THÉORIE DES GROUPES. — *Groupes formels associés aux anneaux de Witt généralisés.* Note (*) de M. **Pierre Cartier**, présentée par M. Jean Leray.

A tout anneau commutatif A, on peut associer ([1]) un anneau de Witt généralisé W (A) et ([2]) un λ-anneau universel Λ (A). L'existence d'un isomorphisme entre ces deux anneaux permet de généraliser les résultats de Dieudonné ([3]) concernant les groupes formels associés aux groupes de Witt usuels. En particulier, nous déterminons l'anneau des endomorphismes et la bialgèbre des groupes de Witt généralisés, et nous définissons une autodualité pour ces groupes.

1. Anneaux de Witt généralisés. — Il existe un foncteur W de la catégorie des anneaux commutatifs dans elle-même et un seul, qui jouisse des propriétés suivantes :

a. Pour tout anneau commutatif A, l'ensemble W(A) se compose des suites $\mathbf{a} = (a_n)_{n\geq 1}$ d'éléments de A, et pour tout homomorphisme d'anneaux $\sigma : A \to B$, l'homomorphisme $W(\sigma)$ transforme la suite $\mathbf{a}$ en la suite $(\sigma(a_n))_{n\geq 1}$.

b. Pour tout anneau commutatif A, et tout entier $n \geq 1$, l'application $w_n : \mathbf{a} \mapsto \sum_{d|n} d.a_d^{n/d}$ est un homomorphisme d'anneaux de W(A) dans A.

Par ailleurs, si A est un anneau commutatif, on note Λ(A) l'ensemble des séries formelles à coefficients dans A, de terme constant égal à 1. L'application $E : \mathbf{a} \mapsto \prod_{n\geq 1} (1 - a_n t^n)^{-1}$ est une bijection de W(A) sur Λ(A) telle que $E(\mathbf{a} + \mathbf{b}) = E(\mathbf{a}).E(\mathbf{b})$; on peut donc définir dans Λ(A) une loi de composition par la règle $f \star g = E(E^{-1}(f).E^{-1}(g))$. La multiplication usuelle dans Λ(A) et l'opération $\star$ définissent sur Λ(A) une structure d'anneau commutatif, qui coïncide avec celle que Grothendieck a introduite dans ([2]).

2. Endomorphismes des groupes de Witt. — Soit K un anneau commutatif. On notera $\mathbf{Alg}_K$ la catégorie des K-algèbres commutatives, et W_K^+ le foncteur en groupes commutatifs sur $\mathbf{Alg}_K$ qui associe à toute algèbre A le groupe additif de l'anneau W(A). La définition de Λ_K^+ est analogue. Selon l'usage, on note G_{aK} et G_{mK} les foncteurs en groupes sur $\mathbf{Alg}_K$ associant respectivement à une algèbre A son groupe additif et le groupe multiplicatif de ses unités. On note A_0 l'anneau de polynômes K [a] et f_0 l'élément $(1 - at)^{-1}$ de $\Lambda_K^+(A_0)$.

Lemme. — *Soit* G *un foncteur en groupes commutatifs sur* $\mathbf{Alg}_K$, *transformant une injection en une injection. Si deux homomorphismes* u *et* v *de foncteurs en groupes de* Λ_K^+ *dans* G *sont tels que* $u_{A_0}(f_0) = v_{A_0}(f_0)$, *on a* $u = v$.

L'isomorphisme $E : W_K^+ \to \Lambda_K^+$ permet de traduire le lemme en termes de W_K^+. On en déduit les conséquences suivantes :

a. La suite $(w_n)_{n\geq 1}$ est une base du K-module $\mathrm{Hom}(W_K^+, G_{aK})$.

b. On définit pour tout entier $n \geq 1$ des endomorphismes V_n et F_n de Λ_K^+ en notant $V_n f$ la série $f(t^n)$ et en posant $N[f] = (F_n f)(t^n)$, où $N[\ldots]$ désigne la norme prise de $A[[t]]$ à $A[[t^n]]$. Les formules suivantes caractérisent V_n et F_n :

$$V_n(1 - at) = 1 - at^n, \qquad F_n(1 - at) = 1 - a^n t. \tag{1}$$

Nous définirons aussi l'endomorphisme $[c]$ de Λ_K^+ par la formule $([c].f)(t) = f(ct)$ pour $c \in K$; enfin, nous identifierons grâce à l'isomorphisme E les anneaux d'endomorphismes $\mathrm{End}(\Lambda_K^+)$ et $\mathrm{End}(W_K^+)$.

Théorème 1. — *Tout endomorphisme u de W_K^+ s'écrit de manière unique sous la forme $u = \sum_{m,n} V_m.[c_{mn}].F_n$, où pour chaque entier $m \geq 1$, l'ensemble des entiers $n \geq 1$ avec $c_{mn} \neq 0$ est fini.*

[Démonstration au moyen du lemme, les coefficients c_{mn} sont définis par $u_{A_0}(f_0) = \prod_{m,n} (1 - c_{mn} a^n t^m)^{-1}$.]

Le théorème 1 permet de décrire comme suit l'anneau $\mathrm{End}(W_K^+)$. Tout d'abord, on identifie de manière naturelle $W(K)$ à un sous-anneau de $\mathrm{End}(W_K^+)$. Quels que soient les entiers m et n, on a $F_m F_n = F_{mn}$; par suite, le sous-anneau **H** de $\mathrm{End}(W_K^+)$ engendré par $W(K)$ et les F_n est isomorphe à l'anneau des polynômes à coefficients dans $W(K)$ en des variables F_p (p premier) qui commutent entre elles et telles que $F_p.\mathbf{a} = \mathbf{a}^{(p)}.F_p$ pour tout $\mathbf{a} \in W(K)$ (on note $\mathbf{a}^{(p)}$ l'image de $\mathbf{a}$ par F_p). Introduisons ensuite l'anneau **S** des séries formelles à coefficients dans **H** en des variables V_p(p premier) qui commutent deux à deux et dont les règles de commutation avec les éléments de **H** sont les suivantes :

$$\mathbf{a}.V_p = V_p.\mathbf{a}^{(p)}, \qquad F_q.V_p = V_p.F_q \quad (\text{pour } p \neq q). \tag{2}$$

On peut alors identifier $\mathrm{End}(W_K^+)$ au quotient de l'anneau **S** par l'idéal bilatère engendré par les éléments $F_p.V_p - p$, $V_p.\mathbf{a}.F_p - \mathbf{b}$ où $\mathbf{a}$ est dans $W(K)$ et $\mathbf{b}$ est l'image de $\mathbf{a}$ par V_p.

3. Décompositions des groupes de Witt.

a. Supposons d'abord que K *soit une algèbre sur le corps* **Q** *des nombres rationnels.* On notera I l'ensemble des entiers $n \geq 1$ et N_K l'intersection des noyaux des endomorphismes F_n de W_K^+ pour $n > 1$. Pour toute K-algèbre commutative A, tout élément de $W_K^+(A)$ s'écrit de manière unique sous la forme $\sum_{n \in I} V_n.\mathbf{a}(n)$ avec $\mathbf{a}(n) \in N_K(A)$ pour tout $n \in I$.

La multiplication par un entier $n \geq 1$ est un automorphisme de W_K^+, et le projecteur de W_K^+ sur N_K nul sur $V_m N_K$ pour $m > 1$ est égal à $\sum_{n \in I} [\mu(n)/n]\, V_n F_n$ (en notant μ la fonction de Möbius). Pour tout entier $n \in I$, ω_n est nul sur $V_m N_K$ pour $m \neq n$ et induit un isomorphisme

de $V_n N_K$ sur G_{aK}; le foncteur en groupes W_K^+ est donc isomorphe à $(G_{aK})^I$. On peut par suite identifier $\mathrm{End}(W_K^+)$ à l'anneau des matrices carrées de type I à coefficients dans K, dont chaque ligne a un nombre fini d'éléments non nuls, l'anneau W(K) s'identifiant à l'anneau des matrices diagonales.

b. Soit p un nombre premier. On note I(p) l'ensemble des nombres entiers positifs non divisibles par p, et l'on suppose que les éléments de I(p) sont inversibles dans K.

Par ailleurs, on note N_{pK} l'intersection des noyaux des endomorphismes F_n de W_K^+ pour $n \neq 1$ dans I(p), et $W_{p^\infty K}^+$ le foncteur « groupe additif des vecteurs de Witt usuels ». La formule $\varepsilon(\mathbf{a})_m = a_{p^m}$ (pour $m \geq 0$ entier) définit un isomorphisme ε de N_{pK} sur $W_{p^\infty K}^+$; la multiplication par tout entier appartenant à I(p) est un automorphisme de W_K^+, et l'endomorphisme $\sum_{n \in I(p)} [\mu(n)/n]\, V_n F_n$ est un projecteur de W_K^+ sur N_{pK} nul sur l'image de V_n pour tout entier $n \neq 1$ dans I(p); enfin, pour toute K-algèbre commutative A, tout élément de $W_K^+(A)$ s'écrit de manière unique sous la forme $\sum_{n \in I(p)} V_n.\mathbf{a}(n)$ avec $\mathbf{a}(n) \in N_{pK}(A)$ pour $n \in I(p)$.

Ce qui précède définit un isomorphisme de W_K^+ avec le produit $(W_{p^\infty K}^+)^{I(p)}$ Par suite, l'anneau $\mathrm{End}(W_K^+)$ est canoniquement isomorphe à l'anneau des matrices carrées de type I(p) à coefficients dans l'anneau $\mathbf{H}_p = \mathrm{End}(W_{p^\infty K}^+)$, dont chaque ligne n'a qu'un nombre fini d'éléments non nuls. Quant à l'anneau $\mathbf{H}_p$, il peut se représenter comme l'anneau des séries formelles en une variable V_p, dont les coefficients sont des polynômes en une variable F_p à coefficients dans l'anneau de Witt usuel $W_{p^\infty}(K)$, les relations suivantes formant une présentation de $\mathbf{H}_p$:

$$F_p.\mathbf{a} = \mathbf{a}^{(p)}.F_p, \qquad \mathbf{a}.V_p = V_p.\mathbf{a}^{(p)}, \qquad F_p V_p = p, \tag{3}$$

$$V_p.\mathbf{a}.F_p = \mathbf{b} \quad \text{avec} \quad \mathbf{a} \in W_{p^\infty}(K) \quad \text{et} \quad \mathbf{b} = V_p(\mathbf{a}). \tag{4}$$

Plus particulièrement, si K est un corps de caractéristique $p \neq 0$, on peut remplacer (4) par $V_p F_p = p$, et $\mathbf{H}_p$ n'est autre que l'anneau étudié par Dieudonné [3].

4. Dualité. — Pour tout anneau commutatif A, l'ensemble $\hat{W}(A)$ des éléments de W(A) à coordonnées nilpotentes, nulles sauf un nombre fini d'entre elles, est un idéal de l'anneau W(A); on en déduit la définition du sous-foncteur $\hat{W}_K^+$ de W_K^+(« complété formel à l'origine » de W_K^+). Étant donnés $\mathbf{a} \in W(A)$ et $\mathbf{b} \in \hat{W}(A)$, on note $\langle \mathbf{a}, \mathbf{b} \rangle$ la valeur en $t = 1$ du polynôme $E(\mathbf{a}.\mathbf{b}) \in A[t]$. Ceci définit un accouplement de $W_K^+ \times \hat{W}_K^+$ dans G_{mK}. Par application du lemme du n° 2, on obtient facilement le résultat suivant :

Théorème 2. — *Soit u un homomorphisme de foncteurs en groupes de* W_K^+ *dans* G_{mK}. *Il existe un unique élément b dans* $\hat{W}^+(K)$ *tel que*

$u_A(\mathbf{a}) = <\mathbf{a}, \mathbf{b}>$ *pour toute* K-*algèbre commutative* A *et tout* $\mathbf{a}$ *dans* $W_K^+(A)$. *Autrement dit, l'accouplement précédent définit un isomorphisme de groupes commutatifs* $\hat{W}^+(K) \simeq \mathrm{Hom}(W_K^+, G_{mK})$.

En appliquant la théorie de la dualité entre « groupes algébriques » et « groupes formels » ([4]), convenablement généralisée, on déduit les corollaires suivants :

Corollaire 1. — *L'accouplement précédent définit un isomorphisme de groupes commutatifs* $\hat{W}^+(K) \simeq \mathrm{Hom}(W_K^+, G_{mK})$.

Corollaire 2. — *La bialgèbre des distributions sur le groupe formel* $\hat{W}_K^+$ *est une algèbre de polynômes* $K[Z_1, Z_2, \ldots, Z_n, \ldots]$ *dont le coproduit* π *est donné par la formule*

$$\pi(Z_n) = \sum_{i+j=n} Z_i \otimes Z_j \qquad (\text{avec } Z_0 = 1). \tag{5}$$

De plus, l'algèbre de Lie de $\hat{W}_K^+$ *est le* K-*module ayant pour base les polynômes* $r_n(Z_1, \ldots, Z_n)$ *définis par* $r_n(C_1, \ldots, C_n) = X_1^n + \ldots + X_n^n$ *si*

$$1 + C_1 t + C_2 t^2 + \ldots + C_n t^n = \prod_{j=1}^{n} (1 + X_j t).$$

Le théorème 2 et son corollaire 1 entraînent l'existence d'un isomorphisme de l'anneau $\mathrm{End}(\hat{W}_K^+)$ sur l'anneau opposé à $\mathrm{End}(W_K^+)$. Cet isomorphisme échange V_n et F_n d'après les relations

$$<F_n\mathbf{a}, \mathbf{b}> = <\mathbf{a}, V_n\mathbf{b}>, \qquad <V_n\mathbf{a}, \mathbf{b}> = <\mathbf{a}, F_n\mathbf{b}> \tag{6}$$

et par suite tout endomorphisme u de $\hat{W}_K^+$ s'écrit de manière unique sous la forme $u = \sum_{m,n} V_n . [c_{mn}] . F_m$, où les c_{mn} sont comme dans le théorème 1.

(*) Séance du 12 juin 1967.

([1]) D. Mumford, *Ann. Math. Studies*, n° 59, lecture 26.

([2]) A. Grothendieck, *Bull. Soc. math. Fr.*, 86, 1958, p. 137 à 154 (*voir* surtout p. 149).

([3]) Soit W le groupe de Witt formel usuel sur un corps de caractéristique $p \neq 0$. L'anneau des endomorphismes de W est donné dans J. Dieudonné, *Amer. J. Math.*, 77, 1955, p. 429 à 452 (*voir* théorème 1); la bialgèbre est donnée dans J. Dieudonné, *Mathematika*, 2, 1955, p. 21 à 31 (*voir* prop. 1); enfin, pour le dual de W, *voir* J. Dieudonné, *Proc. Amer. Math. Soc.*, 8, 1957, p. 210 à 214, prop. 2.

([4]) P. Cartier, *Colloque sur la théorie des groupes algébriques*, Bruxelles, 1962, p. 87 à 114 (*voir* surtout le n° 14).

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