THÉORIE DES GROUPES. — *Modules associés à un groupe formel commutatif. Courbes typiques.* Note (*) de M. **Pierre Cartier**, transmise par M. Jean Leray.

A tout groupe formel commutatif (au sens de Dieudonné), on peut associer un module sur l'anneau des endomorphismes du groupe de Witt généralisé $\hat{W}_K^+$. On définit ainsi une équivalence de la catégorie des groupes formels commutatifs avec une certaine catégorie de modules. Le cas le plus important est celui où l'anneau de base est une algèbre sur l'anneau des entiers p-adiques : ceci permet de définir la notion de courbe typique.

1. Préliminaires fonctoriels. — On note K un anneau commutatif et $\mathbf{Alg}_K$ la catégorie des K-algèbres commutatives. La « droite formelle » sur K est le foncteur en ensembles D sur $\mathbf{Alg}_K$ associant à toute algèbre A l'ensemble D(A) de ses éléments nilpotents. Soient V un foncteur en ensembles sur $\mathbf{Alg}_K$, et o un élément de V(K). Un *système de coordonnées* centré en o sur V est une suite $(x_1, \ldots, x_r)$ de morphismes de V dans D satisfaisant aux conditions suivantes :

a. On a $(x_1)_K(o) = \ldots = (x_r)_K(o) = 0$.

b. Pour toute algèbre A, l'application $v \mapsto ((x_1)_A(v), \ldots, (x_r)_A(v))$ est une bijection de V(A) sur $D^r(A) = D(A) \times \ldots \times D(A)$ (r facteurs). S'il existe un tel système de coordonnées, on dit que V est une *variété formelle* de dimension r.

Soient V et W deux variétés formelles, munies de points-base $o \in V(K)$ et $o' \in W(K)$. On choisit des systèmes de coordonnées centrés, $(x_1, \ldots, x_r)$ pour V et $(y_1, \ldots, y_s)$ pour W. La formule

$$(1) \quad y_j(u_A(v)) = U_j((x_1)_A(v), \ldots, (x_r)_A(v)) \qquad [1 \leq j \leq s,\ A \in \mathbf{Alg}_K,\ v \in V(A)]$$

établit une bijection de l'ensemble des morphismes u de V dans W tels que $u_K(o) = o'$ sur l'ensemble des systèmes de s séries formelles $U_j(X_1, \ldots, X_r)$ sans termes constants à coefficients dans K. La composition des morphismes correspond à celle des séries formelles.

Un *groupe formel de dimension r* est un foncteur en groupes G sur $\mathbf{Alg}_K$ admettant un système de coordonnées $(x_1, \ldots, x_r)$, qu'on peut supposer centré en l'élément neutre de G(K); la composition $\mu : G \times G \to G$ s'exprime par une suite de r séries formelles $\mu_j(X_1, \ldots, X_r; Y_1, \ldots, Y_r)$ à coefficients dans K et sans termes constants. La notion de loi de groupe formel au sens de Dieudonné et Lazard correspond donc à celle de groupe formel muni d'un système de coordonnées.

2. Courbes dans un groupe formel. — Soit G un groupe formel commutatif, noté additivement. Une *courbe* (issue de l'origine) dans G

Source gallica.bnf.fr / Archives de l'Académie des sciences

est un morphisme γ de D dans G tel que $\gamma_K(o) = o$. L'ensemble $C = C(G)$ des courbes dans G est un groupe commutatif, la somme de deux courbes γ et γ' étant définie par $(\gamma + \gamma')_A(t) = \gamma_A(t) + \gamma'_A(t)$ pour A dans $\mathbf{Alg}_K$ et t dans $D(A)$.

Le groupe C est muni des endomorphismes suivants :

a. Homothéties $[c]$ définies pour c dans K par $([c]\gamma)_A(t) = \gamma_A(ct)$.

b. Décalages V_n définis pour $n \geqq 1$ par $(V_n\gamma)_A(t) = \gamma_A(t^n)$.

c. Opérateurs de Frobenius F_n : Soit γ dans C. Il existe un unique morphisme de variétés formelles $c : D^n \to G$ tel qu'on ait

$$\gamma_A(t_1) + \ldots + \gamma_A(t_n) = c_A(u_1, \ldots, u_n) \quad \text{si} \quad \prod_{j=1}^{n}(1 + t_j X) = 1 + \sum_{k=1}^{n} u_k X^k.$$

On a

$$(F_n\gamma)_A(t) = c_A(o, \ldots, o, (-1)^{n-1}t).$$

Entre ces opérateurs, on a les relations suivantes [1] :

$$(2) \qquad [c] + [c'] = \sum_{n=1}^{\infty} V_n.[s_n(c, c')].F_n \qquad \text{avec} \quad X^n + Y^n = \sum_{d \mid n} d.s_d(X, Y)^{n/d},$$

$$(3) \qquad [c].[c'] = [cc'],$$

$$(4) \qquad V_m.V_n = V_{mn}, \qquad F_m.F_n = F_{mn},$$

$$(5) \qquad V_n.[c^n] = [c].V_n, \qquad F_n.[c] = [c^n].F_n,$$

$$(6) \qquad F_n.V_m = V_m.F_n \quad \text{si} \quad (n, m) = 1,$$

$$(7) \qquad F_n.V_n = n.I_C, \qquad [1] = V_1 = F_1 = I_C.$$

Pour tout entier $n \geqq 1$, l'ensemble des courbes γ telles que l'on ait $\gamma_A(t) = o$ lorsque $t^n = o$ est un sous-groupe $C_n = C_n(G)$ de C. De plus :

(A) *La suite* $(C_n)_{n \geqq 1}$ *est décroissante, on a* $C_1 = C$, *et l'application naturelle de* C *dans la limite projective* $\varprojlim C/C_n$ *est bijective* (autrement dit, C est un groupe filtré séparé et complet).

(B) *Les opérateurs* V_n *sont injectifs; on a de plus*

$$(8) \qquad C_{nm} = V_n(C_m) + C_{nm+1}, \qquad V_n(C_m) \cap C_{nm+1} = V_n(C_{m+1}).$$

(C) *Le* K-*module* C_1/C_2 *est libre de type fini.*

La propriété (C) provient de ce que C_1/C_2 est isomorphe à l'algèbre de Lie de G.

3. Théorèmes d'existence. — On renvoie à une Note précédente [2] pour la définition des foncteurs en groupes $\hat{W}_K^+$ et l'étude de leurs endomorphismes. On notera $[t]$ le vecteur de Witt $(t, o, o, \ldots, o, \ldots)$.

Théorème 1. — *Soit* G *un groupe formel commutatif. Pour toute courbe* γ *dans* G, *il existe un homomorphisme de foncteurs en groupes* $u : \hat{W}_K^+ \to G$ *et un seul tel que*

$$(9) \qquad \gamma_A(t) = u_A([t]) \qquad \textit{pour } A \textit{ dans } \mathbf{Alg}_K \textit{ et } t \textit{ dans } D(A).$$

Si γ *et* u *se correspondent ainsi, il en est de même de* $[c].\gamma$ *et* $u \circ [c]$ *d'une part, de* $V_n\gamma$ *et* $u \circ F_n$ *de l'autre, enfin de* $F_n\gamma$ *et* $u \circ V_n$.

THÉORÈME 2. — *Soient* G *et* G′ *deux groupes formels commutatifs. Étant donnés une courbe* γ *dans* G *et un homomorphisme* u *de* G *dans* G′, *la courbe* $u \circ \gamma$ *dans* G′ *sera notée* $C(u).\gamma$.

L'application $u \mapsto C(u)$ *est une bijection de* Hom (G, G′) *sur l'ensemble des homomorphismes de groupes de* C(G) *dans* C(G′) *compatibles avec les filtrations et les opérateurs* $[c]$, V_n *et* F_n.

THÉORÈME 3. — *On suppose donnés un groupe commutatif* C, *des endomorphismes* $[c]$, V_n *et* F_n *de* C *satisfaisant aux relations* (2) *à* (7), *et une suite de sous-groupes* C_n *de* C *satisfaisant à* (A), (B) *et* (C). *Il existe alors un groupe formel commutatif* G *et un isomorphisme de* C(G) *sur* C *compatible avec les filtrations et les opérateurs* $[c]$, V_n *et* F_n. *Ce groupe formel* G *est défini à un isomorphisme près.*

La démonstration du théorème 1 repose sur le corollaire 2 du théorème 2 de la Note [2]. Celles des théorèmes 2 et 3 utilisent la construction de groupes formels quotients des produits $\hat{W}_K^+ \times \ldots \times \hat{W}_K^+$.

4. COURBES TYPIQUES. — Dans ce numéro, on suppose que p est un nombre premier et que tout nombre premier distinct de p admet un inverse dans K. Ce sera le cas si K est l'anneau des entiers p-adiques, ou un corps de caractéristique p.

Une courbe γ dans un groupe formel commutatif G sera dite *typique* si l'on a $F_q\gamma = 0$ pour tout nombre premier $q \neq p$. L'ensemble de ces courbes est un sous-groupe CT(G) de C(G), stable pour les opérateurs $[c]$, $V = V_p$ et $F = F_p$. On munit CT(G) d'une filtration définie par $CT_n(G) = CT(G) \cap C_{p^n}(G)$ pour $n \geq 0$; le groupe filtré CT(G) est séparé et complet. Si l'on désigne par μ la fonction de Möbius et $I(p)$ l'ensemble des entiers non divisibles par p, l'application $\sum_{n \in I(p)} [\mu(n)/n] V_n . F_n$ est un projecteur de C(G) sur CT(G). Toute courbe dans G s'écrit de manière unique sous la forme $\sum_{n \in I(p)} V_n \gamma_n$ avec des courbes typiques γ_n; on peut donc identifier C(G) à $CT(G)^{I(p)}$.

On peut prouver des résultats analogues aux théorèmes 1, 2 et 3, dans lesquels on remplace C(G) par CT(G), et $\hat{W}_K^+$ par le groupe de Witt usuel $\hat{W}_{p^\infty K}^+$. Lorsque K est un corps de caractéristique p, on retrouve ainsi les résultats de Dieudonné [3].

Nous allons interpréter la notion de courbe typique au moyen du *logarithme*. On suppose que p n'est pas diviseur de 0 dans K et l'on note L l'anneau obtenu par adjonction de $1/p$ à K. Soient G un groupe formel commutatif sur K, et $\mathfrak{g}$ son algèbre de Lie [4]. Comme L est une algèbre sur le corps des nombres rationnels, les groupes formels G_L et $\mathfrak{g}_L$ obtenus

par extension des scalaires de K à L sont isomorphes. Il existe un unique isomorphisme de G_L sur $\mathfrak{g}_L$ dont l'application tangente à l'origine soit l'identité; on le note log.

THÉORÈME 4. — *Soit γ une courbe dans* G. *Pour que γ soit typique, il faut et il suffit qu'il existe des éléments m_j de $\mathfrak{g}(L)$ tels qu'on ait*

$$\log \gamma_A(t) = \sum_{j \geq 0} \frac{m_j t^{p^j}}{p^j} \quad \textit{pour } A \textit{ dans } \mathbf{Alg}_L \textit{ et } t \textit{ dans } D(A). \tag{10}$$

La suite $(m_j)_{j \geq 0}$ est déterminée de manière unique et se compose en fait d'éléments de $\mathfrak{g}(K)$.

(*) Reçue le 17 mai 1967.

(1) On note I_C l'endomorphisme identique du groupe C.

(2) P. CARTIER, *Comptes rendus*, 265, série A, 1967, p. 49.

(3) J. DIEUDONNÉ, *Amer. J. Math.*, 77, 1955, p. 429 à 452.

(4) L'algèbre de Lie de G est le groupe formel commutatif défini comme suit : soient A dans $\mathbf{Alg}_K$ et $B = A \oplus A.\varepsilon$ avec $\varepsilon^2 = 0$; on note π l'homomorphisme de B sur A induisant l'identité sur A et annulant ε. Alors $\mathfrak{g}(A)$ est le noyau de l'homomorphisme $G(\pi) : G(B) \to G(A)$.

(*Institut de Recherche mathématique avancée, rue Descartes, Strasbourg, Bas-Rhin.*)