UNIVERSITÉ PARIS XI
U.E.R. MATHÉMATIQUE
91405 ORSAY FRANCE

N^os 149 – 75.42

Bert DITTERS

GROUPES FORMELS

Cours 3e cycle 1973-1974

N^os 149 – 75.42

Bert DITTERS

GROUPES FORMELS

Cours 3e cycle 1973-1974

Table des matières

Introduction

La théorie des groupes formels se présente sous deux formes différentes : soit on fait des calculs (fâcheux) par la méthode directe, (Lazard, Lubin, Fröhlich, Honda, Hill, Hazewinkel) -, soit on fait des calculs (fâcheux) par la méthode indirecte ou hyperalgébrique, (Dieudonné, Manin). En tout cas on devrait se méfier d'une méthode, qui ne saurait pas donner les démonstrations des théorèmes de classification de Cartier, ceux-ci généralisant les théorèmes classiques de Dieudonné.

Dans ce travail, qui résulte d'un cours des groupes formels, donné par l'auteur à l'Université de Paris-Sud, Orsay, 1974, on se propose de démontrer les théorèmes de Cartier en utilisant la méthode hyperalgébrique. De cette façon ce travail doit être nécessairement complémentaire au livre prochainement à apparaître de Lazard, parce que malheureusement, les bourgeons n'apparaissent pas ici (Lazard, [1] p.281). La méthode suivie n'étant choisie que parce que la loi du groupe formel universel non commutatif n'est pas encore déterminée de façon suffisamment explicite, bien que son hyperalgèbre soit bien connue : elle est l'algèbre de Hopf universel des puissances divisées. Le résultat principal de classification est une classification des lois des groupes formels plutôt que des groupes formels (th. III.3.6). En faisant les raisonnements indépendants d'une base choisie on trouve la classification de Cartier. L'idée de démontrer un théorème de décomposition (th. II.6.4), qui généralise la notion "S-typique" de Cartier-Lazard au cas non commutatif ainsi qu'un théorème de Campbell-Haussdorf-Dieudonné (th. II.6.9) sur un anneau de base arbitraire était suggéré par Lazard [1]. On donne deux applications : une démonstration des conjectures d'Atkin-Swinnerton Dyer (th. V.1.4) sous une forme différente de celle, énoncée par Cartier [3] à Nice 1970, peut-être même contradictoire à cet énoncé.

L'autre application touche les rudiments d'une théorie générale, encore embryonale, des composantes fantômes (th. V.2.9). Avertissement : ce théorème se démontre à l'heure actuelle par les arguments originaux de Witt (Crelle, 176, p. 126-140, 1937), une fois les points de départ étant convenablement (même trivialement) modifiés. Pour plus de détails sur ce point, ainsi pour un résumé non-abstrait des résultats exposés ici, on pourrait consulter : Formale Gruppen, die Vermutung von Atkin-Swinnerton-Dyer und verzweigte Wittsche Vektoren, notes miméographées, Göttingen, 1975).

Finalement, ce travail donne les démonstrations des résultats, annoncés antérieurement dans Comptes Rendus, Série A, t 268, p 580-582, (1968), t 275, p 251-254 (1972), t 276, p 531-534, (1973), t 279, p 403-406, (1974) et t 279, p 443-446,(1974).

L'auteur remercie vivement tous ceux, qui en prodiguant leurs efforts - soit de caractère mathématique, soit de caractère extramathématique, (les musiciens d'Orsay sous la direction sage de Mme Suzanne Schuhl et de maître Roger Roche) ont créé une atmosphère cordiale et encourageante. En particulier il tient à exprimer sa reconnaissance sincère à Mme Bonnardel, qui a accompli sans moindre plainte la tâche ingrate de faire apparaître ce travail.

Chapitre I : Les catégories fondamentales

Le but de ce chapitre sera de rappeller certains faits connus ainsi que de fixer les notations. Pour plus de détails (et pour les démonstrations) on se réfère aux livres de

M. Demazure	p-Divisible Groups	Lect. Notes in Math. 302 (1972)
A. Fröhlich	Formal Groups	Lect. Notes in Math. 74 (1968)

cités [D] et [F].

§1. Lois de groupes formels

1.1 Soit k un anneau de base, unitaire et commutatif. On renvoie à [F], Ch.I pour ce qui concerne les anneaux de séries formelles k_n en n indéterminées $X = (X_1,\dots,X_n)$ à coefficients dans k, ainsi pour la notation vectorielle qui rend les formules plus transparentes. On notera $(k_n)^m$ la somme directe de m copies de k_n.

On rappelle que $F = F(X,Y) \in (k_{2n})^n$ est une loi de groupe formel, (bref : une loi) de dimension n sur k si

a) $F(X,0) = X$, $F(0,Y) = Y$

b) $F(F(X,Y),Z) = F(X,F(Y,Z))$

b) se justifie par a), qui implique que chaque F_i est sans terme constant. On dit encore que F est abélien, si $F(X,Y) = F(Y,X)$.

1.2 Soient F et G deux lois sur k de dimension n et m . Un morphisme $f : F \to G$ des lois est un élément $f \in (k_n)^m$ sans termes constants tel que

$$f(F(X,Y)) = G(f(X),f(Y)) \qquad (1)$$

On obtient de cette façon une catégorie $FG(k)$ des lois sur k . On notera $FG(n,k)$ la sous-catégorie pleine des lois de dimension n sur k et encore $F(n,k)$ la sous-catégorie pleine des lois abéliennes. On notera $\mathrm{Hom}_k(F,G)$ l'ensemble des flèches dans $FG(k)$. Si $\varphi : k \to k'$ est une extension de base, alors

en appliquant φ aux coefficients des séries formelles $F = F(X,Y) \in FG(k)$, on obtient de façon naturelle une loi $\varphi_* F$ sur k', d'où un foncteur covariant $\varphi_* : FG(k) \to FG(k')$.

1.3 Il existe des lois dans la nature :

a. Soit $k \in \{\mathbb{R},\mathbb{C}\}$ et soit G un groupe de Lie de dimension n sur k. Alors il est bien connu, qu'il existe un voisinage V d'élément neutre $e \in G$, un voisinage Ω de 0 dans k^n et un homéomorphisme $\varphi : V \to \Omega$ tels que si $X,Y \in V$, alors le produit $Z = XY$ appartient à V et en posant $\varphi X = (x_1,\dots,x_n)$, $\varphi Y = (y_1,\dots,y_n)$, $\varphi Z = (z_1,\dots,z_n)$ alors

$$z_i = z_i(x_1,\dots,x_n,y_1,\dots,y_n) \quad \text{pour} \quad 1 \leqslant i \leqslant n,$$

ce qui définit de façon naturelle une loi de dimension n sur k.

b. On pose $\hat{G}_a^n = X+Y$ avec $\hat{G}_{a,i}^n = X_i + Y_i$ pour $1 \leqslant i \leqslant n$. C'est une loi abélienne de dimension n sur un anneau quelconque. Si $n = 1$ on appelle $\hat{G}_a = \hat{G}_a^1$ la loi additive.

c. $\hat{G}_m = X + Y + XY \in F(1,k)$. $\hat{G}_m$ sera appelé la loi multiplicative. Noter, que si $k = \mathbb{Q}$ on a un isomorphisme $\log(1+X) : \hat{G}_m \to \hat{G}_a$, qui admet $e^X - 1$ comme inverse.

Il importe d'introduire des lois qui sont de dimension infinie sur k, ainsi que des lois qui ne sont pas triviales, de dimension zéro.

§2. Co-algèbres, co-algèbres en groupes

k sera un anneau de base. On notera $\otimes = \otimes_k$ et 1 toute application identité.

2.1 Définition : Une co-algèbre sur k est un k-module C, muni d'une application k-linéaire $d_C = d : C \to C \otimes C$, dite diagonale, satisfaisante aux conditions suivantes :

C1 : d est co-associatif.

C2 : d est co-commutatif.

C3 : Il existe une application k-linéaire $\varepsilon_C = \varepsilon : C \to k$, dite counité, de façon

unique déterminée par : $\varepsilon \otimes 1 \circ d = 1 \otimes \varepsilon \circ d = 1$ sur $C \cong k \otimes C \cong C \otimes k$. Un morphisme de coalgèbres $f : (C,d_C) \to (D,d_D)$, bref, $f : C \to D$ sera une application k-linéaire $f : C \to D$, qui satisfait à $f \otimes f \circ d_C = d_D \circ f$ et $\varepsilon_D \circ f = \varepsilon_C$ (compatibilité avec les morphismes structuraux). De cette façon les coalgèbres sur k constituent une catégorie. Dans ce qui suit on notera C_k la sous-catégorie pleine des coalgèbres sur k, qui satisfont à la condition supplémentaire (F) :

(F) : $C \in C_k$ est réunion filtrante croissante d'une suite $\{C_i \mid i \in I\}$, où I est un ensemble dénombrable d'indices, où les C_i sont des coalgèbres sur k, libres et de type fini sur k en tant que k-modules et où chaque inclusion $C_i \subset C_j$ se prolonge en une suite exacte de k-modules libres

$$0 \to C_i \to C_j \to C_j/C_i \to 0 \qquad (1)$$

Il en résulte en particulier que C est un k-module libre. Noter que, lorsque k est un corps et C est une coalgèbre sur k, alors C satisfait à (F). [D], 1.6.

2.2 C_k admet un objet final, à savoir $(k,1)$ et des produits. De façon explicite: $(C,d_C) \times (D,d_D) = (E,d_E)$. $E = C \otimes D$ et d_E se donne par le diagramme

$$d_E : C \otimes D \xrightarrow{d_C \otimes d_D} C \otimes C \otimes D \otimes D \xrightarrow{1 \otimes \sigma \otimes 1} C \otimes D \otimes C \otimes D$$

où $\sigma(c \otimes d) = d \otimes c$. On a $\varepsilon_E = \varepsilon_C \otimes \varepsilon_D$ et $C \otimes D$ satisfait à (F).

Si $k \to k'$ est une extension de base, on a un foncteur évident $C_k \to C_{k'}$, induit par $C \mapsto C \otimes_k k'$. Cette extension de base commute avec la formation des produits et avec les objets finaux.

2.3 Soit $\underline{C}$ une catégorie. On dit que $G \in \underline{C}$ est un objet groupe dans $\underline{C}$ si pour tout $X \in \underline{C}$ l'ensemble $\underline{C}(X,G)$ est muni d'une structure de groupe et si pour toute flèche $X \to Y$ dans $\underline{C}$ l'application induite $\underline{C}(Y,G) \to \underline{C}(X,G)$ est un homomorphisme pour cette structure. G sera dit commutatif, si tous les groupes $\underline{C}(X,G)$ sont commutatifs.

Lemme : Soient $\underline{C}$ une catégorie avec produits finis et un objet final e, alors les deux énoncés suivants sont équivalents :

1. G est un objet groupe dans $\underline{C}$.

2. G est muni d'un morphisme structural $m_G = m : G \times G \to G$ dans $\underline{C}$, dit multiplication, satisfaisant aux trois conditions suivantes :

a. m est associatif.

b. Il existe un $\eta_G = \eta : e \to G$ dans $\underline{C}$, dit unité, nécessairement unique, tel que $m \circ (\eta \times 1) = m \circ (1 \times \eta)$ soit l'identité sur $G \cong e \times G \cong G \times e$.

c. Il existe un $c_G = c : G \to G$ dans $\underline{C}$, dit antipodisme, nécessairement unique, tel que $m \circ c \times 1 \circ d = \eta \circ \varepsilon$.

(Ici, $d : G \to G \times G$ est le diagonal et $\varepsilon : G \to e$ la flèche unique).

Dans cette situation encore, le produit fg de f et g dans $\underline{C}(X,G)$ se donne par

$$fg : X \xrightarrow{(f,g)} G \times G \xrightarrow{m} G .$$

De façon duale on a la notion d'un objet cogroupe dans $\underline{C}$ ainsi qu'un lemme évident, si $\underline{C}$ admet sommes finies et un objet cofinal. On définit la catégorie des objets groupe dans $\underline{C}$, $G\underline{C}$ en prenant pour fléches $f : G_1 \to G_2$ dans $G\underline{C}$ celles de $\underline{C}$ qui satisfont à $m_{G_2} \circ f = f \times f \circ m_{G_1}$ et $f \circ \eta_{G_1} = \eta_{G_2}$. De façon duale on construit la catégorie des objets cogroupe dans $\underline{C}$.

2.4 On dira, que $G \in C_k$ est une coalgèbre en groupes si G est un objet groupe dans C_k. Les coalgèbres en groupes constitueront la catégorie GC_k. La sous-catégorie pleine des coalgèbres en groupes commutatifs sera notée $\mathbf{Ab}_k$, les objets de laquelle s'appellent encore bigèbres. La situation de 2.3 rendu explicite pour GC_k donne

Lemme : Soit $G \in GC_k$, alors

a. m et n définissent sur G une structure d'algèbre unitaire, associative sur k, qui est commutatif si et seulement si $G \in \mathbf{Ab}_k$.

b. Pour cette structure d'algèbre, d et ε sont des morphismes et $c : G \to G$ est un anti-isomorphisme, c'est-à-dire on a $c(xy) = c(y)c(x)$ pour $x,y \in G$ et c est bijectif dans C_k.

2.5 Exemples

a) Soit J une algèbre de Lie sur k, libre et de rang dénombrable en tant que k-module. Alors l'algèbre universelle enveloppante $U(J)$ de J est muni d'une structure d'objet dans GC_k. Si la caractéristique de k, $\chi(k)$, est un nombre premier p et si en outre J est une p-algèbre de Lie, alors l'algèbre universelle enveloppante restreinte $U_p(J)$ se trouve dans GC_k

b) Soient k un corps et Ac_k la catégorie des groupes affines commutatifs sur k, alors le foncteur $M \to \operatorname{Spec} M$ induit une anti-équivalence des catégories $Ab_k \to Ac_k$.

c) On utilise ici l'opportunité d'introduire une coalgèbre en groupes, qui jouera un rôle fondamental dans ce qui va suivre. Soit d'abord S un ensemble dénombrable. On notera $k\langle S\rangle$ l'algèbre associative non commutative libre, engendrée sur k par les éléments de S, dits indéterminés. En prenant le quotient de $k\langle S\rangle$ par l'idéal bilatère, engendrée par tous les commutateurs $[x,y] = xy - yx$ pour $x,y \in k\langle S\rangle$, on obtient l'anneau libre commutatif $k[S]$.

Soient maintenant $S = \{Z_m \mid m \in \mathbb{N}^+\}$ et $Z(k) = k\langle S\rangle$. Soit $NAlg_k$ la catégorie des algèbres unitaires associatives sur k. Alors on définit un diagonal $d : Z(k) \to Z(k) \otimes Z(k)$ dans $Nalg_k$ en posant pour $Z_m \in S$:

$$dZ_m = \sum_{o \leqslant a \leqslant m} Z_a \otimes Z_{m-b} \quad \text{avec} \quad Z_o = 1 .$$

On attache à Z_m le poids m. En prenant les sous-espaces H_n dans $Z(k)$, engendrés par les éléments qui sont isobares de poids $\leqslant n$, on voit sans peine qu'on a une structure de coalgèbre sur $Z(k)$, qui satisfait à (F). De plus la structure d'objet de $NAlg_k$ sur $Z(k)$ fait de $Z(k)$ une coalgèbre en groupes. On laisse la vérification à titre d'exercise.

On notera encore $Z(n,k)$ le sous objet dans GC_k de $Z(k)$, engendré par $\{Z_1,\ldots,Z_n\}$. Alors on a : $Z(k) = \varinjlim_n Z(n,k)$ dans GC_k. Si k restera fixé, on écrira Z et $Z(n)$ au lieu de $Z(k)$ et $Z(n,k)$. On notera $Z_c = k[S]$ et $Z_c(n) = k[Z_1,\ldots,Z_n]$, alors on trouve de façon analogue que Z_c, $Z_c(n)$ sont des

bigèbres et que $Z_c = \varinjlim_n Z_c(n)$ dans $\mathbf{Ab}_k$. $Z_c(K)$ est l'objet qui figure dans Cartier [2] cor. 2.

§3. Algèbres profinies et cogroupes formels

On notera $\mathbf{Mf}_k$ la catégorie des algèbres commutatives sur l'anneau de base k qui sont libres et de type fini en tant que k-modules.

3.1 On appelle prosystème strict libre dans $\mathbf{Mf}_k$ tout système projectif $\tilde{A} = \{A_i \mid f_{ij} \; ; \; i,j \in S\}$ où $A_i \in \mathbf{Mf}_k$ et où S est un ensemble d'indices filtrant et dénombrable tel que les morphismes $f_{ij} : A_j \to A_i$ soient surjectifs et se prolongent en une suite exacte de k-modules libres

$$0 \to \operatorname{Ker} f_{ij} \to A_j \to A_i \to 0 \; . \qquad (1)$$

Chaque fois qu'on a un tel système $\tilde{A}$ on y associe l'algèbre $A = \varprojlim \tilde{A}$, que l'on munit avec la $\varprojlim$-topologie, à savoir, la topologie la plus faible qui rend continues toutes les applications canoniques $A \to A_i$, les A_i étant supposés discrets. De cette façon, A est muni d'une structure de k-algèbre topologique séparée, complète dans laquelle les noyaux des applications canoniques $A \to A_i$ constituent un système fondamental d'environ zéro.

Si $\tilde{A}$ et $\tilde{B}$ sont deux prosystèmes stricts libres dans $\mathbf{Mf}_k$ et si $A = \varprojlim \tilde{A}$, $B = \varprojlim \tilde{B}$ on définit un morphisme $f : A \to B$ comme un morphisme continu de k-algèbres. On obtient de cette façon une catégorie, notée $\mathbf{Al}_k$. Lorsque k est un corps on définit $\mathbf{Al}_k$ simplement à être la catégorie $\mathbf{Pro}\text{-}\mathbf{Mf}_k$. Puis on montre que tout proobjet de $\mathbf{Mf}_k$ se définit par un prosystème strict libre. Lorsque k est une limite projective d'anneaux artiniens, on se reporte à SGAD, Exposé VII B.

3.2 La catégorie $\mathbf{Al}_k$ admet un objet cofinal, à savoir k et des sommes directes. Si $A, B \in \mathbf{Al}_k$, la somme $A \hat{\otimes} B$ est le complété de $A \otimes B$ pour la topologie évidente induite. Si A et B sont définis à partir d'un certain système A_i , B_i d'anneaux dans $\mathbf{Mf}_k$, alors il revient au même de définir $A \hat{\otimes} B$ en partant du

système, défini par les $A_i \otimes B_j$. Si $k \to k'$ est une extension de base, on obtient un foncteur évident $\mathbf{Al}_k \to \mathbf{Al}_{k'}$, en partant d'extension de base $\mathbf{Mf}_k \to \mathbf{Mf}_{k'}$.

3.3 On dira, que $X \in \mathbf{Al}_k$ est un cogroupe formel si X est un objet cogroupe dans $\mathbf{Al}_k$. Alors en copiant le dual de la situation de 2.3 on arrive à :

Lemme : $X \in \mathbf{Al}_k$ est un cogroupe formel si et seulement si X est muni d'un morphisme structural $d = d_X : X \to X \hat{\otimes} X$ dans $\mathbf{Al}_k$, dit codiagonal, (comultiplication), tel que :

a. d est coassociatif.

b. Il existe un morphisme, nécessairement unique, $\eta_X = \eta : X \to k$ dans $\mathbf{Al}_k$, dit counité, tel que $1 \hat{\otimes} \eta \circ d = \eta \hat{\otimes} 1 \circ d$ dans $X \simeq X \hat{\otimes} k \simeq k \hat{\otimes} X$.

c. Il existe un morphisme, nécessairement unique $c_X = c : X \to X$ dans $\mathbf{Al}_k$, dit antipodisme, tel que, si (m, ε) définissent la structure d'algèbre sur X, alors on ait $m \circ c \hat{\otimes} 1 \circ d = \varepsilon \circ \eta$.

Dans cette situation encore, le produit fg de f et g dans le groupe $\mathbf{Al}_k(X,Y)$ se donne par le diagramme

$$fg : X \xrightarrow{d} X \hat{\otimes} X \xrightarrow{f \hat{\otimes} g} Y \hat{\otimes} Y \xrightarrow{can} Y .$$

De cette façon on obtient la catégorie $\mathbf{CAl}_k$ des cogroupes formels sur k.

3.4 Exemples

a. $\mathbf{Mf}_k$ s'identifie à une sous catégorie pleine de $\mathbf{Al}_k$.

b. On munit l'anneau $k_n = k[[X_1, \ldots, X_n]]$ de la topologie $(X_1, \ldots, X_n)$-adique. Pour cette structure, $k_n \in \mathbf{Al}_k$.

c. Soit F une loi de dimension n sur k. On définit $\theta(F) = k[[X_{1F}, \ldots, X_{nF}]]$, muni de la comultiplication d, défini par $dX_{iF} = F_i(X_{1F} \hat{\otimes} 1, \ldots, X_{nF} \hat{\otimes} 1, 1 \hat{\otimes} X_{1F}, \ldots, 1 \hat{\otimes}_{nF})$ pour $1 \leqslant i \leqslant n$, bref : $dX_F = F(X_F \hat{\otimes} 1, 1 \hat{\otimes} X_F)$. On obtient de cette façon un foncteur contravariant

$$\theta : FG(k) \to \mathbf{CAl}_k$$

En parlant des lois, on dira que X_F est le système des générateurs canoniques de

F . On notera qu'à partir d'une loi, on arrive à un objet, qui se définit de façon intrinsèque, c'est-à-dire par aide des diagrammes.

d. Soit k un corps et soit G un groupe algébrique sur k . En complétant l'anneau local de l'origine θ_e pour la topologie m_e-adique, où m_e est l'idéal maximal de θ_e , on obtient $\hat{\theta}_e \in Al_k$. Le morphisme structural $G \times G \to G$ induit un morphisme $\hat{\theta}_e \to \hat{\theta}_{e \times e} \simeq \hat{\theta}_e \hat{\otimes} \hat{\theta}_e$, c'est-à-dire on obtient un foncteur à valeurs dans CAl_k .

§4. Dualité de Cartier

Si M est un k-module, on notera M^* le k-module des formes linéaires sur M . Si M est un k-module topologique, on notera également, lorsque aucune confusion ne sera possible, M^* le k-module des formes linéaires continues sur M . On rappelle

4.1 Lemme : Soit Cf_k la sous catégorie pleine de C_k formée des coalgèbres finies, c'est-à-dire de type fini en tant que k-module. Alors

$$?^* : Cf_k \to Mf_k$$

est une antiéquivalence des catégories.

On rappelle également que la structure d'algèbre sur C^* pour $C \in Cf_k$ se définit par la relation $\langle fg, c \rangle = \langle f \otimes g , d_C(c) \rangle$.

4.2 Soit maintenant $C = \underset{i}{\cup} C_i$ dans C_k , alors la suite exacte (1) du §2 donne une suite exacte

$$0 \to (C_j/C_i)^* \to C_j^* \to C_i^* \to 0$$

c'est-à-dire on obtient un prosystème strict libre $\{C_i^* | i\}$ dans Mf_k . D'autre part si l'on se donne un prosystème strict libre $\tilde{A}$ dans Mf_k , alors la suite exacte (1) du §3 donne une suite exacte

$$0 \to A_i^* \to A_j^* \to (\operatorname{Ker} f_{ij})^* \to 0$$

ce qui munit $\varinjlim A_i^*$ d'une structure d'objet de C_k . Si $A = \varinjlim A_i^*$, alors :

Lemme : On a $C^* \simeq \varprojlim C_i^*$ et $\mathbf{A}^* = \varinjlim \mathbf{A}_i^*$.

La démonstration est connue : les inclusions $C_i \to C$ induisent des surjections $C^* \to C_i^*$, d'où une flèche canonique $C^* \to \varprojlim C_i^*$. Soit $\tilde{g} = (g_i)$ un élément de $\varprojlim C_i^*$ avec $g_i \in C_i^*$, on définit $g \in C^*$ par $g(c) = g_i(c)$, si c appartient à C_i . En vue de $C = \bigcup C_i$ on obtient une flèche inverse. De la même façon, les applications canoniques $\mathbf{A} \to \mathbf{A}_i$ induisent $\mathbf{A}_i^* \to \mathbf{A}^*$, donc $\varinjlim \mathbf{A}_i^* \to \mathbf{A}^*$. Si $f \in \mathbf{A}^*$, alors f étant continue, se factorise à travers un $\mathbf{A}_i$, ce qui rend la flèche inversible.

De la même façon on observe que l'on a des flèches canoniques inversibles

$$\varprojlim C_k(C_i, D) \xleftarrow{\sim} C_k(\varinjlim C_i, D) \tag{1}$$

$$\varinjlim \mathbf{Al}_k(\mathbf{A}_i, B) \xrightarrow{\sim} \mathbf{Al}_k(\varprojlim \mathbf{A}_i, B) \tag{2}$$

En ramassant ce qui précède, on arrive à :

4.3 Théorème (Cartier)

a. Le foncteur contravariant $?^* : C_k \to \mathbf{Al}_k$ est une antiéquivalence des catégories, qui admet le foncteur $?^* : \mathbf{Al}_k \to C_k$ comme un foncteur quasi inverse.

b. $?^*$ transforme objet final (cofinal) en objet cofinal (final) et transforme produits (sommes) en sommes(produits), d'où une antiéquivalence

$$?^* \; GC_k \to C\mathbf{Al}_k$$

c. $?^*$ commute avec l'extension de base.

Pour la démonstration : cf. aussi Cartier[1] Exp. 2.

4.4 Exemple à titre d'exercice qui servira plus loin : On note pour $0 \leqslant n < \infty$, $T_n = k[[t]]/(t^{n+1})$ et $T = T_\infty = k[[t]] = \varprojlim T_n$, ce qui définit $T_n \in \mathbf{Al}_k$ pour tout $0 \leqslant n \leqslant \infty$.

Soit $\{t_i \mid 0 \leqslant i \leqslant n\}$ la base duale de $\{t^i \mid 0 \leqslant i \leqslant n\}$ avec $\langle t_i, t^j \rangle = \delta_{ij}$ (Kronecker), alors $dt_i = \sum_{a+b=i} t_a \otimes t_b$. Si l'on prend encore $dt = t \hat{\otimes} 1 + 1 \hat{\otimes} t$, alors $t_i t_j = (i,j) t_{i+j}$, où (i,j) dénote l'image de $(i+j)!/i!j!$ dans k .

§5. Schémas formels et groupes formels

On rassemble ici un peu toutes les catégories qui vont être définies ou dont on aura besoin. Soit k comme toujours un anneau de base. Alors, on prend

M_k : catégorie (pas trop grosse) des k-algèbres commutatives

M_kE : catégorie des foncteurs covariants $M_k \to Ens$

$Mf_k \hookrightarrow M_k$ le foncteur évident, qui donne le foncteur

$\hat{}: M_kE \to Mf_kE$ évident obtenu par restriction à Mf_k, appelé encore complétion

Gr_k : catégorie des schémas en groupes sur k, considérés comme foncteurs dans Mk_E. cf. [D], 2.1

Ac_k : sous-catégorie pleine de Gr_k des groupes affines commutatifs.

5.1 On copie [D] 1.6 : Soit $Spf : Mf_k \to Mf_kE$ le foncteur contravariant défini par $(Spf\ R)(S) = Mf_k(R,S)$. Alors le lemme de Yoneda donne que Spf est pleinement fidèle. On dira que $F \in Mf_kE$ est un schéma formel sur k, s'il existe un prosystème strict libre $\tilde{A}$ dans Mf_k et s'il existe des isomorphismes, fonctoriels en $R \in Mf_k$

$$F(R) \simeq \{\varinjlim Spf\ A_i\}(R) = \varinjlim Mf_k(A_i,R) = Al_k(A,R) \quad (\text{par } §4\ (2))$$

si $\tilde{A} = \varprojlim A_i$ est défini par $\tilde{A}$.

On notera $Schf_k$ la catégorie des schémas formels sur k.

5.2 Lemme : On étend la définition de Spf à la catégorie Al_k en posant pour $R \in Mf_k$:

$$Spf(A)(R) = \{\text{Morphismes continus d'algèbres } A \to R\} = Al_k(A,R).$$

Alors :

$$Spf : Al_k \to Schf_k$$

est une antiéquivalence des catégories, transformant l'objet cofinal en objet final et sommes en produits. De plus Spf commute avec l'extension de base.

5.3 On appelle groupe formel sur k tout objet groupe dans la catégorie $Schf_k$. Les groupes formels constitueront la catégorie Grf_k, celles de groupes formels commutatifs la catégorie $Grfc_k$.

La dualité de Cartier permet donc de définir une équivalence des catégories

$$Spf^* : C_k \to Schf_k$$

en posant $Spf^*C = Spf(C^*)$. Spf^* induit encore des équivalences $GC_k \to Grf_k$ et $\mathbf{Ab}_k \to Grfc_k$.

D'après ce qu'on a vu, il revient donc au même de donner

a. Un groupe formel G sur k .

b. Un objet $A = \varprojlim A_i$ dans CAl_k et un isomorphisme $G \simeq SpfA$. Cet A , noté désormais $\theta(G)$ sera appelé l'algèbre affine de G .

c. Un objet $C \in GC_k$ et un isomorphisme $G \simeq Spf^*C$. Cet objet C , noté abusivement le plus souvent par G^* sera appelé l'algèbre des distributions sur G.

5.4 Exemples de groupes formels

On note pour $R \in Mf_k$, $nil(R)$ le nilradical de R .

1. Groupe formel multiplicatif sur k , $\hat{\alpha}_k$. $\hat{\alpha}_k(R) = 1 + nil(R)$, muni de sa structure additive. On a $Spf\ \theta(\hat{G}_a) = \hat{\alpha}_k$. $\theta(\hat{\alpha}_k) \simeq k[[t]]$, $dt = t \hat{\otimes} 1 + 1 \hat{\otimes} t$. Le dual s'identifie à $T^* \in \mathbf{Ab}_k$ (cf. 4.4).

2. Groupe formel additif sur k , $\hat{\mu}_k$. $\hat{\mu}_k(R) = 1 + nil(R)$, muni de sa structure multiplicative. $\theta(\hat{\mu}_k) \simeq k[[t]]$, $dt = t \hat{\otimes} 1 + t \hat{\otimes} t + 1 \hat{\otimes} t$

3. Si k est un corps et $G \in Gr_k$, alors $\hat{G} \in Grf_k$. Si k est arbitraire il en est ainsi si $\theta(\hat{G}) \in CAl_k$ soit si $(\hat{G})^* \in GC_k$. Par exemple $\hat{\alpha}_k$ et $\hat{\mu}_k$ s'obtiennent par complétion du groupe additif α_k et multiplicatif μ_k .

4. Si k est un corps, la dualité de Cartier s'exprime encore en complétant un autre foncteur. De façon précise: Soit $G \in \mathbf{Ac}_k$. On pose $D(G)(M) = Gr_R(G \otimes_k M , \mu_M)$ pour $M \in M_k$ alors on a le diagramme commutatif, cf.[D] 2.4 th.1 :

$$\begin{array}{ccc} \mathbf{Ac}_k & \xrightarrow{D} & \mathbf{Ac}_k \\ {\scriptstyle Spec}\uparrow & & \downarrow \\ \mathbf{Ab}_k & \xrightarrow{Spf^*} & Grfc_k \end{array}$$

Soit $f : G \to H$ dans Grf_k. On définit $Ker\,f \in Mf_k E$ par

$$(Ker\,f)(R) = Ker\{f(R) : G(R) \to H(R)\} \quad \text{pour} \quad R \in Mf_k$$

$Ker\,f$ appartient à Grf_k s'il est représentable : Exemples

$$_n\hat{\mu}_k = Ker\{n : \hat{\mu}_k \to \hat{\mu}_k\} \; ; \; {}_n\hat{\mu}_k(R) = \{1+x \in \hat{\mu}_k(R) \mid (1+x)^n = 1\}$$

$$\theta(_n\hat{\mu}_k) \simeq k[[t]]/((1+t)^n-1) \; .$$

Si k est un anneau de caractéristique p, premier, on définit $_{p^n}\hat{\alpha}_k$ par son algèbre affine $k[[t]]/(t^{p^r})$, $dt = t \hat{\otimes} 1 + 1 \hat{\otimes} t$. Si $G \in Grfc_k$, on note pour $n \in \mathbb{Z}$ par $[n]$ l'endomorphisme donné par $[n](R)(x) = nx$ dans $G(R)$.

5.5 On résume les flèches importantes :

$$\begin{array}{ccccc}
 & & Grf_k & \xleftarrow{\hat{\ }} & Gr_k \\
 & & Spf \uparrow \downarrow \theta & & \uparrow \downarrow \\
FG(k) & \xrightarrow{\theta} & CAl_k & & Ak_c \quad D \\
 & & * \uparrow \downarrow * & & \uparrow \; Spec \\
 & & GC_k & \hookleftarrow & Ab_k
\end{array}$$

5.6 Définitions de certains types de groupes formels.

Soit $G \in Grf_k$. k anneau de base.

a. G sera dit constant s'il est de la forme $G \simeq Spf(k^E)$ où E est un ensemble et où k^E est muni de la topologie produit.

b. G sera dit fini, s'il est de la forme $Spec\,M$ avec $M \in Mf_k$.

c. Pour tout groupe formel G on note $I_G = Ker\{\varepsilon : \theta(G) \to k\}$ et $\omega_G = I_G/\overline{I_G^2}$. Soit encore $\pi_G : I_G \to \omega_G$ l'application canonique. G sera dit connexe si tout système $\{x_i \in I_G \mid i \in S\}$ tel que $\{\pi_G(x_i) \mid i \in S\}$ engendre le k-module topologique ω_G, engendre lui-même l'algèbre topologique $\theta(G)$.

Si k est un corps, on définit simplement : G est connexe si et seulement si $G(K) = \{1\}$ pour tout corps $K \in Mfl_k$. [D] 2.7 .

d. G sera dit infinitésimal s'il est fini et connexe.

e. G connexe sera dit lisse, ou de Dieudonné, si $\theta(G)$ est de la forme $\theta(G) \simeq k[[X_i]]_{i\in E}$, où E est un ensemble d'indices dénombrable, totalement ordonné et où en cas que $\mathrm{Card}\ E = \infty$, on a $\lim_i X_i = 0$ dans la topologie de $\theta(G)$. Si $\mathrm{Card}\ E < \infty$, on appelle $\mathrm{Card}\ E$ la dimension de G. cf. [D] 2.10. Si $F \in FG(k)$, alors $\mathrm{Spf}\,\theta(F)$ est de Dieudonné.

f. $G \in \mathrm{Grfc}_k$ sera dit p-divisible, ou de Barsotti-Tate si $[p] : G \to G$ est un épimorphisme et si $G = \varinjlim \mathrm{Ker}[p^j]$ avec $\mathrm{Ker}[p^j]$ fini et dans Grf_k pour tout i. cf. [D] 2.11.

5.7 Il va de soi que les catégories C_k et $\mathbf{Al}_k$ se généralisent de façon évidente : on commence avec les k-modules projectifs de type fini. Pour une étude de cette situation encore généralisée cf. Morris-Pareigis : Formal Groups over discrete rings Bull A.M.S. ? Toutefois, les catégories introduites ici seront amplement suffisantes pour une étude des courbes dans un groupes formel.

Chapitre II : Courbes dans un groupe formel

§1. Opérateurs invariants à gauche et algèbres de Lie. Rappels.

1.1 Pour $A \in \mathbf{Al}_k$ on note $\mathrm{End}_{\mathrm{lin}}(A)$ le k-module des endomorphismes k-linéaires continus de A. Soit maintenant $G \in \mathrm{Grf}_k$. On définit

$$\mu(G) : G^* \to \mathrm{End}_{\mathrm{lin}}(\theta(G))$$

par le diagramme :

$$\mu(G)f : G \xrightarrow{d} G \hat{\otimes} G \xrightarrow{1\hat{\otimes}f} k \hat{\otimes} G \simeq G$$

et

$$\sigma(G) : \mathrm{End}_{\mathrm{lin}}(\theta(G)) \to G^*$$

par le diagramme :

$$\sigma(G)g : \theta(G) \xrightarrow{g} \theta(G) \xrightarrow{\varepsilon} k\ .$$

Alors on a :

Proposition : a) $\mu(G)$ est un morphisme injectif de k-algèbres, fonctoriel en G.

b) $\sigma(G)$ est un morphisme k-linéaire, fonctoriel en G .

c) $\sigma(G) \circ \mu(G) =$ identité sur G^* .

Pour la démonstration, qui se fait à l'aide de nombreux diagrammes : cf. par exemple SGAD VII A 2.2 et 2.3.

1.2 Exercice : On définit le sous-module $\mathrm{Inv}(G)$ de $\mathrm{End}_{\mathrm{lin}}(\theta(G))$ par :

$$\mathrm{Inv}(G) = \{f \in \mathrm{End}_{\mathrm{lin}}(\theta(G)) \mid \begin{array}{ccc} \theta(G) & \xrightarrow{d} & \theta(G) \hat{\otimes} \theta(G) \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle 1 \hat{\otimes} f} \\ \theta(G) & \xrightarrow{d} & \theta(G) \hat{\otimes} \theta(G) \end{array}$$

est commutatif}. Montrer que $\mathrm{Inv}(G) = \mathrm{Im}\ \mu(G)$. Les éléments de $\mathrm{Im}\ \mu(G) = \mathrm{Inv}(G)$ s'appellent opérateurs invariants(à gauche).

1.3 Soient $G \in \mathrm{Grf}_k$ et $k[t]$ l'algèbre des nombres duaux sur k , c'est-à-dire $t^2 = 0$. Le morphisme structural $k \to k[t]$ admet une rétraction $p : k[t] \to k$, $p(t) = 0$. On définit l'algèbre de Lie de G par

$$\mathrm{Lie}\ G = \mathrm{Ker}\{G(p) : G(k[t]) \to G(k)\}$$

c'est-à-dire, on a une suite exacte

$$\{1\} \longrightarrow \mathrm{Lie}\ G \longrightarrow G(k[t]) \underset{G(p)}{\overset{\longleftarrow}{\longrightarrow}} G(k) \longrightarrow \{1\} \qquad (1)$$

La structure d'algèbre de Lie sur Lie G , ainsi que sa structure de p-algèbre de Lie, si l'anneau de base est de caractéristique p , premier, résultera des propriétés des courbes. cf. 3.2 cor. 2 ci-dessous.

§2. Courbes dans un groupe formel

On considère comme dans I.4.4 les anneaux $T_n = k[[t]]/(t^{n+1})$ pour $0 \leqslant n \leqslant \infty$. En particulier, T_1 est l'algèbre des nombres duaux sur k . On notera $\pi_n : T_n \to T_o = k$ le morphisme dans Al_k tel que $\pi_n(t) = 0$ et on considère la généralisation de (1), §1 pour n arbitraire :

$$\{1\} \longrightarrow \mathrm{Ker}\ G(\pi_n) \longrightarrow G(T_n) \underset{G(\pi_n)}{\overset{\longleftarrow}{\longrightarrow}} G(k) \longrightarrow \{1\} \qquad (1)$$

(1) est une suite exacte des groupes scindée, qui fait de $G(T_n)$ un groupe produit semidirect de $G(k)$ avec $\mathrm{Ker}\ G(\pi_n)$, fonctoriel en $G \in \mathrm{Grf}_k$.

2.1 Définition : Soit $0 \leqslant n \leqslant \infty$ et soit $G \in \mathrm{Grf}_k$. On appelle groupe de courbes de longueur n, ou d'ordre n dans G, le groupe $\mathrm{Ker}\ G(\pi_n)$. On obtient un foncteur covariant, dit foncteur courbe d'ordre n (ou : de longueur n) :

$$\mathrm{Lie}_n : \mathrm{Grf}_k \to \mathrm{Groupes}\ .$$

On a donc pour $n = 1$, $\mathrm{Lie}_1 = \mathrm{Lie}$.

2.2 Lemme 1 : Le foncteur courbe d'ordre n est représentable dans Grf_k pour $0 \leqslant n \leqslant \infty$.

Remarque : Il faut donc trouver un couple (G_n, ξ_n) avec $G_n \in \mathrm{Grf}_k$ et $\xi_n \in \mathrm{Lie}_n(G_n)$ telle qu'il existe des bijections, fonctorielles en $X \in \mathrm{Grf}_k$

$$\mathrm{Grf}_k(G_n, X) \to \mathrm{Lie}_n(X)$$

où la flèche $f : G_n \to X$ dans Grf_k correspond à $\mathrm{Lie}_n(f)\xi_n$ sous l'application induite $\mathrm{Lie}_n(f) : \mathrm{Lie}_n(G_n) \to \mathrm{Lie}_n(X)$. Malheureusement on ne connaît la structure explicite de G_n que dans le cas commutatif, c'est-à-dire l'objet G_{cn} qui se donne par le lemme : (cf. également Ch. II, 7.6 lemme 6 pour $n = \infty$).

Lemme 2 : Le foncteur courbe d'ordre n est représentable dans Grfc_k pour $0 \leqslant n \leqslant \infty$.

On connaît toutefois de façon explicite G_n^* et G_{cn}^* et il s'avérera que les foncteurs qu'ils représentent dans GC_k resp. $\mathbf{Ab}_k$ sont les foncteurs "puissances divisées", ce qui est la motivation à introduire les foncteurs covariants

$$H_n : \mathrm{GC}_k \to \mathrm{Groupes}\ ,\quad C_n : \mathbf{Ab}_k \to \mathrm{Groupes\ abéliens}$$

en posant $\quad H_n(X) = \mathrm{Lie}_n(X^*)$ pour $X \in \mathrm{GC}_k$

$$C_n(X) = \mathrm{Lie}_n(X^*) \text{ pour } X \in \mathbf{Ab}_k\ .$$

Par dualité de Cartier on a des bijections fonctorielles en X

$H_n(X) = \mathrm{Lie}_n(X^*) \simeq \mathrm{Grf}_k(G_n, X^*) \simeq \mathrm{GC}_k(G_n^*, X)$ ainsi que pour $C_n(X) \simeq \mathbf{Ab}_k(G_{cn}^*, X)$, donc il suffira à montrer :

2.3 Lemme 3 : H_n est représentable pour tout $0 \leqslant n \leqslant \infty$.

Lemme 4 : C_n est représentable pour tout $0 \leqslant n \leqslant \infty$.

Démonstration : On procédera de telle façon qu'on obtienne le plus possible d'information en ce qui concerne la structure explicite.

a. Soit d'abord $G \in \mathrm{Grf}_k$. On pose pour $f \in G(T_n) \simeq \mathbf{Al}_k(\theta(G), T_n)$

$$f(x) = \sum_{i=0}^{n} f_i(x)t^i = (\sum_{i=0}^{n} f_i t^i)(x) \qquad (2)$$

On vérifie aisément que les f_i sont des formes linéaires continues et que l'on a:

(PD) : Une suite $F = \{f_i \mid 0 \leqslant i \leqslant n\} \subset G^*$ définit $f \in \mathrm{Lie}_n(G) \subset G(T_n)$ par (2) si et seulement si elle satisfait à une des trois conditions équivalentes suivantes

1) On a $f_o = \varepsilon : \theta(G) \to k$ et $f_i(xy) = \sum_{a+b=i} f_a(x)f_b(y)$ pour $0 \leqslant i \leqslant n$.

2) On a $f_o = \varepsilon : \theta(G) \to k$ et $df_i = \sum_{a+b} f_a \otimes f_b$ dans G^* pour $0 \leqslant i \leqslant n$.

3) F est une suite de puissances divisées de longueur n au-dessus de ε.

Parce qu'il existe plusieurs définitions de la notion "puissance divisée" (cf. Berthelot, Sweedler), on emploiera ici en même temps 3) comme définition de puissance divisée.

b. Avec les notations de I.4.4, sous la bijection canonique $\mathbf{Al}_k(\theta(G), T_n) \simeq C_k(T_n^*, G^*)$, qui envoie f sur f^* on a

$$f^*(t_i) = f_i \qquad \text{pour } 0 \leqslant i \leqslant n \qquad (3)$$

donc, en écrivant $f, g \in G(T_n)$ sous leur forme (2), le produit fg dans le groupe $G(T_n)$ correspond avec le diagramme

$$(fg)^* : T_n^* \xrightarrow{d} T_n^* \otimes T_n^* \xrightarrow{f^* \otimes g^*} G^* \otimes G^* \xrightarrow{m} G^*$$

donc avec (3) :

$$\sum_{i=o}^{n} (fg)_i t^i = \sum_{i=o}^{n} \Big(\sum_{a+b=i} f_a g_b \Big) t^i \qquad (4)$$

c. Soit $Z(n,k) = Z(n)$ comme dans I.2.5.c, alors l'application $T_n^* \to Z(n)$ dans C_k, qui envoie t_i sur Z_i induit une injection, fonctorielle en $X \in GC_k$

$$\mu(X) : GC_k(Z(n),X) \hookrightarrow C_k(T_n^*,X)$$

dont l'image s'identifie canoniquement à l'ensemble des puissances divisées de longueur n au-dessus de $1 \in X$. En observant que $\varepsilon \in G^*$ s'identifie à $1 \in G^*$, on tire de ce qui précède :

d. L'image de $Lie_n(G)$ dans $C_k(T_n^*,G^*)$ coïncide avec l'image de $\mu(G^*)$ dans $C_k(T_n^*,G^*)$, ce qui donne une bijection, fonctorielle en G

$$H_n(G^*) = Lie_n(G) \xrightarrow{\sim} GC_k(Z(n),G^*) . \qquad (5)$$

De plus, l'application $f \mapsto \sum_{i=o}^{n} f_i t^i$ de $Lie_n(G) \to 1 + tG^*[[t]]/(t^{n+1})$ donnée par (2) est un homomorphisme injectif $\lambda_{n,G}$ pour la structure du groupe multiplicatif (non abélien) de $1 + tG^*[[t]]/(t^{n+1})$. $\lambda_{n,G}$ est fonctoriel en G.

(5) montre que H_n est représentable. Si $G^* \in Ab_k$, l'application canonique $Z(n) \to Z_c(n)$ induit

$$C_n(G^*) = GC_k(Z(n),G^*) \simeq Ab_k(Z_c(n),G^*)$$

ce qui donne le lemme 4.

2.4 En pratique on identifiera le plus souvent les groupes

$$Lie_n(G) = H_n(G^*) = GC_k(Z(n),G^*) = \mathrm{Im}\ \lambda_{n,G}$$

dont les éléments seront dits courbes d'ordre n dans G (ou G^*) et l'on écrira $f = \Sigma f_n t^n$ pour une courbe de longueur connue. Lorsque f est une courbe, on emploiera désormais sans aucune référence le symbole f_n, défini par $f = \Sigma f_n t^n$.

En considérant une courbe f d'ordre n dans $G \in Grf_k$ comme un morphisme $f : \theta(G) \to T_n$, on a donc $f(x) = \Sigma f_m(x) t^m$. Si l'on considère f comme un morphisme $\tilde{f} : Z(n) \to G^*$ on a $\tilde{f}(Z_m) = f_m$ pour $0 \leqslant m \leqslant n$. La fonctorialité impli-

que que $$\tilde{f} = \Sigma f_m t^m = \Sigma \tilde{f}(Z_m)t^m = H_n(\tilde{f})(\Sigma Z_m t^m) \qquad (6)$$

autrement dit, H_n se représente par le couple $(Z(n),\xi_n)$ avec $\xi_n = \sum_{in=o} Z_m t^m$. ξ_n sera dit courbe canonique d'ordre n. On notera $H = H_\infty$, $C = C_\infty$, $\xi = \xi_\infty$.

2.5 On définit pour $a \in \mathbb{N}^+$, $G \in Grf_k$, $f \in Lie_n(G)$ le décalage V_a par aide du diagramme :

$$V_a f : \theta(G) \xrightarrow{f} T_n \xrightarrow{g_a} T_{a(n+1)-1}$$

où g_a est la flèche dans Al_k déterminée par $g_a(t) = t^a$.

De même, si $\underline{\lambda} \in k$ on notera $\underline{\lambda}f$ le morphisme composé dans Al_k donné par :

$$\underline{\lambda}f : \theta(G) \xrightarrow{f} T_n \xrightarrow{g_\lambda} T_n \ , \ g_\lambda(t) = \lambda t \ .$$

Alors, on vérifie sans peine

Lemme : Soit $X \in GC_k$.

a. $V_a : H_n(X) \to H_{a(n+1)-1}(X)$ est un homomorphisme de groupes, fonctoriel en X.

b. $\underline{\lambda} : H_n(X) \to H_n(X)$ est un endomorphisme de groupes, fonctoriel en X.

c. $V_a V_b = V_{ab}$; $\underline{\lambda} V_a = V_a \underline{\lambda^a}$; $\underline{\lambda}.\underline{\mu} = \underline{\lambda\mu}$; $V_1 = \underline{1} = id$.

On écrira encore (par abus) la courbe $\underline{\lambda}f$ comme λf. Noter qu'on n'a pas $\lambda f + \mu f = (\lambda+\mu)f$. Pour $n \in \mathbb{Z}$, on notera $[n]f$ la courbe f^n.

2.6 La relation $T = \varprojlim T_n$ entraîne pour $X \in GC_k$ la relation $H(X) = \varprojlim H_n(X)$, ce qui munit le groupe $H(X)$ d'une structure de groupe topologique séparé complet. L'inclusion $\lambda_{\infty,X^*} : GC_k(Z,X) \hookrightarrow 1 + tX[[t]] \hookrightarrow X[[t]]$ est continue pour la topologie (t)-adique sur $X[[t]]$, noté désormais X_t, et son image est fermée. Si $m \leqslant n$ on note $\rho_{n,m} : H_n(X) \to H_m(X)$ l'application canonique, dite restriction des courbes de longueur n à celles de longueur m. On dira que $f \in H_m(X)$ s'étend à une courbe d'ordre n si $f \in \operatorname{Im} \rho_{n,m}$. Si $\rho_{n,m}(f) = \rho_{n,m}(g)$ on écrira $f \equiv g \bmod t^{m+1}$. Pour $X \in GC_k$ on note $P(X)$ l'ensemble de ses éléments primitifs, c'est-à-dire $x \in P(X)$ si $dx = x \otimes 1 + 1 \otimes x$. $P(X)$ est muni d'une structure naturelle d'algèbre de Lie, (p-algèbre si

$\chi(k) = p$, premier).

2.7 Exemples

a. Soient $k \in \mathrm{Alg}_{\mathbb{Q}}$, $G \in \mathrm{Grf}_k$ et $\partial \in P(G^*)$ alors $\exp \partial t \in H(G^*)$. Plus généralement si $\{\partial_i \mid i \in \mathbb{N}^+\} \subset P(G^*)$ et $\{\lambda_i \mid i \in \mathbb{N}^+\} \subset k$ alors le produit ordonné $\prod_i \exp \partial_i t^i = \prod_i V_i \exp \partial_i t$ est une courbe dans G .

b. Soit $\chi(k) = p$, premier, alors $C_n({}_p\alpha_k) \neq 0$ pour tout $n < \infty$, $C({}_p\alpha_k) = 0$.

c. Soient $\mathbf{A} = \theta(\alpha_{\mathbb{Z}_p}) = \mathbb{Z}_p[X]$, $X \in P(\mathbf{A})$ dans $\mathbf{Ab}_{\mathbb{Z}_p}$, alors la courbe d'ordre $p-1$, $\exp Xt \bmod t^p$ ne s'étend pas à une courbe d'ordre $\geqslant p$. On a $\exp pXt \in C(\mathbf{A})$, donc $C(\mathbf{A}) \neq \{0\}$.

2.8 Les exemples montrent qu'en général une courbe d'ordre finie ne s'étend pas à une courbe d'ordre plus grande. Dans le lemme suivant on ramasse quelques propriétés qui seront utilisées désormais sans référence.

Lemme : Soit $X \in GC_k$.

a. Soient $n > m$ et $f, g \in H_n(X)$ telles que $f \equiv g \bmod t^{m+1}$, alors $f_{m+1} - g_{m+1} \in P(X)$.

b. L'application $1 + \partial t \mapsto \partial$ induit une bijection $H_1(X) \xrightarrow{\sim} P(X)$.

c. Chaque courbe dans X s'étend à une courbe infinie si et seulement si l'application canonique $H(X) \to H_1(X)$ est surjective.

Démonstration : a et b résultent immédiatement de (PD), 2 dans 2.3. La condition de c est évidemment nécessaire. Démontrons qu'elle est suffisante. Soit f une courbe et suppose que

$$f \equiv \prod_{m=1}^{s-1} V_m g(m) = h = \sum h_m t^m \bmod t^s$$

avec $s \geqslant 1$ et $g(m) \in H(X)$; $s = 1$ est trivial parce que $1 \in X$ est une courbe infinie. Si $s = 2$ on utilise les données, donc soit $s > 2$. Si $f \in H_{s-1}(X)$ il n'y a plus rien à prouver. Si $f \in H_t(X)$, $t > s-1$ on a par a. que $f_s - h_s \in P(X)$, donc par b. on peut trouver une extension infinie $g(s)$ de

$1 + (f_s - h_s)t$. On voit que $f \equiv h.V_s g(s) \bmod t^{s+1}$ ce qui démontre le lemme.

2.9 On posera encore $E(k) = H(Z(k)) \simeq \mathrm{End}_{GC_k}(Z(k))$ et $E_c(k) = C(Z_c(k)) \simeq \mathrm{End}_{Ab_k}(Z_c(k))$. $E(k)$ et $E_c(k)$ sont munis de deux opérations à savoir celle induite par groupe des courbes et celle induite par composition des endomorphismes. On vérifie que ces opérations induisent sur $E_c(k)$ une structure d'anneau unitaire associatif topologique séparé complet. Lorsqu'il est clair que certaines propriétés de $E(k)$ induisent des propriétés tout à fait analogues pour $E_c(k)$ sous l'application canonique $Z(k) \to Z_c(k)$, on se restreindra à les formuler pour $E(k)$. Sinon, on convient de noter les différences.

Une courbe $f \in E(k)$ sera dite r-isobare, si f_m est isobare de poids rm pour tout m . Les courbes r-isobares constituent un sous-groupe $\mathrm{Iso}_r(E(k))$. Les courbes 1-isobares seront appelées isobares et on écrira $\mathrm{Iso}_1(E(k)) = \mathrm{Iso}(k)$. Si f est r-isobare, alors $V_r f$ est isobare. Si $f \in E(k)$ on écrira parfois $\tilde{f}$ l'endomorphisme de $Z(k)$ défini par f . En particulier on notera $\widetilde{V_a C} = v_a$. Noter que pour chaque sous ensemble S de l'ensemble nombres premiers, tous les $\tilde{f}$ avec $f \in E(k)$, qui commutent avec v_p pour $p \in S$ constituent un sous groupe $H(S,k)$. Il en résulte : $f \in H(S,k) \Longleftrightarrow v_p(f_m) = \begin{cases} f_{m/p} & \text{si } p \mid m \\ 0 & \text{sinon} \end{cases}$ pour tout $m \in \mathbb{N}^+$, tout $p \in S$, ce qui s'écrira encore sous forme abrégée $v_p(f_m) = f_{m//p}$.

§3. Quelques outils techniques

Il importe à voir comment les coefficients des courbes opèrent sous l'application $\mu : G^* \hookrightarrow \mathrm{Inv}(G)$ de §1. On posera $\mu(f) = \bar{f}$.

3.1 Lemme : Soient $G \in \mathrm{Grf}_k$ et $\varphi \in G^*$ avec $d\varphi = \Sigma\, \varphi_i \otimes \varphi_i'$ (somme finie). Alors on a

a. $\bar{\varphi}(xy) = \Sigma\, \bar{\varphi}_i(x)\bar{\varphi}_{i'}(y)$ pour $x,y \in \theta(G)$.

b. Supposons $\chi(k) = p$, premier et supposons que l'on ait une relation $\varphi(x^p) = \Sigma\, \alpha_i \{\psi_i(x)\}^p$ avec $\psi_i, \varphi \in G^*$ et $\alpha_i \in k$; $x \in \theta(G)$. Alors on a :

$\bar{\varphi}(x^p) = \Sigma\ \alpha_i \{\bar{\psi}_i(x)\}^p$.

Démonstration : a. Soient $dx = \sum_\alpha x_\alpha \hat{\otimes} x'_\alpha$ et $dy = \sum_\beta y_\beta \hat{\otimes} y'_\beta$, alors

$$\bar{\varphi}(xy) = \varepsilon \hat{\otimes} \varphi(\sum_{\alpha,\beta} x_\alpha y_\beta \hat{\otimes} x'_\alpha y'_\beta) = \sum_{\alpha,\beta} \varepsilon(x_\alpha y_\beta)(\sum_i \varphi_i(x'_\alpha)\varphi'_i(y'_\beta))$$

$$= \sum_i (\sum_\alpha \varepsilon(x_\alpha)\varphi_i(x'_\alpha))(\sum_\beta \varepsilon(y_\beta)\varphi'_i(y'_\beta)) = \sum_i \bar{\varphi}_i(x)\bar{\varphi}_i(y) .$$

b. se démontre de façon analogue.

3.2 Corollaire 1 : Soient $G \in Grf_k$ et $f \in H_n(G^*)$ pour n , $0 \leqslant n \leqslant \infty$. Alors les $\bar{f}_m$ satisfont aux relations de Leibniz

$$\bar{f}_o = id \quad ; \quad \bar{f}_m(xy) = \sum_{a+b=m} \bar{f}_a(x)\bar{f}_b(y) \qquad \text{pour} \quad 0 \leqslant m \leqslant n .$$

En particulier, $\bar{f}_1$ est une dérivation invariante à gauche de $\theta(G)$.

Corollaire 2 : Soit $G \in Grf_k$, alors Lie est un foncteur covariant Lie : $Grf_k \to$ {Lie algèbres sur k} (où p-Lie algèbres sur k , le cas échéant).

En effet, on a l'application

$$j(G) : \text{Lie } G \xrightarrow{\sim} H_1(G^*) \xrightarrow{2.8b}_{\sim} P(G^*) \xhookrightarrow{\mu} \text{Inv}(G)$$

et on voit d'après le corollaire 1, que Im $j(G)$ est une algèbre de Lie des dérivations invariantes (p-algèbre de Lie), ce qui montre le corollaire.

3.3 Définition : Soit $G \in Grf_k$. Soit S un ensemble dénombrable, totalement ordonné. Soit F un ensemble des courbes, finies ou non, dans G , indexées par S ,

$$F = \{f(n) = \sum_{i=o}^{h(n)} f_{n,i} t^i \mid n \in S \ ; \ 1 \leqslant h(n) \leqslant \infty\} . \qquad (1)$$

On pose $B(F)$ l'ensemble de tous les produits ordonnés de la forme $\prod_{n\in S} f_{n,\alpha_n}$ avec $0 \leqslant \alpha_n \leqslant h(n)$ pour tout $n \in S$ et les α_n presque tous nuls. Alors on dit que F est un ensemble fondamental des courbes dans G , si $B(F)$ est une base du k-module libre G^* (libre, parce que $G^* \in C_k$) . Dans ce cas on dira encore: G est engendré par ses courbes.

3.4 Soit F un ensemble fondamental des courbes dans G. L'ensemble $B(F)$ admet une bijection canonique sur le produit restreint $T = \prod_{n\in S}^{\text{restr.}} I_n$ où I_n est l'intervalle des entiers $I_n = [0,h(n)]$. On écrira donc de façon évidente $\varphi \in B(F)$ sous forme φ_α, avec $\alpha \in T$. On écrit $\alpha \leqslant \beta$ pour $\alpha,\beta \in T$ si $\beta_n - \alpha_n \geqslant 0$ pour tout $n \in S$, ce qui permet d'écrire $\beta = \alpha+\gamma$ si $\beta_n - \alpha_n = \gamma_n \geqslant 0$ pour $n \in S$. Il suit de là que les éléments de $B(F)$ constituent une base structurale de G^*, c'est-à-dire on a

$$d\varphi_\beta = \sum_{\alpha+\gamma=\beta} \varphi_\alpha \otimes \varphi_\gamma \qquad (2)$$

pour $\beta \in T$. En particulier, (2) entraîne que les éléments spéciaux $f_{n,1}$ pour $n \in S$, constituent une base de $P(G^*)$. Cette base sera notée

$$\{\partial_n \mid n \in S\}. \qquad (3)$$

3.5 Théorème : Soient $G \in \mathrm{Grf}_k$ et F comme ci-dessus. Alors les deux conditions suivantes sont équivalentes :

a. F est un système fondamental des courbes dans G.

b. 1) Il existe $y_m \in \theta(G)$ pour $m \in S$ t.q. $f(n)(y_m) = \delta_{n,m}t$ pour tout $n,m \in S$.

2) Si $\mathrm{Card}\, S = \infty$, alors $\lim_S y_m = 0$ dans la topologie de $\theta(G)$.

3) L'application d'algèbres $k[[T_m]]/(T_m^{h(m)+1})_{m\in S} \to \theta(G)$ qui envoie T_m sur y_m est bijective.

Démonstration : Soit d'abord F fondamental et soit $B^*(F) = \{e_\alpha \mid \alpha \in T\}$ dans $\theta(G)$ la base duale de $B(F)$. Soit de plus $\{z_m \mid m \in S\}$ le sous ensemble de $B^*(F)$ avec $\langle \partial_m, z_n \rangle = \delta_{n,m}$ pour $n,m \in S$. G^*, en tant que objet de C_k, est réunion filtrante croissante d'une suite de sous co algèbres $\{G^*_m \mid m \in E\}$ avec E dénombrable, qui sont libres et de type fini. Soit $I_m = \mathrm{Ker}\{\theta(G) \to G^{**}_m\}$, alors on voit que chaque I_m contient presque tous les z_m, ce qui entraîne que $\lim_S z_m = 0$. Pour les courbes $f(n)$ on a de plus $f(n)(z_m) \equiv 1 + \langle \partial_n, z_m \rangle t = \delta_{n,m}t \bmod t^2$. Supposons donc qu'il existe x_m, $m \in S$ avec $\lim_S x_m = 0$ et

$f(n)(x_m) \equiv \delta_{n,m}t + \lambda_{n,m}t^r \bmod t^{r+1}$, $r \geqslant 2$ (avec $\lambda_{n,m} = 0$ si $r > h(n)$) . Soit

$$y_m = x_m - \sum_{k\in S} \lambda_{k,m} x_k^r$$

alors $\lim_S y_m = 0$ puisque $\lim_S x_m^r = 0$ pour tout $r \geqslant 1$. De plus :

$$\begin{aligned} f(n)(y_m) &\equiv f(n)(x_m) - \sum_{k\in S} \lambda_{k,m}\{f(n)x_k\}^r \\ &\equiv \delta_{n,m}t + \lambda_{n,m}t^r - \sum_{k\in S} \lambda_{k,m}(\delta_{n,k}t)^r \\ &\equiv \delta_{n,m}t \bmod t^{r+1} \end{aligned}$$

ce qui démontre 1 et 2.

Soit $B^* = \{y^\alpha = \prod_{n\in S} y_n^{\alpha_n} \mid \alpha = (\alpha_n \mid n \in S) \in T\}$, où T est comme dans 3.4. On appellera une partie $\{x_r \mid r \in E'\} \subset \theta(G)$ pour un ensemble convenable d'indices E' une base topologique de $\theta(G)$, si $\theta(G) \simeq \prod_{r\in E'} kx_r$ en tant que k-module. Alors on a

Lemme 1 : Soient $G \in Grf_k$ et F , donné par (1) un ensemble des courbes. On suppose 1 et 2 de la condition b. du théorème vraie, alors on a : B^* est une base topologique de $\theta(G)$ si et seulement si $B(F)$ est une base de G^* .

Noter que le lemme implique immédiatement le théorème.

On pose pour $\alpha \in T$, $|\alpha| = \Sigma \alpha_i$, alors le lemme résulte de façon évidente du lemme 2 :

Lemme 2 : Sous les conditions du lemme 1 on a : Si $\alpha,\beta \in T$, alors

$$\langle \varphi_\alpha , y^\beta \rangle = \begin{cases} \delta_{\alpha,\beta} & \text{si} \quad |\alpha| = |\beta| \\ 0 & \text{si} \quad |\alpha| < |\beta| \end{cases} \tag{4}$$

On raisonne par récurrence sur $|\alpha|$. Si $|\alpha| = 0$, (4) est vrai, parce que $\langle \varepsilon, y^\beta \rangle = 1$ si et seulement si $|\beta| = 0$, $\varepsilon : \theta(G) \to k$ s'identifiant à $1 \in G^*$. Si $|\alpha| = 1$, (4) est vrai en vertu de la relation $f(n)(y_m) = \delta_{n,m}t$. Soit donc (4) vrai si $|\alpha| < r$, avec $r \geqslant 2$.

Si $|\beta| \geqslant |\alpha| = r \geqslant 2$, y^β s'écrit $y^\mu y^\nu$ avec $\mu,\nu \in T$, $|\mu| \geqslant 1$, $|\nu| \geqslant 1$ et on a

$$\langle \varphi_\alpha, y^\beta \rangle \overset{(2)}{=} \langle \sum_{\gamma+\delta=\alpha} \varphi_\gamma \otimes \varphi_\delta \ , \ y^\mu y^\nu \rangle = \varepsilon(y^\mu)\varphi_\alpha(y^\nu) + \varphi_\alpha(y^\mu)\varepsilon(y^\nu) + \sum_{\substack{\gamma+\delta=\alpha \\ \gamma\neq\alpha \\ \delta\neq\alpha}} \varphi_\gamma(y^\mu)\varphi_\delta(y^\nu) \ . \qquad (5)$$

Les deux premiers termes sont nuls. Si $|\beta| > |\alpha| = |\gamma| + |\delta|$, alors $|\mu| \leqslant |\gamma|$ et $|\nu| \leqslant |\delta|$ entraîneraient : $|\beta| = |\mu| + |\nu| \leqslant |\gamma| + |\delta| = |\alpha|$ ce qui est contraire à l'hypothèse $|\beta| > |\alpha|$. Il suit que chaque terme de la somme dans (5) est nul. On a donc $\langle \varphi_\alpha, y^\beta \rangle = 0$ dans ce cas, comme il faudrait.
On raisonne de façon pareille si $|\beta| = |\alpha|$, le théorème en résulte.

3.6 Le théorème entraîne les corollaires :

Corollaire 1 : Si $G \in \mathrm{Grf}_k$ est engendré par ses courbes, alors G est connexe.

C'est bien évident.

Remarque : La converse n'est pas vraie : on pose : k un corps non parfait, $\chi(k) = p$, $\alpha \in k - k^p$, $\theta(G) = k[X,Y]/(X^p - \alpha Y^p, X^{p^2})$ avec X,Y primitifs.

Corollaire 2 : $G \in \mathrm{Grf}_k$ est de Dieudonné si et seulement si G est engendré par un ensemble de ses courbes infinies.

Dans cette situation mentionnons une forme affaiblie du SGAD VII B th. 5.2 : G est infinitésimal sur un corps parfait k, $\chi(k) = p > 0$, si et seulement si G est engendré par un ensemble fini de ses courbes finies.

§4. Exemple fondamental : Algèbres sur $\mathbb{Q}$

Convention générale : Soient P l'ensemble des nombres premiers et $S \cup S^* = P$ une partition. Chaque S engendre un sous-monoid multiplicatif pointé $\mathbb{N}(S)$ de $\mathbb{N}^+$ tel que $\mathbb{N}^+$ se décompose en produit de deux monoids $\mathbb{N}^+ = \mathbb{N}(S) \times \mathbb{N}(S^*)$. En effet, $m \in \mathbb{N}(S)$, (resp. $m \in \mathbb{N}(S^*)$) $\Longleftrightarrow$ si $p \in P$ divise m, alors $p \in S$ (resp. $p \in S^*$).

On pose $\mathbb{Z}_S = \bigcap_{p \in S} \mathbb{Z}_{(p)}$ si $S \neq \{\emptyset\}$ et $\mathbb{Z}_\emptyset = \mathbb{Q}$. Ceci entraîne que tous les éléments de $\mathbb{N}(S^*)$ sont inversibles dans $\mathbb{Z}_S$. Si k est donc un anneau de base, il existe un unique $S = S(k)$ qui est minimal tel que le morphisme structural $\varphi : Z \to k$ s'étend à $\mathbb{Z}_S \to k$, à savoir on prend pour $S(k)$ la partie complémen-

taire dans P de l'ensemble $\{p \in P \mid \varphi(p)$ inversible dans $k\}$.

Dans ce §1 on étudiera le cas $S(k) = \{\emptyset\}$, c'est-à-dire $k \in \mathrm{Alg}_{\mathbb{Q}}$.

On pose $Z = Z(k)$ et $\xi = \Sigma\, Z_m t^m$, la courbe canonique. On dira encore que $x \in Z$, isobare de poids $s > 1$, contient Z_s si $x \equiv Z_s \bmod \{Z_1 = \ldots = Z_{s-1} = 0\}$. Si $s = 1$, x ne contiendra Z_1 que si $x = Z_1$.

4.1 Théorème (Décomposition) : Il existe une famille unique

$$X = \{X_i \mid i \in \mathbb{N}^+\} \subset P(Z) \quad \text{t.q}$$

a. Chaque X_i est isobare de poids i et contient Z_i.

b. $\xi = \prod_{i=1}^{\infty} V_i \exp X_i t$ dans $\mathrm{Iso}(k)$ (produit ordonné).

c. $v_a(X_i) = X_{i//a}$ pour tout $i,a \in \mathbb{N}^+$.

Démonstration : Soit $W = k\langle X\rangle \in GC_k$ défini par $X \subset P(W)$. On attache à X_i le poids i, donc $\exp X_i t^i = V_i \exp X_i t$ est une courbe isobare, d'où encore : $\prod_{i=1}^{\infty} V_i \exp X_i t$ est une courbe isobare dans W, nécessairement de la forme $H(f)\xi$ avec $f : Z \to W$. On a $f(Z_i) \equiv X_i \bmod X_1 = \ldots = X_{i-1} = 0$, donc f est un isomorphisme ce qui permet d'identifier Z avec W. L'unicité est évidente. On a

$$V_a\xi = \prod_{i=1}^{\infty} V_{ai} \exp X_i t = \prod_{i=1}^{\infty} \exp X_i t^{ai} \tag{1}$$

$$= H(v_a)\xi = \prod_{i=1}^{\infty} H(v_a) \exp X_i t^i \quad \text{(fonctorialité de } V_a\text{)}$$

$$= \prod_{i=1}^{\infty} \exp v_a(X_i) t^i \tag{2}$$

(1) et (2) démontrent que $v_a(X_i) = X_{i//a}$ pour tout $i,a \in \mathbb{N}^+$, d'où le théorème.

4.2 Le théorème entraîne :

Corollaire 1 : Soit $G \in Grf_k$, alors l'application

$$e : P(G^*)^{\mathbb{N}^+} \to H(G^*)$$

définie par $e((\partial_i \mid i \in \mathbb{N}^+)) = \prod_{i=1}^{\infty} \exp \partial_i t^i$

est bijective, ce qui permet d'écrire $\varphi \in H(G^*)$ uniquement sous la forme :

$$\varphi = \prod_{i=1}^{\infty} \exp i^{-1}\, \sigma_i(\varphi) t^i \quad \text{avec} \quad \sigma_i(\varphi) \in P(G^*). \tag{3}$$

En effet $\varphi = H(\varphi)C = \prod_{i=1}^{\infty} V^i \exp \varphi(X_i)t^i$. On pose donc $\sigma_i(\varphi) = i\varphi(X_i)$.

Corollaire 2 : Les X_i sont à coefficients dans $\mathbb{Q}$. On note $E = \exp Z_1 t$.

Corollaire 3 : $Z = k\langle X\rangle$ est somme amalgamée de Card $\mathbb{N}^+$ copies de ImE . L'algèbre de Lie $P(Z)$ est l'algèbre de Lie libre (en tant qu'algèbre de Lie) engendrée par X .

Corollaire 4 : ImE est l'unique sous objet minimal de Z dans lequel $1 + Z_1 t$ se prolonge à une courbe infinie.

Corollaire 5 : Notons $U(k) = \mathrm{Im}(E) = k[Z_1]$. Alors il existe une unique k_t-dérivation de $U(k)_t$ telle que

$$\partial E = Et \ .$$ (On rappelle : $X_t = X[[t]]$).

Tous les corollaires sont triviaux, sauf le Corollaire 3, pour lequel on renvoie à Serre [1] LA Ch. IV. On ne les a donné ici que pour comparaison plus loin avec le cas d'un S arbitraire (cf. §6).

4.3 Une autre conséquence du théorème de décomposition est :

On considère $Z_t = Z(k)[[t]]$ comme coalgèbre en groupes sur $k[[t]]$. Si $u \in tZ_t$, alors $\exp u \in 1 + tZ_t$.

Théorème :(Campbell-Hausdorff): Il existe une unique $Y = \sum_{i=1}^{\infty} Y_i t^i \in P(Z_t)$ tel que $\xi = \exp Y$.

Démonstration : On identifie Z à $k\langle X\rangle$ (4.2 cor. 3), donc

$$F(n) = \exp (X_1 + \ldots + X_n)t = \sum F_{n,m} t^m$$

est une courbe dans Z . On écrit de façon unique $F_{n,m} = \sum_{\rho} F_{n,m,\rho}$ comme somme (finie) des parties $F_{n,m,\rho}$, isobares de poids ρ .

Définissons $G(n) = \sum_{\rho=0}^{\infty} (\sum_{m=0}^{\infty} F_{n,m,\rho})t^\rho = \sum G_{n,\rho} t^\rho$ ou ce qui revient au même

$$G(n) = \exp(X_1 t + \ldots + X_n t^n)$$

$G(n)$ est une courbe si et seulement si $\{G_{n,\rho} \mid \rho \in \mathbb{N}\}$ est une suite des puis-

sances divisées au-dessus de $1 \in Z$, condition que l'on vérifie être satisfaite, tenant compte que le diagonal d de Z est un morphisme d'algèbres graduées. De plus, par construction, $G(n)$ est isobare, $G(n) \equiv G(n+1) \bmod t^{n+1}$, d'où

$$G = \lim_n G(n) = \exp \sum_{i=1}^{\infty} X_i t^i$$

existe et est une courbe isobare. De plus G_i contient Z_i d'après le th. 4.1 a. Soit $G = H(\tilde{G})\xi$, alors $\tilde{G}$ est un automorphisme de Z dans GC_k, donc $\tilde{G}^{-1}$ existe dans GC_k et $H(\tilde{G}^{-1})\xi$ est une courbe isobare dans Z. Posons $\tilde{G}^{-1}(X_i) = Y_i$, alors Y_i est primitive, isobare et contient Z_i. On trouve :

$$\xi = H(\tilde{G}^{-1} \circ \tilde{G})\xi = H(\tilde{G}^{-1}) \exp \sum_{i=1}^{\infty} X_i t^i = \exp \sum_{i=1}^{\infty} Y_i t^i$$

ce qui démontre le théorème.

4.4 Le théorème entraîne :

<u>Corollaire</u> 1 : Soit $G \in Grf_k$, alors l'application

$$e_t : P(G^*)^{\mathbb{N}^+} \to H(G^*)$$

définie par $e_t((\partial_i \mid i \in \mathbb{N}^+)) = \exp \sum_{i=1}^{\infty} \partial_i t^i$ est bijective, ce qui permet d'écrire $\varphi \in H(G^*)$ uniquement sous la forme

$$\varphi = \exp \sum_{i=1}^{\infty} i^{-1} s_i(\varphi) t^i \quad \text{avec} \quad s_i(\varphi) \in P(G^*) \tag{4}$$

En effet $\varphi = H(\varphi) \exp \sum_{i=1}^{\infty} Y_i t^i = \exp \sum_{i=1}^{\infty} \varphi(Y_i) t^i$.

<u>Corollaire</u> 2 : $Z = k\langle Y \rangle$ et $v_a Y_i = Y_{i//a}$ pour tout $a,i \in \mathbb{N}^+$.

En effet $V_a \xi = \exp \sum_{i=1}^{\infty} Y_i t^{ai} = \exp \sum_{i=1}^{\infty} v_a(Y_i) t^i$.

<u>Corollaire</u> 3 : Soit $B = Q\langle U,W \rangle \in GC_k$ avec $U = \{U_i \mid i \in \mathbb{N}^+\}$, $W = \{W_i \mid i \in \mathbb{N}^+\} \subset P(B)$. On attache à U_i, W_i le poids i. Alors il existe pour $\geqslant 0$ un unique $z_i = z_i(U_1,\ldots,U_i,W_1,\ldots,W_i)$ dans $P(B)$, isobare de poids i, tel que pour tout $G \in Grf_k$ et tout $\varphi,\psi \in H(G)$ on ait

$$s_i(\varphi\psi) = z_i(s_1(\varphi),\ldots,s_i(\varphi),s_1(\psi),\ldots,s_i(\psi)) . \tag{5}$$

En effet, la courbe isobare produit $\exp(\sum_{i=1}^{\infty} i^{-1} U_i t^i)\exp(\sum_{i=1}^{\infty} i^{-1} W_i t^i)$ dans

B est une courbe, donc d'après le cor. 1 de forme unique $\exp(\sum_{i=1}^{\infty} i^{-1} z_i t^i)$ avec $z_i \in P(B)$. Le cor. en découle aisément. En posant $U_i = W_i = 0$ dans z_i on arrive au point de départ pour calculer de façon explicite la formule de Campbell-Hausdorff classique.(Serre [1] LA. Ch. IV).

4.5 A titre d'application aux groupes formels nous indiquons comment se démontre de façon courbique :

Théorème (Cartier) : Soit k un corps, $k \in \mathrm{Alg}_{\mathbb{Q}}$ et soit $G \in \mathrm{Grf}_k$ connexe, alors l'application canonique $P(G^*) \hookrightarrow G^*$ se prolonge en un isomorphisme $U(P(G^*)) \to G^*$ dans GC_k, autrement dit le foncteur covariant

$$\mathrm{Lie} : \{\text{Groupes formels connexes sur } k\} \to \{\text{Lie algèbres sur } k \text{ de dimension dénombrable}\}$$

est une équivalence des catégories.

Démonstration (abrégée, cf. SGAD VII B th. 3.3) :

a. On prend une base B de $P(G^*)$ que l'on prolonge en une base B_1 de G^*. Soient B_1^* la base topologique duale de B_1 et $B^* \subset B_1^*$ le sous ensemble qui constitue une base topologique duale de B. Soit donc $B = \{\partial_i \mid i \in \mathbb{N}^+\}$, $B^* = \{y_i \mid i \in \mathbb{N}^+\}$.

b. Les courbes $f(i) = \exp \partial_i t$ dans G^* satisfont à $f(i)(y_j) = \delta_{ij} t \bmod t^2$. En raisonnant comme dans le th. 3.5 on trouve $\{x_i \mid i \in \mathbb{N}^+\} \subset \theta(G)$ t.q. $\lim x_i = 0$ et $f(i)(x_j) = \delta_{ij} t$.

c. La connexité de G implique que $\theta(G)$ est engendrée par l'ensemble $\{x_i \mid i \in \mathbb{N}^+\}$, d'où : tout élément de $\theta(G)$ s'écrit sous somme simplement convergente $\Sigma \lambda_\alpha x^\alpha$ où les x^α sont des monômes de l'ensemble $\{x_i \mid i \in \mathbb{N}^+\}$. Le lemme 2 du §3.5 montre qu'il n'existe pas une relation non triviale $\Sigma \lambda_\alpha x^\alpha = 0$. Le lemme 1 montre que l'ensemble $F = \{\exp \partial_i t \mid i \in \mathbb{N}^+\}$ est fondamental.

d. D'après Serre [1] LA Ch. III, la base $B(F)$ de G^* est aussi une base de $U(P(G^*))$, ce qui entraîne que $U(P(G^*)) \simeq G^*$.

e. On définit S : {algèbres de Lie sur k de dimension dénombrable} → {Groupes formels connexes sur k} en posant $S(J) = Spf^*(U(J))$. Alors on a $Lie \circ S(J) \simeq Lie \circ Spf^*(U(J)) = Lie\{Spf(U(J))^*\} = P(U(J)^{**}) \simeq P(U(J)) \simeq J$ d'après Serre[1], loc. cit. De la même façon, $S \circ Lie(G) \simeq S(P(G^*)) \simeq Spf^*(U(P(G^*))) \simeq Spf^*(G^*)$ d'après d., ce qui est encore canoniquement isomorphe à $Spf(G^{**}) \simeq Spf(\theta(G)) \simeq G$. Le foncteur U à valeurs dans GC_k étant pleinement fidèle, le théorème s'ensuit.

§5. Sur la structure de Z^* et Z_c^*

5.1 La courbe $V_a\xi$ définit un endomorphisme v_a de $Z(k)$ dans GC_k qui satisfait à $v_a(Z_m) = Z_{m//a}$. L'action de v_a est étroitement liée à l'action de Frobenius $F : x \mapsto x^p$ en caractéristique p . De façon explicite :

Lemme : Soit $F : x \to x^p$ le Frobenius de $Z(\mathbb{F}_p)^*$, alors $v_p = F^*$.

Démonstration : Si $f = \Sigma f_m t^m$ est une courbe dans $Z(\mathbb{F}_p)$, on trouve

$$f(x^p) = f(x)^p = \Sigma f_m(x)^p t^{mp} = \Sigma f_m(x) t^{mp} = \Sigma f_m(x^p) t^m .$$

La comparaison des coefficients de t^n donne

$$\langle f_{n//p}, x\rangle = \langle f_n, Fx\rangle = \langle F^* f_n, x\rangle$$

d'où $F^* f_n = f_{n//p}$ pour $n \in \mathbb{N}$. F^* étant un morphisme de coalgèbres en groupes, est déterminé par ses valeurs $F^*(Z_m)$ ce qui donne le résultat voulu en prenant $f = \xi$, la courbe canonique.

Il résulte en particulier que $v_p(x) = 0$ pour tout $x \in P(Z(\mathbb{F}_p))$, en d'autres termes, v_p induit un morphisme $v_p : P(Z(\mathbb{Z})) \to pP(Z(\mathbb{Z}))$. Il semble en ce moment-ci peu opportun de donner des démonstrations des théorèmes 5.2 et 5.3 ci-dessous. Comme Cartier l'a observé, la démonstration de 5.2 qui figure dans Ditters [1] a l'air d'être trop optimiste. Une démonstration de 5.2 figurerait toutefois dans la thèse de Brian Shay, qui devrait contenir également des théorèmes concernant la structure de $P(Z(\mathbb{Z}))$. La démonstration de 5.3 a, qui est tri-

viale dans le cas commutatif (lemmes 7.2 a et 7.5 ci-dessous), qui figure dans Ditters [2] et utilise les familles de P. Hall est peu constructive. Il importerait de trouver des résultats explicites dans le cas non commutatif, qui redonnent les résultats du §7 ci-dessous. Le rôle du th. 5.3 a dans ce qui suit est de nature secondaire, mais devrait se justifier un jour dans une étude approfondie du relèvement de Frobenius à caractéristique zéro.

5.2 Théorème : Soit k arbitraire, alors $Z(k)^*$ et $Z_c(k)^*$ sont de Dieudonné.

5.3 Théorème : a) Soit $n \to \bar{n}$ l'application canonique $Z \to k$, k anneau de base arbitraire. Alors les morphismes induits

$$v_n : P(Z(k)) \to \bar{n}P(Z(k))$$

$$v_n : P(Z_c(k)) \to \bar{n}P(Z_c(k))$$

sont surjectifs.

b) De même façon, l'application canonique $P(Z(k)) \to P(Z_c(k))$ est surjective. On posera dans le reste de ce §, $Z = Z(k)$ et $Z_c = Z_c(k)$. On n'énonce que les résultats pour Z. Le cas Z_c étant tout pareil.

5.4 Corollaire : Soient $Y = \{Y_i \mid i \in \mathbb{N}^+\}$ et $Z^* = k[[Y]]$. Soit pour $i \in \mathbb{N}^+$, $\varphi_i \equiv 1 + u_i t \bmod t^2$ la courbe définie par $\varphi_i(Y_j) = \delta_{ij} t$. Alors :

a. $F = \{\varphi_i \mid i \in \mathbb{N}^+\}$ est un ensemble fondamental des courbes dans Z.

b. $u = \{u_i \mid i \in \mathbb{N}^+\}$ est une base de $P(Z)$.

Démonstration : On raisonne comme dans le th. 3.5, lemme 2.

5.5 De façon inverse :

Corollaire : Soit $v = \{v_i \mid i \in \mathbb{N}^+\}$ une base de $P(Z)$, alors les courbes $1 + v_i t$ s'étendent aux courbes infinies ψ_i dans Z et on a

a. $F' = \{\psi_i \mid i \in \mathbb{N}^+\}$ est un ensemble fondamental des courbes dans Z.

b. Il existe $X = \{X_i \mid i \in \mathbb{N}^+\} \subset Z^*$ tel que $Z^* = k[[X]]$ et $\psi_i(X_j) = \delta_{ij} t$ pour $i,j \in \mathbb{N}^+$.

Démonstration : On prend la base u du cor. 5.4 b., alors on a $v_i = \Sigma \lambda_{ij} u_j$, d'où $1 + v_i t \equiv \prod_j \lambda_{ij} \varphi_j \bmod t^2$. Le membre droit se compose de courbes infinies, ce qui nous donne les ϕ_i. Comme dans le th. 4.5 a on se choisit $x_i \in Z^*$ tq $\langle x_i, v_j \rangle = \delta_{ij}$. Comme dans le th. 3.5 on construit les X_i tels que $\phi_i(X_j) = \delta_{ij} t$, ce qui montre b ce qui entraîne à son tour c.

5.6 Corollaire :

a. Chaque courbe finie f dans Z s'étend à une courbe infinie φ.

b. Si encore f est r-isobare on peut prendre φ r-isobare..

Démonstration :

a. D'après le lemme 2.8 c il suffit de montrer que si $x \in P(Z)$, alors $1 + xt$ s'étend à une courbe infinie. Avec les notations du cor. 5.4 b on a $x = \Sigma \lambda_i u_i$, d'où $1 + xt \equiv \prod_i \lambda_i \varphi_i \bmod t^2$ ce qui donne a.

b. Soit m minimal tel que φ_m ne soit pas isobare de poids rm. Alors $\varphi_m = \varphi'_m + \partial$ où φ'_m est la partie homogène de poids rm de φ_m. Il en résulte que $\partial \in P(Z)$. Soit ψ une extension infinie de $1 - \partial t$, alors en considérant la courbe $\varphi \circ V_n \psi$ on gagne.

5.7 Soit $F = \{\varphi_i \mid i \in \mathbb{N}^+\}$ un ensemble fondamental des courbes dans Z, t.q $\varphi_i \equiv 1 + u_i t \bmod t^2$ et u_i soit homogène de poids $\phi(i)$. On suppose $\phi : \mathbb{N}^+ \to \mathbb{N}^+$ monotone. Soit de plus $k(\mathbb{N}^+, 2) = \{x = (x_{ij}) \in k^{\mathbb{N}^+ \times \mathbb{N}^+} \mid$ Pour chaque i on a $\mathrm{Card}\{j \mid x_{ij} \neq 0\} < \infty\}$. Alors :

Corollaire : L'application $f : k(\mathbb{N}^+, 2) \to H(Z)$, donnée par

$$f(x) = \prod_i \prod_j V_i x_{ij} \varphi_j \qquad \text{(produit ordonné)} \qquad (1)$$

est bijective. De plus $f(x)$ est isobare si et seulement si $f(x)$ s'écrit sous la forme

$$f(x) = \prod_i V_{\phi(i)} x_i \varphi_i \qquad (2)$$

Démonstration : Noter que le membre droit de (1) définit bien une courbe. Il s'ensuit que f est injective. Soit maintenant φ une courbe et supposons que

$$\varphi = \Sigma\, \varphi_m t^m \equiv \prod_{i=1}^{s-1} \prod_j V_i x_{ij} \varphi_j = \psi = \Sigma\, \psi_m t^m \bmod t^s \qquad (3)$$

alors $\varphi_s - \psi_s$ est primitif, d'où $\varphi_s - \psi_s = \Sigma\, x_{s,j} u_j$ (somme finie). On a donc

$$\chi = V_s \prod_j x_{s,j}\, \varphi_j \equiv 1 + (\varphi_s - \psi_s) t^s \bmod t^{s+1}$$

En considérant la courbe $\varphi\chi$ on voit que (3) est vrai mod t^{s+1} ce qui montre (1) par récurrence. Pour (2) on notera que $\varphi_s - \psi_s$ est homogène de poids s si et seulement si $x_{s,j} \neq 0$ implique $\psi(j) = s$, ce qui donne (2).

5.9 Soient $Y = \{Y_i \mid i \in \mathbb{N}^+\}$, $X = \{X_i \mid i \in \mathbb{N}^+\}$ et $B = k[Y,X]$. Avec les notations de 5.4 on pose $Z^* = k[[Y]]$ et $Z^* \hat{\otimes} Z^* = k[[Y,X]] \supset B$. Alors le morphisme structural d de Z^* se donne par les deux relations

$$\prod_{i=1}^{\infty} V_{\psi(i)} {}^{Y_i}\varphi_i \prod_{i=1}^{\infty} V_{\psi(i)} {}^{X_i}\varphi_i = \prod_{i=1}^{\infty} V_{\psi(i)} {}^{F_i}\varphi_i \qquad (4)$$

$$dY_i = F_i \in B \qquad \text{pour } i \in \mathbb{N}^+ . \qquad (5)$$

En effet le membre gauche de (4) est un produit de deux courbes génériques sur un anneau de base convenable C, donc est une courbe dans $Z(C)$ avec $F_i \in C$ d'après (2). Soit $x = (x_i \mid i \in \mathbb{N}^+) \subset G$,

alors on vérifie qu'il existe $U = \{U_i \mid i \in \mathbb{N}^+\} \subset Z(C)$ telle que $Z(C) \simeq C[[U]]$ et telle que

$$\Big(\prod_{i=1}^{\infty} V_{\psi(i)} {}^{x_i}\varphi_i\Big)(U_j) = x_j t^{\psi(j)}$$

Ecrivons (4) sous forme $fg = h$, alors on a

$$h(U_i) = F_i t^{\psi(i)}$$

$$= fg(U_i) = m \circ f \hat{\otimes} g \circ dU_i$$

$$= \text{coefficient de } t^{\psi(i)} \text{ dans } dU_i .$$

Exemple : Soient $u_1 = Z_1$, $u_2 = 2Z_2 - Z_1^2$, $u_3 = [Z_1, Z_2]$, $u_4 = 3Z_3 - 3Z_1Z_2 + Z_1^3$ alors on trouve : $F_1 = X_1 + Y_1$, $F_2 = X_2 + Y_2 - X_1Y_1$; $F_3 = X_3 + Y_3 - X_1^2Y_1 - 2X_2Y_1$, $F_4 = X_4 + Y_4 - X_1^2Y_2 - X_2Y_1^2$.

§6. Les théorèmes fondamentaux dans le cas non commutatif

On reprend ici la situation du §4, mais pour un anneau k arbitraire. Soient $S = S(k)$ et $Z = Z(k)$. ξ est la courbe canonique.

6.1 Définition : On dit qu'une courbe isobare $E = \sum^{n} E_m t^m \equiv 1 + Z_1 t \bmod t^2$ d'ordre n dans Z est une courbe pure si $\mathrm{Im}E$ est la sous algèbre (nécessairement libre) de Z engendrée par les E_m avec $m \in \mathbb{N}(S)$.

6.2 Motivation : Si $k = \mathbb{Z}_p$ alors on a vu que la courbe $\exp Z_1 t \bmod t^p$ ne s'étend pas dans $k[Z_1] \subset Z(k)$, mais s'étend à une courbe infinie φ dans $Z(k)$ d'après le cor. 5.6 a. La condition que $\varphi \bmod t^{p^2-1}$ est pure signifie que cette courbe est dans $k\langle\varphi_1, \varphi_p\rangle$. Dans ce § on démontrera que telles courbes pures existent et que la notion "pure" est liée à la façon la plus économique afin d'étendre $1 + Z_1 t$ à une courbe infinie dans une sous algèbre aussi petite que possible de $Z(k)$.

6.3 On posera généralement

$$Y_m = \begin{cases} E_m & \text{si} \quad m \in \mathbb{N}(S) \\ 0 & \text{sinon} \end{cases}$$

de sorte qu'une courbe pure E d'ordre n s'écrit sous la forme

$$E = \sum_{m=1}^{n} E_m(Y_1, \ldots, Y_m) t^m \qquad (1)$$

donc si $\varphi \in H(Z)$, on a $H(\varphi)E = \sum_{m=1}^{n} E_m(\varphi Y_1, \ldots, \varphi Y_m) t^m$, ce qui donne lieu à :

Définition : Soit E une courbe pure d'ordre n dans Z et soit $r \leqslant n$. On dit que $n = (n_m \mid 1 \leqslant m \leqslant s,\ n_m = 0 \text{ si } m \notin \mathbb{N}(S)) \subset G \in GC_k$ est un ensemble pur pour E si

$$\sum_{m=1}^{r} E_m(n_1, \ldots, n_m) t^r \qquad (2)$$

est une courbe d'ordre r dans G. Soit maintenant $\tau(r) > r$ minimal tel que $\tau(r) \in \mathbb{N}(S)$, alors il suit de (1) que la courbe (2) s'étend de façon naturelle à une courbe d'ordre $\min\{n, \tau(r)-1\}$. Cette courbe sera notée $E(n)$, et on dira en-

core que $E(n)$ est une courbe pure pour E .

6.4 Théorème (Décomposition) : Soient k un anneau et $S = S(k)$. Alors il existe une courbe pure $E = \Sigma\, E_m(Y_1,\dots,Y_m)t^m$ d'ordre infini dans Z et pour chaque $m = (n,n^*) \in \mathbb{N}(S) \times \mathbb{N}(S^*)$ il existe un élément isobare $Y_{n,n^*} \in Z$ uniquement déterminé par les propriétés suivantes

a. Y_{n,n^*} contient Z_m .

b. Pour $n^* \in \mathbb{N}(S^*)$, l'ensemble $\{Y_{n,n^*} \mid n \in \mathbb{N}(S)\}$ est pur pour E et définit la courbe n^*-isobare $H_{n^*} = \Sigma\, E_n(Y_{1,n^*},\dots,Y_{m,n^*})t^m$.

c. $\xi = \prod\limits_{n^* \in \mathbb{N}(S^*)} V_{n^*} H_{n^*}$ dans $\mathrm{Iso}(k)$ (produit ordonné).

d. Si $m \in \mathbb{N}(S)$, alors $v_m\, Y_{n,n^*} = Y_{n//m,n^*}$ et $v_m\, E_n = E_{n//m}$ pour tout $n \in \mathbb{N}^+$.

Remarque : Si $S = \emptyset$, on retrouve le théorème 4.1.

Démonstration : On procède par récurrence. Soit pour $n \in \mathbb{N}^+$, $n \geqslant 2$, $P(n)$ l'hypothèse suivante :

$P(n,1)$: Il existe une courbe pure $E(n)$ d'ordre $n-1$ dans Z .

$P(n,2)$: Il existe un ensemble $S(n) = \{Y_{a,a^*} \mid aa^* \leqslant n-1$, $a \in \mathbb{N}(S)$ et $a^* \in \mathbb{N}(S^*)\}$, tel que Y_{a,a^*} soit isobare et contienne Z_{aa^*} et tel que pour tout $a^* \in \mathbb{N}(S^*)$ le sous ensemble $S(n,a^*) = \{Y_{b,a^*} \mid b \in \mathbb{N}(S)\}$ soit pur pour $E(n)$.

Soit $\bar{b} \in \mathbb{N}(S)$ maximal tel que $Y_{\bar{b},a^*}$ appartienne à $S(n,a^*)$ alors d'après 6.3, l'ordre de la courbe $E(n)(S(n,a^*))$ est égal à $\min\{n-1\,,\,\tau(\bar{b})-1\}$. Supposons que le minimum est $\tau(\bar{b})-1$, alors d'après 2.5 c, l'ordre de la courbe $V_{a^*}E(n)(S(n,a^*))$ est donc égal à $a^*\{\tau(\bar{b})-1\} + a^* - 1 = a^*\tau(\bar{b}) - 1 \geqslant n-1$, parce que si $\bar{b}$ est maximal on a : $a^*\bar{b}$ est maximal, tel que $a^*\bar{b} \leqslant n-1$ et puisque $\tau(\bar{b}) > \bar{b}$ on a $a^*\tau(\bar{b}) > n-1$, ce qui entraîne $a^*\tau(\bar{b}) - 1 \geqslant n-1$. Si le minimum est égal à $n-1$, cette courbe est d'ordre $a^*n-1 \geqslant n-1$. On notera donc $W(n,a^*)$ la restriction de $V_{a^*}E(n)(S(n,a^*))$ à une courbe d'ordre $n-1$.

$P(n,3)$: $\xi_{n-1} \equiv \prod\limits_{a^*} W(n,a^*)$ dans $\mathrm{Iso}(Z(n-1))$.

$P(n,4)$: Si $m \in \mathbb{N}(S)$, alors $v_m Y_{a,a^*} = Y_{a//m,a^*}$ et $v_m E_r = E_{r//m}$ pour $1 \leqslant r \leqslant n-1$.

On voit tout de suite que $P(2)$ est en effet vrai : Prendre $E(2) = 1 + Z_1 t = 1 + Y_{1,1} t$. On suppose donc $P(n)$ vrai. Soit $n = (m,m^*)$ la décomposition de $n \in \mathbb{N}^+$. On considérera les trois situations suivantes :

Cas A : $m = 1$, c'est-à-dire $n = m^* \in \mathbb{N}(S^*)$.

On étend la courbe $W(n,1)$ d'ordre $n-1$ à une courbe isobare F d'ordre n (cor. 5.6). Si $F = W(n,1) + F_n t^n$ et si F_n contient αZ_n avec $\alpha \neq 0$, alors d'après le théorème 5.3 b et le lemme 7.2 b ci-dessous qui est indépendant de ce §, il existe $\partial \in P(Z)$ isobare de poids n , qui contient $-\alpha Z_n$, puisque n est inversible dans Z . Alors la courbe $F' = W(n,1) + (F_n + \partial)t^n$ est encore une extension de $W(n,1)$ mais maintenant dans $Z(n-1) = k\langle Y_{a,a^*}\rangle_{aa^*<n}$. Soit φ le morphisme dans GC_k de $Z(n-1)$ qui envoie Y_{a,a^*} sur $Y_{a,1}$. On pose $E(n+1) = H_n(\varphi)(F') = W(n+1,1)$ qui est en effet une courbe d'ordre n dans $\mathrm{Im}E(n)$.

On considère $S(n,a^*)$ pour $a > 1$ avec les notations de $P(n,2)$. Alors $a^*\tau(\bar{b}) \geqslant n = m^*$ entraîne que $a^*\tau(\bar{b}) > n$, parce que $a^*\tau(\bar{b}) = n = m^*$ implique $\tau(\bar{b}) = 1$ ce qui est impossible. De plus si $a^* > 1$ alors $a^*n-1 \geqslant n-1$. Soit donc pour $a^* > 1$, $W(n+1,a^*)$ la restriction de $V_{a^*}E(n)(S(n,a^*))$ à une courbe d'ordre n . $P(n,3)$ donne maintenant

$$\xi_n \equiv \prod_{n>a^*\geqslant 1} W(n+1,a^*) := \sum^{n} G_m t^m \bmod t^n \qquad (1)$$

Posons $Z_n - G_n = Y_{1,m^*} = Y_{1,n}$ qui est primitif et isobare de poids n . On pose également $W(n+1,m^*) = 1 + Y_{1,m^*}t$

$$S(n+1,m^*) = \{Y_{1.m^*}\} \quad \text{et} \quad S(n+1,a^*) = S(n,a^*) \quad \text{si} \quad a^* < m^* .$$

Alors (1) donne :

$$\xi_n = \prod_{n\geqslant a^*\geqslant 1} W(n+1,a^*) \quad \text{dans} \quad \mathrm{Iso}(Z(n))$$

d'où $P(n+1,1)$, $P(n+1,2)$ et $P(n+1,3)$. De plus pour $P(n+1,4)$ il suffit de considérer $v_b Y_{1.m^*}$ et $v_b E_{m^*}$ qui sont nulles puisque isobares de poids $m^*//b = 0$.

Cas B : $m^* = 1$, c'est-à-dire $n = m \in \mathbb{N}(S)$.

On prolonge $W(n,1)$ à une courbe isobare F . Si $a^* > 1$ on considère la relation $a^*\tau(\bar{b}) \geqslant n$. $a^*\tau(\bar{b}) = n \in \mathbb{N}(S)$ étant exclu, on a $a^*\tau(\bar{b}) > n$ ce qui permet également de poser $W(n+1,a^*)$ égal à la restriction de $V_{a^*}E(n)(S(n,a^*))$ à une courbe d'ordre n . Avec $P(n,3)$ on voit

$$\xi_n \equiv F \prod_{1<a^*<n} W(n+1,a^*) := \sum^{n} G_m t^m \bmod t^n \qquad (2)$$

ce qui entraîne que $Z_n - G_n = \partial$ est primitif et isobare.

On pose $W(n+1,1) = F + \partial t^n$ ce qui implique que $P(n+1,3)$ est vrai.

L'ensemble des courbes $f = \sum^{n} f_m t^m$ dans $Z(n)$, telles que $v_b f_m = f_{m//b}$ pour $1 \leqslant m \leqslant n$ et $b \in \mathbb{N}(S)$ constitue un sous-groupe qui contient ξ_n et les $W(n+1,a^*)$ avec $a^* > 1$ donc contient nécessairement $W(n+1,1)$. On pose $Y_{n,1}$ le coefficient de t^n dans $W(n+1,1)$. Les autres modifications sont évidentes.

Cas C : $n = mm^*$, $m > 1$, $m^* > 1$.

On étend maintenant deux courbes, à savoir $W(n,1)$ à une courbe isobare M d'ordre n et $W(n,m^*)$ à une courbe isobare F d'ordre n . D'après le th. 5.3a on peut supposer que $v_a M_n = M_{n//a}$ et $v_a F_n = F_{n//a}$ pour tout $a \in \mathbb{N}(S)$.

En vue de $v_m F_n = F_{m^*}$ on voit que F_n contient $Z_{mm^*} = Z_n$, de sorte que l'on ait

$$Z(n) = k\langle Y_{a,a^*}, F_n \rangle_{aa^*<n}$$

On définit φ d'abord comme un endomorphisme de l'algèbre $Z(n)$ par $\varphi(Y_{a,a^*}) = Y_{a,1}$, $\varphi(F_n) = Y_{m,1}$ et on notera qu'en effet φ est un morphisme dans GC_k . Soit $E(n+1) = W(n+1,1) = H_n(\varphi)M$, alors parce que φ et v_a commutent si $a \in \mathbb{N}(S)$, on voit que $E(n+1) = \Sigma E'_r t^r$ satisfait à $v_a E'_r = E'_{r//a}$.

Si $a^* \notin \{1, m^*\}$, on voit comme dans les autres cas que $a^*\varphi(b') \geqslant n$, donc pour ces valeurs de a^* on pose $W(n+1,a^*)$ la restriction de $V_{a^*}E(n)(S(n,a^*))$ à une courbe d'ordre n . Il suit que

$$\xi_n \equiv \prod_{a^*<m^*} W(n+1,a^*).F.\prod_{a^*>m^*} W(n+1,a^*) := \Sigma G_r t^r \bmod t^n$$

d'où : $Z_n - G_n = \partial \in P(Z)$. On pose $W(n+1,m^*) = F + \partial t^n = W(n,m^*) + Y_{m,m^*} t^n$, $S(n+1,a^*) = S(n,a^*)$ si $a^* \neq m^*$ et $S(n+1,m^*) = S(n,m^*) \cup \{Y_{m,m^*}\}$. Parce que $1+\partial t^n$ appartient au centre de $H_n(Z)$ il suit que

$$\xi_n \equiv \prod_{a^*<n} W(n+1,a^*) \bmod t^{n+1} .$$

Le fait que tous les ξ_n et $W(n+1,a^*)$ pour $a^* \neq m^*$ commutent avec v_a pour $a \in N(S)$, entraîne immédiatement que $W(n+1,m^*)$ aussi commute avec tels v_a d'où en particulier $v_m Y_{m,m^*} = Y_{1,m^*} = Z_{m^*} + u_{m^*}(Z_1,\ldots,Z_{m^*-1})$, c'est-à-dire Y_{m,m^*} contient Z_n .

Il résulte que $P(n)$ est vrai pour tout n . Parce que $W(n,a^*) \equiv W(n+1,a^*) \bmod t^n$, la limite $V_{a^*} H_{a^*} = \lim_n W(n,a^*)$ existe. On prend $E = H_1$ comme courbe pure isobare ce qui achève le théorème.

6.5 Les courbes pures ne sont pas uniques dans le cas non commutatif. Les sous objets de Z qu'elles déterminent sont toutefois uniques à isomorphie près en vue du

Lemme : Soient E et F deux courbes pures telles que $v_a E_m = E_{m//a}$ et $v_a F_m = F_{m//a}$ pour $a \in \mathbb{N}(S)$ et $m \in \mathbb{N}^+$, alors $\mathrm{Im}E \simeq \mathrm{Im}F$ dans GC_k .

Démonstration : Les données entraînent que pour $a \in \mathbb{N}(S)$ on ait, $E_a = Z_a + u_a(Z_1,\ldots,Z_{a-1})$ et $F_a = Z_a + v_a(Z_1,\ldots,Z_{a-1})$. Considérons l'application composée

$$\mathrm{Im}E \xrightarrow{j} Z \xrightarrow{F} \mathrm{Im}F$$

où j est l'injection canonique. Alors $F \circ j(E_a) = F\{Z_a + u_a\} = F_a + u_a(F_1,\ldots,F_{a-1})$ donc $F \circ j$ applique l'ensemble des générateurs libres de $\mathrm{Im}E$ bijectivement sur l'ensemble des générateurs libres de $\mathrm{Im}F$.

6.6 Dans ce qui suit on fixera une courbe pure E et on posera

$$U(k) = \mathrm{Im}E = k\langle Y_a \rangle_{a \in \mathbb{N}(S)}$$

$$dY_a = \sum_{m+n=a} E_m \otimes E_n \quad ; \quad (Y_a = E_a \text{ pour } a \in \mathbb{N}(S)) .$$

On a les endomorphismes v_a de $U(k)$, définis pour $a \in \mathbb{N}(S)$, satisfaisant à $v_a Y_b = Y_{b//a}$. De plus : $v_a E_n = E_{n//a}$ pour $n \in \mathbb{N}^+$. Il est clair que si $G \in GC_k$, alors l'ensemble $GC_k(U(k),G)$ s'identifie canoniquement à l'ensemble des ensembles purs pour E dans G. Dans le cas commutatif, l'objet correspondant sera noté par $U_c(k)$. Si $G \in Grfc_k$, on note $C_S(G) = Ab_k(U_c(k),G^*)$ ce qui s'identifie canoniquement au groupe abélien des courbes pures pour E, encore appelé groupe des courbes S-typiques, ou des courbes typiques.

6.7 Comme dans 4.2, le théorème de décomposition entraîne les corollaires suivants :

Corollaire 1 : Soit $G \in Grf_k$, alors l'application

$$e : GC_k(U(k),G)^{\mathbb{N}(S^*)} \to H(G^*)$$

définie par $e((\xi_{a,a^*} \mid a \in \mathbb{N}(S), a^* \in \mathbb{N}(S^*)) = \prod_{a^*} (\Sigma E_n(\xi_{1,a^*},\dots,\xi_{n,a^*})t^{a^*n})$ est bijective, ce qui permet d'écrire $\varphi \in H(G^*)$ uniquement sous la forme

$$\varphi = \prod_{a^* \in \mathbb{N}(S^*)} V_{a^*} H_{a^*}(\varphi) .$$

Corollaire 2 : $Z = k\langle Y_{a,a^*}\rangle$ est somme amalgamée de Card $\mathbb{N}(S^*)$ copies de $\mathrm{Im}E = U(k)$.

On conjecture :

Corollaire 3 : $U(k)$ est un sous objet minimal de Z dans lequel $1 + Z_1 t$ s'étend à une courbe infinie.

Corollaire 4 : Les propriétés d'isobaricité entraînent un théorème de décomposition pour les sous objets $Z(n)$ de Z et pour les courbes finies.

Corollaire 5 : Il existe une k_t-dérivation ∂ de $U(k)_t$, telle que $\partial E = Et$.

Démonstration : Soit $U(k) = k\langle Y_a\rangle_{a \in \mathbb{N}(S)}$ et soit $\{M_\alpha \mid \alpha \in T\}$ une base de monômes dans les indéterminés Y_a. On prend $\{N_\alpha \mid \alpha \in T\} \subset U(k)^*$ la base duale. En particulier on note N l'élément de cette base tel que $\langle N, Y_1\rangle = 1$. Soit ∂ l'application composée

$$\partial : U(k) \to U(k) \otimes U(k) \xrightarrow{1 \otimes N} U(k) \otimes k \simeq U(k) .$$

Alors on vérifie que $dN = N \hat{\otimes} 1 + 1 \hat{\otimes} N$, ce qui entraîne que ∂ est une dérivation et on a bien

$$\partial E_n = 1 \otimes N\Big(\sum_{a+b=n} E_a \otimes E_b \Big) = E_{n-1} \text{ , d'où le corollaire.}$$

6.8 Afin de déduire le théorème de Campbell-Hausdorff (4.3) on pose pour $G \in Grf_k$, $CS(G) = (tG_t^*)^{\mathbb{N}(S)}$. Si $\eta = (\eta_a \mid a \in \mathbb{N}(S)) \in CS(G)$ alors

$$E(\eta) = \sum_{n=0}^{\infty} E_n(\eta_1, \ldots, \eta_n)$$

est bien défini et appartient à $1 + tG_t^*$.

Soit $L(G) = GC_k(U(k), G^*)$ et soit $L_v(Z) = \{\xi = (\xi_a \mid a \in \mathbb{N}(S)) \in L(Z) \mid v_b \xi_a = \xi_{a//b}$ pour tout $a,b \in \mathbb{N}(S)\}$. De plus, si $\xi = (\xi_a \mid a \in \mathbb{N}(S)) \in L(G)$, on pose $E(\xi,t) = \Sigma\, E_n(\xi_1, \ldots, \xi_n) t^n$. oSoit $D = k\langle X_a, Y_a \rangle_{a \in \mathbb{N}(S)}$ l'objet de GC_k défini par la condition que $X = \{X_a \mid a \in \mathbb{N}(S)\}$ et $Y = \{Y_a \mid a \in \mathbb{N}(S)\}$ appartiennent à $L(D)$, c'est-à-dire X et Y sont des ensembles purs pour E , alors le théorème de décomposition entraîne que

$$E(X,t)E(Y,t) = \prod_{a^* \in \mathbb{N}(S^*)} V_{a^*} H_{a^*} .$$

Soit donc H_1 défini par l'ensemble pur pour E , noté $X * Y = ((X * Y)_a \mid a \in \mathbb{N}(S))$, alors on voit que

$$(X * Y)_a = X_a + Y_a + g_a(X_1, \ldots, X_{a-1}, Y_1, \ldots, Y_{a-1})$$

$$g_a(X_1, \ldots, X_{a-1}, 0, \ldots, 0) = 0 .$$

L'application $U(k) \to D$ dans GC_k , définie par $Y_a \mapsto (X * Y)_a$ induit une loi de composition, fonctorielle en $G \in Grf_k$

$$* : L(G) \times L(G) \to L(G) .$$

En général, $*$ n'est pas une loi associative. Dans le cas commutatif, $*$ induit la structure du groupe abélien sur $L(G)$.

On a vu que $Z = k\langle Y_{a,a^*} \rangle_{a \in \mathbb{N}(S), a^* \in \mathbb{N}(S^*)}$ et pour chaque a^* , $Y(a^*) = \{Y_{a,a^*} \mid a \in \mathbb{N}(S)\} \in L_v(Z)$. On définit par récurrence $S(n) \in L(Z)$ par :

$$S(1) = Y(1)$$

$$S(n+1) = \begin{cases} S(n) & \text{si } n+1 \notin \mathbb{N}(S^*) \\ S(n) * Y(n+1) & \text{si } n+1 \in \mathbb{N}(S^*) \end{cases} .$$

Il n'est pas difficile de voir que $S(n)$ appartient en effet à $L_v(Z)$ pour tout n . De plus, si $S(n) = \{S(a,n) \mid a \in \mathbb{N}(S)\}$ alors

$$S(a,n+1) = S_{a,n} + Y_{a,n+1} + g_a(S_{1,n+1}, \ldots, Y_{a-1,n+1})$$

($Y_{a,n+1} = 0$ si $n+1 \notin \mathbb{N}(S^*)$) . Parce que $Y_{a,n+1}$ ne contient que des termes de poids $\geqslant n+1$, on voit

$$S_{a,n+1} = S_{a,n} + \text{termes de poids} \geqslant n+1 .$$

On définit $\phi : Z \to Z_t$ par $\phi(Z_j) = Z_j t^j$ et on pose $\xi(a,n) = \phi S(a,n)$, alors $\xi(n) = (\xi(a,n) \mid a \in \mathbb{N}(S)) \in CS(Z)$ et $E(\xi(n))$ est une courbe dans Z . Cela se voit de la même façon que dans la démonstration du théorème 4.3, où l'on a construit la courbe $G(n)$ à partir de la courbe $F(n)$. On voit de la même façon que

$$E(\xi(n)) \equiv E(\xi(n+1)) \bmod t^{n+1}$$

et en posant $E(\xi) = \lim_n E(\xi_n)$ on voit que $E(\xi)$ est une courbe isobare qui définit un automorphisme de Z dans GC_k . De la même façon que dans 4.3 on déduit

6.9 Théorème (Campbell-Hausdorff-Dieudonné) : Soit E la courbe pure, alors il existe un unique $\eta \in CS(Z)$ tel que pour la courbe canonique ξ on ait :

$$\xi = E(\eta) .$$

6.10 Comme dans 4.4 on en déduit les corollaires :

Corollaire 1 : Soit $G \in Grf_k$, alors chaque courbe φ dans G s'écrit de façon unique $\varphi = E(\eta(\varphi))$ avec $\eta(\varphi) \in CS(G)$.

Corollaire 2 : Comme dans 4.4 Corollaire 3 on construit des séries universelles η telles que pour chaque $G \in Grf_k$ et chaque couple des courbes φ, ψ dans G on ait

$$E(\eta(\varphi))E(\eta(\psi)) = E(\eta(\varphi.\psi)) \ .$$

Noter que l'isobaricité permet de trouver aussi un théorème de Campbell-Hausdorff-Dieudonné pour les courbes finies. Les résultats trouvés ici généralisent ceux de Dieudonné V à un anneau de base quelconque.

§7. Le cas commutatif. Frobenius et anneaux de Cartier

7.1 Soit d'abord l'anneau de base k égal à $\mathbb{Z}$. On pose $\mathbf{Ab} = \mathbf{Ab}_{\mathbb{Z}}$. Si $G \in \mathbf{Ab}$ on identifie $C(G)$ avec son image canonique dans $C(G \otimes \mathbb{Q})$.

Donc, si $\varphi \in C(G)$ on a par 4.2 cor. 1 soit par 4.4 cor. 1 :

$$\sum \varphi_n t^n = \varphi = \exp \sum_{n=1}^{\infty} n^{-1} \sigma_n(\varphi) t^n \qquad (1)$$

avec $\sigma_n(\varphi) \in P(G \otimes \mathbb{Q})$, uniquement déterminé par φ.

En posant $B_{n,m} = \{(\alpha_1,\ldots,\alpha_n) \in \mathbb{N}^n \mid \Sigma\, i\alpha_i = n \ ; \ \Sigma\, \alpha_i = m\}$ on trouve en prenant le logarithme dans (1) :

$$\sigma_n(\varphi) = \sum_{m=1}^{n} (-1)^{m+1} (m-1)!n \sum_{B_{n,m}} \frac{\varphi_1^{\alpha_1} \ldots \varphi_n^{\alpha_n}}{\alpha_1! \ldots \alpha_n!} \qquad (2)$$

Parce que $(m-1)!n/\alpha_1! \ldots \alpha_n! \in \mathbb{Z}$ si $(\alpha_1,\ldots,\alpha_n) \in B_{n,m}$ on voit donc que $\sigma_n(\varphi) \in P(G)$. On pose $\sigma_n = \sigma_n(\xi)$ où ξ est la courbe canonique.

7.2 Lemme : a. σ_n est isobare de poids n et $\{\sigma_n \mid n \in \mathbb{N}^+\}$ est une base de $P(Z_c)$. $(Z_c = Z_c(\mathbb{Z}))$.

b. $\sigma_n \equiv nZ_n - (-Z_1)^n \bmod Z_2 = \ldots = Z_{n-1} = 0$.

Démonstration : b se déduit immédiatement de (2). Pour a : σ_n est évidemment isobare. Soit $x \in P(Z_c)$ que l'on peut supposer en outre isobare de poids t. On écrit

$$x = \sum_{i=0}^{r} \lambda_i Z_n^i \quad \text{avec} \quad \lambda_i \in Z_c(n-1) \ , \ \lambda_r \neq 0 \ .$$

Alors en considérant le terme $\lambda_r \otimes Z_n^r$ dans dx on conclut que $r = 1$ et $\lambda_1 \in \mathbb{Z}$, d'où $n = t$. En passant à $Z_c \otimes \mathbb{Q}$ on peut appliquer le même raisonnement à l'élément primitif $x - \mu\sigma_t$ avec $\mu \in \mathbb{Q}$ choisi tel que $x - \mu\sigma_t \in Z_c(t-1)$. Il s'en-

suit que $x - \mu\sigma_t = 0$ mais dans ce cas on a nécessairement $\mu \in \mathbb{Z}$, sinon x n'appartiendrait pas à $P(Z_c)$.

7.3 Soient maintenant k un anneau de base quelconque et $G \in \mathbf{Ab}_k$. On considère $\varphi \in C(G)$ comme un morphisme

$$\varphi : Z_c(k) \to G . \tag{3}$$

On notera encore σ_m l'image de $\sigma_m \in P(Z_c(\mathbb{Z}))$ sous l'application canonique $Z_c(\mathbb{Z}) \to Z_c(k)$ et en particulier, par abus de notation on pose

$$\sigma_m(\varphi) = \text{l'image de } \sigma_m \in Z_c(k) \text{ sous (3).} \tag{4}$$

En observant que la courbe canonique ξ s'écrit

$$\xi = \exp \sum_{n=1}^{\infty} n^{-1}\sigma_n t^n$$

on voit que pour $\mathbf{Ab}_{\mathbb{Z}}$, (1) n'est autre que la relation $H(\varphi)\xi = \varphi$.

Lemme : Soit k arbitraire et $G \in \mathbf{Ab}_k$. Il existe pour $a \in \mathbb{N}^+$ un endomorphisme F_a, dit de Frobenius, de $C(G)$, fonctoriel en G tel que

$$\sigma_m(F_a\varphi) = \sigma_{am}(\varphi) \quad \text{pour tout } m \in \mathbb{N}^+ \text{ et tout } \varphi \in C(G).$$

Démonstration : Par fonctorialité il suffit de vérifier que $F_a\xi$ est une courbe dans $C(Z_c(k))$. En effet, $F_a\varphi = F_aH(\varphi)\xi = H(\varphi)(F_a\xi)$. En outre on peut prendre $k = \mathbb{Z}$ et dans $Z_c(\mathbb{Q})$ on a $F_a\xi = \exp \sum_{n=1}^{\infty} n^{-1}\sigma_{an}t^n$, ce qui est évidemment une courbe dans $C(Z_c(\mathbb{Q}))$ en vue de 4.4 cor. 1. $F_a\xi = \Sigma F_{a,m}t^m \equiv 1 + \sigma_a t \bmod t^2$. Soit donc $n > 1$ minimal tel que $F_{a,n}$ appartienne à $Z_c(\mathbb{Q})$ mais non à $Z_c(\mathbb{Z})$. Soit, par le cor. 5.6 b, $\Sigma D_m t^m$ une extension a-isobare de $\sum_{}^{n-1} F_{a,m}t^m$ dans $Z_c(\mathbb{Z})$. (Noter que $F_a\xi$ est bien a-isobare).

Il suit que $F_{a,n} - D_n = \lambda\sigma_{an}$ avec $\lambda \in \mathbb{Q}-\mathbb{Z}$. En effet, la différence est isobare de poids an et primitive, donc d'après 7.2 a, une multiple de σ_{an}, tandis que $\lambda \in \mathbb{Z}$ entraînerait que $F_{a,n} \in Z_c(\mathbb{Z})$, contrairement à l'hypothèse. Par 7.2 b on voit que le coefficient de Z_1^{an} dans $F_{a,n}$ n'appartient pas à $\mathbb{Z}$, ce qui permet de raisonner modulo $Z_i = 0$ pour $i > 1$. Or, d'après 7.2 b on voit

$$F_a\xi \equiv \exp \sum_{n=1}^{\infty} (-1)(-Z_1)^{an} \frac{t^n}{n} = \exp \circ \log(1-(-Z_1)^a t) = 1-(-Z_1)^a t \ .$$

On a donc obtenu une contradiction. Il en résulte que $F_a\xi$ est une courbe dans $Z_c(\mathbb{Z})$ ce qui démontre le lemme.

7.4 Soit maintenant k arbitraire et soit $S = S(k)$. Si E est une courbe pure, définissant $U_c(k)$ (cf. 6.6) on a dans le cas que l'anneau de base est $\mathbb{Z}_{S(k)}$:

$$\xi = \exp \sum_{n=1}^{\infty} n^{-1}\sigma_n t^n = \sum_{a^* \in \mathbb{N}(S^*)} V_{a^*} \exp \sum_{a \in \mathbb{N}(S)} (aa^*)^{-1}\sigma_{aa^*} t^a \qquad (5)$$

ce qui montre que la courbe pure E est unique et s'écrit

$$E = \exp \sum_{a \in \mathbb{N}(S)} a^{-1}\sigma_a t^a \qquad (6)$$

En posant $E = \Sigma\, E_m t^m = \Sigma\, E_m(Y_1,\dots,Y_m)t^m$, où $E_a = Y_a$ si $a \in \mathbb{N}(S)$ et $Y_b = 0$ si $b \notin \mathbb{N}(S)$, on a $U_c(\mathbb{Z}_{S(k)}) = \mathbb{Z}_{S(k)}[Y_a]_{a \in \mathbb{N}(S)}$ et $U_c(k)$ s'obtient en appliquant le morphisme canonique $\mathbb{Z}_{S(k)} \to k$. On trouve donc une généralisation de la construction de la série hyperexponentielle de Dieudonné III, §5 qui correspond au cas $S(k) = \{p\}$, p premier. On a également l'endomorphisme v_m pour $m \in \mathbb{N}(S)$ de $U_c(k)$, défini par $v_m(Y_a) = Y_{a//m}$ et satisfaisant à $v_m E_n = E_{n//m}$.

On a une injection canonique $U_c(k) \hookrightarrow Z_c(k)$ ainsi qu'une injection du groupe des courbes $S(k)$-typiques $C_S(G)$ dans $C(G)$ pour $G \in \mathrm{Ab}_k$. On trouve sans peine que $\{\sigma_m \mid m \in \mathbb{N}(S)\}$ est une base de $P(U_c(k)) \subset P(Z_c(k))$. Noter que si $\varphi \in C_S(G)$ alors $F_b\varphi = 0$ si $b \notin \mathbb{N}(S)$ et que pour $a \in \mathbb{N}(S)$, alors $F_a\varphi$, qui se trouve dans $C(G)$, d'après 7.3, est encore S-typique. De même, $V_a\varphi \in C_S(G)$ pour $a \in \mathbb{N}(S)$.

7.5 On va ramasser les opérateurs fonctoriels agissants sur le groupe des courbes S-typiques $C_S(G)$ pour $G \in \mathrm{Ab}_k$, k arbitraire.

a. Les Frobenius F_a pour $a \in \mathbb{N}(S)$, définis par

$$\sigma_m(F_a\varphi) = \sigma_{am}(\varphi)$$

b. Les décalages V_a pour $a \in \mathbb{N}(S)$, définis par

$$\sigma_m(V_a\varphi) = a\sigma_{m//a}(\varphi)$$

c. L'action de k, définie par

$$\sigma_m(\lambda\varphi) = \lambda^m \sigma_m(\varphi) .$$

d. Une action du $\mathbb{Z}_{S(k)}$, définie à partir du :

Lemme : Soit $n \in \mathbb{N}(S^*)$, alors l'endomorphisme $\varphi \mapsto [n]\varphi = \varphi + \ldots + \varphi$ (n fois) de $C_S(G)$ est inversible.

Démonstration : Parce que chaque courbe typique φ dans G correspond de façon canonique à un morphisme $\varphi : U_c(k) \to G$ dans Ab_k et parce qu'on a la relation évidente $\varphi = C_S(\varphi)E$, il suffit de vérifier que la courbe pure $[n]E$ définit un automorphisme de $U_c(k)$. Or, on a

$$[n]E = (\Sigma\, E_m t^m)^n \underset{(\text{soit})}{=} \Sigma\, F_m t^m$$

et pour $m \in \mathbb{N}(S)$ on a $F_m \equiv nY_m \bmod Y_{m-1} = \ldots = Y_1 = 0$. Le lemme en résulte parce que n est inversible dans $\mathbb{Z}_S(k)$.

On obtient l'action voulue en posant pour $b \in \mathbb{Z}_S(k)$

$$\sigma_m([b]\varphi) = b\sigma_m(\varphi) .$$

e. L'action de $\mathbb{Z}_{S(k)}$ s'étend encore à un sous anneau k_G de k de la façon suivante : Soit $k_G = \{\lambda \in k \mid$ pour toute courbe typique φ on a : $\tilde{\lambda}\varphi$ avec $\sigma_m(\tilde{\lambda}\varphi) = \lambda\sigma_m(\varphi)$ est une courbe typique$\}$, alors k_G contient l'image de $\mathbb{Z}_{S(k)}$ dans k, comme il se voit par d, et est en effet un sous anneau de k.

Il se peut que k_G contienne de façon stricte l'image de $Z_{S(k)}$. Noter que si φ_1, φ_2 sont deux courbes typiques, alors on a $\sigma_m(\varphi_1+\varphi_2) = \sigma_m(\varphi_1) + \sigma_m(\varphi_2)$.

On notera désormais indifféremment $\tilde{\lambda}$ ou $[\lambda]$.

7.6 Avant de déduire les relations mutuelles des opérateurs de 7.5, on rassemble ici les résultats explicites qui se déduisent des §§ précédents :

Lemme 1 : L'ensemble des courbes $\{F_a E \mid a \in \mathbb{N}(S)\}$ est fondamental pour $U_c(k)$.

Démonstration : A titre d'exercice, en identifiant $U_c(k)$ à un sous objet de $Z_c(k)$ et en utilisant 5.5.

On pose comme dans 5.7 : $k(\mathbb{N}(S),2)$ le sous ensemble de $k^{\mathbb{N}(S)} \times k^{\mathbb{N}(S)}$ formé des $x = (x_{ij} \mid x_{ij} \in k$ pour $(i,j) \in \mathbb{N}(S)^2)$ tels que pour tout i, on ait $\mathrm{Card}\{j \mid x_{ij} \neq 0\} < \infty$. Alors on a :

Lemme 2 : L'application $f : k(\mathbb{N}(S),2) \to C_S(U_c(k))$, défini par

$$f(x) = \sum_{i,j} V_i x_{ij} F_j E$$

est bijective. En outre, $f(x)$ est isobare (ce qui a un sens parce que $C_s(U_c(k)) \subset C(Z_c(k))$, si et seulement si

$$f(x) = \sum V_i x_i F_i E .$$

Démonstration : On raisonne comme dans 5.7 tenant compte du lemme 1. Ce sous groupe des courbes isobares se notera encore $\mathrm{Iso}(U_c(k))$.

En vue du lemme 2, on écrira désormais les courbes typiques dans $U_c(k)$ sous forme $\Sigma V_i x_{ij} F_j$.

On écrira d'après Lazard [1], p. 282 encore $C_S(U_c(k)) = \mathrm{Cart}_S(k)$ et $\mathrm{Cart}(k)$ si $S = P$. Noter qu'on a ici $S = S(k)$, ce qui n'est pas une restriction essentielle, cf. lemme 5 ci-dessous.

Lemme 3 : Soient x,y deux courbes typiques dans $\mathrm{Cart}_S(k)$, donc uniquement de la forme $C_S(\tilde{x})E$, $C_S(\tilde{y})E$ avec $\tilde{x},\tilde{y}$ les endomorphismes de $U_c(k)$, définis par x,y. Alors on a $C_S(\tilde{x} \circ \tilde{y}) = yx$, c'est-à-dire on a un isomorphisme

$$\mathrm{End}_{\mathrm{Ab}_k}(U_c(k))^{\mathrm{opp}} \to \mathrm{Cart}_S(k) .$$

Démonstration : En effet, on a $C_S(\tilde{x} \circ \tilde{y})E = C_S(\tilde{x})\{C_S(\tilde{y})E\} = C_S(\tilde{x})(\sum_{i,j} V_i y_{ij} F_j E) = \sum_{i,j} V_i y_{ij} F_j (C_S(\tilde{x})E) = \sum_{i,j} V_i y_{ij} F_j \circ \sum_{i,j} V_i x_{ij} F_j E$. Le produit se calcule à partir des règles de commutation entre les V_i, F_j et les scalaires, donc correspond bien au produit yx.

Lemme 4 : $\mathrm{Iso}(U_c(k))$ est un sous anneau commutatif, canoniquement isomorphe à $W_S(k)$. (Lazard, [1] p. 283).

Démonstration : Ecrivons $\Sigma V_i x_i F_i = x$. Alors appliquant σ_m on voit avec 7.5 que $\sigma_m(x) = \sum_{d|m} d\lambda_d^{m/d}\sigma_m$. Il s'ensuit sans peine que l'on a

$$\sigma_m(xy) = \sigma_m(x)\ \sigma_m(y)$$
$$\sigma_m(x+y) = \sigma_m(x) + \sigma_m(y)$$

Lemme 5 : On prend maintenant $k[X,Y]$ comme anneau de base. Alors, $XE+YE$ étant une courbe isobare, est nécessairement de la forme $\Sigma V_i s_i F_i$ avec $s_i \in k[X,Y]$ (lemme 2), et on a :

$$X^m + Y^m = \sum_{d|m} d s_d^{m/d} \qquad (7)$$

En effet, il suffit d'appliquer σ_m et 7.5 .

Lemme 6 : Tout à fait analogue à 5.9, qui en est un cas particulier, on a : la structure de $U_c(k)^*$ se donne par les relations :

$$X+Y = \Sigma V_i X_i F_i + \Sigma V_i Y_i F_i = \Sigma V_i F_i(X,Y) F_i = F$$

ou encore, en applicant σ_m :

$$\sum_{d|m} d(X_d^{m/d} + Y_d^{m/d}) = \sum_{d|m} d F_d(X,Y)^{m/d}$$

Les $F_d(X,Y)$ sont en effet à coefficients dans $\mathbb{Z}$.

Noter, que l'intégralité des coefficients des $F_d(X,Y)$ suit directement du fait que $S^* = \emptyset$ est le cas correspondant à l'anneau de base $\mathbb{Z}$, ce qui donne déjà tous les $F_d(X,Y)$ à coefficients dans l'anneau de base, c'est-à-dire dans $\mathbb{Z}$. Si $m \in \mathbb{N}(S)$, alors m n'admet que des diviseurs $d \in \mathbb{N}(S)$.

7.7 Les relations entre les opérateurs de 7.5 se rassemblent dans la liste suivante : cf. Cartier[2], (2)-(7). Pour $m,n \in \mathbb{N}(S)$ et $\lambda,\mu \in k$ on a :

a $\lambda \oplus \mu = \sum_{d \in \mathbb{N}(S)} V_d s_d(\lambda,\mu) F_d$ avec s_d donné par (7) et où $\oplus$ note l'addition dans $Cart_S(k)$.

b $\lambda \circ \mu = \lambda\mu$

c $V_m V_n = V_{mn}$; $F_m F_n = F_{mn}$

d $V_n \lambda^n = \lambda V_n$; $F_n \lambda = \lambda^n F$

e $V_m F_n = F_n V_m$ si $(m,n) = 1$

f $F_n \cdot V_n = [n]$; $[1] = V_1 = F_1$

g $\tilde{\lambda} \in k_{Z_c(k)}$ est dans le centre de $\mathrm{Cart}_S(k)$.

h Les opérateurs F_n et V_n laissent stable le sous anneau $W_S(k)$ de $\mathrm{Cart}_S(k)$. En effet, il suffit de vérifier cela pour $n = p$, premier, et dans ce cas on a, si $x = \sum_{d \in \mathbb{N}(S)} V_d x_d F_d$:

$$F_p x = F_p \left\{ \sum_{(d,p)=1} V_d x_d F_d + \sum_{d \in \mathbb{N}(S)} V_{dp} x_{dp} F_{dp} \right\}$$

$$= \sum_{(d,p)=1} V_d x_d^p F_d \cdot F_p + \sum_{d \in \mathbb{N}(S)} V_d [p] x_{dp} F_d \cdot F_p \qquad (8)$$

$$= x^{(p)} F_p \text{ , avec } x^{(p)} \in W_S(k)$$

parce que (8) s'écrit sous la forme $(a+b)F_p$ avec $a,b \in W_S(k)$. Avec les mêmes notations on voit que $xV_p = V_p x^{(p)}$.

7.8 Comme dans Cartier [1] p. 51 on trouve la description suivante de l'anneau $\mathrm{Cart}_S(k)$: Soit $S \neq \emptyset$ et soit $H_k = W_S(k)[F_p]_{p \in S}$, soumis aux seules règles de commutation $F_p x = x^{(p)} F_p$ pour $p \in S$ et $x \in W_S(k)$.

Soit $S_k = H_k[[V_q]]_{q \in S}$, l'anneau de séries formelles à coefficients dans H_k, dont les règles de commutation se donnent par : $xV_q = V_q x^{(q)}$, $F_p V_q = V_q F_p$ si $q \neq p$, $F_p V_p = \sum_{d \in \mathbb{N}(S)} V_d y_d F_d \in W_S(k)$, avec $\sum_{d/n} d\, y_d^{n/d} = p$ et finalement $V_p F_p = z = \sum_{d \in \mathbb{N}(S)} V_d z_d F_d \in W_S(k)$ avec $z_d = \delta_{d,p}$. Alors S_k n'est autre que $\mathrm{Cart}_S(k)$.

7.9 Ce qui précède définit donc un foncteur covariant C_S : Groupes formels commutatifs sur k → modules à droite sur $\mathrm{End}\, U_c(k)$ → Modules à gauche sur $\mathrm{Cart}_S(k)$ (d'après 7.6 lemme 3). On vérifie sans peine que si φ est une courbe typique dans $G \in \mathrm{Grfc}_k$ et $x = \Sigma V_i x_{ij} F_j \in \mathrm{Cart}_S(k)$ alors, la structure de module sur $C_S(G)$ se définit par

$$x \cdot \varphi = \Sigma V_i x_{ij} F_j \varphi$$

De la même façon C s'interprète comme un foncteur à valeurs dans la catégorie de $\mathrm{Cart}(k)$-modules à gauche. On procède de façon analogue pour les modules des courbes typiques finies. Il intervient des problèmes de nature arithmétique, à cause du fait que tandis que ξ_n est une courbe dans $Z(n)$, $F_a \xi_n$ n'en est plus si $a \neq 1$.

Chapitre III : Lois abéliennes de dimension n

§1. Généralités

On reprend la situation de I.3.4c : soient k un anneau de base arbitraire et $F \in F(n,k)$, c'est-à-dire F est une loi de groupe formel abélien de dimension n sur k. On a vu : $\theta(F) = k[[X_F]]$ où $X_F = {}^t(X_{1F},\dots,X_{nF})$ est le système de générateurs canoniques de F. On notera encore $F^* = \theta(F)^*$ et $\varphi_F = {}^t(\varphi_{1F},\dots,\varphi_{nF}) \in C(F^*)^n$ l'ensemble des courbes qui satisfont à

$$\varphi_{jF}(X_{iF}) = \delta_{ij}t \qquad \text{pour } 1 \leqslant i,j \leqslant n$$

Il s'ensuit sans problèmes que φ_F est un ensemble fondamental des courbes et si $\varphi_{iF} \equiv 1 + \partial_{iF}t \bmod t^2$, alors $\partial_F = {}^t(\partial_{1F},\dots,\partial_{nF})$ constitue une base du k-module $P(F^*)$. On notera le plus souvent $C(F)$ resp. $C_S(F)$ au lieu de $C(F^*)$, $C_S(F^*)$.

1.1 Lemme : Soit $F \in F(n,k)$, alors

a. Si ψ_j est une courbe dans F^*, alors ψ_j s'écrit de façon unique

$$\psi_j = \sum_{m=1}^{\infty} \sum_{i=1}^{n} V_m \lambda(j,i,m)\varphi_{iF} \quad \text{avec } \lambda(j,i,m) \in k \qquad (1)$$

Si de plus $k = k_{F^*}$ (II, 7.5e), alors ψ_j s'écrit de façon unique

$$\psi_j = \sum_{m=1}^{\infty} \sum_{i=1}^{m} V_m \widetilde{\mu(j,i,m)}\varphi_{iF} \quad \text{avec } \mu(j,i,m) \in k \qquad (2)$$

b. L'ensemble $\psi = {}^t(\psi_1,\dots,\psi_n) \in C(F)^n$ est fondamental, avec ψ_j comme dans (1) si et seulement si la matrice $\lambda(1)$, à coefficients $\lambda(j,i,1)$, est inversible.

c. Si $\psi \in C(F)^n$ est fondamental, il existe $Y \in \theta(F)^n$ tel que $Y \equiv {}^t\lambda(1)^{-1}X_F \bmod \deg 2$ et $\psi_i(Y_j) = \delta_{ij}t$ pour $1 \leqslant i,j \leqslant n$.

Démonstration : La topologie sur $C(F)$ fait de (1) et (2) une expression bien définie. Supposons que

$$\sum \psi_{j,m}t^m = \psi_j \equiv \sum_{m=1}^{s-1} \sum_{i=1}^{n} V_m \lambda(j,i,m)\varphi_{iF} = \sum \chi_m t^m \bmod t^s$$

alors $\psi_{j,s} - \chi_s \in P(F^*)$, d'où $\psi_{j,s} - \chi_s = \sum_{i=1}^{n} \lambda(j,i,s)\partial_{iF}$ de façon unique avec

$\lambda(j,i,s) \in k$. Il suit que

$$\psi_j \equiv \sum_{m=1}^{s} \sum_{i=1}^{n} V_m \lambda(j,i,m) \varphi_{iF} \bmod t^{s+1}$$

ce qui démontre (1). Il va de même pour (2).

Soit maintenant ψ un ensemble fondamental. Si $\psi_j \equiv 1 + \xi_j t \bmod t^2$ alors $\xi_j = \sum_{i=1}^{n} \lambda(j,i,1)\partial_{iF}$ pour $1 \leqslant j \leqslant n$, c'est-à-dire $\xi = \lambda(1)\partial_F$, et parce que ξ doit constituer une base de $P(F^*)$, il suit que $\lambda(1)$ doit être inversible. De façon inverse, soit $\lambda(1)$ inversible et posons $Y = {}^t\lambda(1)^{-1}X_F$.

Si $\lambda(1)^{-1} = (\mu(i,j))$, alors

$$\begin{aligned}
\psi_j(Y_r) &= \psi_j\Big(\sum_{s=1}^{n} \mu(s,r)X_{sF}\Big) \\
&= \sum_{i=1}^{n} \lambda(j,i,1)\varphi_{iF}\Big(\sum_{s=1}^{n} \mu(s,r)X_{sF}\Big) \bmod t^2 \\
&= \sum_{i=1}^{n} \sum_{s=1}^{n} \lambda(j,i,1)\mu(s,r)\delta_{i,s}t \bmod t^2 \\
&= \delta_{j,r}t \bmod t^2
\end{aligned}$$

Supposons donc qu'on a $Y(m) \in \theta(F)^n$ t.q. $Y(m) \equiv {}^t\lambda(1)^{-1}X_F \bmod \deg 2$ et t.q. $\psi_j(Y_r(m)) = \delta_{j,r}t + \alpha_{r,j}t^m \bmod t^{m+1}$. On pose $Y_r(m+1) = Y_r(m) - \sum_{j=1}^{n} \alpha_{r,j}\, Y_j(m)^m$, alors on trouve

$$\begin{aligned}
\psi_j(Y_r(m+1)) &= \psi_j(Y_r(m)) - \sum_{s=1}^{n} \alpha_{r,s}\, \psi_j(Y_s(m))^m \\
&\equiv \delta_{j,r}t + \alpha_{r,j}t^m - \sum_{s=1}^{n} \alpha_{r,s}(\delta_{j,s}t)^m \bmod t^{m+1} \\
&\equiv \delta_{j,r}t \bmod t^{m+1}
\end{aligned}$$

On conclut qu'il existe $Y \in \theta(F)^n$ t.q. $Y \equiv {}^t\lambda(1)^{-1}X_F \bmod \deg 2$ et $\psi_j(Y_i) = \delta_{i,j}t$. Il s'ensuit que $\theta(F) = k[[Y]]$ mais alors il se vérifie aisément que $\psi \in C(F)^n$ est un ensemble fondamental.

1.2 Lemme : Soient $F \in F(n,k)$ et $S = S(k)$. Alors

a. Il existe $Y \in \theta(F)^n$ et il existe un ensemble fondamental des courbes typiques $\varphi \in C_S(F)$ t.q. $Y = X_F \bmod \deg 2$ et $\varphi_i(Y_j) = \delta_{i,j}t$. Dans cette situation là on a:

b. Une courbe typique $\psi_j \in C_S(F)$ s'écrit de façon unique

$$\phi_j = \sum_{m\in N(S)} \sum_{i=1}^{n} V_m \lambda(j,i,m)\varphi_i \qquad \text{avec } \lambda(j,i,m) \in k \qquad (3)$$

Si de plus $k = k_{F^*}$, ϕ_j s'écrit encore

$$\phi_j = \sum_{m\in N(S)} \sum_{i=1}^{n} V_m \widetilde{\mu(j,i,m)}\varphi_i \qquad \text{avec } \mu(j,i,m) \in k \qquad (4)$$

c. L'ensemble $\phi = {}^t(\phi_1,\dots,\phi_n)$ est fondamental avec ϕ_j comme dans (3), si et seulement si la matrice $\lambda(1)$ à coefficients $\lambda(j,i,1)$ est inversible.

d. Si ϕ est un ensemble fondamental dans $C_S(F)^n$, alors il existe $U \in \theta(F)^n$ t.q. $\theta(F) = k[[U]]$, $U \equiv {}^t\lambda(1)^{-1}X_F \bmod \deg 2$ et $\phi_i(U_j) = \delta_{i,j}t$.

Démonstration : Soit $\varphi_{iF} = \sum_{a^*\in N(S^*)} V_{a^*} H_{a^*}(\varphi_{iF})$ la décomposition de φ_{iF} en courbes typiques (II.6.7), alors $\{H_1(\varphi_{iF}) \mid 1 \leqslant i \leqslant n\} \in C_S(F)^n$ est un ensemble fondamental en vertu du lemme 1.1.b. Par le lemme 1.1.c on conclut que a est vrai. Pour b on note dans (1), (2) si les φ_{iF} sont typiques, alors φ_j est typique si et seulement si $m \notin N(S)$ entraîne que $\lambda(j,i,m) = 0$. Finalement, c et d sont des cas spéciaux du lemme 1.1 b et c.

1.3 En retournant à I.1.2 soit $f : F \to G$ un morphisme de lois où $\dim_k F = n$ et $\dim_k G = m$. Alors on peut écrire

$$f \equiv J(f)X \bmod \deg 2$$

où $X = {}^t(X_1,\dots,X_n)$ et $J(f) \in M(m\times n,k)$. La matrice $J(f)$ s'appelle la matrice de Jacobi de f. Soit maintenant $m=n$, alors on dit que f est un isomorphisme, si $J(f)$ est inversible et un isomorphisme strict si $J(f) = I_n$, la matrice identique. Si f est un isomorphisme, c'est-à-dire $J(f) \in Gl(n,k)$, alors il existe bien un morphisme $g : G \to F$ t.q. $f \circ g = 1_G$ et $g \circ f = 1_F$.

On écrit $F \sim G$ s'il existe un isomorphisme $f : F \to G$ et $F \approx G$ s'il existe un isomorphisme strict $f : F \to G$. Alors $\sim$ et $\approx$ définissent une relation d'équivalence sur l'ensemble $F(n,k)$ dont les quotients seront notés $\Phi(n,k,\sim)$ et $\Phi(n,k,\approx)$. Avec ces notations les lemmes 1 et 2 entraînent :

Corollaire 1 : Soit $F \in F(n,k)$, alors il existe une correspondance biunivoque entre : classe de F dans $\Phi(n,k,\approx)$ et l'ensemble de $\psi \in C(F)^n$ t.q. $\psi = \sum_{m=1}^{\infty} V_m \lambda(m) \varphi_F$ avec $\lambda(m) \in M(n,k)$ et $\lambda(1) = I_n$.

Corollaire 2 : Soient $F \in F(n,k)$ et $S = S(k)$, alors il existe $G \in F(n,k)$ t.q. $\varphi_G \in C_S(G)^n$ et t.q. $F \approx G$. Si maintenant G , $H \in F(n,k)$ sont telles que φ_G , φ_H se composent des courbes typiques et $G \approx H$, alors $\varphi_H = \sum_{m \in \mathbb{N}(S)} V_m \mu(m) \varphi_G$ avec $\mu(m) \in M(n,k)$, $\mu(1) = I_n$.

Dans ces corollaires on a fait opérer V_m et $\mu(m)$, $\lambda(m)$ de façon naturelle sur $C(G)^n$, $C_S(G)^n$. Si $k = k_G$ on a naturellement des corollaires analogues avec opérateurs $\widetilde{\mu(m)}$ et $\widetilde{\lambda(m)}$, opérant de façon naturelle.

1.4 Avec la terminologie de Lazard[1], p. 284 et d'après II.7.9 on voit que si $F \in F(n,k)$ alors $C(F)$ est un $Cart(k)$-module réduit. De la même façon, $C_S(F)$ est un $Cart_S(k)$-module réduit. φ_F est une V-base pour $C(F)$. On appellera $F \in F(n,k)$ une loi typique, si $\varphi_F \in C_S(F)^n$ avec $S = S(k)$. D'après 1.3 Cor.2, chaque loi dans $F(n,k)$ est strictement isomorphe sur k à une loi typique. En faisant opérer F_a de façon naturelle sur $C(F)$ et $C_S(F)$ il suit des lemmes précédents :

Corollaire 1 : Soit $F \in F(n,k)$, alors pour $a \in \mathbb{N}$ on a

$$F_a \varphi_F = \sum_{m=1}^{\infty} V_m \, \sigma(a,m) \varphi_F \tag{5}$$

avec $\sigma(a,m) \in M(n,k)$.

L'application $\sigma : \mathbb{N}^+ \times \mathbb{N}^+ \to M(n,k)$ sera dite le type de F .

Corollaire 2 : Soit $F \in F(n,k)$ typique, alors pour $a \in \mathbb{N}(S)$, $S = S(k)$, on a

$$F_a \varphi_F = \sum_{m \in \mathbb{N}(S)} V_m \sigma(a,m) \varphi_F \tag{6}$$

avec $\sigma(a,m) \in M(n,k)$.

L'application $\sigma : \mathbb{N}(S) \times \mathbb{N}(S) \to M(n,k)$ sera dite le $S(k)$-type de F .

Chaque loi (typique) a donc un type ($S(k)$-type) bien défini. En vue des relations $F_a F_b = F_{ab}$ on ne peut pas attendre que chaque $\sigma : \mathbb{N}^+ \times \mathbb{N}^+ \to M(n,k)$

sera le type d'un $F \in F(n,k)$. Le but de ce chapitre sera d'étudier les applications $\sigma : \mathbb{N}^+ \times \mathbb{N}^+ \to M(n,k)$ qui définissent les lois de dimension n sur k . Noter que si $k = k_F$, alors (5) et (6) s'écrivent encore sous la forme

$$F_a\varphi = \sum_{m=1}^{\infty} V_m \widetilde{\lambda(a,m)}\varphi_F \tag{7}$$

$$F_a\varphi = \sum_{m\in\mathbb{N}(S)} V_m \widetilde{\lambda(a,m)}\varphi_F \tag{8}$$

1.5 Soit k un anneau d'intégrité de caractéristique zéro, de corps des fractions K . Soient $F \in F(n,k)$ et F_* la loi obtenue sur K à partir d'application canonique $k \hookrightarrow K$. Le théorème de Cartier II.4.5 implique que Spf $\theta(F_*)$ est isomorphe sur K à la somme directe de n copies de $\hat{\alpha}_K$ (I.5.4.1), parce qu'il n'existe à isomorphie près qu'une seule algèbre de Lie abélienne de dimension n sur K . Il s'ensuit qu'il existe un isomorphisme $f : F_* \to \hat{G}_a^n$ (I.1.3 b), c'est-à-dire $J(f)$ est inversible. D'autre part, le théorème de Cartier II.4.5 montre en même temps que $\mathrm{End}(\hat{\alpha}_K^n) \simeq \mathrm{End}_K(\hat{G}_a^n) = M(n,K)$, c'est-à-dire il existe un isomorphisme $\ell_F : F_* \xrightarrow{f} \hat{G}_a^n \xrightarrow{J(f)^{-1}} \hat{G}_a^n$ qui est strict. En raisonnant sur $\theta(F_*)$ et $\theta(\hat{G}_a^n)$, il n'est pas difficile de voir que $\ell_F : F_* \to \hat{G}_a^n$ est uniquement déterminé par la condition qu'elle soit une isomorphie stricte. Ce ℓ_F , à coefficients dans K , sera appelé le logarithme ou encore d'après Honda[2], p.219, le transformateur de F . Pour un exemple : I.1.3 c.

§2. Une loi de logarithme générique

2.1 On pose $B = \mathbb{Q}[Z(i,j)]_{1\leqslant i\leqslant n;\, j\in\mathbb{N}^+}$ que l'on fait encore un objet de $Ab_{\mathbb{Q}}$ en posant $dZ(i,j) = \sum_{a+b=j} Z(i,a) \otimes Z(i,b)$, $(Z(i,0) = 1$ pour $1 \leqslant i \leqslant n)$. Donc B s'identifie à une somme directe de n copies de $Z_c(\mathbb{Q})$ dans $Ab_{\mathbb{Q}}$. On définit l'ensemble $\{\sigma(i,j) \mid 1 \leqslant i \leqslant n \,;\, j \in \mathbb{N}^+\} \subset P(B)$ par les relations suivantes des courbes

$$C_i = \sum Z(i,j)t^j = \exp \sum_{m=1}^{\infty} m^{-1}\sigma(i,m)t^m \tag{1}$$

(cf. II.7.1). Soit maintenant $C = \mathbb{Q}[Y(k,\ell,m)]$ avec $1 \leqslant k,\ell \leqslant n$ et $m \geqslant 2$.

On considère dans $C \otimes_{\mathbb{Q}} B$ l'idéal $\mathfrak{a}$ engendré par

$$\sigma(k,m) - \sum_{j=1}^{n} Y(k,j,m)\sigma(j,1) \quad , \quad 1 \leqslant k \leqslant n \; ; \; m \geqslant 1 \tag{2}$$

où on convient que $Y(k,j,1) = \delta_{k,j}$. Alors on a :

Lemme : $M = C \otimes_{\mathbb{Q}} B/\mathfrak{a}$ est un C-module libre et appartient à $\mathbf{Ab}_C$.

Démonstration : Notons que $\mathfrak{a}$ est engendré par des éléments primitifs de sorte que M soit muni d'une structure naturelle de bigèbre sur C . Soit $f : C \otimes_{\mathbb{Q}} B \to M$ l'application canonique. Comme algèbre sur C , M est engendrée par tous les $f(Z(i,j))$, ou encore par (1) par tous les $f(\sigma(i,j))$, ou encore par (2) on voit que M est engendrée par les $f(\sigma(j,1)) = \xi_j$ pour $1 \leqslant j \leqslant n$. Il n'est pas difficile de voir que les ξ_j sont linéairement indépendants sur C , donc si $J = \bigoplus_{j=1}^{n} C\xi_j$ on a $J \hookrightarrow P(M)$ d'où $U(J) \to U(P(M)) \to M$ lesquelles deviennent isomorphismes en passant à corps de fractions $K(C)$ de C en vertu du théorème (II.4.5). Il n'est maintenant plus difficile de voir qu'en effet $U(J) \xrightarrow{\sim} M$ est déjà un isomorphisme sur C ce qui entraîne que $C[\xi_1,\ldots,\xi_n] \simeq U(J) \simeq M \in \mathbf{Ab}_C$.

2.2 L'isomorphisme $M \simeq C[\xi_1,\ldots,\xi_n]$ fait voir que

$$\psi = \{\psi_k = \exp \xi_k t \mid 1 \leqslant k \leqslant n\}$$

est un ensemble fondamental des courbes pour M . Ceci entraîne encore, si

$$\varphi_k := H(f)C_k = \exp \sum_{m=1}^{\infty} m^{-1} f(\sigma(k,m))t^m \underset{(\text{soit})}{=} \sum \varphi(k,m)t^m \tag{3}$$

alors $\varphi = \{\varphi_k \mid 1 \leqslant k \leqslant n\}$ est un ensemble fondamental des courbes pour M . En effet en dualisant M par aide de ψ , on voit que $M^* \simeq \theta(\hat{G}_a^n)$, donc M^* provient d'une loi de dimension n sur k . On a : $\psi_k \equiv \varphi_k \bmod t^2$, donc d'après le lemme 1.1.b on conclut que φ est fondamental.

Soient $B = \mathbb{N}^n$ et pour $\alpha = (\alpha_1,\ldots,\alpha_n) \in B$ soit $\varphi(\alpha) = \prod_i \varphi(i,\alpha_i)$ et $\xi^\alpha = \prod_i \xi_i^{\alpha_i}$ alors on voit que

$$B_1 = \{\xi^\alpha \mid \alpha \in B\} \quad \text{et} \quad B_2 = \{\varphi(\alpha) \mid \alpha \in B\}$$

sont

des bases du C-module M et en particulier, B_2 est une base structurale. On en tire des relations

$$\varphi(\alpha) = \sum_{\beta} P(\alpha,\beta)\xi^{\beta} \qquad \text{(somme finie)} \tag{4}$$

avec $P(\alpha,\beta) \in C$. Soit $\varepsilon_i = (\underbrace{0,..0}_{i-1},1,0..0) \in B$. On définit $X_i(\beta)$ pour $1 \leqslant i \leqslant n$, $\beta \in B$ par

$$\delta_{\alpha,\varepsilon_i} = \sum_{\beta} P(\alpha,\beta)X_i(\beta) \tag{5}$$

Parce que B_1 et B_2 sont des bases, $X_i(\beta)$ est uniquement déterminé et élément de C . Finalement on pose

$$R_i(\alpha,\beta) = \sum_{\gamma,\delta} P(\alpha,\gamma)P(\beta,\delta)X_i(\gamma+\delta)$$

ce qui encore est une somme finie d'après (4).

D'ailleurs, soit $\alpha = (\alpha_{ij}) \in M(n\times n',k)$, alors on note $\alpha_{ij} = \pi(i,j)\alpha$. Si $m \in \mathbb{N}$ on notera encore $\alpha^{(m)} \in M(n\times n',k)$ la matrice telle que $\pi(i,j)\alpha^{(m)} = \alpha(i,j)^m$. Avec ces préparations on a :

2.3 Théorème de logarithme générique : Définissons $F \in C[[X,Y]]^n$, $X = {}^t(X_1,\ldots,X_n)$, $Y = {}^t(Y_1,\ldots,Y_n)$ par

$$F_i = \sum_{\alpha,\beta} R_i(\alpha,\beta)X^{\alpha}Y^{\beta}$$

alors :

a. $F \in F(n,C)$

b. Soit $Y(m) \in M(n,C)$ avec $\pi(i,j)Y(m) = Y(i,j,m)$, alors le logarithme $\ell_F = {}^t(\ell_{1F},\ldots,\ell_{nF})$ de F est donné par

$$\ell_F = \sum_{m=1}^{\infty} m^{-1}\ {}^tY(m)X^{(m)} .$$

Démonstration : Prenons $X_i \in M^* \in CAl_C$ t.q. $\varphi_k(X_i) = \delta_{i,k}t$, ce qui est possible en vertu du lemme 1.1. Il s'ensuit que $\langle\varphi(\alpha),X_i\rangle = \delta_{\alpha,\varepsilon_i}$, par conséquent on a

$$\delta_{\alpha,\varepsilon_i} = \langle\varphi(\alpha),X_i\rangle = \sum_{\beta} P(\alpha,\beta)\ \langle\xi^{\beta},X_i\rangle$$

d'où par unicité

$$X_i(\beta) = \langle \xi^\beta, X_i \rangle .$$

L'ensemble $\varphi = \{\varphi_k \mid 1 \leqslant k \leqslant n\}$ étant fondamental, lemme 1.1 donne que $M^* \simeq C[[X_1,\ldots,X_n]]$ et la structure du co-groupe formel sur M^* se donne par :

$$\begin{aligned} \langle \varphi(\alpha)\otimes\varphi(\beta), dX_i \rangle &= \langle \varphi(\alpha)\varphi(\beta), X_i \rangle \\ &= \langle \sum_{\gamma,\delta} P(\alpha,\gamma)P(\beta,\delta)\xi^{\gamma+\delta}, X_i \rangle \\ &= R_i(\alpha,\beta) \end{aligned} \tag{6}$$

ce qui donne a, parce qu'il est évident que F est telle que $\theta(F) = M^*$ avec $X_F = {}^t(X_1,\ldots,X_n)$.

Pour b il faut calculer un peu. Posons

$$\begin{aligned} w &= \sum_{\alpha,\beta} \varphi(\alpha)\varphi(\beta) X^\alpha Y^\beta \\ &= \prod_{i=1}^{n} \Big(\sum_{\alpha_i=0}^{\infty} \varphi(i,\alpha_i) X_i^{\alpha_i}\Big) \prod_{i=1}^{n} \Big(\sum_{\beta_i=0}^{\infty} \varphi(i,\beta_i) Y_i^{\beta_i}\Big) \\ &= \prod_{i=1}^{n} \exp\Big(\sum_{m=1}^{\infty} m^{-1} f(\sigma(i,m)) X_i^m\Big) \prod_{i=1}^{n} \exp\Big(\sum_{m=1}^{\infty} m^{-1} f(\sigma(i,m)) Y_i^m\Big) \quad (3) \\ &= \exp \sum_{i=1}^{n} \sum_{m=1}^{\infty} m^{-1} f(\sigma(i,m))(X_i^m + Y_i^m) \\ &= \exp \sum_{i=1}^{n} \sum_{j=1}^{n} \sum_{m=1}^{\infty} m^{-1} Y(i,j,m) \xi_j (X_i^m + Y_i^m) \quad (2) \end{aligned} \tag{7}$$

D'autre part, définissons $w : M^* \to C[[X,Y]]$ comme application C-linéaire continue en posant

$$w(x) = \sum_{\alpha,\beta} \langle \varphi(\alpha)\varphi(\beta), x \rangle X^\alpha Y^\beta .$$

Le fait que $B_2 = \{\varphi(\alpha) \mid \alpha \in B\}$ est une base structurale entraîne que w même est un homomorphisme d'algèbres, qui satisfait à

$$w(X_i) = \sum_{\alpha,\beta} \langle \varphi(\alpha)\varphi(\beta), X_i \rangle X^\alpha Y^\beta = F_i \tag{8}$$

De la même façon, soit

$$\chi = \sum_{\alpha} \varphi(\alpha) F^\alpha = \exp \sum_{i=1}^{n} \sum_{j=1}^{n} \sum_{m=1}^{\infty} m^{-1} Y(i,j,m)\, \xi_j F_i^m \tag{9}$$

alors on voit que $\chi : M^* \to C[[X,Y]]$, défini par

$$\chi(x) = \sum_{\alpha} \langle \varphi(\alpha), x \rangle F^{\alpha}$$

est un morphisme continu d'algèbres qui satisfait à

$$\chi(X_i) = \sum \langle \varphi(\alpha), X_i \rangle F^{\alpha} = F_i \qquad (10)$$

Il suit par (8) et (10) que $w = \chi$, c'est-à-dire (7) et (9) donnent, parce que les ξ_i sont linéairement indépendants sur C :

$$\sum_{i=1}^{n} \sum_{m=1}^{\infty} m^{-1} Y(i,j,m)(X_i^m + Y_i^m) = \sum_{i=1}^{n} \sum_{m=1}^{\infty} m^{-1} Y(i,j,m) F_i^m$$

ce qui n'est autre que $\ell_F(F) = \ell_F(X) + \ell_F(Y)$ ce qui démontre le théorème.

2.4 Remarque : Soit $n = 1$ et posons $Y(1,1,m) = y_m$. Alors un peu de calcul donne : $R(1,1) = -y_2$; $R(1,2) = y_2^2 - y_3$; $R(1,3) = 2y_2y_3 - y_2^3 - y_4$, $R(2,2) = 4y_2y_3 - \frac{1}{2}(5y_2^3 + 3y_4)$, c'est-à-dire F n'est pas définie sur $\mathbb{Z}[y_i]_{i \geqslant 2}$.

2.5 Soit k un anneau d'intégrité de caractéristique zéro, de corps de fractions K . Soit $f : \mathbb{N} \to \mathbb{M}(n,K)$ une application telle que $f(1) = I_n$. On considère K comme une algèbre sur C à moyen du morphisme structural $\bar{f} : C \to K$ qui envoie $Y(i,j,m)$ sur $\pi(i,j)f(m) = f(i,j,m)$. D'après I.1.2 on obtient une loi $\bar{f}_* F$, noté fF avec F comme dans le th. 2.3. On note $f\ell_F \in K[[X]]^n$, où $X = {}^t(X_1, \ldots, X_n)$, l'élément, donné par

$$(f\ell_F)_i = \sum_{m=1}^{\infty} \sum_{j=1}^{n} m^{-1} f(j,i,m) X_j^m \quad , \quad 1 \leqslant i \leqslant n \ .$$

Alors il est clair que $f\ell_F$ est le logarithme de fF et on a

Proposition : Soit $f : \mathbb{N}^+ \to \mathbb{M}(n,K)$ t.q. $f(1) = I_n$. Alors les trois assertions suivantes sont équivalentes :

a. $G \in F(n,K)$ a le transformateur $f\ell_F$.

b. $G \in F(n,K)$ et $\varphi_G = \exp \sum_{m=1}^{\infty} m^{-1} f(m) \partial_G t^m$.

c. $G = fF$.

Dans ce cas on a encore : $G^* \cong K \otimes_{\mathbb{Q}} B / \alpha_f$ où α_f est l'idéal engendré par tous

$$\sigma(i,m) - \sum_{j=1}^{n} f(i,j,m)\sigma(j,1)$$

de plus $\partial_{jG} \equiv \sigma(j,1) \bmod \mathfrak{a}_f$.

En outre, si $G \in F(n,K)$ il existe un unique $f : \mathbb{N}^+ \to M(n,K)$ t.q. $f(1) = I_n$ et $G = fF$.

Démonstration : Il est évident que $G \in F(n,K)$ est déterminée par son transformateur et par son ensemble canonique des courbes φ_G . De plus chaque $G \in F(n,K)$ a un logarithme (1.5). La proposition résulte du théorème 2.3 par spécialisation.

2.6 Considérons maintenant la somme directe de n copies de $U_c(\mathbb{Z}_S)$ (II.7.4), soit $U' = \mathbb{Z}_S[Y(i,a)]_{1\leqslant i\leqslant n;\, a\in\mathbb{N}(S)}$. On pose $U = U' \otimes_{\mathbb{Z}_S} \mathbb{Q}$ et on fait de $C \otimes_{\mathbb{Q}} U$ un sous objet (ainsi qu'un objet quotient) de $C \otimes_{\mathbb{Q}} B$ en posant $P(C \otimes_{\mathbb{Q}} U) = \{\sigma(i,m) \mid 1 \leqslant i \leqslant n \ ; \ m \in \mathbb{N}(S)\}$ (cf. également II.7.4). Supposons maintenant que $f : \mathbb{N}^+ \to M(n,K)$ de la proposition 2.5 a la propriété que $f(m) = 0$ si $m \notin \mathbb{N}(S)$, alors il est clair qu'avec les notations de 2.5 on a $G^* \simeq K \otimes_{\mathbb{Q}} U/\mathfrak{a}_f$ où $\mathfrak{a}_f$ est l'idéal engendré par tous

$$\sigma(i,m) - \sum_{j=1}^{n} f(i,j,m)\ \sigma(j,1) \qquad \text{avec } m \in \mathbb{N}(S) .$$

Cette remarque nous servira plus loin quand il s'agira des domaines de définition des lois. Noter en effet, que dans U on a

$$\begin{aligned} dY(i,a) &= \sum_{m+n=a} E_m(Y(i,1),\ldots,Y(i,m)) \otimes E_n(Y(i,1),\ldots,Y(i,n)) \\ &= \sum E_{m,i} \otimes E_{n,i} \qquad \text{(soit)} \end{aligned}$$

où les $E_{m,i}$ sont à coefficients dans $\mathbb{Z}_S$.

§3. Sur les domaines de définition des lois

3.1 Soient $G \in F(n,k)$ et $\varphi \in C(G)^n$, $\varphi = {}^t(\varphi_1,\ldots,\varphi_n)$, alors φ s'interprète de façon canonique comme un morphisme $\tilde{\varphi} : B \otimes_{\mathbb{Q}} k \to G^*$

En effet on pose $\tilde{\varphi}(Z(i,j)) = \varphi_{i,j}$ si $\varphi_i = \sum \varphi_{i,j} t^j$. Alors, la définition de l'opérateur σ_m de II.7.3 s'étend à cette situation-ci en posant

$$\begin{aligned} \sigma_m(\varphi) &= \text{image de } {}^t(\sigma(1,m),\ldots,\sigma(n,m)) \text{ sous } \tilde{\varphi} \qquad (1) \\ &= \tau_m(\varphi)\partial_G \end{aligned}$$

où $\tau_m(\varphi) \in M(n,k)$. En faisant opérer F_a , V_a , $\lambda \in k$ de façon naturelle sur $C(G)^n$, on trouve facilement les relations

$$\tau_m(F_a\varphi) = \tau_{am}(\varphi) \qquad \tau_m(V_a\varphi) = a\tau_{m//a}(\varphi) \tag{2}$$

$$\tau_m(\lambda\varphi) = \lambda^m\tau_m(\varphi) \qquad \tau_m(\tilde{\lambda}\varphi) = \lambda\tau_m(\varphi)$$

pour $a,m \in \mathbb{N}^+$. (En supposant pour $\tilde{\lambda}\varphi$, que $\lambda \in k_G$).

De plus, si l'on a une relation $\varphi = \sum_d V_d\lambda(d)\varphi_G$ dans $C(G)^n$ avec $\lambda(d) \in M(n,k)$ on a

$$\tau_m(\varphi) = \sum_{d|m} d\,\lambda(d)^{(m/d)}\,\tau_{m/d}(\varphi_G) \tag{3}$$

où comme dans 2.2 (iii), $\lambda(d)^{(m/d)}$ est la matrice obtenue en élevant chaque élément de $\lambda(d)$ à sa puissance m/d-ième.

3.2 On pose pour S arbitraire, F_S la loi abélienne qui admet

$$\ell_{F_S} = \ell_S = \sum_{m\in\mathbb{N}(S)} m^{-1}\,{}^tY(m)X^{(m)} \tag{1}$$

comme logarithme. En prenant $f : C \to C$, définie par $fY(i,j,m) = 0$ si $m \in \mathbb{N}(S)$, on voit que $F_S = fF$, donc F_S est définie sur C .

De plus on a

$$\varphi_{F_S} = \exp \sum_{m\in\mathbb{N}(S)} m^{-1}\,Y(m)\partial_{F_S}\,t^m \tag{2}$$

c'est-à-dire $\varphi_{F_S} \in C_S(F_S)^n$.

On définit par récurrence pour $a,m,d \in \mathbb{N}^+$ les matrices $\sigma(a,d)$ par

$$Y(am) = \sum_{d|m} d\,\sigma(a,d)^{(m/d)}\,Y(m/d) \ . \tag{3}$$

Alors les $\sigma(a,d) \in M(n,C)$. En particulier $\sigma(1,1) = I_n$.

Noter que
$$\tau_m(\varphi_{F_S}) = \begin{cases} Y(m) & \text{si } m \in \mathbb{N}(S) \\ 0 & \text{sinon} \end{cases} \tag{4}$$

<u>Proposition</u> : Soit $S = T \amalg T^*$ une partition arbitraire de S , alors :

a. $$\varphi_{F_S} = \sum_{\substack{a\in\mathbb{N}(T)\\ a^*\in\mathbb{N}(T^*)}} V_{aa^*}\,\widetilde{a^{*-1}}\,\sigma(a^*,a)\varphi_{F_T} \tag{5}$$

b. $$F_a\varphi_{F_S} = \sum_{d\in\mathbb{N}(S)} V_d\,\sigma(a,d)\varphi_{F_S} \qquad \text{si } a \in \mathbb{N}(S) \ . \tag{6}$$

Démonstration : Noter d'abord que $F_S \simeq F_T$ sur C . D'après le cor. 2 de 1.3 on peut donc poser $\partial_{F_S} = \partial_{F_T}$. En appliquant l'opérateur τ_m de (4) on voit

$$\tau_m(\varphi_{F_S}) = \begin{cases} Y(m) & \text{si } m \in \mathbb{N}(S) \text{ . Pour le membre droit de (5),} \\ 0 & \text{sinon} \end{cases}$$

soit md , on trouve

$$\tau_m(md) = \sum_{a,a^*} aa^* . a^{*-1} . \sigma(a^*,a)^{(m//aa^*)} \tau_{m//aa^*}(\varphi_{F_T}) \quad . \tag{7}$$

Si $m \notin \mathbb{N}(S)$, alors il est clair que $\tau_m(md) = 0$, on peut donc se restreindre à $m \in \mathbb{N}(S)$. Soit donc $m = bb^*$ avec $b \in \mathbb{N}(T)$ et $b^* \in \mathbb{N}(T^*)$, alors $m//aa^* = bb^*//aa^*$ se trouve dans $\mathbb{N}(T)$ si et seulement si $a^* = b^*$ et $a \mid b$, c'est-à-dire (7) réduit à

$$\begin{aligned} \tau_m(md) &= \sum_{a \mid b} a\, \sigma(b^*,a)^{(b/a)} \tau_{b/a}(\varphi_{F_T}) \\ &= \sum_{a \mid b} a\, \sigma(b^*,a)^{(b/a)} Y(b/a) \qquad \text{par (4)} \\ &= Y(b^*b) = Y(m) \qquad \text{d'après (3).} \end{aligned}$$

b va de la même façon : en applicant τ_m on voit tout de suite que (6) est vrai.

3.3 Le point crucial de ce § est :

Proposition : Si $S = \{p\}$, alors F_S est définie sur l'anneau $\mathbb{Z}_{(p)}[\sigma(p,p^i)]_{i>0}$.

Démonstration : Celle-ci se fait en plusieurs étapes.

Posons d'abord $K = \mathbb{Q}[Y(i,j,p^r)]_{1 \leqslant i,j \leqslant n, r \geqslant 0}$.

a. On applique 2.6 afin de trouver $F_S^* \simeq K \otimes_{\mathbb{Q}} U/\mathfrak{a}_f$, où $\mathfrak{a}_f$ est l'idéal engendré par tous $\sigma(i,p^r) - \sum_{j=1}^{n} Y(i,j,p^r)\sigma(j,1)$. De plus, $U = \mathbb{Q}[Y(i,p^r)]_{1 \leqslant i \leqslant n; r \geqslant 0}$ avec

$$\begin{aligned} dY(i,p^r) &= \sum_{m+n=p^r} E_m(Y(i,1),\ldots,Y(i,p^m)) \otimes E_n(Y(i,1),\ldots,Y(i,p^n)) \\ &= \sum E_{m,i} \otimes E_{n,i} \quad \text{(soit)} \end{aligned}$$

où les $E_{m,i}$ sont à coefficients dans $\mathbb{Z}_{(p)}$.

b. On a

$$\varphi_{F_S} = \exp \sum_{i=0}^{\infty} p^{-i}\, t_{Y(p^{-})X^{(p^i)}} \qquad (2) \text{ de } 3.2$$

est un ensemble fondamental des courbes dans F_S^*, et d'après toutes les conventions faites, on voit que si l'on note $\xi(m,r)$ l'image de $Y(m,p^r)$ dans F_S^*, alors on a

$$\varphi_{m,F_S} = \sum_{n=0}^{\infty} E_n(\xi(m,1),\ldots,\xi(m,n))t^m = \sum_{n=0}^{\infty} E_{n,m}t^n$$

avec $E_{p^r,m} = \xi(m,r)$. De plus, en attachant à $\xi(m,n)$ le poids p^n, on voit que $E_{n,m}$ est isobare de poids n. On sait déjà donc que l'ensemble de tous les produits (ordonnés, ce qui n'est pas très relevant, parce qu'on se trouve dans le cas commutatif) qu'on peut faire avec les $E_{n,m}$, à coefficients déjà dans $\mathbb{Z}_{(p)}$, constitue une base du K-module F_S^*.

c. La proposition résulte évidemment du lemme suivant :

Lemme : Tous les $\xi(m,r)$ constituent une p-base du K-module F_S^*, soit $B = \{\xi^\alpha \mid \alpha \in T\}$ pour un ensemble d'indices T convenable. De plus on a : chaque $\xi(m,r)^p$ s'écrit comme une combinaison linéaire d'éléments de B à coefficients dans $\mathbb{Z}_{(p)}[\sigma(p,p^i)]_{i\geqslant 0}$.

d. Afin de démontrer le lemme, on considère d'abord le cas où F_S est de dimension 1, ce qui permet de simplifier les notations :

Soit $E = \Sigma\, E_m(\xi_0,\ldots,\xi_m)t^m = \Sigma\, E_m t^m$ la courbe φ_{F_S}. Il s'agit d'abord de montrer que $B = \{\xi^\alpha = \prod_{i=0}^{\infty} \xi_i^{\alpha_i} \mid 0 \leqslant \alpha_i < p$, presque tous les α_i nuls$\}$ est une base du $\mathbb{Q}[y_m]_{m\geqslant 0}$ - module F_S^*. ($y_m = Y(1,1,p^m)$). Notons pour $n \in \mathbb{N}$, $G(n)$ le sous-module sur $\mathbb{Z}_{(p)}[\sigma(p,p^i)]_{i\geqslant 0} = A$ (soit), de base $E_0,\ldots,E_n$. Soit $P(n)$, pour $n \in \mathbb{N}$ l'hypothèse de récurrence suivante, satisfaisant à $P(n,1)$ et $P(n,2)$ ci-dessous :

$P(n,1)$: $\{\xi_0^{\alpha_0}\ldots\xi_r^{\alpha_r} \mid 0 \leqslant \alpha_i < p$, $\sum_i \alpha_i p^i \leqslant n\}$ est une base du A-module libre $G(n)$.

Pour $x,y \in G(n)$ on écrit $x \equiv y \bmod G(m)$ avec $m < n$, si $x-y \in G(m)$, alors :

$P(n,2)$: Si $p^{i+1} \leqslant n$, alors $\xi_i^p \in G(n)$ et $\xi_i^p \equiv a_i \xi_{i+1} \bmod G(p^{i+1}-1)$ avec a_i dans $(p)\mathbb{Z}_{(p)}$.

Maintenant $P(0)$ et $P(1)$ sont visiblement vraies. Supposons donc $P(n-1)$ vraie avec $n-1 \geqslant 1$. On considère deux situations :

Cas A : n n'est pas une puissance de p . Soit $E_n(Y_0,\dots,Y_n) = \Sigma\, c_\alpha Y_0^{\alpha_1}\dots Y_n^{\alpha_n}$, isobare de poids n et soit $\beta = \Sigma\, \beta_i p^i$ le développement p-adique de n . Alors on sait d'après Dieudonné soit par vérification directe que $c_\beta = (\Pi_i\, \beta_i!)^{-1}$, donc inversible dans $\mathbb{Z}_{(p)}$. Considérons un autre terme $c_\alpha\, \xi_0^{\alpha_0}\dots\xi_n^{\alpha_n}$ avec $\alpha \neq \beta$ dans $E_n(\xi_0,\dots,\xi_n)$. Soit $j \geqslant 0$ minimal tel que $\alpha_j \geqslant p$, alors par isobaricité on a certainement que $p^{j+1} \leqslant n$, d'où

$$c_\alpha\, \xi_0^{\alpha_0}\dots\xi_n^{\alpha_n} \equiv c_\alpha\, \xi_0^{\alpha_0}\dots\xi_{j-1}^{\alpha_{j-1}}\, \xi_j^{\alpha_j-p} \cdot a_j\, \xi_{j+1}^{\alpha_{j+1}+1}\, \xi_{j+2}^{\alpha_{j+2}}\dots\xi_n^{\alpha_n} \bmod G(n-1)$$

avec $a_j \in p\mathbb{Z}_{(p)}$. En itérant cette construction, on voit que l'on aboutit à $c_\alpha\, \xi_0^{\alpha_0}\dots\xi_n^{\alpha_n} \equiv c_{\alpha,\beta}\, \xi_0^{\beta_0}\dots\xi_n^{\beta_n} \bmod G(n-1)$ avec $c_{\alpha,\beta} \in p\mathbb{Z}_{(p)}$, ou encore : $E_n(\xi_0,\dots,\xi_n) \equiv c'_\beta\, \xi_0^{\beta_0}\dots\xi_n^{\beta_n} \bmod G(n-1)$ avec c'_β inversible dans $\mathbb{Z}_{(p)}$. Parce que $\{E\}$ est un ensemble fondamental pour F_S , on voit que $P(n,1)$ est vraie. Si n n'est pas une puissance de p , alors $P(n,2)$ est la même condition que $P(n-1,2)$.

Cas B : $n = p^{r+1}$ avec $r \geqslant 0$. Alors puisque $E_n = \xi_{r+1}$, on voit tout de suite que $P(n,1)$ est vrai. Il s'agit de montrer que $\xi_r^p \equiv a_r \xi_{r+1} \bmod G(n-1)$ avec $a_r \in p\mathbb{Z}_{(p)}$.

Soit $U = \mathbb{Z}_{(p)}[Y_i]_{i\geqslant 0}$ avec $E = \Sigma\, E_n(Y_0,\dots,Y_n)t^n$ la courbe pure. Notons v et f l'endomorphisme dans $\mathbf{Ab}_{\mathbb{Z}_{(p)}}$ correspondant avec les courbes V_pE et F_pE . Alors, de II.7.3 on voit que $vY_i = Y_{i-1}\,(Y_{-1}=0)$. De plus on a $F_pV_pE = [p]E$, ce qui montre que

$$fY_r = pY_{r+1} + aY_r^p + g_r(Y_1,\dots,Y_r) \qquad (1)$$

avec g_r isobare de poids p^{r+1} et $g_r(0,\dots,0,Y_r) = 0$. De plus, en réduisant

mod p , on voit que $fY_r \equiv Y_r^p$ ce qui veut dire que $a \equiv 1 \bmod p\mathbb{Z}_{(p)}$, donc a est inversible dans $\mathbb{Z}_{(p)}$.

Notons d'autre part que la formule (6) de 3.2 pour $a = p$ s'écrit

$$F_p E = \sum_{i=0}^{\infty} V_{p^i} \sigma(p,p^i)E \qquad (2)$$

$$= \sum E_m(\overline{fY}_0,\ldots,\overline{fY}_m)t^m \qquad (3)$$

où $\overline{fY}_i$ est l'image de fY_i dans F_S^* . On en tire que le coefficient de t^{p^r} dans (3), qui n'est autre que $\overline{fY}_r$, appartient à $G(p^r) \subset G(n-1)$, comme on le voit en explicitant le membre droit de (2) comme somme des produits de $E_m(Y_1,\ldots,Y_m)$, à coefficients dans $\mathbb{Z}_{(p)}$. Il s'ensuit que (1) se réduit à

$$p\,\xi_{r+1} + a\,\xi_r^p + g_r(\xi_1,\ldots,\xi_r) \equiv 0 \bmod G(n-1) .$$

En écrivant $g_r(Y_1,\ldots,Y_r) = \Sigma\, c_\alpha\, Y_o^{\alpha_o}\ldots Y_r^{\alpha_r}$ on voit comme dans le cas **A**, que chaque terme $c_\alpha\, Y_o^{\alpha_o}\ldots Y_r^{\alpha_r} \equiv c'_\alpha\, Y_r^p \bmod G(n-1)$ avec $c'_\alpha \in p\mathbb{Z}_{(p)}$. Il s'ensuit que $p\,\xi_{r+1} + a'\xi_r^p \equiv 0 \bmod G(n-1)$ avec a' inversible dans $\mathbb{Z}_{(p)}$ ce qui donne $P(n,2)$, donc ce qui montre le lemme si la dimension de F_S est égale à 1.

e. Si la dimension de F_S est n , on procède avec les $E_{n,m}$ de b de la même façon que dans c, avec maintenant $\xi(m,a)$ au lieu de ξ_a , mais pour m fixé, $1 \leqslant m \leqslant n$. Il est clair que la propriété d'être un ensemble fondamental des courbes permet de réduire les calculations au cas de dimension 1, donc le cas général s'ensuit directement de ce qu'on a fait dans c. La proposition en résulte.

3.4 Soit $S \neq \emptyset$ et soit pour $a,d \in \mathbb{N}(S)$, $\tau(a,d)$ une matrice dont les coefficients sont des indéterminés. Soit $\mathbf{A}(S)$ l'anneau polynomial engendré sur $\mathbb{Z}$ par tous les éléments de tous les $\tau(a,d)$. On fixe $p \in S$ de sorte que $n \in \mathbb{N}(S)$ s'écrit sous une forme unique $n = ap^r$ avec soit $(a,p) = 1$ soit $a = p$ et on définit $\tilde{Y}(n)$ à coefficients dans $\mathbf{A}$ par récurrence par

$$\tilde{Y}(n) = \sum_{i=0}^{r} p^i\, \tau(a,p^i)^{(p^{r-i})}\, \tilde{Y}(p^{r-i}) \qquad (1)$$

Soit α_S l'idéal dans $\mathbf{A}(S)$ engendré par tous les éléments de

$$\tilde{Y}(am) = \sum_{d|m} d\tau(a,d)^{(m/d)}\tilde{Y}(m/d) \qquad (2)$$

pour $a,m \in \mathbb{N}(S)$. Soit $L(S) = A(S)/\mathfrak{a}_S$ et notons que $L(S)$ ne dépend pas du nombre premier p , choisi dans (1). Les images de $\tilde{Y}(m)$ et $\tau(a,d)$ dans $L(S)$ seront notés par $Y(m)$ et $\sigma(a,d)$. Alors on a

Proposition : F_S est défini sur $L(S)$ si $S \neq \emptyset$. $F_\emptyset$ est défini sur $\mathbb{Z}$.

Démonstration : Soit d'abord $S = P$ et choisissons $p \in P$. Alors la proposition 3.2 donne les relations

$$\varphi_F = \sum_{(a,p)=1} \sum_{i=0}^{\infty} V_{ap^i}\, \tilde{a}^{-1}\, \sigma(a,p^i)\varphi_{F_{\{p\}}} \qquad (3)$$

$$\varphi_{F_{\{p\}}} = \sum_{i=0}^{\infty} V_{p^i}\, \sigma(p,p^i)\varphi_{F_{\{p\}}} \qquad (4)$$

La proposition 3.3 entraîne que $F_{\{p\}}$ est définie sur $\mathbb{Z}_{(p)}[\sigma(p,p^i)]_{i\geq 0} \subset L(P)\otimes\mathbb{Z}_{(p)}$. Le cor. 1 de 1.3 ainsi que (3) donnent que F est strictement isomorphe avec $F_{\{p\}}$ sur l'anneau $\mathbb{Z}_{(p)}[\sigma(p,p^i),\sigma(a,p^i)]_{i\geq 0,(a,p)=1} \subset L(P)\otimes\mathbb{Z}_{(p)}$. Il s'ensuit que F est définie sur $\bigcap_p L(P)\otimes\mathbb{Z}_{(p)} = L(P)$.

Soit maintenant $S \subset P$. Considérons $\varphi : A(P) \to A(S)$, le morphisme d'algèbres défini par $\varphi\tau(a,d) = 0$ si $ad \notin \mathbb{N}(S)$. Observer que $\varphi(\mathfrak{a}_p) \subset \mathfrak{a}_S$, de sorte qu'on obtienne $\tilde{\varphi} : L(P) \to L(S)$. Parce que $F_S = \tilde{\varphi}_* F_p$, on voit que la proposition en résulte.

3.5 Définition : Soit k un anneau d'intégrité de caractéristique zéro. On dit que $f : \mathbb{N}(S) \to M(n,k)$ avec $f(1) = I_n$ est S-admissible s'il existe $\sigma_f : \mathbb{N}(S)\times\mathbb{N}(S) \to M(n,k)$ tel que pour $a,m \in \mathbb{N}(S)$ on ait

$$f(am) = \sum_{d|m} d\ \sigma_f(a,d)^{(m/d)}f(m/d) \ .$$

On dira que f est S-lexoide, s'il existe $\lambda_f : \mathbb{N}(S)\times\mathbb{N}(S) \to M(n,k)$ tel que pour $a,m \in \mathbb{N}(S)$ on ait

$$f(am) = \sum_{d|m} d\ \lambda_f(a,d)f(m/d) \ .$$

Noter que $f(a) = \lambda_f(a,1) = \sigma_f(a,1)$. L'ensemble des fonctions S-admissibles (S-lexoides) à valeurs dans $M(n,k)$ sera noté $\mathrm{Adm}(S,k)$ resp. $\mathrm{Lex}(S,k)$. Si k est arbitraire, on dira que le couple (f,σ_f) (resp. (f,λ_f)) est S-admissible

(resp. S-lexcide) si ces conditions sont satisfaites.
Noter qu'il existe une bijection évidente $Alg_{\mathbb{Z}}(L(S),k) \simeq Adm(S,k)$.

3.6 Soient k un anneau et $G \in F(n,k)$. On associe à G la fonction $f(G) : \mathbb{N}(P) \to \mathbb{M}(n,k)$ en posant $f(G)(n) = \tau_n(\varphi_G)$. (cf. 3.1).

Le résultat principal de ce chapitre est :

Théorème : f induit une bijection $F(n,k) \to Adm(P,k)$. Si de plus $k = k_G$ pour tout $G \in F(n,k)$, alors f induit une bijection $f : F(n,k) \to Lex(P,k)$.

Démonstration : En appliquant τ_n aux relations (5) et (6) de 1.4 on voit bien que $f(G)$ est P-admissible (resp. P-lexoide, le cas échéant). Soit de façon inverse φ une fonction P-admissible, qui se voit encore comme un morphisme d'algèbres $\varphi : L(P) \to k$, alors $\varphi_* F \in F(n,k)$ comme il résulte de la proposition 3.4. La proposition 2.5 montre que ces deux applications sont l'inverse l'une à l'autre si k est un anneau d'intégrité de caractéristique zéro. Le cas général s'ensuit facilement de là.

3.7 D'après 1.3 cor. 2 l'étude des lois abéliennes se réduits à isomorphie près à celle des lois typiques. Soit $F_{typ}(n,k)$ l'ensemble des lois typiques dans $F(n,k)$. Alors le théorème de décomposition des courbes donne : Soit $G \in F_{typ}(n,k)$. On associe à G la fonction $f(G) : \mathbb{N}(S) \to M(n,k)$, avec $S = S(k)$, en posant $f(G)(n) = \tau_n(\varphi_G)$ pour $n \in \mathbb{N}(S)$. Alors, comme il est évident :

Corollaire : f induit une bijection : $F_{typ}(n,k) \to Adm(S(k),k)$. Si de plus $k = k_G$ pour tout $G \in F_{typ}(k)$, alors f induit une bijection

$$f : F_{typ}(n,k) \to Lex(S(k),k) .$$

3.8 On a associé à chaque $G \in F(n,k)$ le couple $\{C(G),\varphi_G\}$ où $C(G)$ est un $Cart(k)$-module muni d'une V-base φ_G . Le corollaire 2 de 1.3 montre qu'on obtient ainsi un foncteur covariant : C : {Groupes formels commutatifs de Dieudonné de dimension finie} $\to$ Cart(k)-modules réduits admettant une V-base finie.

En effet

Théorème (Cartier) : Le foncteur C est une équivalence des catégories.

Démonstration : D'après 3.6, C est certainement surjectif sur objets, il reste donc à montrer qu'il est pleinement fidèle. En prenant V-bases, il revient au même de montrer : Soient $F(n,k)$ et $G \in F(m,k)$, alors il existe une bijection

$$\mathrm{Hom}_k(F,G) = \mathbf{Ab}_k(F^*,G^*) \to \mathrm{Hom}_{\mathbf{Cart}(k)\text{-mod}}(C(F),C(G)) .$$

Soit $f : F^* \to G^*$ dans $\mathbf{Ab}_k$, ce qui donne $C(f) : C(F) \to C(G)$ et encore $\tilde{C}(f) : C(F)^n \to C(G)^m$ et $\tilde{C}(f)$ est déterminé de façon unique par $\tilde{C}(f)\varphi_F = {}^t(C(f)\varphi_{1F},\ldots,C(f)\varphi_{nF})$, et on a d'après le lemme 1.1a

$$\tilde{C}(f)\varphi_F = \sum_{i=1}^{\infty} V_i\, f(i)\varphi_G \quad \text{avec} \quad f(i) \in M(n\times m,k) \tag{1}$$

Le fait que l'opération de $\mathbf{Cart}(k)$ sur le module de courbes est définie de façon fonctorielle entraîne que

$$F_a\tilde{C}(f)\varphi_F = \tilde{C}(f)F_a\varphi_F \overset{1.4}{=} \tilde{C}(f)\sum_{j=1}^{\infty} V_j\sigma(a,j)\varphi_F = \sum_{j=1}^{\infty} V_j\sigma(a,j)\tilde{C}(f)\varphi_F$$

ce qui entraîne en particulier que

$$(F_a - \sum_{j=1}^{\infty} V_j\sigma(a,j))\tilde{C}(f)\varphi_F = 0 . \tag{2}$$

Le fait que les relations pour les F_p donnent exactement les relations dans les algèbres F^* et G^* cf. (1), (2) et (3) de 3.3, entraîne que (2) est la condition nécessaire et suffisante afin que (1) définisse un morphisme $F^* \to G^*$, à savoir ce qui envoie le coefficient de t^n dans φ_{iF} sur le coefficient de t^n de la $i^{\text{ième}}$ courbe du membre droit de (1).

Remarque : Il résulte du théorème 3.6 que $F(n,k) \simeq \mathbf{Alg}_{\mathbb{Z}}(L(P),k)$, en d'autres termes, $L(P)$ s'identifie à l'anneau universel de Lazard [2], th. 2. Dans un livre à paraître, Lazard démontre le théorème de Cartier sans conditions de finitude et même sans hyperalgèbres.

3.9 On notera $j(F,G)$ l'application injective

$$j(F,G) : \mathrm{Hom}_k(F,G) \hookrightarrow C(G)^m$$

qui fait correspondre à $f : F \to G$ l'ensemble des courbes $\tilde{C}(f)_{\varphi_F}$. D'après (2) de 3.8, $j(F,G)$ est une bijection de $\mathrm{Hom}_k(F,G)$ sur le sous ensemble $\{\psi \in C(G)^m \mid (F_a - \sum_{j=1}^{\infty} V_j \sigma(a,j)\psi = 0\}$. On notera $j_S(F,G)$ l'application correspondante dans $C_S(G)^n$, le cas échéant.

Chapitre IV : La classification des lois sur certains anneaux de base

§1. Lois de dimension 1 sur un corps séparablement clos de caractéristique $p > 0$

Soit k un tel corps, fixé dans ce §, et soit $F \in F(1,k)$. Par définition même on a une injection canonique $End_k(F) \hookrightarrow k[[X]]$. Soit $[p](X) \equiv a_r X^r \bmod \deg r+1$, alors la relation $[p](F) = F([p](X),[p](Y))$ donne $a_r(X+Y)^r \equiv a_r X^r + a_r Y^r \bmod \deg r+1$ ce qui montre que $r = p^h$ pour un certain $h \in \mathbb{N}^+$. On dit que $h = ht(F)$ est la hauteur de F. Si $[p] = 0$, on dit que F est de hauteur infinie. Soit $S = S(k) = \{p\}$. Il est connu, ce qui se vérifie d'ailleurs sans peine, que F_p et V_p commutent si $\chi(k) = p > 0$.

1.1 Lemme : Les deux assertions suivantes sont équivalentes pour $F \in F(1,k)$.

a. F est isomorphe à $\hat{G}_a$.

b. $[p] = 0$.

Démonstration : a $\Longrightarrow$ b évident. b $\Longrightarrow$ a. On a $[p]\varphi_F = F_p V_p \varphi_F = V_p F_p \varphi_F = 0$, d'où $F_p \varphi_F = 0$. De plus, on peut supposer F typique. Il suit que $F^* \simeq U_c(k)/(Y_i^p)_{i\geqslant 0}$ ce qui est l'algèbre de distributions $\hat{G}_a$, d'où a.

1.2 On considère avec [F] ch. III, §2 les trois théorèmes fondamentaux :

Théorème 1 : Soit $h \in \mathbb{N}^+$, alors il existe $F \in F(1,k)$ tq $[p] = X^{p^h}$.

Théorème 2 : (Dieudonné-Lazard). Si $F_1, F_2 \in F(1,k)$ alors : $F_1 \sim F_2$ sur k si et seulement si $ht(F_1) = ht(F_2)$.

Théorème 3 : (Dieudonné-Lubin). Soit $F \in F(1,k)$ avec $htF < \infty$. Alors $E = End_k(F)$ est isomorphe à l'ordre maximal du corps gauche D d'invariant h^{-1} et de rang h^2 sur $\mathbb{Q}_p$.

Pour la démonstration par aide du lemme fondamental de Lubin-Tate on renvoie à Fröhlich loc. cit. On donne ic les démonstrations du point de vue des courbes.

1.3 On définit $F \in F(1,k)$, typique, par son type $F_p\varphi_F = V_{p^{h-1}}\varphi_F$. ($F$ est défini sur $\mathbb{F}_p$, même : F s'obtient par réduction mod p d'une loi définie sur $\mathbb{Z}$). On a $[p]\varphi_F = V_p F_p \varphi_F = V_{p^h}\varphi_F$, d'où, si $\varphi_F = \Sigma E_m t^m$, alors $[p]\varphi_F = \Sigma E_{m//p^h} t^m$. Soit $\theta(F) = k[[X_F]]$, d'où $\varphi_F(X_F) = t$, alors $\langle E_n, [p](X_F)\rangle = \langle [p]E_n, X_F\rangle = \langle E_{n//p^h}, X_F\rangle = \begin{cases} 1 & \text{si } n = p^h \\ 0 & \text{sinon} \end{cases}$.

Il en résulte que $[p](X) = X^{p^h}$, ce qui démontre le th. 1.

1.4 Démonstration du théorème 2 : Le cas de hauteur infinie est celui du lemme 1.1. Supposons donc G de hauteur finie, $ht(G) = h$. Il suffit d'établir un isomorphisme sur k avec la loi F de 1.3 qui est de hauteur h. D'après III.1.3 cor. 2 il suffit de montrer que $C_S(G)$ contient une courbe fondamentale ϕ telle que $F_p\phi = V_{p^{h-1}}\phi$.

Ecrivons F et V au lieu de F_p, V_p.

Supposons que $\phi \in C_S(G)$ soit fondamentale avec $F\phi \equiv V^{h-1}\mu\phi \bmod V^h$ et $\mu \in k^*$ cf. III lemme 1.2 b. On suppose en ce moment que h soit la hauteur de G. (Cela en effet en résultera). On pose $\chi = X\phi$ avec $X \in k^*$ à déterminer plus loin. Alors $F\chi = FX\phi = X^p F\phi \equiv X^p V^{h-1} \mu\phi \equiv X^p V^{h-1} \mu X^{-1} \chi = V^{h-1} X^{p^h-1} \mu\chi \bmod V^h$. k étant séparablement clos, on peut prendre X tq $X^{p^h-1} = \mu^{-1}$. On peut donc supposer que ϕ est fondamentale et que l'on ait

$$F\phi = V^{h-1}\phi + V^r\lambda\phi \bmod V^{r+1} \quad \text{avec} \quad \lambda \in k .$$

Soit $\chi = \phi + V^{r-h+1}X\phi$ avec $X \in k$, à déterminer plus loin.

Alors
$$\begin{aligned} F\chi &= F\phi + V^{r-h+1}X^p F\phi \\ &\equiv F\phi + V^{r-h+1}X^p \{V^{h-1}\phi + V^r\lambda\phi\} \bmod V^{r+1} \\ &\equiv F\phi + V^r X^{p^h}\phi \bmod V^{r+1} . \end{aligned} \tag{1}$$

D'autre part :

$$V^{h-1}\chi = V^{h-1}\phi + V^r X\phi \equiv F\phi - V^r\lambda\phi + V^r X\phi \bmod V^{r+1} \tag{2}$$

Il suit de (1) et (2) :

$$F\chi - V^{h-1}\chi \equiv V^r \{X^{p^h}\phi - X\phi + \lambda\phi\} \bmod V^{r+1} \equiv V^r(X^{p^h} - X + \lambda)\phi \bmod V^{r+1} .$$

On prend $X \in k$ comme racine du polynôme séparable $X^{p^h} - X + \lambda$. Il s'ensuit bien que $C_S(G)$ contient une courbe fondamentale ψ t.q $F\psi = V^{h-1}\psi$, et d'après 1.3, $h = htG$.

1.5 Démonstration du théorème 3 : D'après ce qui précède, on peut supposer que le S-type de F se donne par $F\varphi = V^{h-1}\varphi$. D'après III 3.8, (2) on a

$$End_k(F) \simeq \{\lambda = \sum_{i=0}^{\infty} V^i\lambda_i \mid \lambda_i \in k \; ; \; (F - V^{h-1})\lambda\varphi = 0\}$$, donc $\lambda \in End_k(F)$ si et seulement si

$$F \sum_{i=0}^{\infty} V^i \lambda_i \varphi = V^{h-1} \sum_{i=0}^{\infty} V^i \lambda_i \varphi = \sum_{i=0}^{\infty} V^{h+i-1} \lambda_i \varphi . \qquad (3)$$

D'autre part

$$F\lambda = \sum_{i=0}^{\infty} V^i \lambda_i^p F\varphi = \sum_{i=0}^{\infty} V^i \lambda_i^p V^{h-1} \varphi = \sum_{i=0}^{\infty} V^{h+i-1} \lambda_i^{p^h} \varphi \qquad (4)$$

c'est-à-dire (3) et (4) donnent : $\lambda \in End_k(F) \iff \lambda_i \in \mathbb{F}_{p^h}$ pour tout $i \geqslant 0$.

Considérons l'application $\mathbb{Z}_{(p)} \simeq W(\mathbb{F}_p) \to C_S(F)$ qui envoie $\Sigma V^i\lambda_i F^i$ sur $\Sigma V^i\lambda_i F^i\varphi_F = \Sigma V^i\lambda_i V^{(h-1)i}\varphi_F = \Sigma V^{hi}\lambda_i\varphi_F$. Il se voit que l'image de cette application est contenue dans l'image E de $End_k(F)$ et en effet est un homomorphisme injectif d'anneaux, ce qui munit E d'une structure de $\mathbb{Z}_{(p)}$-module topologique séparé complet. De plus $pE = FV(E) = V^h(E)$, d'où : E/pE s'identifie à $\mathbb{F}_p$-vectoriel $\{\sum_{i=0}^{h-1} V^i\lambda_i \mid \lambda_i \in \mathbb{F}_{p^h}\}$ de dimension h^2 sur $\mathbb{F}_p$. Soit $f \in E$, alors il est clair que $Vf \equiv f^pV \bmod VE$. On renvoie donc à Fröhlich loc. cit. pour les détails de nature algébrique, qui achèvent la démonstration du th. 3.

1.6 Soient $F,G \in F(1,k)$, de hauteur différente, soient h_1 et h_2. Soit de plus $f : F \to G$ et posons $j(F,G)f = \sum_{i=0}^{\infty} V^i f_i$. On prend les types de F et G, définis par $F\varphi_F = V^{h_1-1}\varphi_F$, $F\varphi_G = V^{h_2-1}\varphi_G$. Alors, il suit facilement de la relation

$$F \Sigma V_i f_i \varphi_G = \Sigma V^i f_i^p F\varphi_G = \Sigma V^i f_i^p V^{h_2-1} \varphi_G = \Sigma V^{i+h_2-1} f_i^{p^{h_2-1}} \varphi_G = V^{h_1-1} \Sigma V^i f_i \varphi_G =$$

$$= \Sigma V^{i+h_1-1} f_i \varphi_G$$

que tous les f_i sont nulles, d'où $Hom_k(F,G) = \{0\}$. Le théorème 2 montre qu'en général $Hom_k(F,G) = \{0\}$ si F et G sont de hauteur différente.

1.7 Si $\lambda = \sum_{i=0}^{\infty} V^i \lambda_i F^i$ et si $\varphi \in C(G)$ pour $G \in F(n,k)$, alors la définition $\lambda\varphi = \sum_{i=0}^{\infty} V^i \lambda_i F^i \varphi$ fait de $C(G)$ un $W(k)$-module à gauche, où $W(k)$ est l'anneau de vecteurs de Witt à coefficients dans k. Soit $B(k)$ le corps de fractions de $W(k)$ et posons

$$F(G) = C(G) \otimes_{W(k)} B(k) .$$

Alors $F(G)$ est un $B(k)$-vectoriel et parce que $FV = VF = p$, on peut oublier l'action de V sur $F(G)$. Autrement dit, $F(G)$ est un F-espace au sens de [D], ch. IV.

$G,H \in F(n,k)$ seront dits isogènes si $F(G) \simeq F(H)$ en tant que F-espace, ce qui donne une relation d'équivalence sur l'ensemble $F(n,k)$, et l'on note le quotient par $Isog(n,k)$ (et $Isog(k)$ si l'on part de $\bigcup_n F(n,k) = F(k)$).

Les résultats 1.6 et le th. 2 donnent que $Isog(1,k)$ est classifié par la notion "hauteur" ou encore par la relation $F = V^{h-1}$ pour $h \in \mathbb{N}^+ \cup \{\infty\}$. A partir du lemme fondamental on déduit le résultat de Manin :

Théorème : Si k est algébriquement clos, alors $Isog(n,k)$ est représenté par des lois $G_{n,m}$ avec $(n,m) = 1$ telles qu'il existe un ensemble fondamental des courbes de la forme $\{\varphi, F\varphi, \ldots, F^{n-1}\varphi\}$ et $F^n\varphi = V^m\varphi$.

§2. Groupes formels infinitésimaux sur un corps k, $\chi(k) = p > 0$

Le but de ce § est d'indiquer, comment la théorie des courbes (déformées) s'applique à la théorie des groupes infinitésimaux sur un corps de caractéristique $p > 0$.

2.1 On appelle algèbre tronquée sur k, toute k-algèbre A de la forme $A = k[X_1,\ldots,X_n]/(X_i^{p^{h(i)}})_{1 \leqslant i \leqslant n}$ avec $0 < h(i) < \infty$. Dans un anneau polynomial $k[X_1,\ldots,X_n]$ on appelle p-polynôme tout élément $f(X_1,\ldots,X_n) = \Sigma\, c_\alpha X_1^{\alpha_1}\ldots X_n^{\alpha_n}$ où $c_\alpha \neq 0$ implique $0 \leqslant \alpha_i < p$ pour tout i. On appelle algèbre semi-tronquée sur k toute k-algèbre de la forme $A = k[X_1,\ldots,X_n]/\mathcal{A}$, où l'idéal des relations $\mathcal{A}$ est engendré par $X_i^{p^{h(i)}} - f_i(X_{i+1}^{p^{g(i+1)}} \ldots X_n^{p^{g(n)}})$ pour $1 \leqslant i \leqslant n$ avec :

chaque f_i est un p-polynôme et $g(j) \geqslant h(i) \geqslant 1$ pour $i+1 \leqslant j \leqslant n$. Soit $\tilde{k} = k^{p^{-\infty}}$, alors il est clair : si A est semi tronquée sur k, alors $A \otimes_k \tilde{k}$ est tronquée sur k.

2.2 Soit maintenant $G \in Grf_k$ infinitésimal. On notera $A = \theta(G)$ et $m = \operatorname{Ker} \varepsilon : A \to k$. Soient $x_1,\ldots,x_n \in m$ tels que leurs images mod m^2 sont une base du k-vectoriel m/m^2. Soient maintenant aussi pour $1 \leqslant j \leqslant n$

$$\varphi_j : A/m^2 \to k[t]/(t^2)$$

les courbes d'ordre 1, définies par $\varphi_j(x_j) = \delta_{ij} t$. Alors la théorie des courbes pures montre que chaque φ_j s'étend à une courbe d'ordre $p-1$, soit

$$\varphi_j = 1 + \partial_{o,j} t + \ldots + \frac{\partial^i_{o,j}}{i!} t^i + \ldots + \frac{\partial^{p-1}_{o,j}\, t^{p-1}}{(p-1)!} \qquad (1)$$

On pose $\partial^{(\alpha)} = \dfrac{\partial^{\alpha_1}_{o,j}\, \partial^{\alpha_2}_{o,2} \cdots \partial^{\alpha_n}_{o,n}}{\alpha_1! \ldots \alpha_n!}$ pour $0 \leqslant \alpha_i < p$. De la même façon soit $x^\alpha = x_1^{\alpha_1} \ldots x_n^{\alpha_n}$ dans A. En observant que les $\overline{\partial^{(\alpha)}}$ sont produits des dérivations invariants à gauche de A (cf. II §1), on déduit sans peine :

$$\partial^{(\alpha)}(x^\beta) = \begin{cases} 0 & \text{si } \Sigma \beta_i > \Sigma \alpha_i \\ \delta_{\alpha,\beta} & \text{si } \Sigma \beta_i = \Sigma \alpha_i \end{cases} \qquad (2)$$

ce qui nous dit que les $x_1,\ldots,x_n$ sont une p-base pour un sous vectoriel L_1 de A. Soit $m^{\{p\}}$ l'idéal de A, engendré par $(x_1^p,\ldots,x_n^p)$, alors on a une décomposition

$$A \simeq L_1 \oplus m^{\{p\}}/m^{\{p\}}m \oplus m^{\{p\}}m \,. \qquad (3)$$

2.3 Soit d'abord $m^{\{p\}}/m^{\{p\}}m = 0$, ce qui veut dire que

$$x_i^p = \sum_{j=1}^{n} \lambda_{ij} x_j^p \quad \text{avec} \quad \lambda_{ij} \in m$$

pour $1 \leqslant i \leqslant n$,

ou encore $$0 = \sum_{j=0}^{n} (\lambda_{ij} - \delta_{i,j}) x_j^p \qquad (\delta_{i,j} \text{ de Kronecker}).$$

G étant infinitésimal, il s'ensuit que la matrice à coefficients $\lambda_{ij} - \delta_{i,j}$ est inversible ce qui entraîne que $m^{\{p\}} = 0$, ou encore que A est de hauteur $\leqslant 1$.

Dans ce cas-ci, l'ensemble des courbes $\varphi_1,\dots\varphi_n$ est fondamental et on retrouve de la même façon que dans le théorème de Cartier I.4.3 que l'application naturelle Lie $G \hookrightarrow G^*$ se prolonge en un isomorphisme $U_p(\text{Lie } G) \xrightarrow{\sim} G^*$ et que tels groupes infinitésimaux se classifient par aide de leurs p-Lie algèbres. (U_p signifie le foncteur : algèbre enveloppante restreinte, cf. SGAD VII A).

En excluant ce cas, soient, après renumérotation éventuelle $x_1^p,\dots,x_{k_1}^p$ tels que leurs images dans $m^{\{p\}}/m^{\{p\}}m$ sont une base.

Lemme : Soit $\sum_{i=1}^{n} \lambda_i x_i^p + \ell_1 \equiv 0 \bmod m^{\{p\}}m$ une relation dans $\mathbf{A}$ avec $\ell_1 \in L_1$, alors $\ell_1 = 0$.

Démonstration : Les $\partial^{(\alpha)}$, qui forment une partie linéairement indépendante dans G^*, s'annulent sur $m^{\{p\}}m$, et s'annulent également sur $m^{\{p\}}$. En appliquant une $\partial^{(\alpha)}$ convenable, on voit que $\ell_1 = 0$.

Il en résulte, que les relations dans l'algèbre $\mathbf{A}$ sont de la forme

$$x_r^p \equiv \sum_{i=1}^{k_1} \alpha_{r,i}\, x_i^p \bmod m^{\{p\}}m \; ; \; k_1 < r \leqslant n \qquad (3)$$

($k_1 = n$ signifie l'absence de telles relations).

2.4 Soit T_1 l'algèbre quotient de $k[t_1,\dots,t_n]$ modulo l'idéal $\mathfrak{a}$ engendré par les éléments suivants : Si $I = (t_1,\dots,t_n)$, alors $I^{\{p\}}I \subset \mathfrak{a}$. De plus $t_r^p - \sum_{i=1}^{k_1} \alpha_{r,i}\, t_i^p \in \mathfrak{a}$ avec les $\alpha_{r,i}$ comme dans (3). Il est bien évident que les monômes

$$t^\beta = t_1^{\beta_1}\dots t_n^{\beta_n} \quad \text{avec} \quad \begin{cases} 0 \leqslant \beta_i \leqslant p & \text{pour } 1 \leqslant i \leqslant k_1 \\ 0 \leqslant \beta_i < p & \text{pour } k_1 < i \leqslant n \end{cases}$$

constituent une base $B_1 = \{t^\beta \mid \beta \in S_1\}$ de T_1. De plus, il est clair qu'il existe un homomorphisme évident de k-algèbres

$$\psi : A \to T_1 \quad , \quad \psi(x_i) = t_i \, .$$

Posons pour $a \in \mathbf{A}$, $\psi(a) = \sum_{\alpha \in S_1} \psi_\alpha(a) t^\alpha$, alors les ψ_α appartiennent à G^*.

Soient $\varepsilon_j = (\underbrace{0,\dots,0}_{j-1},1,0\dots0) \in S_1$ et $\varepsilon_{pj} = (\underbrace{0,\dots,0}_{j-1},p,0\dots0)$, alors de la

relation

$$\psi(a^p) = \sum_{\alpha \in S_1} \psi_\alpha(a^p) t^\alpha = \psi(a)^p = \sum_{\alpha \in S_1} \psi_\alpha(a)^p \, t^{p\alpha}$$

on déduit :

$$\psi_{\varepsilon_{pj}}(a^p) = \{\psi_{\varepsilon_j}(a)\}^p + \sum_{r=k_1+1}^{n} \alpha_{r,j} \{\psi_{\varepsilon_r}(u)\}^p \tag{4}$$

pour $1 \leqslant j \leqslant k_1$. Posons $\begin{cases} \partial_{1,j} = \psi_{\varepsilon_{pj}} & \text{pour } 1 \leqslant j \leqslant k_1 \\ \partial_{o,j} = \psi_{\varepsilon_j} & \text{pour } 1 \leqslant j \leqslant n \end{cases}$.

Il est clair que les $\partial_{o,j}$ sont ceux de (1).

On posera $\partial^{(a,b)} = \dfrac{\partial_{1,1}^{\alpha_1} \cdots \partial_{1,k_1}^{\alpha_{k_1}} \partial_{o,1}^{\beta_1} \cdots \partial_{o,n}^{\beta_n}}{\alpha_1! \cdots \alpha_{k_1}! \, \beta_1! \cdots \beta_n!}$ si $0 \leqslant \alpha_i, \beta_j < p$ pour (5)

toutes les valeurs i,j considérées.

2.5 Lemme : Les monômes $x_1^{\alpha_1} \cdots x_n^{\alpha_n} = x^\alpha$, avec $0 \leqslant \alpha_i < p^2$ pour $1 \leqslant i \leqslant k_1$ et $0 \leqslant \alpha_i < p$ pour $k_1 < i \leqslant n$ sont linéairement indépendants dans $\mathbf{A}$ et sont donc une base pour un sous vectoriel L_2 de $\mathbf{A}$.

Démonstration : Soit $\alpha_i = \delta_i + p\gamma_i$ le développement p-adique de α_i pour $1 \leqslant i \leqslant k_1$.

On applique $\bar{\partial}^{(a,b)}$ sur x^α . Le fait que les $\bar{\partial}_{o,i}$ s'annulent sur $m^{\{p\}}$ entraîne que l'on a :

$$s: = \bar{\partial}^{(a,b)}(x^\alpha) = \frac{\bar{\partial}_{1,1}^{\alpha_1} \cdots \bar{\partial}_{1,k_1}^{\alpha_{k_1}}}{\alpha_1! \cdots \alpha_{k_1}!} \{(x_1^{\gamma_1} \cdots x_{k_1}^{\gamma_{k_1}})^p\} \cdot \frac{\bar{\partial}_{o,1}^{\beta_1} \cdots \bar{\partial}_{o,n}^{\beta_n}}{\beta_1! \cdots \beta_n!} (x_1^{\delta_1} \cdots x_n^{\delta_n})$$

$$= \bar{\partial}_1^\alpha(x^{\gamma p}) \, \bar{\partial}_o^\beta(x^\delta) \quad \text{(de façon abrégée)} \tag{6}$$

(2) donne les valeurs $\partial_o^\beta(x^\delta)$, il reste à calculer $\bar{\partial}_1^\alpha(x^{\gamma p})$.

(4) donne :

$$\partial_{1,j}(a^p) = \{\partial_{o,j}(a)\}^p + \sum_{k_1+1}^{n} \alpha_{r,i} \{\partial_{o,i}(a)\}^p$$

ce qui encore entraîne d'après le lemme II.3.1 b

$$\bar{\partial}_{i,j}(a^p) = \{\bar{\partial}_{o,j}(a)\}^p + \sum_{k_1+1}^{n} \alpha_{r,i} \{\bar{\partial}_{o,i}(a)\}^p \quad . \tag{7}$$

En prenant $a = x_m$ avec $1 < m < k_1$ dans (7), on voit par (2), en utilisant que les indices, intervenant dans la somme de (7), sont $\geqslant k_1+1$, que :

$$\partial_{1,j}(x_m^p) = \{\partial_{o,j}(x_m)\}^p = \delta_{j,m}$$

c'est-à-dire (6) se réduit à

$$s \equiv \bar{\partial}_o^{\alpha}(x^{\gamma})\ \bar{\partial}_o^{\beta}(x^{\delta}) \bmod \mathrm{Ker}\ \varepsilon$$

ce qui entraîne le lemme en raisonnant de la même façon afin de déduire les relations (2).

2.6 On décompose $\mathbf{A}$ en somme directe

$$\mathbf{A} \simeq L_2 \oplus m\{p^2\}/m\{p^2\}_m \oplus m\{p^2\}_m \ . \tag{8}$$

Les relations (3) se prolongent en relations

$$x_r^p - \sum_{i=1}^{k_1} \alpha_{r,i} x_i^p + \ell_2 \equiv 0 \bmod m\{p^2\}_m \tag{9}$$

avec $\ell_2 \in L_2$. En supposant qu'il y a un terme x^{α} dans ℓ_2 à coefficient non nul et dont les puissances α_i qui interviennent ne sont pas toutes des puissances de p , alors par choix d'un $\partial^{(a,b)}$ avec b convenable, non nul, on arriverait à la contradiction $0 \neq c = 0$, ce qui dit que les relations (9) en effet sont relations dans laquelle interviennent p-polynômes. Le raisonnement fait à partir de (3) pour arriver à (8) se généralise. On en déduit :

2.7 <u>Proposition</u> : Si k est un corps, $\chi(k) = p > 0$ et si $G \in \mathrm{Grf}_k$ est infinitésimal, alors $\theta(G)$ est semi tronquée. Si de plus k est parfait, alors $\theta(G)$ est tronquée.

<u>Corollaire</u> : Si $G \in \mathrm{Grf}_k$ est infinitésimal et si k est parfait, alors G est engendré par un ensemble fini des courbes finies.

2.8 Soit E la courbe pure, alors le théorème de décomposition entraîne que $E^p = \prod_{(a,p)=1} V_a H_a(E^p)$ et $H_1(E^p)$ est défini par un ensemble pur pour E de la forme $(0, fY_o, fY_1, \ldots) = (0, Y_o^p, \ldots)$ où $fY_i \equiv Y_i^p \bmod Y_o = \ldots = Y_{i-1} = 0$. De même, si F est une autre courbe pure générique, on a

$$EFE^{-1}F^{-1} = \prod_{(a,p)=1} V_a H_a \ .$$

Si $p \neq 2$, on voit que H_2 est définie par un ensemble pur pour E de la forme $([Y_o,X_o],\ldots,(Y_i,X_i),\ldots)$ où $(Y_i,X_i) \equiv Y_iX_i - X_iY_i + g(X_o,\ldots,X_i,Y_o,\ldots,Y_i)$ avec $g(0,\ldots,0,X_i,0,\ldots,0,Y_i) = 0$. A partir de là il est possible, en principe de généraliser l'application $x \mapsto x^{(p)}$ et le crochet dans une p-algèbre de Lie à ensembles purs, ou encore aux semi dérivations dans une coalgèbre en groupes. Cela devrait donner une théorie par exemple pour les groupes de hauteur $\leqslant 2$ sur un corps parfait de caractéristique positive, une théorie qui toutefois est encore loin d'être établie.

2.9 Soit encore $G \in Grf_k$ infinitésimal et commutatif. Soit $U_c(n,k) = k[Y_o,\ldots,Y_n]$ le sous objet dans Ab_k tel que $\Sigma E_m(Y_o,\ldots,Y_m)t^m$ soit une courbe pure d'ordre p^n dans $U_c(n,k)$. Alors, l'ensemble des courbes pures d'ordre p^n dans G , c'est-à-dire $Ab_k(U_c(n,k),G^*)$ est de façon naturelle un module sur l'anneau $End_{Ab_k}(U_c(n,k))$. Le morphisme $U_c(n+1,k) \to U_c(n,k)$, $Y_m \to Y_{m-1}$ dans Ab_k induit un système inductif $\{Ab_k(U_c(n,k),G^*\}$ et on se retrouve dans la situation connue de [D] Ch. I, §5. De cette façon, la théorie de modules de Dieudonné s'interprète comme une théorie de courbes, ou plutôt, le converse.

§3. Une digression

3.1 Soit C' l'anneau polynomial commutatif, engendré sur $\mathbb{Z}$ par des indéterminés $A(n,1)$, $B(m,1)$ pour $n \geqslant 2$ et $m \geqslant 1$; $n,m \in \mathbb{N}^+$. Soient P l'ensemble des nombres premiers et C l'anneau quotient de C', obtenu en faisant commuter $A(p^i,1)$ et $A(q^j,1)$ pour $p \neq q$; $p,q \in P$ et $i,j \geqslant 0$ et en posant $A(1,1) = 1$.

Lemme : Soit $m,b \in \mathbb{N}^+$, alors il existe un unique $A(b,m)$ et $B(b,m)$ dans C tels que si $m = ap^{r+1}$ avec $(a,p) = 1$, $p \in P$, on ait

$$A(b,ap^{r+1}) = A(bp,ap^r) - A(b,a)A(p,p^r) \qquad (1)$$

$$B(b,ap^{r+1}) = B(bp,ap^r) - B(b,a)A(p,p^r) \ . \qquad (2)$$

Démonstration : Il suffit de montrer (2) et on procède par récurrence sur le nombre $\sigma(m)$ des $p \in P$ avec $p|m$, y comptant multiplicités. Parce que $\sigma(ap^{r+1}) > \max\{\sigma(ap^r), \sigma(a), \sigma(p^r)\}$, (2) affirme l'existence d'un $B(b,m)$, mais celui-là peut dépendre du p choisi. Donc soit (2) vrai pour tout b et pour toutes les décompositions $m = ap^{r+1}$ si $\sigma(m) < k$. Soient $\sigma(m) = k$ et $m = ap^{r+1}q^{t+1}$ avec $p \neq q$ dans P, $(a,p) = (a,q) = 1$. Si on suppose $B(b,m)$ construit à partir de (2) avec p, alors

$$B(b,m) = B(b,ap^{r+1}q^{t+1}) = B(bp,ap^rq^{t+1}) - B(b,aq^{t+1})A(p,p^r)$$
$$= B(bpq,ap^rq^t) - B(bp,ap^r)A(q,q^t) - B(bq,aq^t)A(p,p^r) + B(b,a)A(q,q^t)A(p,p^r).$$

De plus $A(p,p^r)$ étant un polynôme dans les $A(p^i,1)$ avec $0 \leqslant i \leqslant r+1$, commute avec $A(q,q^t)$, donc en combinaisant les 1er et 3è termes ainsi que les 2è et 4è termes on trouve : $B(b,m) = B(bq,ap^{r+1}q^t) - B(b,ap^{r+1})A(q,q^t)$, ce qui dit que (2) est vrai pour q.

3.2 On définit pour $a \in \mathbb{N}$ l'endomorphisme d'algèbre F_a de C par $F_aA(n,1) = A(n,1)$ et $F_aB(n,1) = B(an,1)$. Alors il suit de (1) et (2) que l'on a :

$$F_aA(b,m) = A(b,m) \quad \text{et} \quad F_aB(b,m) = B(ab,m).$$

Si $m = \prod p_i^{\alpha_i}$, on pose $C(m) = \prod_i A(p_i^{\alpha_i},1)$ dans C (produit ordonné). Alors on a :

Lemme : $B(rm,1) = \sum_{d|m} B(r,d)C(m/d)$ dans C pour $r \in \mathbb{N}^+$.

Démonstration : Quitte à appliquer F_r, on peut supposer que $r = 1$, de plus il suffit évidemment de démontrer : Si $(a,p) = 1$, $p \in P$ et si $b \in \mathbb{N}$, $k \geqslant 0$, alors

$$B(bp^k,a) = \sum_{i=0}^{k} B(b,ap^i)A(p^{k-i},1). \qquad (3)$$

(3) est vrai si $k = 0$, donc soit (3) vrai pour k. En appliquant F_p à (3) on a

$$B(a,bp^{k+1}) = \sum_{i=0}^{k} B(bp,ap^{i})A(p^{k-i},1)$$

$$= \sum_{i=0}^{k} B(b,ap^{i+1})A(p^{k-i},1) + B(b,a)\sum_{i=0}^{k} A(p,p^{i})A(p^{k-i},1)$$

$$= \sum_{i=1}^{k+1} B(b,ap^{i})A(p^{k+1-i},1) + B(b,a)\sum_{i=0}^{k} (c_i - c_{i+1}) \qquad (4)$$

où $c_i = A(p^{k+1-i},p^{i})$. Il suit que $\sum_{i=0}^{k} (c_i - c_{i+1}) = A(p^{k+1},1) - A(1,p^{k+1}) =$

$= A(p^{k+1},1)$, parce que $a=b=1$ dans (b) montre que $A(1,p^{k+1}) = 0$, c'est-à-dire (4) réduit à (3) avec $k+1$ au lieu de k .

3.3 Soit maintenant D l'algèbre polynomiale non commutative engendrée sur $\mathbb{Z}$ par des indéterminés $A(n,0)$ pour $n \in \mathbb{N}^+$, $B(n,0)$ et $C(n,0)$ avec $n \in \mathbb{N}$. On pose $A(0,0) = 1$. Soit K un anneau muni d'un endomorphisme σ . Alors, en considérant $f \in D$ comme une fonction définie sur un produit convenable de K à valeurs dans K , on notera f^{σ} la fonction obtenue $f \circ \sigma$. On définit par récurrence pour $\ell,n \in \mathbb{N}$

$$A(n,\ell+1) = A(n+1,\ell) - A(n,0)^{\sigma^{\ell+1}} A(1,\ell) \qquad (5a)$$

$$B(n,\ell+1) = B(n+1,\ell) - B(n,0)^{\sigma^{\ell+1}} A(1,\ell) \qquad (5b)$$

$$C(n,\ell+1) = C(n+1,\ell) - C(1,\ell)^{\sigma^{n}} A(n,0) \qquad (5c)$$

$$\begin{cases} D(n,\ell+1) = D(n+1,\ell) - A(1,\ell)^{\sigma^{n}} A(n,0) \qquad (5d) \\ D(n,0) = A(n,0) \ . \end{cases}$$

On définit les endomorphismes Δ et ∇ d'algèbre D par $\Delta B(n,0) = B(n+1,0)$ et $\nabla C(n,0) = C(n,1)$, en convenant que Δ et ∇ sont les applications identiques sur les autres générateurs.

3.4 Les propriétés de D qui serviront après, se résument dans

<u>Proposition</u> : a. $A(0,\ell+1) = C(0,\ell+1) = D(0,\ell+1) = 0$; $A(1,\ell) = D(1,\ell)$ pour $\ell \in \mathbb{N}$

b. $\Delta B(n,\ell) = B(n+1,\ell)$; $\nabla C(n,\ell) = C(n+1,\ell)$

c. $B(n,0) = \sum_{j=0}^{n} B(0,j)^{\sigma^{n-j}} A(n-j,0)$

d. $C(n+1,0) = \sum_{j=0}^{n} C(1,j)^{\sigma^{n-j}} A(n-j,0)$

e. $A(n+1,0) = \sum_{j=0}^{n} A(1,j)^{\sigma^{n-j}} A(n-j,0)$.

Démonstration : b se vérifie sans difficultés. d est vrai si $n=0$, soit donc d vrai pour $0 \leqslant \ell \leqslant n$, alors :

$$C(n+1,0) = C(n,1) + C(1,0)^{\sigma^{n}} A(n,0) \qquad (5c)$$

$$= \nabla C(n,0) + C(1,0)^{\sigma^{n}} A(n,0)$$

$$= \sum_{j=0}^{n-1} C(1,j+1)^{\sigma^{n-j-1}} A(n-j-1,0) + C(1,0)^{\sigma^{n}} A(n,0)$$

$$= \sum_{j=1}^{n} C(1,j)^{\sigma^{n-j}} A(n-j,0) + C(1,0)^{\sigma^{n}} A(n,0) .$$

Les autres assertions se montrent en même temps. c est vrai si $n=0$. On suppose donc c vrai si $0 \leqslant \ell \leqslant n$. Alors

$$B(n+1,0) = \Delta B(n,0) = \sum_{j=0}^{n} B(1,j)^{\sigma^{n-j}} A(n-j,0)$$

$$= \sum_{j=0}^{n} \{B(0,j+1) + B(0,0)^{\sigma^{j+1}} A(1,j)\}^{\sigma^{n-j}} A(n-j,0)$$

$$= \sum_{i=1}^{n+1} B(0,i)^{\sigma^{n+1-i}} A(n+1-i,0) + B(0,0)^{\sigma^{n+1}} \sum_{j=0}^{n} A(1,j)^{\sigma^{n-j}} A(n-j,0) .$$

En appliquant (5d) on voit que la deuxième somme est égale à

$$\sum_{j=0}^{n} \{D(n+1-j,j) - D(n-j,j+1)\} = D(n+1,0) - D(0,n+1) = A(n+1,0) - D(0,n+1) ,$$

ce qui démontrerait c si

$$D(0,n+1) = 0 . \qquad (6)$$

Soit h_1 l'endomorphisme d'algèbre D , défini par $h_1 C(n,0) = A(n,0)$, h_1 étant l'application identique sur les autres générateurs. Il suit que $h_1 C(n,\ell) = D(n,\ell)$ pour tout n,ℓ , donc en appliquant h_1 à d , déjà montré, on voit

$$A(n+1,0) = \sum_{j=0}^{n} D(1,j)^{\sigma^{n-j}} A(n-j,0) . \qquad (7)$$

Soit d'autre part h_2 l'endomorphisme d'algèbre D, défini par $h_2B(n,0) = A(n+1,0)$, h_2 étant l'application identique sur les autres générateurs. Parce que c est supposé vrai pour $0 \leqslant \ell \leqslant n$, et parce qu'on a généralement : $h_2B(n,\ell) = A(n+1,\ell)$, on déduit, en appliquant h_2 à c :

$$A(\ell+1,0) = \sum_{j=0}^{\ell} A(1,j)^{\sigma^{\ell-j}} A(\ell-j,0) \quad \text{si} \quad 0 \leqslant \ell \leqslant n \tag{8}$$

(7) et (8) donnent : $A(1,j) = D(1,j)$ pour $0 \leqslant j \leqslant n$. Mais (5d), en prenant $n=0$ donne :

$$D(0,\ell+1) = D(1,\ell) - A(1,\ell)^{\sigma^0} A(0,0) = D(1,\ell) - A(1,\ell) = 0$$

si $0 \leqslant \ell \leqslant n$. Il suit que (6) est vrai, d'où encore c pour $\ell = n+1$ ce qui prouve la proposition.

§4. Classification des lois abéliennes sur $\mathbf{Z}_S$

4.1 Soit $\emptyset \neq S \subset P$. Parce que pour $\mathbf{Z}_S = k$ on a : $k = k_G$ pour tout $G \in F(n,k)$ et parce que $\mathbf{Z}_S$ est un anneau d'intégrité, on sait que $G \in F_{typ}(n,k)$ est déterminée par son logarithme

$$\ell_G = \sum_{m \in \mathbb{N}(S)} m^{-1}\, {}^t f(m) X^{(m)} \tag{1}$$

avec $f : \mathbb{N}(S) \to \mathbb{M}(n,k)$ S-lexoide. De plus :

$$\varphi_G = \exp \sum_{m \in \mathbb{N}(S)} m^{-1} f(m) \partial_G t^m \text{ . (Ch. III, §2)} \tag{2}$$

Soit $\psi \in G(G)^n$ un autre ensemble des courbes, alors on a

$$\psi = \sum_{m \in \mathbb{N}(S)} V_m \widetilde{\mu(m)} \varphi_G \tag{3}$$

avec $\mu(m) \in \mathbb{M}(n,k)$, ou encore, en posant $\tau_n(\psi) = g(n)$, on trouve

$$g(m) = \sum_{d \mid m} d\mu(d) f(m/d) \text{ .} \tag{4}$$

Supposons que l'on ait $\mu(1) = I_n$ et $g(s) \in \mathbb{M}(n,\mathbf{Z})$ si $s < m$, de plus, supposons que $0 \leqslant \pi(i,j)g(s) < s$ si $1 < s < m$ et $1 \leqslant i,j \leqslant n$. Ecrivons (4) sous la forme $g(m) = \sum_{d<m} + m\mu(m) = x + m\mu(m)$. Parce que pour $y \in \mathbf{Z}_S$ il existe un unique $\bar{y} \in \mathbf{Z}$ tel que $0 \leqslant \bar{y} < m$ et $y \equiv \bar{y} \bmod m$, soit $\bar{y} = y + m\bar{\bar{y}}$,

on peut choisir $\mu(m)$ de façon unique tel que $\pi(i,j)x + m\pi(i,j)\mu(m) \in \mathbb{Z}$, à savoir on pose $\pi(i,j)\mu(m) = \overline{\pi(i,j)x}$. Soit donc $\phi(n,S) = \{f \in \mathrm{Lex}_n(S,\mathbb{Z}) \mid 0 \leqslant \pi(i,j\, f(m) < m$ si $m > 1$ et $1 \leqslant i,j \leqslant n\}$, alors le raisonnement ci-dessus montre :

Lemme 1 : Chaque loi $G \in F_{typ}(n,k)$ est strictement isomorphe à une loi, déterminée par un élément de $\phi(n,S)$.

4.2 En restreignant les domaines de définition, on obtient une application naturelle

$$\phi(n,S) \to \prod_{p \in S} \Phi(n,\{p\}) \tag{5}$$

qui envoie $f \in \Phi(n,S)$ sur $(f_p \mid p \in S)$, $f_p(p^i) = f(p^i)$.

Théorème : L'application (5) est une bijection.

Démonstration : Il est clair que (5) est injective. Soit donc $(g_p \mid p \in S) \in \prod_{p \in S} \Phi(n,\{p\})$ et supposons qu'il existe des relations

$$g(ab) = \sum_{d \mid b} d\sigma_f(a,d)\, g(b/d) \tag{6}$$

pour $a,b \in \mathbb{N}(S)$, $a,b < m$ avec $\sigma_f(a,p^i) \in M(n,\mathbb{Z})$ chaque fois que $ap^i < m$ et $(a,p) = 1$ et où $g(p^j) = g_p(j)$ si $p \in S$ et $p^j < m$, et où encore $g(s) \in M(n,\mathbb{Z})$ si $s < m$ avec $0 \leqslant \pi(i,j)g(s) < s$ et $1 \leqslant i,j \leqslant s$. Si $m \notin \mathbb{N}(S)$, il n'y a rien à faire.

Soit donc $m = \prod_i p_i^{\alpha_i}$ avec $p_i \in S$. Notons $m_i = mp_i^{-\alpha_i}$ et considérons le système d'équations

$$g(m) = g(m_i p_i^{\alpha_i}) = \sum_{j=0}^{\alpha_i} p_i^j\, \sigma_f(m_i, p_i^j)\, g(p_i^{\alpha_i - j}) \tag{7}$$

$$g(m) = \sum_{j < \alpha_i} + p_i^{\alpha_i}\, \sigma_f(m_i, p_i^{\alpha_i}) . \tag{8}$$

Le théorème de reste chinois appliqué à (8) montre qu'il existe un unique $\sigma_f(m_i, p_i^{\alpha_i}) \in M(n,\mathbb{Z})$ et un unique $g(m) \in M(n,\mathbb{Z})$ t.q $0 \leqslant \pi(i,j)g(m) < m$ pour chaque $0 \leqslant i,j \leqslant n$. Il s'ensuit qu'on a une fonction $g : \mathbb{N}(S) \to M(n,\mathbb{Z})$. Soit $G \in F(n,\mathbb{Q})$ définie par son logarithme

$$\ell_G = \sum_{m \in \mathbb{N}(S)} m^{-1}\, {}^t g(m) X^{(m)} \ .$$

Soit de plus $G_p \in F(n, \mathbb{Z}_{(p)})$ la loi définie par g_p. On pose $\varphi_{G_p} = \varphi_p$. Alors en prenant $T = \{p\}$ et $T^* = S - \{p\}$ dans la prop. III 3.2 a, on voit sans peine que l'on a

$$\varphi_G = \sum_{a \in \mathbb{N}(S-\{p\})} \sum_{i=0}^{\infty} V_{ap^i} \widetilde{a^{-1}\, \sigma_f(a, p^i)} \varphi_p$$

ce qui montre que φ_G est isomorphe sur $\mathbb{Z}_{(p)}$ avec G_p, parce que a est inversible dans $\mathbb{Z}_{(p)}$. (III 1.3 cor. 1), en particulier, G est définie sur $\mathbb{Z}_{(p)}$, donc sur $\bigcap_{p \in S} \mathbb{Z}_{(p)} = \mathbb{Z}_S$, c'est-à-dire g est S-lexoide et même d'après la construction, $g \in \Phi(n,S)$.

4.3 D'après le théorème 3.2, la structure de $\Phi(n,S)$ est essentiellement déterminée par les $\Phi(n,\{p\})$ avec $p \in S$. Pour celle-là on a

<u>Proposition</u> : Soit $S = \{p\}$ et soit $\mu : \mathbb{N}(S) \to M(n, \mathbb{Z}_{(p)})$, arbitraire, alors $f : \mathbb{N}(S) \to M(n, \mathbb{Z}_{(p)})$ définie par

$$\sum_{i=0}^{\infty} f(p^i) p^{-is} = (1 - \sum_{j=0}^{\infty} p^j \mu(p^j)\, p^{-(j+1)s})^{-1} \qquad (9)$$

est S-lexoide, et on a

$$f(p^{n+1}) = \sum_{i=0}^{n} p^i \mu(p^i) f(p^{n-i}) = \sum_{i=0}^{n} p^i f(p^{n-i}) \mu(p^i) \ . \qquad (10)$$

De plus, chaque fonction S-lexoide s'obtient de cette façon.

Si f définit $G \in F(n, \mathbb{Z}_{(p)})$, alors on a $F_p \varphi_G = \Sigma\, V_{p^j} \widetilde{\mu(p^j)} \varphi_G$.

<u>Démonstration</u> : En multipliant les deux membres de (9) avec l'inverse du membre droit on voit que

$$\sum_{i=0}^{\infty} f(p^i) p^{-is} = 1 + \sum_{i,j=0} \mu(p^j) f(p^i) p^{-(i+j+1)s}$$

ce qui donne tout de suite (10). et le fait que f soit S-lexoide.

4.4 D'après 4.3 et 4.2, chaque $G \in F_{typ}(n, \mathbb{Z}_S)$ est strictement isomorphe à une loi définie par une fonction S-lexoide, qui admet pour chaque $p \in S$ un facteur local de séries de Dirichlet (9). Il y a une situation, dans laquelle ces lois admettent des séries de Dirichlet globales :

Théorème

Soit pour $p \in P$, $L_p(s) = (I_n - \sum_{i=0}^{\infty} p^i \sigma(p,p^i) p^{-(i+1)s})^{-1} = \sum_{i=0}^{\infty} \mathbf{A}(p^i) p^{-is}$ (11)

avec $\sigma(p,p^i) \in M(n,\mathbb{Z})$. On suppose que $\sigma(p,p^i)$ et $\sigma(q,q^j)$ commutent pour $p \neq q$ dans P et pour chaque $i,j \geqslant 0$. Soit

$$\prod_p L_p(s) = \sum_{m=1}^{\infty} \mathbf{A}(m) m^{-s} \tag{12}$$

et

$$\ell(X) = \sum_{m=1}^{\infty} m^{-1}\, {}^t\mathbf{A}(m) X^{(m)} .$$

Alors : $\mathbf{A} : \mathbb{N}^+ \to M(n,\mathbb{Z})$ est P-lexoide, donc $\ell^{-1}(\ell(X) + \ell(Y)) \in F(n,\mathbb{Z})$, ce qui redonne le théorème 8 de Honda [2].

Démonstration : Il faut établir les relations

$$\mathbf{A}(am) = \sum_{d|m} d\lambda(a,d)\mathbf{A}(m/d) \quad ; \quad a,m \in \mathbb{N} \tag{13}$$

avec $\lambda(a,d) \in M(n,\mathbb{Z})$. Définissons l'homomorphisme d'algèbres $\phi : C \to M(n,\mathbb{Q})$, où C est l'anneau du paragraphe précédent par

$$\phi(\mathbf{A}(m,1)) = \phi(B(m,1)) = m^{-1}\mathbf{A}(m) .$$

Alors en appliquant ϕ au lemme 3.2 on voit avec $r = a$

$$(ma)^{-1}\mathbf{A}(am) = \sum_{d|m} \phi B(a,d).(m/d)^{-1}\mathbf{A}(m/d) .$$

(Noter que $\phi C(m) = m^{-1}\mathbf{A}(m)$) , ou encore :

$$\mathbf{A}(am) = \sum_{d|m} d.a\phi B(a,d).\mathbf{A}(m/d) \tag{14}$$

ce qui entraîne par (13) :

$$\beta(a,d) := \phi B(a,d) = a^{-1}\lambda(a,d) . \tag{15}$$

Notons encore $\alpha(a,d) = \phi\mathbf{A}(a,d)$. Supposons que si $(a,p) = (b,p) = 1$, alors $\beta(bp^s,ap^r) = \beta(b,a)\beta(p^s,p^r)$ si le nombre de facteurs premiers dans ap^r est moins qu'un entier m fixé. Si $m = 1$, alors (12) montre cette hypothèse vraie. Il s'ensuit par récurrence :

$$\beta(bp^s,ap^{r+1}) = \beta(bp^{s+1},ap^r) - \beta(bp^s,a)\alpha(p,p^r) = \beta(b,a)\{\beta(p^{s+1},p^r) - \beta(p^s,1)\alpha(p,p^r)\}$$
$$= \beta(b,a)\beta(p^s,p^{r+1}) \quad \text{d'après (2) du §3.} \tag{16}$$

En multipliant avec bp^s , on voit donc avec (15)

$$\lambda(bp^s,ap^r) = \lambda(b,a)\lambda(p^s,p^r) \quad \text{si} \quad (a,p) = (b,p) = 1 \ . \tag{17}$$

Il reste donc à démontrer que $\lambda(p^s,p^r) \in M(n,\mathbb{Z})$ pour $s,r \geqslant 0$.

Mais en multipliant avec p^{s+1} , on voit de (16) et (15)

$$\lambda(p^{s+1},p^r) = p\lambda(p^s,p^{r+1}) + \lambda(p^s,1)\lambda(p,p^r) \tag{18}$$

le cas $s=0$ étant trivial, (18) montre que l'on a gagné si $\lambda(p,p^i) \in M(n,\mathbb{Z})$ pour tout $i \geqslant 0$. Mais (9) et (10), appliquées à (11) montrent que l'on a

$$A(p^{n+1}) = \sum_{i=0}^{n} p^i \, \sigma(p,p^i)A(p^{n-i})$$

ou avec (13) : $\lambda(p,p^i) = \sigma(p,p^i)$, ce qui appartient à $M(n,\mathbb{Z})$, donc ce qui montre le théorème.

Remarque : Le fait que $\Phi(n,\mathbb{Z}) = \prod_p \Phi(n,\{p\})$ ainsi que la prop. 4.3 montrent, que le théorème n'épuise pas les lois abéliennes de dimension n sur $\mathbb{Z}$.

4.5 Corollaire : Soit $F \in F(1,\mathbb{Z})$, alors F est strictement isomorphe à un $G \in F(1,\mathbb{Z})$ provenant d'une fonction lexoide faiblement multiplicative, c'est-à-dire encore qui s'obtient de la manière du théorème 4.4.

Démonstration : On a vu, (4) de 4.1, que si g et f sont deux fonctions lexoides, définissant des lois qui sont isomorphes, alors

$$g(m) = \sum_{d|m} d\mu(d)f(m/d) \ . \tag{19}$$

Supposons que $g(ab) = g(a)g(b)$ si $ab < m$. La relation $g(ab) = \sum_{d|b} d\sigma(a,d)g(b/d)$ montre que $\sigma(a,1) = g(a)$ et $\sigma(a,d) = 0$ si $ad < m$ et $d > 1$. Soit $m = \prod_i p_i^{\alpha_i}$ et $m_i = mp_i^{-\alpha_i}$.

On considère

$$\begin{aligned} g(m) &= \sum_{j=0}^{\alpha_i} p^j \, \sigma(m_i, p_i^{\alpha_i - j})g(p_i^{\alpha_i - j}) \\ &= g(m_i)g(p^{\alpha_i}) + p_i^{\alpha_i}\sigma(m_i, p_i^{\alpha_i}) \\ &= \prod_i g(p_i^{\alpha_i}) + p_i^{\alpha_i}\sigma(m_i, p_i^{\alpha_i}) \ . \end{aligned}$$

Il s'ensuit : $x = g(m) - \prod_i g(p_i^{\alpha_i}) \equiv 0 \bmod p_i^{\alpha_i}$ pour tout i, donc $x \equiv 0 \bmod m$, soit $x = m\lambda$. Si (19) correspond avec la relation $\varphi_G = \sum_d V_d \widetilde{\mu(d)} \varphi_F$ avec φ_G fondamental, alors on pose $\varphi_H = \varphi_G - V_m \lambda \varphi_G$, ce qui donne par induction le résultat voulu.

4.6 Homomorphismes de lois sur $\mathbb{Z}_S$: Soient $G \in F(n,\mathbb{Z}_S)$ et $H \in F(m,\mathbb{Z}_S)$ déterminées par les fonctions S-lexoides g et h. Soit de plus $f : G \to H$ un morphisme dans $F(\mathbb{Z}_S)$, alors après tensorisation avec $\mathbb{Q}$, on voit que $f^* : G^* \to H^*$ est déterminé par

$$f^*(\partial_{jG}) = \sum_{r=1}^{m} {}^t\varphi(j,r)\partial_{rH} \quad \text{pour} \quad 1 \leqslant j \leqslant n \tag{20}$$

d'où par une matrice $\varphi = (\varphi(p,j)) \in M(m \times n, \mathbb{Z}_S)$. Ceci est clair, parce que les ∂_{jG} et ∂_{rH} engendrent les algèbres G^* et H^*. La condition que les $C(f)\varphi_{iG}$ appartiennent à $C(H)$ s'écrit

$$C^n(f)\varphi_G = \sum_{i \in \mathbb{N}(S)} V_i \, {}^t\widetilde{\mu(i)} \varphi_H$$

avec $\mu : \mathbb{N}(S) \to M(n,\mathbb{Z}_S)$, ce qui s'écrit encore

$$g(n)\,{}^t\varphi = \sum_{d|n} d \, {}^t\mu(d) h(n/d) \quad \text{pour} \quad n \in \mathbb{N}(S). \tag{21}$$

Soient $D(G) = \Sigma \, {}^t g(n) n^{-s-1}$ et $D(H) = \Sigma \, {}^t h(n) n^{-s-1}$, alors on voit aisément que (21) équivaut à

$$\varphi D(G) = D(H) \cdot \sum_{n \in \mathbb{N}(S)} \mu(n) n^{-s}.$$

On laisse à titre d'exercice que les φ ainsi définies, sont en effet des homomorphismes, on trouve donc :

$$\mathrm{Hom}_{\mathbb{Z}_S}(G,H) = \{\varphi \in M(m \times n, \mathbb{Z}_S) \mid \exists \sum_{n \in \mathbb{N}(S)} \mu(n) n^{-s} = \mu \text{ , à coefficients dans } M(n,\mathbb{Z}_S) \text{ , t.q. } \varphi D(G) = D(H)\mu\}. \tag{22}$$

§5. Sur les groupes formels de Honda

Dans Honda [2], §2, l'auteur développe une théorie générale des lois abéliennes ainsi que leurs homomorphismes, de dimension arbitraire sur un anneau d'intégrité p-adique. Rappelons ici les théorèmes fondamentaux :

5.1 Soit p un nombre premier et $q = p^h$. Soient K un corps muni d'un automorphisme σ et v un sous anneau de K, stable sous σ. On note $K_\sigma[[T]]$ (resp. $v_\sigma[[T]]$) l'anneau de Hilbert par rapport à σ, c'est-à-dire l'anneau non commutatif des séries formelles à coefficients dans K (resp. v) soumis à une seule condition de commutation $Tx = x^\sigma T$.

Soit encore $B_{m,n}$ (resp. $A_{m,n}$) le module de $m \times n$-matrices à coefficients dans $K_\sigma[[T]]$ (resp. $v_\sigma[[T]]$). On notera $B_n = B_{n,n}$ et $A_n = A_{n,n}$. $K[[x]]_o^m$ sera la somme directe de m copies de l'idéal maximal de $K[[x]] = K[[x_1,\dots,x_n]]$ et on définit une opération de $B_{\ell,m}$ sur $K[[x]]_o^m$ à valeurs dans $K[[x]]_o^\ell$ de la façon suivante. Pour $u = \sum_{\nu=0}^{\infty} C_\nu T^\nu \in B_{\ell,m}$ et $f \in K[[x]]_o^m$ on pose

$$u*f(x) = \sum_{\nu=0}^{\infty} C_\nu f^{\sigma^\nu}(x^{q^\nu})$$

($x^{q^\nu} = (x_1^{q^\nu},\dots,x_n^{q^\nu})$). On suppose désormais que K soit muni d'une valuation discrète, d'anneau des entiers v, d'idéal maximal $m = (\pi)$ et de corps résiduel k de caractéristique p.

<u>Définition</u> : $u \in A_n$ sera dit spécial si $u \equiv \pi I_n \bmod \deg 1$. Si u est spécial et si $P \in Gl(n,v)$ alors on dit que $f \in K[[x]]_o^n$ est de type (P,u) si

$$f(x) \equiv Px \bmod \deg 2 \qquad x = {}^t(x_1,\dots x_n)$$

$$\text{et si} \qquad u*f(x) \equiv 0 \bmod m .$$

On en déduit que si u est spécial et si i est la fonction identique, alors $u^{-1}\pi * i(x)$ est de type (I_n,u) bref, de type u. Les deux propositions suivantes donnent des caractérisations :

Proposition 1 (loc. cit. prop. 2.5) : f est de type $(P,u) \Longleftrightarrow$ f est de la forme $(u^{-1}\pi_* i)\circ\varphi$ avec $\varphi \in v[[x]]_o^n$ t.q. $\varphi \equiv Px \bmod \deg 2$.

Proposition 2 (loc. cit. prop. 2.6) : Soient f de type (P,u) et $v \in A_{m,n}$, alors : $v_*f \equiv 0 \bmod m \Longleftrightarrow \exists t \in A_{m,n}$ t.q. $v = tu$.

On dira encore que K satisfait à la condition (F) si pour tout $\alpha \in v$ on a

$$\alpha^{\sigma} \equiv \alpha^{q} \bmod m .$$

Alors les groupes formels de Honda ainsi que le module de leurs homomorphismes se décrivent comme suit :

Théorème 1 (loc. cit. th. 2) : Supposons que K satisfait à (F). Soient f resp. g dans $K[[x]]_o^n$ de type (P,u) resp. (Q,u) . Alors : $F = F(x,y) = f^{-1}(f(x) + f(y))$, donc aussi $G = G(x,y) = g^{-1}(g(x) + g(y))$ sont dans $F(n,v)$ et $F \sim G$ sur v . Si $P = Q$, alors $F \simeq G$.

Théorème 2 (loc. cit. th. 3) : Supposons que K satisfait à (F). Soient $f \in K[[x]]^n$ de type u et $g \in K[[x]]_o^m$ de type w , définissant $F \in F(n,v)$ resp. $G \in F(m,v)$. Soit $C \in M(m\times n,v)$, alors $g^{-1} \circ Cf \in \mathrm{Hom}_v(F,G)$ si et seulement s'il existe $t \in A_{m,n}$ tel que $wC = tu$, d'où un isomorphisme canonique $\mathrm{Hom}_v(F,G) \simeq M(m\times n,v) \cap w^{-1}A_{m,n}u$.

5.2 Ces deux théorèmes sont à la base d'une théorie qui épuise dans beaucoup de cas les lois abéliennes qui existent, de plus l'auteur ne croit pas qu'on pourrait trouver des démonstrations plus directes et élégantes que celles données par Honda dans loc. cit. D'autre part, on considère les trois faits suivants :

F1. Le cor. 3.7 du ch. III donne une bijection entre $F_{typ}(n,v)$ et les fonctions $\{p\}$-admissibles à valeurs dans $M(n,v)$. Les lois de Honda sont typiques. Alors il se pose la question : laquelle est le lien ?

F2. Afin de démontrer que dans certains cas on obtient toutes les lois, Honda utilise des arguments cohomologiques. Pourrait-on trouver des arguments qui établissent qu'on obtient toutes les fonctions $\{p\}$-admissibles, ce qui revient

au même.

F3. Prenons $n=1$ et $\sigma : \mathbb{N} \to v$ arbitraire. On définit $f : \mathbb{N}(\{p\}) \to v$ par récurrence en posant $f(1) = 1$ et

$$f(p^{n+1}) = \sum_{i=0}^{n} p^i \, \sigma(i)^{p^{n-i}} f(p^{n-i}) \qquad \text{si } n \geqslant 0 \qquad (1)$$

alors f est $\{p\}$-admissible, donc $\ell(x) = \sum_{i=0}^{\infty} p^{-i} f(p^i) X^{p^i}$ est le logarithme d'une loi sur v.

Soit maintenant $(p) = (\pi^e)$, et avec les notations de 4.1, soit $u = \pi + C_1 T \bmod T^2$, alors $u^{-1}\pi \equiv 1 + (-\pi^{-1}C_1)T \bmod T^2$, d'où encore $(u^{-1}\pi)_* i(X) = X - \pi^{-1}C_1 X^p \bmod X^{p+1}$, où l'on a posé $q = p$. Ecrivant $(u^{-1}\pi)_* i(X) = \sum_{i=0}^{\infty} p^{-i} f(p^i) X^{p^i}$, on trouve donc $f(p) = p\pi^{-1}C_1$, c'est-à-dire $f(p) \in (\pi^{e-1})$. D'autre part, (1) donne : $f(p) = \sigma(0)$ peut être prise arbitraire dans v. Donc, si $e > 1$, les groupes formels de Honda ne donnent certainement pas toutes les lois qui existent.

Tenant compte notamment de F3, il semble que F1 pose une question bien motivée. Il se révélera toutefois, que la réponse est de caractère assez fâcheux. Parce que les groupes formels de Honda serviront plus loin, on donnera dans le reste de ce § le point de vue p-admissible des groupes formels de Honda.

5.3 Soit $u = \sum_{\nu=0} C_\nu T^\nu \in A_n$, c'est-à-dire $C_\nu \in M(n,v)$ pour tout ν. On supposera $C_0 \in Gl(n,v)$ et on pose $u^{-1}C_0 = \Sigma B_\mu T^\mu$ dans $K_\sigma[[T]]$. La relation $u \circ u^{-1}\pi = \pi$ entraîne

$$\sum_{i=0}^{n} C_i \, B_{n-i}^{\sigma^{n-i}} = 0 \qquad \text{si } n > 0 \quad B_0 = I_n. \qquad (1)$$

Soit D l'anneau introduit dans le §3 et définissons le morphisme φ sur la sous algèbre de D, engendrée par les $A(n,0)$, à valeurs dans $M(n,K)$ par

$$\varphi A(n,0) = {}^t B_n .$$

On écrira $\varphi A(n,\ell) = \alpha(n,\ell)$ et $\varphi D(n,\ell) = \delta(n,\ell)$.

On pose pour $\ell \in \mathbb{N}$, $\varepsilon_\ell = \begin{cases} 1 & \text{si } \ell \neq 0 \\ 0 & \text{si } \ell = 0 . \end{cases}$

Lemme :

a. Si $n > 1$ et si $0 \leqslant \ell < n$, alors $\sum_{i=0}^{n-\ell} {}^tC_i \, {}^t\delta(\ell, n-\ell-i) + \varepsilon_\ell^1 C_n = 0$. (2)

b. $\alpha(1,n-1) = -C_o^{-1} C_n$ si $n \geqslant 1$.

c. ${}^tB_{n+1} = \sum_{j=0}^{n} + (-C_o^{-1} C_{j+1})^{\sigma^{n-j}} \, {}^tB_{n-j}$.

d. Si $\pi C_o^{-1} \in M(n,v)$, alors $\pi^m \delta(m,r) \in M(n,v)$ pour tout r,m. En particulier $\pi\alpha(1,m) \in M(n,v)$ pour tout m.

Démonstration : Soient $n=1$ et $\ell=0$, alors ${}^tC_o \, {}^t\delta(1,0) + {}^tC_1^{\sigma} \, {}^t\delta(0,0) + 0 = {}^tC_o B_1 + {}^tC_1 = 0$ en vue de (1). Soient donc n arbitraire et $\ell=0$, alors ${}^t\delta(n-i,0) = B_{n-i}$ et $\varepsilon_\ell = 0$, donc dans ce cas a est vrai. Soit encore a vrai pour ℓ et supposons que $\ell+1 < n$. On considère (1) avec $n \mapsto n-\ell-1$, multiplié à droite avec ${}^t\alpha(1,\ell)^{\sigma^{n-\ell-1}}$, ce qui donne

$$\sum_{i=0}^{n-\ell-1} {}^tC_i \, {}^t\alpha(n-\ell-1-i,0)^{\sigma^i} \, {}^t\alpha(1,\ell)^{\sigma^{n-\ell-1}} = 0 \qquad (3)$$

(2) et (3) donnent

$$\sum_{i=0}^{n-\ell-1} {}^tC_i \{ {}^t\delta(n-\ell-i,\ell)^{\sigma^i} - {}^t\alpha(n-\ell-1-i,0)^{\sigma^i} {}^t\alpha(1,\ell)^{\sigma^{n-\ell-1}} \} + {}^tC_{n-\ell} \, {}^t\delta(0,\ell)^{\sigma^{n-\ell}} + \varepsilon_\ell \, {}^tC_n = 0 .$$

On vérifie que ${}^tC_{n-\ell} \, {}^t\delta(0,\ell)^{\sigma^{n-\ell}} + \varepsilon_\ell \, {}^tC_n = \varepsilon_{\ell+1} \, {}^tC_n$ et la déf. de $D(n,\ell)$ donne

$$\sum_{i=0}^{n-\ell-1} {}^tC_i \, {}^t\delta(n-\ell-1-i,\ell+1)^{\sigma^i} + \varepsilon_{\ell+1} \, {}^tC_n = 0 .$$

Pour b, on considère (2) pour $\ell = n-1$, ce qui donne

$${}^tC_o \, {}^t\delta(1,n-1) + {}^tC_1 \, {}^t\delta(0,n-1)^{\sigma} + \varepsilon_{n-1} \, {}^tC_n = 0 .$$

En tenant compte que $\delta(1,m) = \alpha(1,m)$ et $\delta(0,m) = 0$ si $m > 0$, on trouve b. c résulte de la prop. 3.4 e. Pour d on observe que $\pi^m \delta(m,r) \in M(n,v)$ si $r+m = 0$. Soit donc c vrai pour $r+m < n$. De (2) on obtient

$${}^tC_o \, {}^t\delta(n-r,r) + \sum_{i=1}^{n-r} {}^tC_i \, {}^t\delta(n-r-i,r) + \varepsilon_r {}^tC_n = 0 .$$

En multipliant avec π^{n-r-1} on trouve $\pi^{n-r-1}\,{}^tC_o\,{}^t\delta(n-r,r) \in M(n,v)$ si $r+m < n$ et $0 \leqslant r < n$. Si $r=n$, alors ${}^t\delta(0,r) = 0$ si $r > 0$, ce qui démontre d.

5.4 On considère $f : \mathbb{N}(\{p\}) \to M(n,K)$ définie par la relation

$$\sum_{i=0}^{\infty} p^{-i}\,{}^tf(p^i)x^{(p^i)} = \sum_{\nu=0}^{\infty} B_\nu\, x^{(q^\nu)} \qquad (1)$$

où les B_ν sont ceux de 4.3, (1). On a : $f(p^m) = 0$ si $h|m$ et ${}^tf(p^{hm}) = {}^tf(q^m) = q^m B_m$.

En particulier, si $\pi^{-1}C_o \in M(n,v)$, alors le lemme 4.3d donne que

$$q^m B_m = q^m\alpha(m,0) = q^m\delta(m,0) \in M(n,v) \qquad (2)$$

c'est-à-dire $f : \mathbb{N}(\{p\}) \to M(n,v)$. On écrira $\mathbb{N}(\{p\}) = \mathbb{N}(p)$.

Soit $g : \mathbb{N}(p) \to M(n,K)$ avec

$$g(p^n) = \sum_{i=0}^{n} p^i\,\lambda(i)^{(p^{n-i})}\,f(p^{n-i}) . \qquad (3)$$

On en déduit que $g(p^m) = \lambda(m) = 0$ si $h\nmid m$. En posant $q^{-n}g(q^n) = \beta(n,0)$ et $\xi_n = \lambda(hn)$, on voit avec (2) que (3) se réduit à

$$\beta(n,0) = \sum_{i=0}^{n} \xi_i^{(q^{n-i})}\,\alpha(n-i,0) . \qquad (4)$$

La condition que f soit p-admissible s'exprime par une relation

$$f(p^{n+1}) = \sum_{i=0}^{n} p^i\,\mu(i)^{(p^{n-i})}f(p^{n-i}) \qquad (5)$$

et (5) est nulle sauf si $h|n+1$, soient $n+1 = h(m+1)$ et $n-i = (m-j)h$, d'où $i = n-(m-j)h = h(m+1)-1-(m-j)h = jh+h-1$. On constate que $\mu(i) \neq 0$ entraîne $h|i+1$. Avec $g'(p^n) = f(p^{hn})$ et $\xi_j = \mu(jh+h-1)$, (5) réduit à

$$g'(p^{m+1}) = \sum_{j=0}^{m} p^{jh+h-1}\xi_j^{(q^{n-j})}f(q^{m-j})$$

ou encore, avec $\beta(m,0) = pq^{-m-1}g'(p^{m+1})$ et $\alpha(m,0) = q^{-m}f(q^m)$

$$\beta(m,0) = \sum_{j=0}^{m} \xi_j^{(q^{n-j})}\,\alpha(m-j,0) \qquad (6)$$

ce qui est de la forme (4). On étend la définition de φ dans 4.3 (après (11) en posant $\varphi B(m,0) = \beta(m,0)$, $\varphi B(m,\ell) = \beta(m,\ell)$. Noter que dans la situation

(6) on a $\beta(m,0) = p\alpha(m+1,0)$, ou encore plus généralement :

$$\beta(m,\ell) = p\alpha(m+1,\ell) \ . \tag{7}$$

5.5 Théorème : Supposons que K satisfait à (F) . Soient $\pi\alpha(1,-) : \mathbb{N} \to M(n,v)$ et $\beta(0,-) : \mathbb{N} \to M(n,v)$ alors f est p-admissible et $\xi_i \in M(n,v)$ pour tout $i \geqslant 0$.

Démonstration : Soit pour $k \geqslant 0$, $H(k)$ l'hypothèse :

$H(k,1)$: Si $0 \leqslant i < k$, alors $\beta(i,0) = \sum_{j=0}^{i} \xi_j^{(q^{j-i})}\, \alpha(i-j,0)$

avec $\xi_j \in M(n,v)$ pour $0 \leqslant j < k$.

$H(k,2)$: Si $(r,m) \neq (0,0)$ et $r+m \leqslant k$, alors $p^{m-1}\pi\alpha(m,r) \in M(n,v)$.

Il est évident que $H(1)$ est vrai : $\beta(0,0) = \xi_0$ et $\pi\alpha(1,0) \in M(n,v)$ et $\pi\alpha(0,1) = 0$.

On écrira $\xi_j^{(q^n)} = T(q^n,\xi_j)$. Alors, le théorème sera une conséquence du :

Lemme 1 : Soit $H(k)$ vrai, alors les trois conditions suivantes sont équivalentes:

a. Il existe $\xi_k \in M(n,v)$ tq $\beta(k,0) = \sum_{j=0}^{k} T(q^{k-j},\xi_j)\alpha(k-j,0)$.

b. Si $0 \leqslant \ell \leqslant k$ alors $\beta(k-\ell,\ell) \equiv \sum_{j=0}^{k-\ell} T(q^{k-\ell-j},\xi_j)^{\sigma^\ell}\alpha(k-\ell-j,\ell)$ (8)

où l'on a écrit $x \equiv y$ dans $M(n,K)$ si $x-y \in M(n,v)$.

c. $\beta(0,k) \equiv 0$.

Démonstration du lemme 1 : On démontrera d'abord que si $0 \leqslant \ell < k$, alors (8) est vrai pour la valeur ℓ si et seulement si elle est vraie pour $\ell+1$. Observer que

$$\beta(k-\ell,\ell) \equiv \sum_{j=0}^{k-\ell-1} T(q^{k-\ell-j},\xi_j)^{\sigma^\ell}\alpha(k-\ell-j,\ell) \tag{9}$$

si $\ell > 0$. Si $\ell = 0$, alors (9) est équivalent à (8) si $\xi_k \in M(n,v)$.

Remarquer, que si $\xi \in M(n,v)$ et $m \in \mathbb{N}$, alors

$$T(q^m,\xi)^{\sigma^\ell} - T(q^{m-1},\xi)^{\sigma^{\ell+1}} \in p^{m-1}\pi M(n,v) \tag{10}$$

en effet, il suffit de prendre $n = 1$ et $\ell = 0$. Si $m = 1$ on a

$$\xi^q - \xi^\sigma \in \pi v \qquad \text{d'après l'hypothèse (F) .}$$

Soit donc $\xi^{q^m} = \xi^{q^{m-1}}\sigma + p^{m-1}\pi c$ avec $c \in v$, alors $\xi^{q^{m+1}} = (\xi^{q^{m-1}}\sigma + p^{m-1}\pi c)^q$ ce qui implique $\xi^{q^{m+1}} - \xi^{q^m}\sigma \in p^m\pi v$. On écrit (9)

$$\beta(k-\ell,\ell) \equiv \sum_{j=0}^{k-\ell-1} T(q^{k-\ell-j-1},\xi_i)^{\sigma^{\ell+1}}\alpha(k-\ell-j,\ell) +$$

$$+ \sum_{j=0}^{k-\ell-1}\{T(q^{k-\ell-j},\xi_j)^{\sigma^\ell} - T(q^{k-\ell-j-1},\xi_j)^{\sigma^{\ell+1}}\}\alpha(k-\ell-j,\ell)$$

$$\equiv \sum\nolimits_1 + \sum\nolimits_2 \quad \text{(soit)}. \tag{11}$$

Dans $\sum_2$ on a : $T(q^{k-\ell-j},\xi_j)^{\sigma^\ell} - T(q^{k-\ell-j-1},\xi_j)^{\sigma^{\ell+1}} \in p^{k-\ell-j-1}\pi\mathbb{M}(n,v)$ d'après (10), ce qui entraîne par $H(k,2)$ que $\sum_2 \equiv 0$.

$H(k,1)$ avec $i = k-\ell-1$, donne

$$\beta(k-\ell-1,0) = \sum_{j=0}^{k-\ell-1} T(q^{k-\ell-j-1},\xi_j)\alpha(k-\ell-j-1,0)$$

d'où

$$\beta(k-\ell-1,0)^{\sigma^{\ell+1}}\alpha(1,\ell) = \sum_{j=0}^{k-\ell-1} T(q^{k-\ell-j-1},\xi_j)^{\sigma^{\ell+1}}\alpha(k-\ell-j-1,0)^{\sigma^{\ell+1}}\alpha(1,\ell) \tag{12}$$

(11)-(12) donnent en vue de 3.3 (5b) :

$$\beta(k-\ell-1,\ell+1) \equiv \sum_{j=0}^{k-\ell-1} T(q^{k-\ell-j-1},\xi_j)^{\sigma^{\ell+1}}\alpha(k-\ell-j-1,\ell+1)$$

ce qui en effet n'est autre que (8) pour la valeur $\ell+1$.

Soit a donné, c'est-à-dire (8) pour la valeur $\ell=0$. Alors, (8) est vraie pour les valeurs $0 \leqslant \ell \leqslant k$, en particulier, si $k=\ell$, (8) donne $\beta(0,k) \equiv 0$. Soit inversement, c vrai, donc (8) pour $\ell=k$. Il s'ensuit que (9) est vraie pour $0 \leqslant \ell \leqslant k$ mais (9) implique pour $\ell=0$ l'existence d'un $\xi_k \in M(n,v)$.

Le théorème résulte évidemment du lemme suivant :

Lemme 2 : Si $H(k)$ est vrai et si $\xi_k \equiv 0$ soit si $\beta(k,0) \equiv 0$ alors $H(k+1)$ est vrai.

En effet, a du lemme 1 donne $H(k+1,1)$. On applique (7), ce qui donne dans (8) : Si $0 \leqslant \ell \leqslant k$, alors

$$p\alpha(k-\ell+1,\ell) \equiv \sum_{j=0}^{k-\ell} T(q^{k-\ell-j},\xi_j)^{\sigma^\ell}\alpha(k-\ell-j,\ell). \tag{13}$$

En multipliant (13) avec $p^{k-\ell-1}\pi$ on voit avec $H(k,2)$ si $0 \leqslant \ell \leqslant k$, alors $p^{k-\ell}\pi\,\alpha(k-\ell+1,\ell) \in M(n,v)$, c'est-à-dire $p^{m-1}\pi\,\alpha(m,r) \in M(n,v)$ si $m+r = k+1$ et $r \leqslant k$. Mais $\alpha(0,k+1) = 0$ ce qui donne $H(k+1,2)$.

La converse du théorème n'est pas vraie : prendre $q=p$, $f(p^i) = 1$ pour tout $i \geqslant 0$ ce qui définit une fonction p-admissible en dimension 1. On a $\pi\alpha(1,0) = \pi.p^{-1}f(p) = \pi p^{-1} \notin v$ si $p = (\pi^e)$ avec $e > 1$.

5.6 On en tire :

Corollaire 1 : Supposons que K satisfait à (F). Soit $u = \sum_{v=0}^{\infty} C_v T^v$ avec $C_v \in M(n,v)$ et $C_0 = \pi I_n$. On pose $u^{-1}\pi = \sum_{u=0}^{\infty} B_v T^{\mu}$ dans l'anneau de Hilbert $K_\sigma[[T]]$ et

$$h(x) = \sum_{=0}^{\infty} B_v x^{(q^v)} = \sum_{i=0}^{\infty} p^{-i}\,{}^t f(p^i) x^{(p^i)} \qquad \text{(cf. (1))}$$

alors, $h^{-1}(h(x)+h(y)) \in F(n,v)$.

Démonstration : D'après le lemme 5.3 b on a $\pi\alpha(1,m) = \pi C_0^{-1} C_{m+1} = C_{m+1} \in M(n,v)$, donc d'après 5.5 f est p-admissible, et à valeurs dans $M(n,v)$ parce que d'après le même lemme $\pi^m\delta(m,r) \in M(n,v)$ donc en particulier $\pi^m\delta(m,0) = \pi^m\,{}^t B_m \in M(n,v)$, d'où a fortiori $q^m\,{}^t B_m \in M(n,v)$.

L'énoncé du cor. 1 est le point crucial dans la démonstration du 5.1 du théorème 1, qui s'achève à l'aide de la prop. 1 de 5.1.

Corollaire 2 : Soient $u^{-1}\pi = \sum_{v=0}^{\infty} B_v T^v$ et $w^{-1}\pi = \sum_{v=0}^{\infty} B'_v T^v$ telles qu'elles définissent $F \in F(n,v)$ et $G \in F(m,v)$, alors

$\mathrm{Hom}_v(F,G) \simeq \{C \in M(m\times n,v) \mid \exists t \in \mathbf{A}_{m,n}\ \ t.q\ \ wC = tu\}$.

Démonstration : Soit $\phi : F \to G$ ou encore $\phi^* : F^* \to G^*$. Comme dans 4.6, ϕ^* induit

$$\phi^*(\partial_{jF}) = \Sigma\ {}^t C(j,r)\partial_{rG} \qquad \text{pour } 1 \leqslant j \leqslant n$$

d'où $C \in M(m\times n,v)$. Les images de φ_{iF} sous $C_S(f)$ doivent appartenir à $C_S(G)$, ce qui donne

$$ {}^tB_m\,{}^tC = \sum_{i=0}^{m} T(q^{m-i}, {}^t\xi_i)\,{}^tB'_{m-i} \quad \text{avec} \quad {}^t\xi_i \in \mathbb{M}(m\times n,\nu) $$

$$ = \sum_{i=0}^{m} {}^t\mu(i)^{\sigma^{m-i}}\,{}^tB'_{m-i} \qquad \text{d'après le th. 5.5 avec } \mu(i) \in M(m\times n,\nu) $$

ce qui est équivalent à

$$ C\,u^{-1}\,\pi = w^{-1}\,\pi \sum_{i=0}^{\infty} \mu(i)T^i := w^{-1}\,\pi\,\mu' $$

c'est-à-dire $wC = tu$ avec $t = \pi\mu'\pi^{-1}$. Le corollaire en résulte parce que $(\pi^\sigma) = (\pi) = p$.

5.7 Le but étant plutôt de donner des liens avec les différents points de vue que devrait vouloir traduire tout en termes de courbes, on s'abstient d'entrer de façon plus détaillée dans les groupes formels de Honda [2]. Noter toutefois, que III.4.2 donne toutes les lois de $F(n,\mathbb{Z})$ à isomorphie stricte près, ce qui généralise le th. 8 de loc. cit. Observons en passant que III.4.2 donne également que les groupes $G_{n,m}$ de Dieudonné, qui figurent dans § 5.2 loc. cit. se relèvent aux lois définies sur $\mathbb{Z}$.

Dans ce qui suivra on aura besoin du

Théorème (Honda 1, th. 2) : Soit v l'anneau des entiers dans l'extension $\mathbb{Q}_p \to K$ de degré n. Soit m l'idéal maximal de v et soient e et d l'indice de ramification et le degré de m. On pose $v/m = \mathbb{F}_q$ avec $q = p^d$. Soit $\mathcal{O}$ l'anneau des entiers dans l'extension maximale non ramifiée de K.

On prend une uniformisante π de v et $a \in \mathbb{N}^+$. Soit

$$ f(x) = \sum_{\nu=0}^{\infty} \pi^{-\nu}\, x^{q^{a\nu}} \qquad (1) $$

et $F = f^{-1}(f(x)+f(y))$. Alors :

a. $F \in F(1,v)$; $\mathrm{End}_{\mathcal{O}}(F)$ est l'anneau des entiers dans l'extension non ramifiée de degré a de K.

b. Soit $F_* \in F(1,\mathbb{F}_q)$ obtenu par l'application canonique $v \to \mathbb{F}_q$, alors $\mathrm{ht}\, F_* = an$. Soit $S = \{p\}$, alors, dans le diagramme commutatif (cf. III.3.9 pour les flèches horizontales)

$$\begin{array}{ccc} \mathrm{End}_v(F) & \hookrightarrow & C_S(F) \\ \downarrow & & \downarrow \\ \mathrm{End}_{\mathbb{F}_q}(F_*) & \hookrightarrow & C_S(F_*) \end{array} \qquad (2)$$

l'image de $\pi \in \mathrm{End}_v(F)$ dans $C_S(F_*)$ est $V^{ad}\varphi_{F_*}$ $(V = V_p)$.

c. Soit $G \in F(1,v)$ t.q. $\pi \in \mathrm{End}_v(G)$ et l'image dans (2) est $V^a\varphi_{F_*}$, alors $F \simeq G$ sur v .

Démonstration : Elle se fait dans loc. cit. Remarquer toutefois, que K satisfait à (F) avec σ = identité et que f est de la forme $u^{-1}\pi$ avec $u = \pi - T^a \in K_\sigma[[T]] = K[[T]]$, d'où aussitôt le fait que $F \in F(1,v)$. Le théorème 2 de 5.1 donne aussitôt que $\mathrm{End}_v(F) = v$ puisque $ux = xu$ pour tout $x \in v$. (Cet argument ne s'utilise pas pour $\mathrm{End}_\theta(F)$, parce que θ ne satisfait plus à la condition (F)).

On a évidemment $v_F = v$, d'où : chaque courbe dans $C_S(F)$ s'écrit de façon unique

$$\Sigma\, V^i \widetilde{\mu(i)}\, \varphi_F \qquad (V = V_p) \qquad (3)$$

avec $\mu(i) \in v$. On vérifie que le S-type de F se donne par

$$F_p\varphi_F = V^{ad-1}[p]\,\widetilde{\pi^{-1}}\,\varphi_F$$

donc après réduction mod m on trouve : $[p]\varphi_{F_*} = V^{ad}[p](\widetilde{\pi^{-1}})\varphi_{F_*}$ ce qui donne b. De plus on a $[p]_* = [c\pi^e]_* = \tilde{c}_*\tilde{\pi}_*^e = \tilde{c}_* V^{ade}$.

D'après §1, la hauteur de F_* est $ade = an$.

5.8 Avec les notations de 5.7 on a

Corollaire : L'image de $\mathrm{End}_v(F)$ dans $C_S(F_*)$ est égale à

$$\{\sum_{i=0}^{\infty} V^{adi}\,\lambda_i\,\varphi_{F_*} \mid \lambda_i \in \mathbb{F}_q \text{ pour tout } i \geqslant 0\}$$

π correspond à V^{ad} . L'ensemble des représentants de Teichmüller dans v s'identifie au sous-ensemble $\mathbb{F}_q \subset C_S(F_*)$, $\lambda \mapsto V^o\lambda$.

Chapitre V : Quelques applications

§1. Applications aux courbes elliptiques sur $\mathbb{Q}$

1.1 Soit $F \in F(1,\mathbb{Z})$ de logarithme $\ell_F = \Sigma\, n^{-1} f(n) X^n$, alors on a vu, (III.3.6) que $f : \mathbb{N}^+ \to \mathbb{Z}$ est lexoide. Chaque courbe dans $C(F)$ s'écrit de forme unique $\varphi = \Sigma\, V_i \tilde{\lambda}_i \varphi_F$ et en posant $\tau_m(\varphi) = g(m)$ on obtient la relation

$$g(m) = \sum_{d \mid m} d\, \lambda_d f(m/d) \ . \tag{1}$$

C'est-à-dire on obtient une bijection de $C(F)$ avec l'ensemble $T(f)$ des fonctions $g : \mathbb{N}^+ \to \mathbb{Z}$ qui satisfont à (1) avec tous les $\lambda_d \in \mathbb{Z}$. Ceci permet de transposer les opérateurs V_a, F_a, $m = \underline{m}$ et $\tilde{m}$ sur $T(f)$ en posant

$$(V_a f)(n) = \begin{cases} a f(n/a) & \text{si } a \mid n \\ 0 & \text{sinon} \end{cases} \qquad (\underline{m} f)(n) = m^n f(n)$$

$$(F_a f)(n) = f(an) \qquad (\tilde{m} f)(n) = m f(n)$$

d'où $T(f) = \{\sum_{i=1}^{\infty} V_i \tilde{\lambda}_i f \mid \lambda_i \in \mathbb{Z} \text{ pour tout } i\}$. Si $g \in T(f)$ et $g(1) = \pm 1$, alors $T(f) = T(g)$. Ceci résulte de III.1.1.

De plus on a vu : $T(f)$ contient g avec $g(mn) = g(m)g(n)$ si $(m,n) = 1$ et $g(1) = 1$, (IV, 4.5), c'est-à-dire on peut supposer que f est faiblement multiplicative.

Lemme : Soit f lexoide et donnée par la relation

$$\sum_{n=1}^{\infty} f(n) n^{-s} = \Pi(1 - \sum_{i=0}^{\infty} p^i\, \sigma(p,p^i) p^{-(i+1)s})^{-1}$$

(cf. IV.4.4), alors dans $T(f)$ on a les relations

$$F_p f = \sum_{i=0}^{\infty} V_{p^i} \widetilde{\sigma(p,p^i)} f \tag{2}$$

c'est-à-dire dans $C(F)$, où $F \in F(1,\mathbb{Z})$ est défini par f, on a

$$F_p \varphi_F = \sum_{i=0}^{\infty} V_{p^i} \widetilde{\sigma(p,p^i)} \varphi_F \ . \tag{3}$$

Démonstration : (9) et (10) de IV.4.3 donnent aussitôt

$$f(p^{n+1}) = \sum_{i=0}^{n} p^i \sigma(p,p^i) f(p^{n-i}) \ . \tag{4}$$

IV,(17) et (13) montrent que si $f(am) = \sum_{d|m} d\sigma(a,d)f(m/d)$, alors σ est faiblement bimultiplicative, de plus $\sigma(1,m) = 0$ si $m > 1$. Si donc $m = p^{n+1}b$ avec $(p,b) = 1$ on a

$$f(m) = f(p.p^n b) = \sum_{d|p^n b} d\sigma(p,d)f(p^n b/d) = \sum_{i=o}^{n} p^i \sigma(p,p^i)f(p^{n-i}b) \qquad (5)$$

parce que $\sigma(p,d) = 0$ si $d \notin \mathbb{N}(\{p\})$ ce qui suit des propriétés de σ , mentionnées ci-dessus. Par conséquent

$$(F_p f)(m) = \{\sum_{i=o}^{\infty} V_{p^i} \sigma(p,p^i)f\}(m) \text{ pour tout } m . \qquad \text{cqfd}$$

1.2 Lemme : Soit $f : \mathbb{N}^+ \to \mathbb{Z}$ définie par

$$\Sigma f(n)n^{-s} = \prod_p (1 - a_p p^{-s} + b_p p^{1-2s})^{-1}$$

avec $a_p, b_p \in \mathbb{Z}$, alors f est lexoide et définit une loi F dans $F(1,\mathbb{Z})$. Soit $F_* \in F(1,\mathbb{F}_p)$ obtenu de F par réduction mod p , alors on a dans $\mathrm{End}_{\mathbb{F}_p}(F_*)$, (avec $F' = F_p$, $V = V_p$)

$$F'^2 - a_p F' + b_p = 0 \qquad (6)$$

$$p - a_p V + b_p V^2 = 0 . \qquad (7)$$

Démonstration : D'après IV.4.4 on voit aussitôt que $F \in F(1,\mathbb{Z})$. Observant que l'application canonique $F \mapsto F_*$ commute avec l'action de $\mathbb{Z}$ sur le groupe des courbes ; (3) donne

$$F\varphi_F = [a_p]\varphi_F - V[b_p]\varphi_F . \qquad (8)$$

L'application de F' , V sur (8) donne aussitôt (6) et (7), tenant compte que $VF' = F'V = [p]$ si l'anneau de base est $\mathbb{F}_p$. Observer qu'en effet $F', V \in \mathrm{End}_{\mathbb{F}_p}(F_*)$ parce qu'elles commutent avec $\lambda \in \mathbb{F}_p$ ((2) de III.3.8).

1.3 Soit maintenant C une courbe elliptique sur $\mathbb{Q}$, disons de modèle Weierstraß (affine)

$$y^2 + \lambda xy + \mu y = x^3 + \alpha x^2 + \beta x + \gamma$$

avec $\lambda, \mu, \alpha, \beta, \gamma \in \mathbb{Z}$ et de discriminant minimal. On sait que la réduction

$C_p = C \bmod p$ est une courbe irréductible pour tout nombre premier p. D'après Weil on sait également comment définir la L-série locale $L_p(s)$ de C, qui se donne par :

a. Si le genre de C_p est égal à 1 alors $L_p(s) = (1 - a_p s + p^{1-2s})^{-1}$ si $1 - a_p X + pX^2$ est le numérateur de la fonction ζ de C_p.

b. Si C_p a un point double p-ordinaire, on note $\varepsilon_p = 1$, soit $\varepsilon_p = -1$ selon le cas dans lequel les tangents à P sont rationnels sur $\mathbb{F}_p$ ou non, et on pose

$$L_p(s) = (1 - \varepsilon_p\, p^{-s})^{-1} .$$

c. Si C_p a un point de retroussement, on pose $L_p(s) = 1$.

On sait également que dans le cas b, la réduction de la loi du groupe de C_p est le groupe multiplicatif sur $\mathbb{F}_{p^2}$ et est isomorphe au groupe multiplicatif sur $\mathbb{F}_p$ si et seulement si $\varepsilon_p = 1$. Dans le cas c, la réduction de la loi du groupe est le groupe additif.

On prend $t = x/y$ comme paramètre local à l'origine et d'après Shimura-Taniyama, . . t est un paramètre local à l'origine de C_p pour tout p. On a également que la complétion de C au long de la section unité définit un groupe formel, en particulier, le choix de t, avec $\theta_\ell = \mathbb{Z}[[t]]$ donne une loi $F \in F(1,\mathbb{Z})$ tel que $F(t\hat{\otimes}1, 1\hat{\otimes}t) = dt$, où d est le morphisme structural $d : \hat{\theta}_\ell \to \hat{\theta}_\ell \hat{\otimes} \hat{\theta}_\ell$. Avec Honda [1], p. 211, on dit que $G \in F(1,\mathbb{Z})$ est un modèle formal minimal de C si $G \approx F$ sur $\mathbb{Z}$.

1.3 On rappelle le résultat fondamental de Honda :

<u>Théorème</u> (Honda I,II) :

Soit C une courbe elliptique où la série $L(s)$ se donne sous la forme du lemme 1.2, ce qui définit une loi $G \in F(1,\mathbb{Z})$. Soit d'autre part t un paramètre local à l'origine de C, $t = x/y$ comme ci-dessus, $w = \sum_{n=1}^{\infty} \beta(n) t^{n-1} dt$ une forme de première espèce sur C avec $\beta(n) \in \mathbb{Z}$ et $\beta(1) = 1$ et $F \in F(1,\mathbb{Z})$ obtenue par complétion de θ_ℓ, alors :

a. F et G sont strictement isomorphes sur $\mathbb{Z}$.

b. Le logarithme de F est donné par $\sum_{n=1}^{\infty} n^{-1}\beta(n)t^n$.

La démonstration repose sur le fait qu'après réduction mod p, F et G admettent les mêmes équations caractéristiques pour les Frobenius, ce qui suffit pour affirmer que les lois sont isomorphes, d'abord sur $\mathbb{F}_p$, puis $\mathbb{Z}_p$ et finalement sur $\mathbb{Z}$. Il est clair que tout générateur dans θ_ℓ définit un modèle formal minimal de C.

1.4 Le but de ce § est :

Théorème (Atkin-Swinnerton Dyer-Cartier) : Soit $L(s) = \Pi\,(1 - a_p p^{-s} + b_p p^{1-2s})^{-1}$ la série L d'une courbe elliptique C sur $\mathbb{Q}$ comme ci-dessus et $w = \Sigma\,\beta(n)t'^{n-1}dt'$ comme dans 1.3, où t' engendre θ_ℓ, alors

$$\beta(np) - a_p\beta(n) + pb_p\beta(n//p) \equiv 0 \bmod p^{\alpha} \quad \text{si} \quad n \equiv 0 \bmod p^{\alpha-1}. \tag{9}$$

Remarque : Les congruences (9) ont été conjecturées par Atkin-Swinnerton Dyer en 1969. Cartier était le premier à démontrer ces conjectures (cours de groupes formels. Notes de J.F. Boutot), utilisant l'opérateur de Cartier. Les relations (9) toutefois suggèrent aussi un lien de ces coefficients avec les fonctions lexoides, c'est pourquoi on donne ici une autre démonstration, qui aboutit à une détermination du membre gauche de (9) en termes des coefficients définissant la fonction lexoide β.

Démonstration : On considère $\beta^+ : \mathbb{N}^+ \to \mathbb{Z}$ comme une fonction, alors le fait que F et G sont des lois strictement isomorphes sur $\mathbb{Z}$ s'exprime avec les notations de 1.1 par

$$T(\beta) = T(f)$$

si $\Sigma\, f(n)n^{-s} = L(s)$. On a vu que $T(f) = \{\Sigma\, V_i\tilde{\mu}_i f \mid \mu_i \in \mathbb{Z} \text{ pour tout } i\}$, c'est-à-dire en particulier il suit du fait que $F_a\beta \in T(f)$ pour tout $a \in \mathbb{N}^+$ que l'on a

$$F_a\beta = \sum_{i=1}^{\infty} V_i \widetilde{\lambda(a,i)f} \tag{10}$$

avec $\lambda : \mathbb{N}^+ \times \mathbb{N}^+ \to \mathbb{Z}$

ou encore $$\beta(am) = \sum_{d|m} d\lambda(a,d)f(m/d) \ . \tag{11}$$

D'autre part on a également

$$F_a f = \sum_{i=1}^{\infty} V_i \widetilde{\sigma(a,i)f}$$

avec $\sigma : \mathbb{N}^+ \times \mathbb{N}^+ \to \mathbb{Z}$. D'après IV.4.4 (15) on voit que si l'on définit φ sur la sous algèbre de C , engendrée par les $A(n,1)$, où C est l'algèbre de IV §3, par $\varphi A(n,1) = n^{-1}f(n)$ et si l'on pose $\varphi A(n,m) = \alpha(n,m)$, alors

$$a\alpha(a,d) = \sigma(a,d)$$

et le lemme 1.1 montre notamment que σ , donc α est faiblement bimultiplicative et (3) du 1.1 montre encore que

$$\begin{aligned} p\alpha(p,1) &= a_p \\ p\alpha(p,p) &= -b_p \\ \alpha(p,p^i) &= 0 \quad \text{si} \quad i > 1 \ . \end{aligned} \tag{12}$$

On étend φ à C à un morphisme d'algèbres en posant $\varphi B(n,1) = n^{-1}\beta(n)$ et $\varphi B(n,m) = \beta(n,m)$. Alors, le lemme IV.3.2 donne

$$r\beta(r,d) = \lambda(r,d) \ . \tag{13}$$

Soit maintenant

$$\beta(np) - a_p\beta(n) + pb_p\beta(n//p) = \xi_n$$

c'est-à-dire :

$$\beta(np,1) - \alpha(p,1)\beta(n,1) - \alpha(p,p)\beta(n//p,1) = (np)^{-1}\xi_n \ . \tag{14}$$

Par définition (IV.3.1) on a

$$\beta(np,1) = \beta(n,p) + \beta(n,1)\alpha(p,1) \tag{15}$$

ce qui donne avec (14) :

$$\beta(n,p) - \alpha(p,p)\beta(n//p,1) = (np)^{-1}\xi_n \ . \tag{16}$$

On a par définition

$$\beta(n,p) = \beta(n//p,p^2) + \beta(n//p,1)\,\alpha(p,p) \tag{17}$$

ce qui donne avec (16)

$$\beta(n//p,p^2) = (np)^{-1}\xi_n \ . \tag{18}$$

On a $\beta(n//p,p^2) = \beta(n//p^2,p^3) + \beta(n//p^2,1)\,\alpha(p,p^2) = \beta(n//p^2,p^3)$ d'après (12). En itérant, si $n = p^{\alpha-1}m$ avec $(m,p) = 1$ on voit

$$\beta(n//p,p^2) = \beta(n/p^{\alpha-1},p^\alpha)$$

ce qui donne avec (18):

$$(np)^{-1}\xi_n = \beta(n/p^{\alpha-1},p^\alpha)$$

ou $$\xi_n = np\ \beta(n/p^{\alpha-1},p^\alpha) = p^\alpha m\beta(m,p^\alpha) = p^\alpha\lambda(m,p^\alpha)$$ d'après (13).

La propriété d'être lexoide entraîne par définition que $\lambda(m,p^\alpha) \in \mathbb{Z}$ ce qui démontre le théorème.

1.5 Remarquons que la combinaison du IV th. 4.4 et Shimura [1], th.3.21 donne que les opérateurs de Hecke sont lexoides. On donne encore un autre exemple que l'on ne sait pas interpréter :

Soit $f : \mathbb{N}^+ \to \mathbb{Z}$ défini par

$$\Sigma\, f(n)n^{-s} = \Pi(1 - a_p p^{-s} + b_p p^{k-2s})^{-1} \tag{19}$$

avec $k \geqslant 1$ et $a_p, b_p \in \mathbb{Z}$.

Alors f est lexoide, $T(f)$ est isomorphe avec le groupe des courbes dans le groupe formel défini par f . Il suit également que f est P-admissible, ce qui entraîne l'existence d'un $\lambda : \mathbb{N}^+ \times \mathbb{N}^+ \to \mathbb{Z}$ t.q. pour tout a,m on ait

$$f(am) = \sum_{d|m} d\lambda(a,d)^{m/d} f(m/d) \ . \tag{20}$$

On se demande comment interpréter (20) pour les L-séries des courbes elliptiques sur $\mathbb{Q}$ ou encore pour la fonction τ de Ramanujan.

§2. Applications aux composantes fantômes

2.1 Soit $S \subset P$ et soit k un anneau. On considère ici les foncteurs covariants

$$J : \mathrm{Alg}_k \to \text{groupes abéliens}$$

qui sont tels que l'ensemble sous jacent de $J(K)$ pour $K \in \mathrm{Alg}_k$ s'identifie à $\mathbb{M}(n,K)$ $\mathbb{N}(S)$ pour un $n \in \mathbb{N}^+$.

On dira que J admet des composantes fantômes s'il existe une famille $\{j_m \mid m \in \mathbb{N}(S)\}$ des homomorphismes

$$j_m(K) : J(K) \to \mathbb{M}(n,K)$$

fonctoriels en K , où $\mathbb{M}(n,K)$ est munie de sa structure usuelle de groupe abélien et où pour $x = (x_a \mid a \in \mathbb{N}(S)) \in J(K)$, $j_m(x)$ ne dépend que de $x_1,\dots,x_r$ avec $r \leqslant m$.

2.2 Les exemples les plus importants

a : $k = \mathbb{Z}$, $S = \{p\}$, $J = W$, le foncteur en groupes abéliens des vecteurs de Witt. Ici $n = 1$

$$j_m(K) : W(K) \to K$$

se donne par $j_m(K)(x_{p^i} \mid i \geqslant 0) = \sum_{i=0}^{m} p^i x_{p^i}^{p^{n-i}}$ (1)

W même est un foncteur en anneaux.

b : $k = \mathbb{Z}$, S arbitraire , $J = W_S$, le foncteur en groupes abéliens des vecteurs de Witt généralisées. Ici $n = 1$

$$j_m(K) : W_S(K) \to K$$

se donne par $j_m(K)(x_a \mid a \in \mathbb{N}(S)) = \sum_{d \mid m} d x_d^{m/d}$ (2)

W_S est également un foncteur en anneaux.

2.3 Soient $n \in \mathbb{N}^+$ et X_d , Y_d , $\delta(d)$ pour $d \in \mathbb{N}(S)$, $S \neq \emptyset$, des matrices carrées d'ordre n aux coefficients qui sont des indéterminés.

On pose $T = \{\pi(i,j)X_d \cup \pi(i,j)Y_d \mid 1 \leqslant i,j \leqslant n\ ;\ d \in \mathbb{N}(S)\}$ et

$$U = \{\pi(i,j)\breve{\sigma}(d) \mid 1 \leqslant i,j \leqslant n\ ;\ d \in \mathbb{N}(S)\}\ .$$

Soient k un anneau et $f : \mathbb{Z}[T,U] \to k[T]$ un morphisme d'algèbres qui est l'identité sur l'ensemble T. On considère le système d'équations

$$\sum_{d|m} d(X_d^{(m/d)} + Y_d^{(m/d)} - w_d^{(m/d)})M(n,f)(\breve{\sigma}(d)) = 0 \qquad (3)$$

pour $m \in \mathbb{N}(S)$, et où en général $f : \mathbf{A} \to B$ dans $\mathbf{Alg}_{\mathbb{Z}}$ induit $M(n,f) : M(n,A) \to M(n,B)$. f sera dit admissible, si $M(n,f)(\breve{\sigma}(1)) = I_n$ et si (3) admet une solution, d'ailleurs nécessairement unique, $\{w_d \mid d \in \mathbb{N}(S)\} \subset M(n,k[T])$.

Notons, que si $n=1$ et $f(\breve{\sigma}(d)) = 1$ pour tout d, alors (3) décrit de façon générique la loi du groupe $W(K)$ dans (1) si $S = \{p\}$ et de $W_S(K)$ dans (2) si $S \neq \emptyset$.

2.4 Soit $L(P)$ l'anneau introduit dans III.3.4 et soit $\varphi : \mathbb{Z}[T,U] \to L(P)[T]$ le morphisme tel que $M(n,\varphi)(\breve{\sigma}(d)) = Y(d)$ pour $d \in \mathbb{N}^+$, alors on a :

<u>Théorème</u> : φ est admissible.

La raison d'être de ce théorème est son corollaire suivant :

<u>Corollaire</u> : Soit k un anneau arbitraire, $f : \mathbb{N}(S) \to M(n,k)$ S-admissible, induisant $\tilde{f} : \mathbb{Z}[T,U] \to k[T]$ tel que $M(n,\tilde{f})(\breve{\sigma}(d)) = f(d)$, alors $\tilde{f}$ est admissible au sens que (3) admet une solution à coefficients dans $k[T]$.

Le corollaire se déduit aussitôt du théorème en vue de $\mathbf{Alg}_{\mathbb{Z}}((L(P),k) \simeq \simeq \mathbf{Adm}(S,k)$ (III,3.5).

<u>Démonstration du théorème</u> : Soit $S=P$ et soit $F \in F(n,L(P))$ (III.3.4), donc F est définie sur $L(P)[T]$. On considère sur $L(P)[T]$ le groupe $C^n(F)$ dans lequel se trouvent les deux éléments

$$\sum_{d=1}^{\infty} V_d X_d \varphi_F \quad \text{et} \quad \sum_{d=1}^{\infty} V_d Y_d \varphi_F\ .$$

Leur somme dans $C^n(F)$ est donc un élément $\sum_{d=1}^{\infty} V_d w_d \varphi_F$. En appliquant l'opé-

rateur τ_m (III.3.1), on voit que

$$\sum_{d|m} d(X_d^{(m/d)} + Y_d^{(m/d)})Y(m/d) = \sum_{d|m} dw_d^{(m/d)}Y(m/d)$$

pour $m \in \mathbb{N}^+$, ce qui démontre le théorème.

2.5 Soit $S \supset S(k)$.

Théorème : Soit $f : \mathbb{N}(S) \to \mathbb{M}(n,k)$ admissible, alors il existe un foncteur W_f en groupes abéliens, uniquement déterminé par les trois propriétés suivantes :

a. Pour $R \in \mathrm{Alg}_k$, l'ensemble sous jacent de $W_f(R)$ est $\mathbb{M}(n,R)^{\mathbb{N}(S)}$.

b. Si $\begin{array}{ccc} R' & \xrightarrow{\psi} & R \\ \uparrow & & \uparrow \\ k' & \xrightarrow{\varphi} & k \end{array}$ est un diagramme commutatif dans $\mathrm{Alg}_{\mathbb{Z}}$ et si $f' : \mathbb{N}(S) \to \mathbb{M}(n,k')$ est telle que $f = \mathbb{M}(n,\varphi) \circ f'$, alors l'application naturelle induite $\tilde{\psi} : W_{f'}(R') \to W_f(R)$, qui envoie $(M_\alpha \mid \alpha \in \mathbb{N}(S)) \in W_{f'}(R')$ sur $(\mathbb{M}(n,\psi)M_\alpha \mid \alpha \in \mathbb{N}(S)) \in W_f(R)$ est un homomorphisme de groupes abéliens.

c. Pour chaque $m \in \mathbb{N}(S)$, l'application $j_m(R) : W_f(R) \to \mathbb{M}(n,R)$, définie par $j_m(R)(x) = \sum_{d|m} dx_d^{(m/d)} f(m/d)$ est un homomorphisme de groupes abéliens fonctoriel en R. (Ici $x = (x_d \mid d \in \mathbb{N}(S)) \in W_f(R)$). Autrement dit, W_f admet des composantes fantômes.

Démonstration : Si on élimine la terminologie des lois dans la description de $C_S^n(F)$, si F est la loi définie par f, on tombe sur l'énoncé du théorème, grâce à la description générique de 2.4.

2.6 Il va de soi que $W_f(R)$ est muni d'une structure de groupe-abélien topologique séparé complet. On a les endomorphismes continus de Frobenius F_a, de décalage V_a pour $a \in \mathbb{N}(S)$, ainsi qu'une action de R sur $W_f(R)$, fonctoriels en R et définis par

$$j_m(R)(F_a x) = j_{am}(R)(x)$$

$$j_m(R)(V_a x) = a j_{m//a}(R)(x)$$

$$j_m(R)(\lambda x) = \lambda^m j_m(R)(x)$$

ce qui définit sur $W_f(R)$ une structure de $Cart_S(R)$-module à gauche. On pose $x \mapsto [x]$ l'application de Teichmüller $M(n,R) \to W_f(R)$, à savoir $[x] = \{x_d \mid d \in \mathbb{N}(S)\ ,\ x_1 = x\ ,\ x_i = 0 \text{ si } i > 1\}$. Alors on a : $x \in W_f(R)$ s'écrit sous la forme unique

$$x = \sum_{d\in\mathbb{N}(S)} V_d[x_d] \text{ , noté encore } x = \sum_{d\in\mathbb{N}(S)} V_d x_d \ .$$

On définit

$$E_f(R) = End_{Cart_S(R)\text{-}mod}(W_F(R))^{opp}$$

alors III.3.9 induit un homomorphisme injectif des groupes abéliens, fonctoriel en R :

$$i_f(R) : E_f(R) \to W_f(R)$$

défini par $i_f(R)(\varphi) = \varphi([I_n])$. (5)

2.7 Soit maintenant $S = \{p\}$. Posons $A = \mathbb{Z}[\sigma_i]_{i\geqslant 0}$ et définissons $\tilde{\sigma}_i \in A$ par récurrence :

$$\tilde{\sigma}_0 = 1 \quad \text{et} \quad \tilde{\sigma}_{n+1} = \sum_{i=0}^{n} p^i \sigma_i^{p^{m-i}} \tilde{\sigma}_{n-i}$$

c'est-à-dire la fonction : $p^n \mapsto \tilde{\sigma}_n$ à valeurs dans A est S-admissible.

Il résulte que les relations

$$\sum_{i=0}^{n} p^i (X_i^{p^{n-i}} + Y_i^{p^{n-i}})\tilde{\sigma}_{n-i} = \sum_{i=0}^{n} p^i w_i^{p^{n-i}} \tilde{\sigma}_{n-i} \qquad (6)$$

pour $n \geqslant 0$ admettent une solution

$$w_i = w_i(X_0,\dots,X_i\ ,\ Y_0,\dots,Y_i\ ,\ \sigma_0,\dots,\sigma_i) \ ;\ i \geqslant 0 \qquad (7)$$

à coefficients dans $\mathbb{Z}$.

2.8 On va utiliser ceci afin de construire de façon explicite les composantes fantômes pour les schémas de Greenberg. Reprenons la situation de IV.5.7 et IV.5.8. Soit $f : \mathbb{N}(p) \to v$ la fonction p-admissible, définie par

$$\sum_{\nu=0}^{\infty} \pi^{-\nu} x^{q^\nu} = \sum_{i=0}^{\infty} p^{-i} f(p^i) x^{p^i} \qquad (1) \text{ de IV.5.7}$$

alors f définit par passage au quotient une fonction p-admissible

$$\varphi : \mathbb{N}(p) \xrightarrow{f} v \xrightarrow{can} \mathbb{F}_q$$

et les lois abéliennes $F \in F(1,v)$ et $F_* \in F(1,\mathbb{F}_q)$.

On a une suite de flèches injectives des groupes abéliens

$$\begin{array}{ccccc} v \simeq End_v(F) & \xhookrightarrow{(*)} & End_{\mathbb{F}_q}(F_*) & & \\ \| & & \| & & \\ E_f(X) & \longrightarrow & E_\varphi(\mathbb{F}_q) & \hookrightarrow & W_\varphi(\mathbb{F}_q) \ . \end{array}$$

L'injectivité de $(*)$ résulte d'un lemma connu de Lubin-Tate. (Honda [1], lemma 3).

Soit $\psi : v \hookrightarrow W_\varphi(\mathbb{F}_q)$ l'application composée, alors $\psi(x)$ se calcule comme suit : On pose

$$xf(p^m) = \sum_{i=0}^{m} p^i \mu_i(x)^{p^{m-i}} f(p^{m-i}) \ , \ \mu \geqslant 0 \tag{8}$$

avec $\mu_i(x) \in v$, de l'image $\overline{\mu_i(x)}$ dans $\mathbb{F}_q$, alors $\psi(x) = \sum_{i=0}^{\infty} V^i \overline{\mu_i(x)}$, ce qui est de la forme, donnée dans IV.5.8 parce que $f(p^m) \neq 0$ entraîne $ad|m$. La structure d'anneau commutatif sur $\mathrm{Im}\,\psi \simeq v$ se donne par les composantes fantômes de $W_\varphi(\mathbb{F}_q)$, ou encore : On pose

$$f(p^{n+1}) = \sum_{i=0}^{n} p^i \sigma(i)^{p^{n-i}} f(p^{n-i}) \ , \ n \geqslant 0 \tag{9}$$

alors on réduit les polynômes (7) mod p puis on remplace les σ_i par les $\overline{\sigma(i)}$ en obtenant

$$\overline{w_i} = \overline{w_i}(X_0,\ldots,X_i\ ,\ Y_0,\ldots,Y_i\ ,\ \overline{\sigma(0)},\ldots,\overline{\sigma(i)}) \tag{10}$$

et on a

$$\sum_{i=0}^{\infty} V^i X_i + \sum_{i=0}^{\infty} V^i Y_i = \sum_{i=0}^{\infty} V^i \overline{w_i} \tag{11}$$

La structure multiplicative sur $\mathrm{Im}\,\psi$ est celle, induite par les opérateurs V et λ pour $\lambda \in \mathbb{F}_q$. Noter que ceci définit une structure d'anneau sur

$$\mathrm{Im}\,\psi \hat{\otimes} \mathbb{F}_{q^a} = \{\Sigma\ V^{adi}\lambda_i \mid \lambda_i \in \mathbb{F}_{q^a}\} \tag{12}$$

où $\mathbb{F}_q \to \mathbb{F}_{q^a}$ est l'extension de degré a , parce que si $x \in \mathbb{F}_{q^a}$ on a $xV^{ad} = V^{ad}x^{p^{ad}} = V^{ad}x$.

Mais on a mieux : on a $f(p^i) = 0$ si $ad|i$, ce qui entraîne dans (9) que $\sigma(i) = 0$ si i n'est pas de la forme $j\,ad-1$, $j \in \mathbb{N}^+$. Soit $\bar{v}_i$ le polynôme obtenu de w_{adi} de (9) en posant $X_i = Y_i = 0$ si $ad|i$ dans le polynôme w_{adi} et $X_{adi} = X_i'$, $Y_{adi} = Y_i'$, et $\tau_i = \sigma(iad + ad - 1)$, alors

Lemme : $\bar{v}_i = \bar{v}_i(X_0', \ldots, X_i', Y_0', \ldots, Y_0', \tau_0, \ldots, \tau_i)$ ne dépend pas du $a \in \mathbb{N}^+$ choisi.

Démonstration : Le lemme suit facilement de (6) de IV.5.4, le seul point embarrassant étant la puissance q^{m-j} qui intervient, mais on a $x = x^{p^{ad}}$ pour $x \in \mathbb{F}_q$, donc après réduction $\mathrm{mod}(\pi)$ on a ce qu'on veut.

Le lemme permet donc de définir pour tout $k \in \mathbf{Alg}_{\mathbb{F}_q}$,

$$J_\varphi(k) = \{\sum_{i=0}^{\infty} V^{di}\lambda_i \mid \lambda_i \in k\}$$

que l'on munit d'une structure d'anneau par les relations

$$\sum_{i=0}^{\infty} V^{di}X_i' + \sum_{i=0}^{\infty} V^{di}Y_i' = \sum_{i=0}^{\infty} V^{di}\bar{v}_i \tag{13}$$

$$V^d x = x V^d \quad \text{pour} \quad x \in k\,. \tag{14}$$

Si l'on voulait on pourrait exprimer la structure additive par les composantes fantômes. Si $\lambda = \sum_{i=0}^{\infty} V^{di}\lambda_i$, on a

$$j_m(k)(\lambda) = \sum_{i=0}^{m} q^i\, \lambda_i^{q^{m-i}}\, \varphi(q^{m-i}) = \lambda_0^{q^m}\,.$$

Tenant compte du th. IV.5.7 on trouve :

2.9 Théorème : J_φ est un foncteur en anneaux topologiques séparés complets : $\mathbf{Alg}_{\mathbb{F}_q} \to \mathbf{Alg}_V$. J_φ admet des composantes fantômes. $J_\varphi(\mathbb{F}_q) = v$. Si $\mathbb{F}_q \to \mathbb{F}_{q^a}$ est l'extension de degré a, alors $J_\varphi(\mathbb{F}_{q^a})$ est l'anneau des entiers dans l'extension non ramifié de K de degré a.

On pourrait donc considérer les formules (7) comme formules universelles qui donnent après une spécialisation convenable les composantes fantômes pour les schémas de Greenberg ou encore qui permettent l'extension du corps résiduel dans les extensions ramifiées.(Serre : Corps Locaux).

2.10 La construction faite dans 2.8 se traduit encore en termes de polynômes d'Eisenstein : Soit $\mathbb{Z}_p \to A \to v$ avec $\mathbb{Z}_p \to A$ non ramifié de degré d et $A \to v$ totalement ramifié. Soit $\sum_{i=0}^{e} c_i X^i = u(X)$ le polynôme d'Eisenstein de l'uniformisante π. On considère $u(T) \in A_\sigma[[T]]$, où σ est le Frobenius de A. D'après le théorème de Honda du §1, $u^{-1}(T)c_o * i(x)$ définit une loi G sur A, donc après extension des scalaires sur v. On a $\mathrm{End}_A(G) = A$ et $\mathrm{End}_v(G) = v$. Le dernier énoncé se vérifiant en observant que $x - x^q \in (\pi)$ pour $x \in v$, $(q = p^d)$ donc on peut prendre $\sigma = \mathrm{id}$ afin de satisfaire à la condition (F).

Soit $$u^{-1}(T)c_o * i(x) = \sum_{i=0}^{\infty} q^{-i} f(q^i) x^{q^i} .$$

On étend f par zéro à $f : \mathbb{N}(p) \to A$, ce qui est une fonction p-admissible, d'où une fonction p-admissible $\psi : \mathbb{N}(p) \xrightarrow{f} A \xrightarrow{\mathrm{can}} \mathbb{F}_q$. On obtient de la même façon que dans 2.9 un foncteur en anneaux topologiques séparés complets

$$J_\psi : \mathrm{Alg}_{\mathbb{F}_q} \to \mathrm{Alg}_v .$$

D'après le th. 5.7c J_ψ et J_φ (du 2.8) sont isomorphes sur v, mais J_ψ a l'avantage d'être défini sur une extension non ramifiée de $\mathbb{Z}_p$. Si l'on prend le polynôme d'Eisenstein par excellence $u(X) = p - X$ sur $\mathbb{Z}$, alors on voit facilement que $J_\psi = W$, le foncteur usuel des vecteurs de Witt.

manuscrit reçu juin 1974

Bibliographie

CARTIER P [1] Séminaire Sophus Lie.

[2] Groupes formels associés aux anneaux de Witt généralisées. C. R. Acad. Sc. Paris t. 265, p. 50-52 (1967) et Modules associés à un groupe formel commutatif. Courbes typiques. C. R. Acad. Sc. Paris, t. 265, p. 129-132 (1967).

[3] Groupes formels, fonctions automorphes et fonctions zéta des courbes elliptiques, Actes Congrès intern. Math., t. 2, p. 291-299 (1970).

DEMAZURE M. [D] p-Divisible groups, Springer Lect. Notes in Math. 302 (1972).

DIEUDONNE J. III Groupes de Lie et hyperalgèbres de Lie sur un corps de caractéristique $p > 0$, Math. Z. 63, p. 53-75 (1955).

V Groupes de Lie et hyperalgèbres de Lie sur un corps de caractéristique $p > 0$. Bull. Soc. Math. France 84, p. 207-239 (1956).

DITTERS E.J. [1] Curves and formal (cc)-groups. Inventiones math. 17, p. 1-20 (1972).

[2] On the structure of $P(Z(Z))$. Mimeographed notes, Univ. of Nymegen, p. 1-8 (1971).

FROHLICH A. [F] Formal Groups, Springer Lect. Notes in Math. 74 (1960).

HAREWINKEL M. [1] Constructing formal groups over $\mathbb{Z}$-algebras. Neth-School of Ec., Report 7201, 1-21 (1972).

HILL W. [1] Formal Groups and Zéta-functions of elliptic curves. Inventiones Math. 12, p. 321-336 (1971).

HONDA T. [1] Formal Groups and Zéta-functions. Osaka J. Math. 5, p. 199-213 (1968)

[2] On the theory of commutative formal groups. J. Math. Soc. Japan 22, n° 2, p. 213-246 (1970).

LAZARD M. [1] Sur les théorèmes fondamentaux des groupes formels commutatifs 1, 2. In dajationes Math. 35 n° 4, p. 201-300 (1973).

[2] Sur les groupes de Lie formels à un paramètre. Bull. Soc. Math. France, 83, p. 251-274 (1955).

MANIN Y. [1] The theory of commutatives formal groups over fields of finite characteristic. Russian Math. Surveys, 18, p. 1-51 (1963).

SERRE J.P. [1] Corps Locaux.

[2] Lie algebras and Lie groups. Harvard Lectures 1964, Benjamin Inc.

SHIMURA G. [1] Arithmetic theory of automorphic function. Princeton University Press (1971).