$, c'est gaux) [illegible] groupes [illegible]). C'est que j'étais entrain de construire une classification de ces groupes et que c'était une conséquence du résultat escompté. Tu m'as un peu découragé, mais ça n'a sans doute pas été un mal parce que, d'u part ça m'a incité à une grande prudence, d'autre part ça m'a un peu vexé, donc un peu stimulé. Maintenant, je ne donnerais pas ma tête à couper du résultat, parce qu'il ne le mérite pas, mais j'en suis vraiment sûr. Il entre que la catégorie des p-groupes finis sur un corps parfait de les vecteurs de Witt d'un corps parfait de caract. p (et toujours $p \neq 2$, sinon il faut se restre dre aux groupes unipotents) est abélienne, ce qui entraîne à peu près trivialement ce que je te disais.

+

Je vais donc essayer de t'expliquer le résultat, sans machine à écrire, et sans pouvoir faire plus ici que de donner quelques idées su

les démonstrations.

0. Notations et terminologie

p = nombre premier fixé, k = corps parfait de car. p, $A = W(k)$ = vecteurs de Witt à coeff dans k, on a $p A$, K = corps des fractions de A, σ le Frobenius absolu sur $k, A, K, -$, $O = A[F, V]$ l'anneau non commutatif habituel.

Pour tout anneau commutatif B, avec élément-unité, un B-anneau R est un anneau commutatif, avec élément-unité, muni d'un homomorphisme unitaire $i_R : B \to R$.

Je dis que R est un B-anneau fini si i_R fait de R un B-module libre de rang fini (un A-anneau fini n'est donc jamais de longueur finie).

Si $B = k$ ou A, un groupe formel sur B est un foncteur en groupes commutatifs sur la catégorie des B-anneaux de longueur finie qui est de la forme

$$G(S) = \mathrm{Hom}_{\mathrm{cont}}(R, S)$$

où $R = O(G)$ est un B-anneau profini.

1. Les p-groupes finis sur k.

On peut construire un foncteur en groupes commut. sur la catégorie des k-anneaux finis, qui est en fait un groupe formel, CW_k, le groupe formel des vecteurs de Witt, et qui est définie ainsi :

si R est un k-anneau fini

$$CW_k(R) = \{ \underline{a} = (\cdots a_{-n}, \cdots, a_{-1}, a_0) \mid a_{-n} \in R \text{ pour presque tout } n,\ a_n \in \text{radical de } R \}$$

Si $S_0(x_0, y_0) = x_0 + y_0$, $S_1(x_0, x_1, y_0, y_1)$, $\cdots$, $S_m(x_0, x_1, \cdots x_m; y_0, y_1 \cdots y_m)$, $\cdots$ sont les polynômes qui définissent l'addition dans les vecteurs de Witt, l'addition dans $CW_k(R)$ est définie par (avec des not. évidentes)

$$\underline{a} + \underline{b} = \underline{c}$$

et $c_{-n} = \lim_{m \to \infty} S_m(a_{-n-m}, a_{-n-m+1}, \cdots a_{-n}, b_{-n-m}, \cdots b_{-n})$,

ce qui a un sens, car on peut montrer que la suite est, en fait, stationnaire

L'anneau des endomorphismes de CW_k semble être assez compliqué, mais il contient $D = A[F,V]$. La structure de D-module sur $CW_k(R)$ est définie par :

- si $\lambda \in k$ et $\tau(\lambda)$ est le représentant multiplicatif dans les vecteurs de Witt

$$\tau(\lambda)\underline{a} = (\cdots \quad \sigma^{-n}(\lambda)a_{-n}, \cdots, \sigma^{-1}(\lambda)a_{-1}, \lambda a_0)$$

et on a

$$\begin{cases} F\underline{a} = (\cdots, a_{-n}^p, \cdots a_{-1}^p, a_0^p) \\ V\underline{a} = (\cdots a_{-n+1}, \cdots a_{-2}, a_{-1}) \end{cases}$$

Maintenant si G est un p-groupe fini sur k, je peux le considérer comme un groupe formel sur k, et j'définis le module de Dieudonné de G comme étant le D-module à gauche

$$M(G) = \mathrm{Hom}(G, CW_k)$$

Si j'emploie l'expression « D-module fini » pour D-module à gauche, de longueur finie en tant que A-module, alors $M(G)$ est un D-module fini et c'est « presque » le module de Dieudonné défini par Gabriel et Manin (si je note G^σ le groupe déduit de G par l'extension des scalaires $\sigma : k \to k$, avec $\sigma(a) = a^p$, le module de Dieudonné de G au sens de Gabriel-Manin est canoniquement isomorphe, avec mes notations, à $M(G^\sigma)$).

En particulier M est un foncteur contravariant pleinement fidèle qui induit une antiéquivalence entre la catégorie des p-groupes finis sur k et celle des D-modules finis.

Remarque enfin que si $O(G) = R$, alors

$$M(G) = \{ \underline{a} \in CW_k(R) \mid \Delta\underline{a} = \underline{a} \otimes 1 + 1 \otimes \underline{a} \}$$

(où, si $\Delta : R \to R \otimes R$ est le coproduit, $\Delta\underline{a}$, $\underline{a} \otimes 1$ et $1 \otimes \underline{a}$ sont des éléments de $CW_k(R \otimes R)$ définis par

$$\begin{cases} \Delta\underline{a} = (\cdots \quad \Delta a_{-n}, \cdots \Delta a_{-1}, \Delta a_0) \\ \underline{a} \otimes 1 = (\cdots \quad a_n \otimes 1, \cdots, a_{-1} \otimes 1, a_0 \otimes 1) \\ 1 \otimes \underline{a} = (\cdots, 1 \otimes a_{-n}, \cdots, 1 \otimes a_{-1}, 1 \otimes a_0) \end{cases}$$

2. Les WD-systèmes (je ne suis pas particulièrement fier de la terminologie qui va suivre).

Définition. Soit M un O-module fini et soit M_0 un sous-A-module de M. Je dis que M_0 est un W-facteur de M si les conditions suivantes sont satisfaites :

i) $FM \cap M_0 = pM_0$;

ii) $M_0/pM_0 = M/FM$;

iii) La restriction de V à M_0 est injective.

Il est clair qu'il existe des O-modules finis qui n'admettent pas de W-facteurs. Une condition nécessaire (mais pas suffisante si M est d'exposant $> p$) pour que M admette un W-facteur est que la suite

$$0 \to M/VM \xrightarrow{F} M/pM \to M/FM \to 0$$

soit exacte.

Définition. Un WD-système est la donnée d'un couple (M_0, M) où M est un O-module fini et M_0 un W-facteur de M.

Les WD-systèmes forment une catégorie si on définit un morphisme $\varphi : (M_0, M) \to (N_0, N)$ comme étant un homomorphisme de O-modules $\varphi : M \to N$ tel que $\varphi(M_0) \subset N_0$.

Il n'est pas très difficile de montrer que la catégorie des WD-systèmes est abélienne.

3. L'homomorphisme w. (Je pose $CW = CW_k$: pas de confusion possible car k est fixé)

Pour tout A-anneau fini R, je pose $R_K = R \otimes_A K$, $R_k = R \otimes_A k = R/pR$.

On peut définir une application $w : CW(R_k) \to R_K/R$ de la façon suivante :

Si $\underline{a} = (\dots a_{-n}, \dots, a_0) \in CW(R_k)$, on choisit des $\hat{a}_{-n}$ dans R qui relèvent les a_{-n}. Si on pose

$$w_n(\underline{a}) = \frac{\hat{a}_0}{p} + \frac{\hat{a}_{-1}^{\,p}}{p^2} + \dots + \frac{\hat{a}_{-n}^{\,p^n}}{p^{n+1}},$$

les $w_n(\underline{a})$ sont des éléments de R_K qui dépendent du choix des relèvements. Le fait que presque tous les a_n sont dans le radical de R_k implique que la suite de $w_n(\underline{a})$ converge, dans R_K, vers un élément $w_\infty(\underline{a})$. Maintenant il est trivial que l'image $w(\underline{a})$ de w_∞ dans R_K/R ne dépend plus du choix des relèvements. On a donc une application bien définie

$$w : CW_A(R_k) \to R_K/R.$$

Il n'est pas difficile de montrer que w est A-linéaire et je noterai $CW_0(R)$ le noyau (c'est un sous-A-module de $CW(R_k)$ qui dépend de R et pas seulement de R_k).

Par exemple, si R est étale, w est un isomorphisme, et, en particulier, $CW_0(R) = 0$.

4. Le WO-système d'un p-groupe fini sur A.

Soit G un p-groupe fini sur A et soit $R = O(G)$. Donc R est un anneau commutatif et est aussi un A-module libre de rang une puissance de p. Par extension des scalaires on associe à G un p-groupe fini $G_k = G \otimes_A k$ sur k, de même ordre, et $O(G_k) = R_k$. Je peux donc considérer le module de Dieudonné $\Pi = M(G_k) = \mathrm{Hom}(G_k, CW)$ de G_k, qui est un D-module fini. C'est un sous-O-module de $CW(R_k)$. Je peux donc considérer la restriction de w à $M(G_k)$ qui est une application A-linéaire

$$\Pi(G_k) \longrightarrow R_K/R$$

Je note $M_0(G) = M_0 = CW_0(R) \cap \Pi(G_k)$ le noyau et $\bar{\Pi}(G) = \bar{M} = w(\Pi(G_k))$ l'image.

Théorème : le couple (M_0, Π) est un WO-système.

Pour démontrer ce théorème, on commence par montrer le lemme suivant :

Lemme : Soit $\underline{a}$ un élément de $CW_0(R)$. Si $V\underline{a} \in M(G_k)$, alors $\underline{a} \in M_0(G)$

La démonstration de ce lemme n'est pas très difficile. Il faut regarder de près comment tout est défini.

En appliquant trois fois ce lemme, on démontre alors très facilement que

i) $FM \cap \Pi_0 = p M_0$;

~~ii) $\ker(p|_\Pi) = \ker p|_{\Pi_0} \oplus \ker V$~~

ii) dans Π, $\ker p = \ker p|_{\Pi_0} \oplus \ker V$

iii) dans M, $\ker F \subset \operatorname{Im} V$.

Et il est facile de voir que ces trois propriétés caractérisent les WO-systèmes.

5. Classification des p-groupes finis sur A.

Il est clair que $G \longmapsto (\Pi_0, \Pi)$ est un foncteur contravariant de la catégorie des p-groupes finis sur A dans la catégorie des WO-systèmes.

Maintenant, parce que je vais raconter dans la suite, il faut supposer, si $p=2$ que les groupes considérés sont unipotents et, par conséquent, que le Verschiebung est nilpotent sur les O-modules finis.

Théorème : Le foncteur $G \longrightarrow (\Pi_0, \Pi)$ est pleinement fidèle et induit une autre équivalence de la catégorie des p-groupes finis sur A sur la catégorie des WO-systèmes.

La démonstration se fait en plusieurs étapes :

1ère étape : Soit S une A-algèbre finie. Alors l'homomorphisme canonique

$$G(S) \longrightarrow G(S_k) = G_k(S_k)$$

est injectif.

~~Un élément de $G(S)$~~ Un élément de $G(S)$ est un homomorphisme $\varphi : R \to S$ (si $R = O(G)$). ~~Tout élément de $G(S)$ est déterminé~~ auquel correspond $\varphi_k : R_k \to S_k$.

Tout élément de $G(S)$ est d'ordre une puissance de p et comme la réduction modulo p commute à la multiplication par p, on peut supposer que $p\varphi = 0$. Soit I_R l'idéal d'augmentation de R. On voit qu'il suffit de montrer que si $(p\varphi)(I_R) = 0$ et $\varphi(I_R) \subset pS$, alors $\varphi(I_R) = 0$.

C'est un petit calcul ~~[illegible]~~ on procède par l'absurde en regardant comment est définie la multiplication par p, par itération du coproduit.

C'est d'ailleurs un résultat un peu plus général qui reste ~~[illegible]~~ vrai en remplaçant les vecteurs de Witt par une extension assez peu ramifiée (il faut que $e < p-1$).

Ce petit résultat a deux conséquences très importantes pour la suite:

- la première, c'est qu'on peut considérer $G(S)$ comme un sous-groupe de $G_k(S_k)$;
- la deuxième, c'est que le foncteur $G \to G_k$ est fidèle, donc aussi le foncteur $G \to M(G_k)$, donc a fortiori le foncteur $G \to (\Pi_0, \Pi)$.

2ème étape. On considère toujours G, $\Pi_0 = \Pi_0(G)$, $\Pi = \Pi(G_k)$, $R = O(G)$, et S un A-anneau fini. Si $\lambda \in G_k(S_k)$, λ est un homomorphisme de R_k dans S_k, auquel correspond un homomorphisme $CW(\lambda) : CW(R_k) \to CW(S_k)$. Si λ est la réduction modulo p d'un élément φ de $G(S)$, on voit que $CW(\lambda)$ envoie $CW_0(R)$ dans $CW_0(S)$, et par conséquent M_0 dans $CW_0(S)$. Donc $G(S)$ s'identifie à un sous-groupe de

$$(*) \quad G'(S) = \{ \lambda \in G_k(S_k) \mid CW(\lambda)(M_0) \subset CW_0(S) \}$$

~~On voudrait que pour achever la démonstration du théorème, il suffise de~~ montrer ~~que l'on a~~ $G(S) = G'(S)$ parce que

~~- si on connaît M, on connaît G_k (et il existe toujours)~~

3ème étape : On se donne un WD-système (Π_0, Π) et on suppose M connexe, i.e. que Π est le module de Dieudonné d'un groupe connexe sur k. On construit un p-groupe fini G' sur A qui a les vertus suivantes :

→ $(M_0(G'), \Pi(G'_k)) \simeq (\Pi_0, \Pi)$

→ pour toute A-anneau fini S, $G'(S) = \{ \lambda \in G'_k(S_k) \mid CW(\lambda)(\Pi_0) \subset CW_0($

Je construis G' comme un sous-groupe d'un groupe p-divisible sur A et cette construction est assez pénible et utilise la classification des groupes p-divisibles sur A (que je connais et qui n'est pas autre chose dans le cas connexe que la traduction en langage adéquat des travaux de Honda) et aussi la possi

lité de relever M en le module de Dieudonné d'un groupe p-divi sur k avec des contraintes supplémentaires portant sur Π_0. Cela utilise également l'analogue de la 1ère étape pour les groupes p-divisibles, qui est un exercice facile.

4ème étape : le théorème pour les groupes connexes est alors une conséqu des trois premières étapes. En effet :

- étant donné G, et (Π_0, Π), alors la deuxième étape montre que G est un sous-groupe du groupe G' construit dans la troisième (car si l'on suppose que l'algèbre affine de G est un A-anneau fini, il suffit, par Yoneda de connaître $G(S)$ pour S A-anneau fini) et il est facile de voir que l'inclusion $G \hookrightarrow G'$ correspond à un isomorphisme

$$G_k \xrightarrow{\sim} G'_k$$

sur les réductions modulo p, donc $G = G'$ et la formule (*) donne $G(S)$ en fait.

- La première étape montre que le foncteur $G \to (\Pi_0, \Pi)$ est fidèle. On sait que $G(S)$ est donné par la formule (*) on déduit facilement qu'il est pleinement fidèle, et réciproquement, à tout couple (Π_0, Π) correspond un p-groupe fini d'après la troisième étape.

5e étape : le théorème est trivialement vrai pour les groupes étales : si Π est le module de Dieudonné d'un p-groupe étale sur k, alors $\Pi/F\Pi = 0$, donc $\Pi_0 = 0$, et un W-système, dans ce cas, est juste la donnée de M. On sait bien qu'il y a équivalence entre groupes finis étales sur k et groupes finis étales sur A.

6e étape : On recolle le morceau connexe et le morceau étale en utilisant la formule (*). Il n'y a pas de difficultés.

Je ne sais pas trop ce que tu auras pu tirer de ce que je viens de te raconter. Je voudrais conclure par :

6. Une interprétation de M_0 et $\bar{\Pi}$.

Soit G un p-groupe qui agit sur A, soit $R = O(G)$ et I_R l'idéal d'augmentation de R. Pour tout A-module Λ, je pose

$$\begin{cases} t_G^*(\Lambda) = (I_R/I_R^2) \otimes_A \Lambda \\ t_G(\Lambda) = \mathrm{Hom}_A(I_R/I_R^2, \Lambda) \end{cases}$$

Il est facile voir que

- $t_G^*(A) = I_R/I_R^2 \simeq \Omega_A^1(R)$, module des A-différentielles de l'anneau R, invariantes à gauche.

~~Si $D(G)$ désigne le dual du groupe G, $t_{D(G)}(K/A)$ est canoniquement isomorphe à Der~~

- $t_G(K/A)$ est canoniquement isomorphe au module des A-dérivations de R à valeurs dans K/A (avec la structure de R-module définie par l'augmentation).

Si à G on associe son WD-système (Π_0, Π), il n'est pas très difficile de montrer que le quotient $\bar{\Pi} = \Pi/M_0$ s'identifie à

$$\{a \in R_K \mid \Delta a \equiv a \otimes 1 + 1 \otimes a \bmod R\xi\} / R$$

ou encore à $t_{D(G)}(K/A)$, si $D(G)$ désigne le dual de G.

On peut aussi construire une application $\delta : \Pi_0 \to \Omega_A^1(R)$.

Si $\underline{a} = (\ldots a_{-n}, \ldots a_0) \in \Pi_0$, cela signifie que l'on peut choisir des relèvements $\hat{a}_n$ des a_n dans R de telle sorte que

$$\sum_{n=0}^{\infty} \frac{\hat{a}_{-n}^{p^n}}{p^n} = 0$$

On suppose un tel choix fait et on pose

$$\delta(\underline{a}) = \sum \hat{a}_{-n}^{p^n - 1} d\hat{a}_{-n}$$

Il se trouve que $\delta(\underline{a})$ ne dépend pas du choix des $\hat{a}_{-n}$ tels que $\Sigma' p^{-n} \hat{a}_{-n} p^n = 0$ et que δ est en fait un isomorphisme de M_0 sur $\Omega^g_A(R) \simeq t^*_G(A)$.

Finalement la suite exacte

$$0 \to M_0 \to M \to \bar{M} \to 0$$

peut donc se réinterpréter comme une suite exacte

$$0 \to t^*_G(A) \longrightarrow M(G_k) \longrightarrow t_{D(G)}(K/A) \longrightarrow 0$$

Et voilà.

+

Bon courage pour Borel ! Shame on you pour Arcata !

Amitiés. A bientôt

Jean-Marc Fontaine