CHAPITRE IX

Anneaux locaux noethériens complets

Dans ce chapitre, tous les anneaux sont supposés commutatifs ; les algèbres sont associatives, commutatives et unifères. On note 1_A *l'élément unité d'un anneau* A.

Si A *est un anneau et* $\mathfrak{p}$ *un idéal premier de* A, *on note* $\kappa(\mathfrak{p})$ *le corps résiduel de l'anneau local* $A_\mathfrak{p}$. *Si l'anneau* A *est local, on note* $\mathfrak{m}_A$ *son idéal maximal et* κ_A *ou* $\kappa(\mathfrak{m}_A)$ *son corps résiduel.*

On dit qu'un homomorphisme d'anneaux $\rho : A \to B$ *est plat* (resp. *fidèlement plat*) *s'il fait de* B *un* A*-module plat* (resp. *fidèlement plat*). *Rappelons* (I, § 3, n° 5, prop. 9) *que si* A *et* B *sont locaux,* ρ *est fidèlement plat si et seulement s'il est plat et local.*

§ 1. VECTEURS DE WITT

Dans tout ce paragraphe, p désigne un nombre premier.

1. Polynômes de Witt

Pour tout entier $n \geqslant 0$, on appelle n-ième polynôme de Witt l'élément Φ_n de $\mathbf{Z}[X_0, ..., X_n]$ défini par

$$\Phi_n(X_0, ..., X_n) = \sum_{i=0}^{n} p^i X_i^{p^{n-i}} = X_0^{p^n} + pX_1^{p^{n-1}} + \cdots + p^n X_n . \tag{1}$$

On a évidemment $\Phi_0 = X_0$ et les relations de récurrence

$$\Phi_{n+1}(X_0, ..., X_{n+1}) = \Phi_n(X_0^p, ..., X_n^p) + p^{n+1} X_{n+1} \tag{2}$$

$$\Phi_{n+1}(X_0, ..., X_{n+1}) = X_0^{p^{n+1}} + p\Phi_n(X_1, ..., X_{n+1}) . \tag{3}$$

Lorsqu'on affecte X_i du poids p^i, le polynôme Φ_n est isobare de poids p^n (A, IV, p. 3).

PROPOSITION 1. — *Soient* A *un anneau filtré et* $(J_n)_{n\in\mathbf{Z}}$ *sa filtration. On suppose que l'on a* $J_0 = A$ *et* $p.1_A \in J_1$. *Soient* m *et* n *des entiers tels que* $m \geqslant 1$ *et* $n \geqslant 0$, *et* $a_0, ..., a_n, b_0, ..., b_n$ *des éléments de* A.

a) Si l'on a $a_i \equiv b_i \bmod. J_m$ *pour* $0 \leqslant i \leqslant n$, *alors on a*

$$\Phi_i(a_0, ..., a_i) \equiv \Phi_i(b_0, ..., b_i) \bmod. J_{m+i} \quad \text{pour} \quad 0 \leqslant i \leqslant n.$$

b) Supposons que, pour tout entier $k \geqslant 1$, *et tout* $x \in A$, *la relation* $p.x \in J_{k+1}$ *entraîne* $x \in J_k$. *Si l'on a* $\Phi_i(a_0, ..., a_i) \equiv \Phi_i(b_0, ..., b_i) \bmod. J_{m+i}$ *pour* $0 \leqslant i \leqslant n$, *alors on a* $a_i \equiv b_i \bmod. J_m$ *pour* $0 \leqslant i \leqslant n$.

Lemme 1. — *Si* x *et* y *sont deux éléments de* A *congrus modulo* J_m, *on a*

$$x^{p^n} \equiv y^{p^n} \bmod. J_{m+n}.$$

Par récurrence sur n, on se ramène au cas où $n = 1$. Notons P le polynôme $\sum_{i=0}^{p-1} X^i Y^{p-1-i}$ de $\mathbf{Z}[X, Y]$. Vu l'hypothèse faite sur x et y, on a $P(x, y) \equiv P(x, x) \equiv p.x^{p-1} \bmod. J_m$. Or on a $J_m + p.A \subset J_1$, d'où $P(x, y) \in J_1$. Finalement, $x^p - y^p = (x - y)\,P(x, y)$ appartient à $J_m J_1 \subset J_{m+1}$.

Démontrons *a)* par récurrence sur n. Le cas $n = 0$ est immédiat. Supposons $n \geqslant 1$. Sous les hypothèses de *a)*, on a

$$a_i^p \equiv b_i^p \bmod. J_{m+1} \quad \text{pour} \quad 0 \leqslant i \leqslant n-1 \quad \text{d'après le lemme 1,} \tag{4}$$

$$\Phi_{n-1}(a_0^p, ..., a_{n-1}^p) \equiv \Phi_{n-1}(b_0^p, ..., b_{n-1}^p) \bmod. J_{m+n} \tag{5}$$

d'après l'hypothèse de récurrence appliquée aux éléments $a_0^p, ..., a_{n-1}^p, b_0^p, ..., b_{n-1}^p$ de A, et

$$\Phi_n(a_0, ..., a_n) - p^n.a_n \equiv \Phi_n(b_0, ..., b_n) - p^n.b_n \bmod. J_{m+n} \tag{6}$$

d'après les formules (2) et (5). Comme $a_n - b_n$ appartient à J_m, l'élément $p^n.a_n - p^n.b_n$ appartient à J_{m+n} et on déduit de (6) la congruence

$$\Phi_n(a_0, ..., a_n) \equiv \Phi_n(b_0, ..., b_n) \bmod. J_{m+n},$$

d'où *a)*.

Démontrons *b)* par récurrence sur n. Le cas $n = 0$ est immédiat. Supposons $n \geqslant 1$. Sous les hypothèses de *b)*, on a $a_i \equiv b_i \bmod. J_m$ pour $0 \leqslant i \leqslant n-1$ d'après l'hypothèse de récurrence, et on en déduit comme précédemment les congruences (4), (5) et (6). Mais par hypothèse $\Phi_n(a_0, ..., a_n)$ et $\Phi_n(b_0, ..., b_n)$ sont congrus mod. J_{m+n}, et l'on a donc $p^n.(a_n - b_n) \in J_{m+n}$. Comme la relation $p.x \in J_{k+1}$ entraîne $x \in J_k$ pour tout $x \in A$ et tout $k \geqslant 1$, on a $a_n - b_n \in J_m$, ce qui achève la démonstration.

2. Les applications f, v et Φ

Soit A un anneau. Munissons $A^{\mathbf{N}}$ de la structure d'anneau produit. Notons f_A, ou simplement f, l'endomorphisme $(a_n)_{n\in\mathbf{N}} \mapsto (a_{n+1})_{n\in\mathbf{N}}$ de $A^{\mathbf{N}}$. Notons v_A, ou simple-

ment v, l'endomorphisme du groupe additif sous-jacent à $A^{\mathbf{N}}$ qui à $(a_n)_{n\in\mathbf{N}}$ associe $(0, p.a_0, p.a_1, ...)$.

Pour tout entier $m \geqslant 0$, notons Φ_m l'application de $A^{\mathbf{N}}$ dans A qui à $\boldsymbol{a} = (a_n)_{n\in\mathbf{N}}$ associe $\Phi_m(a_0, ..., a_m)$. On note Φ_A, ou simplement Φ, l'application $\boldsymbol{a} \mapsto (\Phi_n(\boldsymbol{a}))_{n\in\mathbf{N}}$ de $A^{\mathbf{N}}$ dans lui-même.

Lemme 2. — *Soit* A *un anneau muni d'un endomorphisme* σ *vérifiant* $\sigma(a) \equiv a^p \bmod p.A$ *pour tout* $a \in A$. *Soient* $n \geqslant 1$ *un entier et* $a_0, ..., a_{n-1}$ *des éléments de* A. *Posons* $u_i = \Phi_i(a_0, ..., a_i)$ *pour* $0 \leqslant i \leqslant n-1$. *Soit* u_n *un élément de* A. *Les conditions suivantes sont équivalentes* :

a) Il existe $a_n \in A$ *tel que* $u_n = \Phi_n(a_0, ..., a_n)$.

b) On a $\sigma(u_{n-1}) \equiv u_n \bmod p^n.A$.

Pour $0 \leqslant i \leqslant n-1$, on a $\sigma(a_i) \equiv a_i^p \bmod p.A$. D'après la prop. 1 du n° 1 appliquée au cas où $J_k = p^k.A$ (pour $k \in \mathbf{N}$) et où $m = 1$, on a la congruence

$$\Phi_{n-1}(\sigma(a_0), ..., \sigma(a_{n-1})) \equiv \Phi_{n-1}(a_0^p, ..., a_{n-1}^p) \bmod p^n.A\,, \tag{7}$$

c'est-à-dire

$$\sigma(u_{n-1}) \equiv \Phi_{n-1}(a_0^p, ..., a_{n-1}^p) \bmod p^n.A\,. \tag{8}$$

Or, d'après la formule (2), la relation $u_n = \Phi_n(a_0, ..., a_n)$ équivaut à

$$u_n = \Phi_{n-1}(a_0^p, ..., a_{n-1}^p) + p^n.a_n\,. \tag{9}$$

Le lemme en résulte.

PROPOSITION 2. — *Soit* A *un anneau.*

a) Si $p.1_A$ *est non diviseur de* 0 *dans* A, *l'application* Φ_A *est injective.*

b) Si $p.1_A$ *est inversible dans* A, *l'application* Φ_A *est bijective.*

c) Si σ *est un endomorphisme de l'anneau* A, *vérifiant* $\sigma(a) \equiv a^p \bmod p.A$ *pour tout* $a \in A$, *l'image* A′ *de* Φ_A *est un sous-anneau de* $A^{\mathbf{N}}$, *stable par* f_A *et* v_A. *C'est l'ensemble des éléments* $(u_n)_{n\in\mathbf{N}}$ *de* $A^{\mathbf{N}}$ *tels que* $\sigma(u_n) \equiv u_{n+1} \bmod p^{n+1}.A$ *pour tout* $n \in \mathbf{N}$.

Si $\boldsymbol{a} = (a_n)_{n\in\mathbf{N}}$ et $\boldsymbol{u} = (u_n)_{n\in\mathbf{N}}$ sont des éléments de $A^{\mathbf{N}}$, la relation $\Phi_A(\boldsymbol{a}) = \boldsymbol{u}$ est équivalente, d'après la formule (2), aux égalités

$$\begin{cases} u_0 = a_0\,, \\ u_n = \Phi_{n-1}(a_0^p, ..., a_{n-1}^p) + p^n.a_n \quad \text{pour tout} \quad n \geqslant 1\,. \end{cases} \tag{10}$$

Soit $\boldsymbol{u} = (u_n)_{n\in\mathbf{N}}$ dans $A^{\mathbf{N}}$. Lorsque $p.1_A$ est non diviseur de 0 dans A (resp. lorsque $p.1_A$ est inversible dans A), il existe au plus une suite $(a_n)_{n\in\mathbf{N}}$ dans A (resp. exactement une suite $(a_n)_{n\in\mathbf{N}}$ dans A) satisfaisant aux égalités (10), d'où *a*) et *b*).

Démontrons *c*). D'après le lemme 2, l'image A′ de $A^{\mathbf{N}}$ par Φ_A est l'ensemble des $\boldsymbol{u} = (u_n)_{n\in\mathbf{N}}$ dans $A^{\mathbf{N}}$ tels que $\sigma(u_n) \equiv u_{n+1} \bmod p^{n+1}.A$ pour tout $n \in \mathbf{N}$. Il en résulte aussitôt que A′ est un sous-anneau de $A^{\mathbf{N}}$, stable par f_A et v_A.

Remarque. — Soient $\boldsymbol{a} = (a_n)_{n\in\mathbf{N}}$ et $\boldsymbol{u} = (u_n)_{n\in\mathbf{N}}$ des éléments de $A^{\mathbf{N}}$ tels que $\boldsymbol{u} = \Phi_A(\boldsymbol{a})$, et m un entier $\geqslant 0$. On déduit de (10) les assertions suivantes :

Si les u_n, pour $0 \leqslant n \leqslant m$, appartiennent à un sous-anneau B de A et si, pour tout $x \in A$, la relation $p.x \in B$ entraîne $x \in B$, alors les a_n, pour $0 \leqslant n \leqslant m$, appartiennent à B.

Si A est muni d'une graduation de type $\mathbf{N}$, si $p.1_A$ est non diviseur de 0 dans A, si $d \in \mathbf{N}$ et si u_n est homogène de degré dp^n pour $0 \leqslant n \leqslant m$, alors a_n est homogène de degré dp^n pour $0 \leqslant n \leqslant m$.

3. Construction de polynômes

Soit A l'anneau $\mathbf{Z}[\mathbf{X}, \mathbf{Y}]$ des polynômes à coefficients entiers en deux familles d'indéterminées $\mathbf{X} = (X_n)_{n\in\mathbf{N}}$ et $\mathbf{Y} = (Y_n)_{n\in\mathbf{N}}$. Soit θ l'endomorphisme de A défini par $\theta(X_n) = X_n^p$ et $\theta(Y_n) = Y_n^p$ pour tout $n \in \mathbf{N}$. Alors p n'est pas diviseur de 0 dans A et l'ensemble des a dans A tels que $\theta(a) \equiv a^p$ mod. $p.A$ est un sous-anneau de A contenant les X_n et les Y_n, donc égal à A tout entier.

D'après la prop. 2, *a*) et *c*) du n° 2, il existe des éléments $\mathbf{S} = (S_n)_{n\in\mathbf{N}}$, $\mathbf{P} = (P_n)_{n\in\mathbf{N}}$, $\mathbf{I} = (I_n)_{n\in\mathbf{N}}$ et $\mathbf{F} = (F_n)_{n\in\mathbf{N}}$ de $A^{\mathbf{N}}$ caractérisés respectivement par les égalités

$$(11)\qquad \begin{cases} \Phi_A(\mathbf{S}) = \Phi_A(\mathbf{X}) + \Phi_A(\mathbf{Y}) \\ \Phi_A(\mathbf{P}) = \Phi_A(\mathbf{X})\,\Phi_A(\mathbf{Y}) \\ \Phi_A(\mathbf{I}) = -\Phi_A(\mathbf{X}) \\ \Phi_A(\mathbf{F}) = f_A(\Phi_A(\mathbf{X}))\,. \end{cases}$$

Les éléments S_n, P_n, I_n et F_n de A sont donc caractérisés par les formules suivantes (où n parcourt $\mathbf{N}$) :

$$(12)\qquad \Phi_n(S_0, \ldots, S_n) = \Phi_n(X_0, \ldots, X_n) + \Phi_n(Y_0, \ldots, Y_n)\,,$$

$$(13)\qquad \Phi_n(P_0, \ldots, P_n) = \Phi_n(X_0, \ldots, X_n)\,\Phi_n(Y_0, \ldots, Y_n)\,,$$

$$(14)\qquad \Phi_n(I_0, \ldots, I_n) = -\Phi_n(X_0, \ldots, X_n)\,,$$

$$(15)\qquad \Phi_n(F_0, \ldots, F_n) = \Phi_{n+1}(X_0, \ldots, X_{n+1})\,.$$

Affectons X_n et Y_n du poids p^n pour tout $n \in \mathbf{N}$. On déduit de la remarque du n° 2 les assertions suivantes :

a) On a $S_n \in \mathbf{Z}[X_0, \ldots, X_n, Y_0, \ldots, Y_n]$ et S_n est isobare de poids p^n.

b) On a $P_n \in \mathbf{Z}[X_0, \ldots, X_n, Y_0, \ldots, Y_n]$ et P_n est isobare de poids p^n en chacune des familles $(X_0, \ldots, X_n)$ et $(Y_0, \ldots, Y_n)$.

c) On a $I_n \in \mathbf{Z}[X_0, \ldots, X_n]$ et I_n est isobare de poids p^n.

d) On a $F_n \in \mathbf{Z}[X_0, \ldots, X_{n+1}]$ et F_n est isobare de poids p^{n+1}.

La formule (2) permet dans la pratique de déterminer les polynômes S_n, P_n, I_n et F_n de proche en proche.

Exemples. — 1) On a

$$S_0 = X_0 + Y_0$$

$$S_1 = X_1 + Y_1 - \sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} X_0^i Y_0^{p-i}.$$

De plus, $S_n - X_n - Y_n$ appartient à l'anneau $\mathbf{Z}[X_0, ..., X_{n-1}, Y_0, ..., Y_{n-1}]$.

2) On a

$$P_0 = X_0 Y_0$$

$$P_1 = pX_1Y_1 + X_0^p Y_1 + X_1 Y_0^p.$$

3) Lorsque $p \neq 2$, on a $I_n = -X_n$. Pour $p = 2$, on a

$$I_0 = -X_0$$

$$I_1 = -(X_0^2 + X_1)$$

$$I_2 = -X_0^4 - X_0^2 X_1 - X_1^2 - X_2.$$

4) On a

$$F_0 = X_0^p + pX_1$$

$$F_1 = X_1^p + pX_2 - \sum_{i=0}^{p-1} \binom{p}{i} p^{p-i-1} X_0^{pi} X_1^{p-i}.$$

Comme on a $\Phi_n(F_0, ..., F_n) \equiv \Phi_n(X_0^p, ..., X_n^p) \bmod p^{n+1}$. A pour tout $n \in \mathbf{N}$ (formules (2) et (15)), il résulte de la prop. 1, *b*) qu'on a $F_n \equiv X_n^p \bmod p$. A pour tout $n \in \mathbf{N}$.

Remarque. — Soit **J** l'ensemble des entiers $j \geqslant 1$. Pour tout élément j de **J**, définissons le polynôme φ_j de $\mathbf{Z}[(X_j)_{j\in\mathbf{J}}]$ par la formule

$$\varphi_j = \sum_d d X_d^{j/d},$$

où la somme porte sur les éléments de **J** qui divisent j. Pour tout entier $n \geqslant 0$, on a

$$\varphi_{p^n} = \Phi_n(X_{p^0}, ..., X_{p^n}).$$

Pour tout anneau A et tout élément m de **J**, on note φ_m l'application de $A^{\mathbf{J}}$ dans A qui à $(a_j)_{j\in\mathbf{J}}$ associe $\varphi_m((a_j)_{j\in\mathbf{J}})$; on note φ_A, ou simplement φ, l'application de $A^{\mathbf{J}}$ dans lui-même qui à $\boldsymbol{a} = (a_j)_{j\in\mathbf{J}}$ associe $(\varphi_m(\boldsymbol{a}))_{m\in\mathbf{J}}$.

Soit $\mathscr{A} = \mathbf{Z}[(X_j)_{j\in\mathbf{J}}, (Y_j)_{j\in\mathbf{J}}]$ l'anneau des polynômes à coefficients entiers en les deux familles d'indéterminées $\mathbf{X} = (X_j)_{j\in\mathbf{J}}$ et $\mathbf{Y} = (Y_j)_{j\in\mathbf{J}}$. On peut montrer (p. 51, exerc. 34) qu'il existe dans $\mathscr{A}$ des éléments

$$\boldsymbol{s} = (s_j)_{j\in\mathbf{J}}, \quad \boldsymbol{p} = (p_j)_{j\in\mathbf{J}} \quad \text{et} \quad \boldsymbol{i} = (i_j)_{j\in\mathbf{J}},$$

caractérisés par les égalités suivantes :

$$\varphi_{\mathcal{A}}(s) = \varphi_{\mathcal{A}}(\mathbf{X}) + \varphi_{\mathcal{A}}(\mathbf{Y})$$
$$\varphi_{\mathcal{A}}(p) = \varphi_{\mathcal{A}}(\mathbf{X})\,\varphi_{\mathcal{A}}(\mathbf{Y})$$
$$\varphi_{\mathcal{A}}(i) = -\varphi_{\mathcal{A}}(\mathbf{X}).$$

4. L'anneau W(A) des vecteurs de Witt

Soit A un anneau. Si $\boldsymbol{a} = (a_n)_{n\in\mathbf{N}}$ et $\boldsymbol{b} = (b_n)_{n\in\mathbf{N}}$ sont des éléments de $\mathrm{A}^{\mathbf{N}}$, nous noterons $\mathrm{S_A}(\boldsymbol{a}, \boldsymbol{b})$ (resp. $\mathrm{P_A}(\boldsymbol{a}, \boldsymbol{b})$, resp. $\mathrm{I_A}(\boldsymbol{a})$) ou simplement $\mathrm{S}(\boldsymbol{a}, \boldsymbol{b})$ (resp. $\mathrm{P}(\boldsymbol{a}, \boldsymbol{b})$, resp. $\mathrm{I}(\boldsymbol{a})$) la suite $(\mathrm{S}_n(a_0, ..., a_n;\ b_0, ..., b_n))_{n\in\mathbf{N}}$ (resp. $(\mathrm{P}_n(a_0, ..., a_n\,;\, b_0, ..., b_n))_{n\in\mathbf{N}}$, resp. $(\mathrm{I}_n(a_0, ..., a_n))_{n\in\mathbf{N}}$). En substituant a_n à X_n et b_n à Y_n, pour tout $n \in \mathbf{N}$, dans les formules (12), (13) et (14), on obtient les égalités

$$\Phi_{\mathrm{A}}(\mathrm{S_A}(\boldsymbol{a}, \boldsymbol{b})) = \Phi_{\mathrm{A}}(\boldsymbol{a}) + \Phi_{\mathrm{A}}(\boldsymbol{b}) \tag{16}$$

$$\Phi_{\mathrm{A}}(\mathrm{P_A}(\boldsymbol{a}, \boldsymbol{b})) = \Phi_{\mathrm{A}}(\boldsymbol{a})\,\Phi_{\mathrm{A}}(\boldsymbol{b}) \tag{17}$$

$$\Phi_{\mathrm{A}}(\mathrm{I_A}(\boldsymbol{a})) = -\Phi_{\mathrm{A}}(\boldsymbol{a}). \tag{18}$$

Nous noterons W(A) l'ensemble $\mathrm{A}^{\mathbf{N}}$ muni des lois de composition $\mathrm{S_A}$ et $\mathrm{P_A}$.

Soit $\rho : \mathrm{B} \to \mathrm{A}$ un homomorphisme d'anneaux. Nous noterons $\rho^{\mathbf{N}}$ ou encore $\mathrm{W}(\rho)$ l'application de $\mathrm{B}^{\mathbf{N}}$ dans $\mathrm{A}^{\mathbf{N}}$ qui à l'élément $\boldsymbol{b} = (b_n)_{n\in\mathbf{N}}$ de $\mathrm{B}^{\mathbf{N}}$ associe $(\rho(b_n))_{n\in\mathbf{N}}$. Il résulte aussitôt des définitions qu'on a

$$\mathrm{W}(\rho) \circ \mathrm{S_B} = \mathrm{S_A} \circ (\mathrm{W}(\rho) \times \mathrm{W}(\rho)) \tag{19}$$

$$\mathrm{W}(\rho) \circ \mathrm{P_B} = \mathrm{P_A} \circ (\mathrm{W}(\rho) \times \mathrm{W}(\rho)) \tag{20}$$

$$\mathrm{W}(\rho) \circ \mathrm{I_B} = \mathrm{I_A} \circ \mathrm{W}(\rho) \tag{21}$$

$$\rho^{\mathbf{N}} \circ \Phi_{\mathrm{B}} = \Phi_{\mathrm{A}} \circ \mathrm{W}(\rho). \tag{22}$$

Lemme 3. — *Soit* A *un anneau. Il existe un homomorphisme surjectif d'anneaux* $\rho : \mathrm{B} \to \mathrm{A}$, *où* B *est un anneau satisfaisant aux conditions suivantes : p n'est pas diviseur de* 0 *dans* B, *et il existe un endomorphisme* σ *de* B *tel que* $\sigma(b) \equiv b^p$ mod. $p.\mathrm{B}$ *pour tout* $b \in \mathrm{B}$.

Il suffit en effet de poser $\mathrm{B} = \mathbf{Z}[(\mathrm{X}_a)_{a\in\mathrm{A}}]$, de prendre pour σ l'endomorphisme de B défini par $\sigma(\mathrm{X}_a) = \mathrm{X}_a^p$ pour tout $a \in \mathrm{A}$, et pour ρ l'homomorphisme de B dans A défini par $\rho(\mathrm{X}_a) = a$ pour tout $a \in \mathrm{A}$.

THÉORÈME 1. — *a) Soit* A *un anneau* (commutatif). *Muni de l'addition* $\mathrm{S_A}$ *et de la multiplication* $\mathrm{P_A}$, W(A) *est un anneau* (commutatif). *L'élément neutre pour l'addition est la suite* $\mathbf{0}_{\mathrm{A}}$ *dont tous les termes sont nuls ; l'élément neutre pour la multiplication est la suite* $\mathbf{1}_{\mathrm{A}}$ *dont tous les termes sont nuls sauf celui d'indice* 0 *qui vaut* 1_{A}. *L'opposé d'un élément* $\boldsymbol{a}$ *de* W(A) *est* $\mathrm{I_A}(\boldsymbol{a})$.

b) Soit $\rho : B \to A$ *un homomorphisme d'anneaux. Alors* $W(\rho) : W(B) \to W(A)$ *est un homomorphisme d'anneaux.*

c) Soit A *un anneau. L'application* Φ_A *est un homomorphisme d'anneaux de* W(A) *dans l'anneau produit* $A^{\mathbf{N}}$. *En particulier, pour tout* $n \in \mathbf{N}$, *l'application* $\Phi_n : \boldsymbol{a} \mapsto \Phi_n(a_0, ..., a_n)$ *est un homomorphisme d'anneaux de* W(A) *dans* A.

Compte tenu des formules (16), (17), (19) et (20), il suffit de démontrer l'assertion *a*).

Soit $\rho : B \to A$ un homomorphisme d'anneaux satisfaisant aux conditions du lemme 3. Soit B′ le sous-anneau de $B^{\mathbf{N}}$ formé des éléments $(b_n)_{n \in \mathbf{N}}$ tels que $\sigma(b_n) \equiv b_{n+1}$ mod. $p^{n+1}.B$ pour tout $n \in \mathbf{N}$. D'après la prop. 2 du n° 2, Φ_B induit une *bijection* Φ'_B *de* W(B) *sur* B′. Au vu des formules (16) à (18) et des relations $\Phi_n(\mathbf{0}_B) = 0$ et $\Phi_n(\mathbf{1}_B) = 1_B$ ($n \in \mathbf{N}$), on voit par transport de structure que W(B) est un anneau, d'élément neutre $\mathbf{0}_B$ pour l'addition, $\mathbf{1}_B$ pour la multiplication, l'opposé de $\boldsymbol{b}$ étant $\mathbf{I}_B(\boldsymbol{b})$.

L'application $W(\rho) : W(B) \to W(A)$ est *surjective*. D'après les formules (19) et (20), la relation d'équivalence R sur W(B) associée à l'application $W(\rho)$ est compatible avec la structure d'anneau de W(B). Comme $W(\rho)$ induit une bijection Ψ de l'anneau quotient W(B)/R sur W(A), compatible avec les lois d'addition et de multiplication, l'assertion *a*) se déduit de là par transport de structure.

DÉFINITION 1. — *Soit* A *un anneau. L'anneau* W(A) *est appelé* l'anneau des vecteurs de Witt *à coefficients dans* A.

Pour $\boldsymbol{a}$ dans W(A) et n dans $\mathbf{N}$, l'élément $\Phi_n(\boldsymbol{a}) = \Phi_n(a_0, ..., a_n)$ est parfois appelé la *composante fantôme* d'indice n de $\boldsymbol{a}$.

Remarque. — Reprenons les notations de la remarque du n° 3. Soit A un anneau. Si $\boldsymbol{a}$ et $\boldsymbol{b}$ sont des éléments de $A^{\mathbf{J}}$ et $\boldsymbol{r} = (r_j)_{j \in \mathbf{J}}$ un élément de $\mathscr{A}^{\mathbf{J}}$, on note $\boldsymbol{r}_A(\boldsymbol{a}, \boldsymbol{b})$ l'élément $(r_j(\boldsymbol{a}, \boldsymbol{b}))_{j \in \mathbf{J}}$ de $A^{\mathbf{J}}$. Notons U(A) l'ensemble $A^{\mathbf{J}}$ muni des lois de composition $\boldsymbol{s}_A$ et $\boldsymbol{p}_A$. On peut montrer (p. 52, exerc. 35) que, muni de l'addition $\boldsymbol{s}_A$ et de la multiplication $\boldsymbol{p}_A$, U(A) est un anneau (commutatif) ; on l'appelle l'*anneau de Witt universel de* A. L'élément neutre pour l'addition est l'élément de U(A) dont toutes les composantes sont nulles ; l'élément neutre pour la multiplication est l'élément de U(A) dont toutes les composantes sont nulles sauf celle d'indice 1 qui vaut 1_A ; l'opposé d'un élément $\boldsymbol{a}$ de U(A) est $\boldsymbol{i}_A(\boldsymbol{a})$. L'application φ_A est un homomorphisme d'anneaux de U(A) dans l'anneau produit $A^{\mathbf{J}}$.

Soit $\rho : B \to A$ un homomorphisme d'anneaux ; on note $U(\rho)$ l'application de $B^{\mathbf{J}}$ dans $A^{\mathbf{J}}$ qui à l'élément $(b_j)_{j \in \mathbf{J}}$ de $B^{\mathbf{J}}$ associe l'élément $(\rho(b_j))_{j \in \mathbf{J}}$ de $A^{\mathbf{J}}$. On peut montrer (*loc. cit.*) que $U(\rho)$ est un homomorphisme d'anneaux de U(B) dans U(A).

5. L'homomorphisme F et le décalage V

Soit A un anneau. Dans la suite de ce paragraphe, on note respectivement $+$ et $\times$ les lois d'addition et de multiplication dans W(A). Nous écrirons aussi $\mathbf{0}$ pour $\mathbf{0}_A$ et $\mathbf{1}$

pour $\mathbf{1}_A$. On définit [1] deux applications F_A et V_A (notées aussi simplement F et V) de W(A) dans lui-même par les formules

$$F_A(\boldsymbol{a}) = (F_n(a_0, ..., a_{n+1}))_{n\in\mathbf{N}}, \tag{23}$$

$$V_A(\boldsymbol{a}) = (0, a_0, a_1, ...) \tag{24}$$

(pour $\boldsymbol{a} = (a_n)_{n\in\mathbf{N}}$ dans W(A)). L'application V_A s'appelle le *décalage*.

La formule

$$\Phi_n(F_0(\boldsymbol{a}), ..., F_n(\boldsymbol{a})) = \Phi_{n+1}(a_0, ..., a_{n+1}) \qquad (n \in \mathbf{N}) \tag{25}$$

résulte aussitôt de (15). On peut aussi l'écrire sous la forme

$$\Phi_A \circ F_A = f_A \circ \Phi_A . \tag{26}$$

La formule

$$\Phi_A \circ V_A = v_A \circ \Phi_A \tag{27}$$

résulte de la relation (3).

Soit $\rho : B \to A$ un homomorphisme d'anneaux. Les relations

$$W(\rho) \circ F_B = F_A \circ W(\rho) \tag{28}$$

$$W(\rho) \circ V_B = V_A \circ W(\rho) \tag{29}$$

résultent aussitôt des définitions.

PROPOSITION 3. — *Soit* A *un anneau.*

a) L'application F_A *est un endomorphisme de l'anneau* W(A).

b) L'application V_A *est un endomorphisme du groupe additif sous-jacent à l'anneau* W(A).

c) Pour tout $\boldsymbol{a}$ *dans* W(A), *on a* $F_A(V_A(\boldsymbol{a})) = p.\boldsymbol{a}$ (somme dans W(A) de p termes égaux à $\boldsymbol{a}$).

d) Quels que soient $\boldsymbol{a}$ *et* $\boldsymbol{b}$ *dans* W(A), *on a*

$$V_A(\boldsymbol{a} \times F_A(\boldsymbol{b})) = V_A(\boldsymbol{a}) \times \boldsymbol{b} \tag{30}$$

$$V_A(\boldsymbol{a}) \times V_A(\boldsymbol{b}) = p.V_A(\boldsymbol{a} \times \boldsymbol{b}) \tag{31}$$

(somme dans W(A) de p termes égaux à $V_A(\boldsymbol{a} \times \boldsymbol{b})$).

e) Posons $\mu = V_A(\mathbf{1}) = (0, 1, 0, ...)$. *Pour tout* $\boldsymbol{b}$ *dans* W(A), *on a*

$$V_A(F_A(\boldsymbol{b})) = \mu \times \boldsymbol{b} . \tag{32}$$

[1] La lettre F est l'initiale du nom de Frobenius, et la lettre V celle du mot allemand *Verschiebung*.

f) Pour tout élément $\boldsymbol{a}$ *de* W(A) *notons* $\boldsymbol{a}^{*p}$ *le produit dans* W(A) *de p éléments égaux à a. Alors on a*

(33) $\quad F_A(\boldsymbol{a}) \equiv \boldsymbol{a}^{*p} \text{ mod. } p.W(A)$ (idéal de W(A) engendré par $p.\mathbf{1}$).

Soit $\rho : B \to A$ un homomorphisme d'anneaux satisfaisant aux conditions du lemme 3 du n° 4. Alors $W(\rho) : W(B) \to W(A)$ est un homomorphisme *surjectif* d'anneaux, et $\Phi_B : W(B) \to B^{\mathbf{N}}$ est un homomorphisme *injectif* d'anneaux. De plus, $f_B : B^{\mathbf{N}} \to B^{\mathbf{N}}$ est un homomorphisme d'anneaux. D'après les formules (26) et (28), on a

$$\Phi_B \circ F_B = f_B \circ \Phi_B, \quad W(\rho) \circ F_B = F_A \circ W(\rho),$$

d'où aussitôt l'assertion *a*). L'assertion *b*) résulte de manière analogue des formules (27) et (29) et du fait que v_B est un endomorphisme du groupe additif sous-jacent à $B^{\mathbf{N}}$.

Soit $\boldsymbol{a}$ un élément de W(A), et choisissons un élément $\boldsymbol{x}$ de W(B) que $W(\rho)$ applique sur $\boldsymbol{a}$. Posons $\xi = \Phi_B(\boldsymbol{x})$. Il résulte aussitôt des définitions de f_B et v_B qu'on a $f_B(v_B(\xi)) = p.\xi$ (somme dans $B^{\mathbf{N}}$ de p termes égaux à ξ). D'après les formules (26) et (27) (où l'on remplace A par B), les éléments $F_B(V_B(\boldsymbol{x}))$ et $p.\boldsymbol{x}$ de W(B) ont donc même image $p.\xi$ par l'application injective Φ_B, et ainsi sont égaux. La formule $F_A(V_A(\boldsymbol{a})) = p.\boldsymbol{a}$ résulte alors des relations (28) et (29). Ceci prouve *c*).

Raisonnant de manière analogue, on ramène la démonstration de la formule (30) à celle de la relation

$$v_B(\xi f_B(\eta)) = v_B(\xi)\,\eta$$

pour ξ, η dans $B^{\mathbf{N}}$. Or cela résulte des égalités

$$\xi f_B(\eta) = (\xi_0\eta_1, \xi_1\eta_2, \ldots)$$
$$v_B(\xi)\,\eta = (0, p\xi_0\eta_1, p\xi_1\eta_2, \ldots).$$

Compte tenu de *b*) et *c*), la formule (31) résulte de la formule (30), où l'on remplace $\boldsymbol{b}$ par $V_A(\boldsymbol{b})$. La formule (32) est le cas particulier $\boldsymbol{a} = \mathbf{1}$ de la formule (30).

De façon analogue, on ramène la démonstration de la formule (33) à celle de la relation

$$f_B(\xi) \equiv \xi^p \text{ mod. } p.\Phi_B(B^{\mathbf{N}}),$$

où ξ^p désigne le produit dans $B^{\mathbf{N}}$ de p éléments égaux à ξ. Par la prop. 2, *c*) du n° 2, ceci équivaut au fait que pour tout $n \geqslant 0$, on ait

$$\sigma(\xi_{n+1} - \xi_n^p) \equiv \xi_{n+2} - \xi_{n+1}^p \text{ mod. } p^{n+2}B.$$

Or, pour tout $n \geqslant 0$, on a, par *loc. cit.*,

$$\sigma(\xi_n) \equiv \xi_{n+1} \text{ mod. } p^{n+1}B$$

puisque $\xi = \Phi_B(x)$; on en déduit, grâce au lemme 1 du n° 1,

$$\sigma(\xi_n)^p \equiv \xi_{n+1}^p \bmod. p^{n+2}B .$$

Ceci prouve la relation voulue.

Remarque. — Pour la définition d'applications analogues aux applications F et V, dans le cas de l'anneau de Witt universel, voir les exerc. 36, 37 et 38, p. 52 et suivantes.

6. Filtration et topologie de l'anneau W(A)

Lemme 4. — *Soient* A *un anneau et* $m \geqslant 1$ *un entier. On a*

$$\boldsymbol{a} = (a_0, ..., a_{m-1}, 0, ...) + (\underbrace{0, ..., 0}_{m \text{ termes}}, a_m, a_{m+1}, ...) \tag{34}$$

pour tout $\boldsymbol{a}$ *dans* W(A).

Soit $\rho : B \to A$ un homomorphisme d'anneaux satisfaisant aux conditions du lemme 3 du n° 4. Alors $W(\rho) : W(B) \to W(A)$ est un homomorphisme surjectif d'anneaux, et $\Phi_B : W(B) \to B^{\mathbf{N}}$ est un homomorphisme injectif. Il suffit donc de prouver que l'on a

$$\Phi_n(\boldsymbol{b}) = \Phi_n(b_0, ..., b_{m-1}, 0, ...) + \Phi_n(0, ..., 0, b_m, b_{m+1}, ...) \tag{35}$$

quels que soient $\boldsymbol{b}$ dans W(B) et les entiers $m \geqslant 1$, $n \geqslant 0$. Or on a

$$\begin{aligned}
\Phi_n(b_0, ..., b_{m-1}, ...) &= \Phi_n(b_0, ..., b_n) && \text{si} \quad 0 \leqslant n < m \\
&= \sum_{i=0}^{m-1} p^i . b_i^{p^{n-i}} && \text{si} \quad m \leqslant n \\
\Phi_n(0, ..., 0, b_m, b_{m+1}, ...) &= 0 && \text{si} \quad 0 \leqslant n < m \\
&= \sum_{i=m}^{n} p^i . b_i^{p^{n-i}} && \text{si} \quad m \leqslant n ,
\end{aligned}$$

d'où la formule (35).

Soit A un anneau. Pour tout entier $m \geqslant 0$, on note $V_m(A)$ l'ensemble des vecteurs de Witt $\boldsymbol{a} = (a_n)_{n \in \mathbf{N}}$ tels que $a_n = 0$ pour $0 \leqslant n < m$. C'est l'image de la puissance m-ième V^m de l'application V_A. Les formules

$$V^m(\boldsymbol{a} + \boldsymbol{b}) = V^m(\boldsymbol{a}) + V^m(\boldsymbol{b}) \tag{36}$$

$$V^m(\boldsymbol{a}) \times \boldsymbol{b} = V^m(\boldsymbol{a} \times F^m(\boldsymbol{b})) \tag{37}$$

résultent de la prop. 3 du n° 5 par récurrence sur m. Elles entraînent que $V_m(A)$ est un *idéal* de W(A).

On pose $V_m(A) = W(A)$ si $m < 0$. La suite $(V_m(A))_{m\in\mathbf{Z}}$ est une *filtration décroissante* sur le groupe additif de l'anneau W(A). Elle est compatible avec la structure d'anneau de W(A) (III, § 2, n° 1, déf. 2) si et seulement si A est un anneau de caractéristique p (*cf.* n° 3, exemple 2 et *infra*, n° 8, corollaire de la prop. 5).

Dans la suite, on munira W(A) de la topologie $\mathfrak{T}$ associée à la filtration $(V_m(A))_{m\in\mathbf{Z}}$. Comme $V_m(A)$ est un idéal de W(A) pour tout $m \in \mathbf{Z}$, la topologie $\mathfrak{T}$ est compatible avec la structure d'anneau de W(A) (TG, III, p. 49, exemple 3). Soit $\boldsymbol{a} \in W(A)$; les ensembles $\boldsymbol{a} + V_m(A)$, où m parcourt $\mathbf{N}$, forment un système fondamental de voisinages de $\boldsymbol{a}$ pour $\mathfrak{T}$. Or, il résulte du lemme 4 que $\boldsymbol{a} + V_m(A)$ se compose des vecteurs de Witt $\boldsymbol{b}$ tels que $a_i = b_i$ pour $0 \leqslant i < m$. Par suite, $\mathfrak{T}$ n'est autre que la topologie produit sur $A^{\mathbf{N}}$ de la topologie discrète sur chacun des facteurs, et W(A) est donc un *anneau topologique séparé et complet* (TG, II, p. 17, prop. 10 et TG, III, p. 22, prop. 4).

Notons τ_A (ou simplement τ) l'application de A dans W(A) qui à un élément a de A associe $(a, 0, 0, ...)$. On a $\Phi_n(\tau(a)) = a^{p^n}$ pour tout $n \in \mathbf{N}$. Pour tout homomorphisme d'anneaux $\rho : B \to A$, on a $W(\rho) \circ \tau_B = \tau_A \circ \rho$.

PROPOSITION 4. — *Soient a et b dans* A *et* $\boldsymbol{x} = (x_n)_{n\in\mathbf{N}}$ *un élément de* W(A).

a) On a les formules

$$\tau(ab) = \tau(a) \times \tau(b) \tag{38}$$

$$\tau(a) \times \boldsymbol{x} = (a^{p^n} x_n)_{n\in\mathbf{N}}\,. \tag{39}$$

b) La série de terme général $V^n(\tau(x_n))$ *est convergente dans* W(A), *de somme* $\boldsymbol{x}$.

Soit n un entier positif. Le polynôme $P_n(X_0, ..., X_n ; Y_0, ..., Y_n)$ introduit au n° 3 est isobare de poids p^n en la famille $(X_0, ..., X_n)$ lorsqu'on affecte X_i du poids p^i. On a donc

$$P_n(X_0, 0, ..., 0 ; Y_0, ..., Y_n) = X_0^{p^n} P_n(1, 0, ..., 0 ; Y_0, ..., Y_n)\,. \tag{40}$$

Comme $\mathbf{1} = (1, 0, 0, ...)$ est élément unité de l'anneau des vecteurs de Witt à coefficients dans $\mathbf{Z}[(X_n)_{n\in\mathbf{N}}, (Y_n)_{n\in\mathbf{N}}]$, on a

$$P_n(1, 0, ..., 0 ; Y_0, ..., Y_n) = Y_n\,. \tag{41}$$

Par substitution de a à X_0 et de x_i à Y_i, on déduit de (40) et (41) la relation :

$$P_n(a, 0, ..., 0 ; x_0, ..., x_n) = a^{p^n} x_n\,.$$

D'après la définition de la multiplication dans W(A), on a prouvé (39) ; la formule (38) est un cas particulier de (39).

Démontrons *b*). Par définition, $V^n(\tau(x_n))$ est la suite dont toutes les composantes sont nulles, sauf celle d'indice n qui est égale à x_n. Il résulte du lemme 4, par récurrence sur m, qu'on a

$$\sum_{n=0}^{m} V^n(\tau(x_n)) = (x_0, ..., x_m, 0, 0, ...)$$

pour tout entier $m \geqslant 0$; on en déduit *b*) par passage à la limite puisque la topologie $\mathfrak{G}$ sur W(A) est produit des topologies discrètes des facteurs A.

7. Les anneaux $W_n(A)$ des vecteurs de Witt de longueur finie

DÉFINITION 2. — *Soient* A *un anneau et* $n \geqslant 1$ *un entier. On note* $W_n(A)$ *l'anneau quotient* $W(A)/V_n(A)$.

Étant donnés des éléments $a_0, ..., a_{n-1}$ de A, on note $[a_0, ..., a_{n-1}]$ ou $[a_i]_{0 \leqslant i < n}$ la classe modulo $V_n(A)$ de l'élément $(a_0, ..., a_{n-1}, 0, 0, ...)$ de W(A). D'après le lemme 4 du n° 6, l'application $(a_0, ..., a_{n-1}) \mapsto [a_0, ..., a_{n-1}]$ de A^n dans $W_n(A)$ est une bijection. Pour cette raison, on dit que les éléments de $W_n(A)$ sont les *vecteurs de Witt de longueur n* ; par analogie, on qualifie parfois de vecteurs de Witt de longueur infinie les éléments de W(A).

On note π_n l'homomorphisme canonique de W(A) dans $W_n(A)$. D'après le lemme 4 du n° 6, on a

$$\pi_n(\boldsymbol{a}) = [a_0, ..., a_{n-1}] \tag{42}$$

pour tout $\boldsymbol{a} = (a_n)_{n \in \mathbf{N}}$ dans W(A).

D'après la définition des opérations dans W(A), on a la description suivante des opérations dans $W_n(A)$:

$$[a_0, ..., a_{n-1}] + [b_0, ..., b_{n-1}] = [S_i(a_0, ..., a_i ; b_0, ..., b_i)]_{0 \leqslant i < n}$$
$$[a_0, ..., a_{n-1}] \times [b_0, ..., b_{n-1}] = [P_i(a_0, ..., a_i ; b_0, ..., b_i)]_{0 \leqslant i < n}$$
$$- [a_0, ..., a_{n-1}] = [I_i(a_0, ..., a_i)]_{0 \leqslant i < n}.$$

De plus, l'élément neutre de l'addition dans $W_n(A)$ est $[0, ..., 0]$ et celui de la multiplication est $[1, 0, ..., 0]$.

Soit *i* un entier tel que $0 \leqslant i \leqslant n$. Par passage au quotient, l'homomorphisme Φ_i de W(A) dans A définit un homomorphisme Φ_i de $W_n(A)$ dans A. Celui-ci associe au vecteur de Witt $[a_0, ..., a_{n-1}]$ l'élément $\Phi_i(a_0, ..., a_i)$ de A (appelé aussi *composante fantôme* d'indice *i* de $[a_0, ..., a_{n-1}]$).

Soit $\rho : B \to A$ un homomorphisme d'anneaux. Par passage aux quotients, l'homomorphisme $W(\rho)$ de W(B) dans W(A) définit un homomorphisme $W_n(\rho)$ de $W_n(B)$ dans $W_n(A)$. Il se décrit par la formule

$$W_n(\rho)[b_0, ..., b_{n-1}] = [\rho(b_0), ..., \rho(b_{n-1})] \tag{43}$$

pour tout $[b_0, ..., b_{n-1}]$ dans $W_n(B)$.

Soient *m* et *n* deux entiers tels que $1 \leqslant n \leqslant m$. On a $V_n(A) \supset V_m(A)$, d'où un homomorphisme canonique de $W_m(A) = W(A)/V_m(A)$ sur $W_n(A) = W(A)/V_n(A)$; on notera $\pi_{n,m}$ cet homomorphisme. On a explicitement

$$\pi_{n,m}[a_0, ..., a_{m-1}] = [a_0, ..., a_{n-1}] \tag{44}$$

pour $[a_0, ..., a_{m-1}]$ dans $W_m(A)$. La famille $(W_n(A), \pi_{n,m})$ est un système projectif d'anneaux et l'application $\pi : a \mapsto (\pi_n(a))_{n \geqslant 1}$ est un homomorphisme d'anneaux de $W(A)$ dans $\varprojlim W_n(A)$, dit canonique. Comme $W(A)$ est séparé et complet pour la filtration $(V_n(A))_{n \in \mathbf{Z}}$ (*cf.* n° 6), l'homomorphisme canonique π est un isomorphisme d'anneaux topologiques, lorsque l'on munit $W_n(A)$ de la topologie discrète pour tout entier $n \geqslant 1$ (III, § 2, n° 6).

Désormais, les homomorphismes π_n et $\pi_{n,m}$ seront qualifiés d'*homomorphismes de projection* de $W(A)$ dans $W_n(A)$, et de $W_m(A)$ dans $W_n(A)$ respectivement.

Exemples. — 1) L'homomorphisme $\Phi_0 : W_1(A) \to A$ est un isomorphisme.

2) Explicitons les opérations dans $W_2(A)$. On a

$$[a_0, a_1] + [b_0, b_1] = \left[a_0 + b_0, a_1 + b_1 - \sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} a_0^i b_0^{p-i}\right]$$

$$[a_0, a_1] \times [b_0, b_1] = [a_0 b_0, a_0^p b_1 + a_1 b_0^p + p.a_1 b_1]$$

pour $[a_0, a_1]$ et $[b_0, b_1]$ dans $W_2(A)$. Les composantes fantômes de $[a_0, a_1]$ sont a_0 et $a_0^p + p.a_1$.

3) Soit $n \geqslant 1$ un entier. Si $a_0, ..., a_{n-1}, b_0, ..., b_{n-1}$ sont des entiers tels que $a_i \equiv b_i \bmod p$ pour $0 \leqslant i < n$, on a (n° 1, prop. 1)

$$\Phi_{n-1}(a_0, ..., a_{n-1}) \equiv \Phi_{n-1}(b_0, ..., b_{n-1}) \bmod p^n .$$

Par suite, Φ_{n-1} définit par passage aux quotients un homomorphisme d'anneaux $\varphi_n : W_n(\mathbf{Z}/p\mathbf{Z}) \to \mathbf{Z}/p^n\mathbf{Z}$. L'image de φ_n est un sous-groupe de $\mathbf{Z}/p^n\mathbf{Z}$ contenant 1, donc φ_n est surjectif. Comme les ensembles finis $W_n(\mathbf{Z}/p\mathbf{Z})$ et $\mathbf{Z}/p^n\mathbf{Z}$ ont même cardinal p^n, φ_n est un isomorphisme.

Soient m et n des entiers tels que $1 \leqslant n \leqslant m$. Il existe un seul homomorphisme d'anneaux $\alpha_{n,m} : \mathbf{Z}/p^m\mathbf{Z} \to \mathbf{Z}/p^n\mathbf{Z}$; par suite le diagramme

$$\begin{array}{ccc} \mathbf{Z}/p^m\mathbf{Z} & \xrightarrow{\alpha_{n,m}} & \mathbf{Z}/p^n\mathbf{Z} \\ \uparrow{\scriptstyle \varphi_m} & & \uparrow{\scriptstyle \varphi_n} \\ W_m(\mathbf{Z}/p\mathbf{Z}) & \xrightarrow{\pi_{n,m}} & W_n(\mathbf{Z}/p\mathbf{Z}) \end{array}$$

est commutatif. Il en résulte que $\varphi = \varprojlim \varphi_n$ est un isomorphisme d'anneaux topologiques de $W(\mathbf{Z}/p\mathbf{Z}) = \varprojlim W_n(\mathbf{Z}/p\mathbf{Z})$ sur $\mathbf{Z}_p = \varprojlim \mathbf{Z}/p^n\mathbf{Z}$ (III, § 2, n° 12, exemple 3).

Soient m et n deux entiers $\geqslant 1$. Par construction, on a une suite exacte de groupes additifs

$$\text{(E)} \qquad 0 \longrightarrow W(A) \xrightarrow{V^m} W(A) \xrightarrow{\pi_m} W_m(A) \longrightarrow 0 .$$

Par passage aux quotients, l'endomorphisme V^n du groupe additif de W(A) définit un homomorphisme V_m^n du groupe additif de $W_m(A)$ dans celui de $W_{m+n}(A)$. Autrement dit, on a un diagramme commutatif

$$\begin{array}{ccc} W(A) & \xrightarrow{V^n} & W(A) \\ \downarrow{\scriptstyle \pi_m} & & \downarrow{\scriptstyle \pi_{n+m}} \\ W_m(A) & \xrightarrow{V_m^n} & W_{n+m}(A)\,. \end{array}$$

Par passage aux quotients, on déduit de la suite exacte (E) une suite exacte

$$(E') \qquad 0 \longrightarrow W_m(A) \xrightarrow{V_m^n} W_{n+m}(A) \xrightarrow{\pi_{n,n+m}} W_n(A) \longrightarrow 0\,.$$

On a

$$(45) \qquad V_m^n[a_0, \ldots, a_{m-1}] = [\underbrace{0, \ldots, 0}_{n \text{ fois}}, a_0, \ldots, a_{m-1}]\,,$$

pour tout élément $[a_0, \ldots, a_{m-1}]$ de $W_m(A)$.

D'après la prop. 3, *c*) du n° 5, on a $FV^{m+1}(a) = p.V^m(a)$ pour tout a dans W(A) et on a par suite $F(V_{m+1}(A)) \subset V_m(A)$. Par récurrence sur n, on en déduit que F^n applique $V_{n+m}(A)$ dans $V_m(A)$, et définit donc, par passage aux quotients, un homomorphisme d'anneaux $F_m^n : W_{n+m}(A) \to W_m(A)$. Par construction, on a un diagramme commutatif

$$\begin{array}{ccc} W(A) & \xrightarrow{F^n} & W(A) \\ \downarrow{\scriptstyle \pi_{n+m}} & & \downarrow{\scriptstyle \pi_m} \\ W_{n+m}(A) & \xrightarrow{F_m^n} & W_m(A)\,. \end{array}$$

Rappelons (n° 3) que le polynôme F_i appartient à $\mathbf{Z}[X_0, \ldots, X_{i+1}]$ pour tout entier $i \geqslant 0$; l'homomorphisme F_m^1 de $W_{m+1}(A)$ dans $W_m(A)$ s'explicite donc comme suit :

$$(46) \qquad F_m^1[a_0, \ldots, a_m] = [F_i(a_0, \ldots, a_{i+1})]_{0 \leqslant i < m}\,.$$

Soient $a \in W_m(A)$, $a' \in W_m(A)$ et $b \in W_{m+1}(A)$. Les formules suivantes résultent par passages aux quotients de la prop. 3 du n° 5 :

$$(47) \qquad F_m^1(V_m^1(a)) = p.a$$

$$(48) \qquad V_m^1(a \times F_m^1(b)) = V_m^1(a) \times b$$

$$(49) \qquad V_m^1(a) \times V_m^1(a') = p.V_m^1(a \times a')$$

$$(50) \qquad V_m^1(F_m^1(b)) = \mu_{m+1} \times b$$

(avec $\mu_{m+1} = [0, 1, \underbrace{0, \ldots, 0}_{m-1 \text{ fois}}]$).

8. L'anneau des vecteurs de Witt à coefficients dans un anneau de caractéristique p

PROPOSITION 5. — *Soit* A *un anneau de caractéristique* p (A, V, p. 2). *Quels que soient les éléments* $\boldsymbol{a}$ *et* $\boldsymbol{b}$ *de* W(A), *et les entiers positifs* m, n, *on a, si* $\boldsymbol{a} = (a_n)_{n\in\mathbf{N}}$,

$$\mathrm{F}(\boldsymbol{a}) = (a_n^p)_{n\in\mathbf{N}} \tag{51}$$

$$p.\boldsymbol{a} = \mathrm{VF}(\boldsymbol{a}) = \mathrm{FV}(\boldsymbol{a}) = (0, a_0^p, a_1^p, \ldots) \tag{52}$$

$$\mathrm{V}^m(\boldsymbol{a}) \times \mathrm{V}^n(\boldsymbol{b}) = \mathrm{V}^{m+n}(\mathrm{F}^n(\boldsymbol{a}) \times \mathrm{F}^m(\boldsymbol{b})). \tag{53}$$

La formule (51) résulte de l'exemple 4 du n° 3. On déduit aussitôt de là l'égalité

$$\mathrm{VF}(\boldsymbol{a}) = \mathrm{FV}(\boldsymbol{a}) = (0, a_0^p, a_1^p, \ldots),$$

et l'égalité $p.\boldsymbol{a} = \mathrm{FV}(\boldsymbol{a})$ a été prouvée (n° 5, prop. 3), d'où (52).

Prouvons (53). D'après la formule (37) (où l'on substitue $\mathrm{V}^n(\boldsymbol{b})$ à $\boldsymbol{b}$), on a

$$\mathrm{V}^m(\boldsymbol{a}) \times \mathrm{V}^n(\boldsymbol{b}) = \mathrm{V}^m(\boldsymbol{a} \times \mathrm{F}^m(\mathrm{V}^n(\boldsymbol{b}))). \tag{54}$$

De la formule (37), on déduit aussi

$$\mathrm{V}^n(\mathrm{F}^m(\boldsymbol{b})) \times \boldsymbol{a} = \mathrm{V}^n(\mathrm{F}^m(\boldsymbol{b}) \times \mathrm{F}^n(\boldsymbol{a})). \tag{55}$$

La formule (53) résulte alors de (54) et (55) et de la relation $\mathrm{F}^m \circ \mathrm{V}^n = \mathrm{V}^n \circ \mathrm{F}^m$, elle-même conséquence de (51).

COROLLAIRE. — *Si* m *et* n *sont deux entiers positifs, on a*

$$\mathrm{V}_m(\mathrm{A}) \times \mathrm{V}_n(\mathrm{A}) \subset \mathrm{V}_{m+n}(\mathrm{A}).$$

Cela résulte de la formule (53), car $\mathrm{V}_m(\mathrm{A})$ est l'image de $\mathrm{V}^m : \mathrm{W}(\mathrm{A}) \to \mathrm{W}(\mathrm{A})$.

PROPOSITION 6. — *Soit* A *un anneau.*

a) Pour tout entier $k \geqslant 1$, *on a* $(\mathrm{V}_1(\mathrm{A}))^k = p^{k-1}.\mathrm{V}_1(\mathrm{A})$.

b) Supposons que A *soit un anneau de caractéristique* p. *Sur l'anneau* W(A), *la topologie* $\mathrm{V}_1(\mathrm{A})$*-adique et la topologie* p*-adique coïncident, et elles sont plus fines que la topologie produit* $\mathfrak{T}$ (*cf.* n° 6). *L'anneau* W(A) *est séparé et complet pour la topologie* p*-adique.*

Prouvons *a*) par récurrence sur k. Le cas $k = 1$ est évident. Supposons $k \geqslant 2$. D'après l'hypothèse de récurrence, on a $\mathrm{V}_1(\mathrm{A})^{k-1} = p^{k-2}.\mathrm{V}_1(\mathrm{A})$ et par suite $\mathrm{V}_1(\mathrm{A})^k = p^{k-2}.(\mathrm{V}_1(\mathrm{A}))^2$. Mais il résulte de la prop. 3, *d*), formule (31), du n° 5 qu'on a $(\mathrm{V}_1(\mathrm{A}))^2 = p.\mathrm{V}_1(\mathrm{A})$, d'où *a*).

Supposons maintenant que A soit de caractéristique p. Comme on a

$$p.\mathrm{W}(\mathrm{A}) = \mathrm{VF}(\mathrm{W}(\mathrm{A})) \subset \mathrm{V}_1(\mathrm{A}) \quad \text{(formule (52))},$$

on déduit de *a*) les inclusions $p^k.\mathrm{W}(\mathrm{A}) \subset (\mathrm{V}_1(\mathrm{A}))^k \subset p^{k-1}.\mathrm{W}(\mathrm{A})$, et du corollaire à la prop. 5 l'inclusion $(\mathrm{V}_1(\mathrm{A}))^k \subset \mathrm{V}_k(\mathrm{A})$, pour tout entier $k \geqslant 1$. La première assertion de *b*) en résulte.

Soit k un entier $\geqslant 1$. D'après la formule (52), l'idéal $p^k.\mathrm{W}(\mathrm{A})$ de $\mathrm{W}(\mathrm{A})$ est l'ensemble des éléments $\boldsymbol{a} = (a_n)_{n\in\mathbf{N}}$ de $\mathrm{W}(\mathrm{A})$ tels qu'on ait $a_n = 0$ pour $n < k$ et $a_n \in \mathrm{A}^{p^k}$ pour $n \geqslant k$. Il est donc fermé pour la topologie $\mathfrak{C}$. Comme $\mathrm{W}(\mathrm{A})$ est séparé et complet pour la topologie $\mathfrak{C}$ (n° 6) et que les idéaux $p^k.\mathrm{W}(\mathrm{A})$ de $\mathrm{W}(\mathrm{A})$, pour $k \geqslant 1$, forment une base de voisinages de $\mathbf{0}$ dans $\mathrm{W}(\mathrm{A})$ pour la topologie p-adique, l'anneau $\mathrm{W}(\mathrm{A})$ est séparé et complet pour la topologie p-adique (TG, III, p. 26, cor. 1 à la prop. 10).

PROPOSITION 7. — *Soit* A *un anneau parfait de caractéristique p.*

a) *Pour tout élément* $\boldsymbol{a} = (a_n)_{n\in\mathbf{N}}$ *de* $\mathrm{W}(\mathrm{A})$, *la série de terme général* $p^n\tau(a_n^{p^{-n}})$ *est convergente dans* $\mathrm{W}(\mathrm{A})$, *de somme* $\boldsymbol{a}$.

b) *Sur* $\mathrm{W}(\mathrm{A})$, *la topologie* $\mathrm{V}_1(\mathrm{A})$*-adique, la topologie p-adique et la topologie* $\mathfrak{C}$ *coïncident. Plus précisément, on a* $\mathrm{V}_n(\mathrm{A}) = p^n.\mathrm{W}(\mathrm{A}) = (\mathrm{V}_1(\mathrm{A}))^n$ *pour tout entier* $n \geqslant 0$. *En particulier* Φ_0 *définit un isomorphisme de* $\mathrm{W}(\mathrm{A})/p.\mathrm{W}(\mathrm{A})$ *sur* A.

Par définition (A, V, p. 5), l'application $a \mapsto a^p$ est un automorphisme de l'anneau A. D'après la prop. 5, F est donc un automorphisme de l'anneau $\mathrm{W}(\mathrm{A})$, et l'on a, pour tout $n \in \mathbf{N}$,

$$p^n.\mathrm{W}(\mathrm{A}) = \mathrm{V}^n\mathrm{F}^n(\mathrm{W}(\mathrm{A})) = \mathrm{V}^n(\mathrm{W}(\mathrm{A})) = \mathrm{V}_n(\mathrm{A}).$$

En particulier, on a $(\mathrm{V}_1(\mathrm{A}))^n = (p.\mathrm{W}(\mathrm{A}))^n = p^n.\mathrm{W}(\mathrm{A})$. L'assertion *b*) résulte de là.

D'après la prop. 5, on a

$$p^n.\tau(a_n^{p^{-n}}) = \mathrm{V}^n\mathrm{F}^n\tau(a_n^{p^{-n}}) = \mathrm{V}^n\tau(a_n),$$

et l'assertion *a*) résulte de la prop. 4 du n° 6.

PROPOSITION 8. — *Soit* A *un corps de caractéristique p. L'anneau* $\mathrm{W}(\mathrm{A})$ *est un anneau local intègre séparé et complet, d'idéal maximal* $\mathrm{V}_1(\mathrm{A})$ *et de corps résiduel isomorphe à* A. *Si le corps* A *est parfait, l'anneau* $\mathrm{W}(\mathrm{A})$ *est un anneau de valuation discrète, et son idéal maximal est* $p.\mathrm{W}(\mathrm{A})$.

L'homomorphisme Φ_0 définit un isomorphisme de $\mathrm{W}(\mathrm{A})/\mathrm{V}_1(\mathrm{A})$ sur A (n° 7, exemple 1). L'idéal $\mathrm{V}_1(\mathrm{A})$ de $\mathrm{W}(\mathrm{A})$ est donc maximal. Comme l'anneau $\mathrm{W}(\mathrm{A})$ est séparé et complet pour la topologie $\mathrm{V}_1(\mathrm{A})$-adique (prop. 6, *b*)), c'est un anneau local, d'idéal maximal $\mathrm{V}_1(\mathrm{A})$ (III, § 2, n° 13, prop. 19).

Soient $\boldsymbol{a}$ et $\boldsymbol{b}$ deux éléments non nuls de $\mathrm{W}(\mathrm{A})$. Il existe des entiers $m \geqslant 0$ et $n \geqslant 0$, et des éléments $\boldsymbol{a}' = (a'_n)_{n\in\mathbf{N}}$ et $\boldsymbol{b}' = (b'_n)_{n\in\mathbf{N}}$ de $\mathrm{W}(\mathrm{A})$ tels que $\boldsymbol{a} = \mathrm{V}^m(\boldsymbol{a}')$, $\boldsymbol{b} = \mathrm{V}^n(\boldsymbol{b}')$ et que les éléments a'_0 et b'_0 de A soient non nuls. Alors la composante d'indice $m+n$ de $\boldsymbol{a} \times \boldsymbol{b}$ est égale à la composante d'indice 0 de $\mathrm{F}^n(\boldsymbol{a}') \times \mathrm{F}^m(\boldsymbol{b}')$ (formule (53)), c'est-à-dire à $a'^{p^n}_0 b'^{p^m}_0$ (formule (51) et n° 3, exemple 2). Par suite $\boldsymbol{a} \times \boldsymbol{b}$ est non nul et $\mathrm{W}(\mathrm{A})$ est intègre.

Si le corps A est parfait, l'idéal maximal $\mathrm{V}_1(\mathrm{A})$ de $\mathrm{W}(\mathrm{A})$ est égal à $p.\mathrm{W}(\mathrm{A})$

(prop. 7, *b*)) et par suite W(A) est un anneau de valuation discrète (VI, § 3, n° 6, prop. 9, *c*)).

Remarques. — 1) Soit A un corps de caractéristique p. On peut montrer que l'anneau W(A) est noethérien si et seulement si A est parfait (p. 43, exerc. 9).

2) Soit A un anneau de caractéristique p. D'après la prop. 5, on a les formules

$$F_m^n[a_0, ..., a_{n+m-1}] = [a_0^{p^n}, ..., a_{m-1}^{p^n}]$$

$$p^n.[a_0, ..., a_{n+m-1}] = [\underbrace{0, ..., 0}_{n \text{ fois}}, a_0^{p^n}, ..., a_{m-1}^{p^n}]$$

pour tout vecteur de Witt $[a_0, ..., a_{n+m-1}]$ de longueur $n + m$.

En fait, l'application $F : W(A) \to W(A)$ permet, par passage aux quotients par $V_m(A)$, de définir une application $\overline{F}_m : W_m(A) \to W_m(A)$. On a la formule

$$\overline{F}_m[a_0, ..., a_{m-1}] = [a_0^p, ..., a_{m-1}^p] .$$

Les applications $V_m^1 \circ \overline{F}_m$ et $\overline{F}_{m+1} \circ V_m^1$ de $W_m(A)$ dans $W_{m+1}(A)$ sont égales et sont déduites, par passage au quotient, de la multiplication par p dans $W_{m+1}(A)$.

§ 2. ANNEAUX DE COHEN

Dans tout ce paragraphe, p désigne un nombre premier.

1. *p*-anneaux

DÉFINITION 1. — *On dit qu'un anneau* C *est un p-anneau si l'idéal* pC *de* C *est maximal, et si* C *est séparé et complet pour la topologie* pC*-adique.*

Soit C un anneau ; si $p1_C$ est nilpotent et si l'idéal pC de C est maximal, C est un p-anneau, car la topologie pC-adique de C est discrète. Plus particulièrement, tout corps de caractéristique p est un p-anneau.

PROPOSITION 1. — *Soit* C *un p-anneau.*

a) L'anneau C *est local, d'idéal maximal* pC.

b) Supposons $p1_C$ *nilpotent. Soit d le plus petit entier positif tel que* $p^d 1_C = 0$. *Les idéaux de* C *sont de la forme* p^kC *avec* $0 \leqslant k \leqslant d$ *et l'on a* $p^k C \neq p^l C$ *lorsque k et l sont deux entiers distincts vérifiant* $0 \leqslant k \leqslant d, 0 \leqslant l \leqslant d$. *Le* C*-module* C *est de longueur d.*

c) Supposons que $p1_C$ *ne soit pas nilpotent. Alors* C *est un anneau de valuation discrète dont le corps résiduel est de caractéristique p, et le corps des fractions de caractéristique* 0. *Les idéaux de la forme* p^nC, *avec* $n \in \mathbf{N}$, *sont deux à deux distincts ; ils forment tous les idéaux non nuls de* C. *Le* C*-module* C *n'est pas de longueur finie.*

L'assertion *a*) résulte de la prop. 19 de III, § 2, n° 13.

On a $\bigcap_{n\geqslant 0} p^n C = \{0\}$ par hypothèse. Soit $x \neq 0$ dans C ; il existe un entier $n \geqslant 0$ tel que $x \in p^n C$, $x \notin p^{n+1} C$; il existe donc un élément y de C tel que $x = p^n y$; comme y n'appartient pas à pC, y est inversible.

Supposons que $p1_C$ ne soit pas nilpotent. Si x et x' sont deux éléments non nuls de C, il existe deux entiers $n \geqslant 0$, $n' \geqslant 0$ et deux éléments inversibles y, y' de C tels que $x = p^n y$, $x' = p^{n'} y'$. On a alors $xx' = p^{n+n'} yy' \neq 0$, donc C est intègre. Comme C est un anneau local, mais n'est pas un corps et que l'idéal maximal $\mathfrak{m}_C = pC$ de C est principal, C est un anneau de valuation discrète (VI, § 3, n° 6, prop. 9). Les idéaux non nuls de C sont alors de la forme $p^n C$ d'après *loc. cit.*, prop. 8, et sont deux à deux distincts. En particulier, l'anneau C n'est pas artinien, donc le C-module C n'est pas de longueur finie. Le corps résiduel C/pC de C est de caractéristique p. Soit q la caractéristique du corps des fractions de C. On a $p1_C \neq 0$, d'où $p \neq q$. Par ailleurs, si q était non nulle, on aurait $q1_C = 0$ donc C/pC serait de caractéristique $q \neq p$, ce qui est absurde. Ceci prouve *c*).

Supposons que $p1_C$ soit nilpotent. Soit d le plus petit entier positif tel que $p^d 1_C = 0$. On a une suite d'idéaux

$$\text{(E)} \qquad C \supset pC \supset p^2C \supset \ldots \supset p^{d-1}C \supset p^d C = \{0\}.$$

Si k est un entier tel que $0 \leqslant k < d$ et $p^k C = p^{k+1} C$, on en déduit

$$p^{d-k-1} p^k C = p^{d-k-1} p^{k+1} C = \{0\}$$

contrairement à l'hypothèse $p^{d-1} 1_C \neq 0$. Donc les éléments de la suite (E) sont deux à deux distincts. Soit $\mathfrak{a}$ un idéal de C et soit k le plus petit entier positif tel que $\mathfrak{a} \supset p^k C$. Soit x un élément non nul de $\mathfrak{a}$; on a vu que x est de la forme $p^m u$ avec $m \geqslant 0$ et u inversible dans C. On a donc $p^m C \subset \mathfrak{a}$, d'où $m \geqslant k$, et finalement $x \in p^k C$. En conclusion, on a $\mathfrak{a} = p^k C$. La suite (E) est alors une suite de Jordan-Hölder du C-module C, qui est de longueur d.

COROLLAIRE 1. — *Si le p-anneau* C *est intègre, c'est un anneau de valuation discrète, ou un corps de caractéristique p.*

Supposons C intègre. Si $p1_C$ est nilpotent, on a $p1_C = 0$, et $\{0\}$ est un idéal maximal de C, donc C est un corps de caractéristique p. Si $p1_C$ n'est pas nilpotent, alors C est un anneau de valuation discrète d'après la prop. 1, *c*).

COROLLAIRE 2. — *Soient* C *un p-anneau et* $\mathfrak{a}$ *un idéal de* C *distinct de* C. *L'anneau* $C/\mathfrak{a}$ *est un p-anneau.*

On peut supposer $\mathfrak{a} \neq \{0\}$. Il existe alors un entier $i \geqslant 1$ tel que $\mathfrak{a} = p^i C$; l'idéal $pC/\mathfrak{a}$ de $C/\mathfrak{a}$ est maximal et l'on a $p^i 1_{C/\mathfrak{a}} = 0$, donc $C/\mathfrak{a}$ est un p-anneau.

Soit C un p-anneau. On appelle *longueur de* C, et l'on note $l(C)$, la borne supérieure dans $\overline{\mathbf{R}}$ de l'ensemble des entiers $n \geqslant 1$ tels que $p^{n-1} 1_C \neq 0$. Lorsque $l(C)$ est finie, c'est la longueur du C-module C, et lorsque $l(C)$ est égale à $+\infty$, le C-module C n'est pas de longueur finie (prop. 1).

Exemples. — 1) Pour tout entier $n \geqslant 1$, l'anneau $\mathbf{Z}/p^n\mathbf{Z}$ est un p-anneau de longueur n. L'anneau $\mathbf{Z}_p$ des entiers p-adiques est un p-anneau de longueur infinie.

2) Soit K un corps *parfait* de caractéristique p. D'après la prop. 8 du § 1, n° 8, l'anneau W(K) des vecteurs de Witt est un p-anneau de longueur infinie. L'application $(a_n)_{n\in\mathbf{N}} \mapsto a_0$ induit par passage au quotient un isomorphisme de W(K)/pW(K) sur le corps K (*loc. cit.*, prop. 7). Pour tout entier $n \geqslant 1$, l'anneau

$$\mathrm{W}_n(\mathrm{K}) = \mathrm{W}(\mathrm{K})/p^n\mathrm{W}(\mathrm{K})$$

est un p-anneau de longueur n.

PROPOSITION 2. — *Soient* C *et* C′ *deux p-anneaux et u un homomorphisme de* C *dans* C′. *Soit v l'homomorphisme de* $\kappa_{\mathrm{C}} = \mathrm{C}/p\mathrm{C}$ *dans* $\kappa_{\mathrm{C}'} = \mathrm{C}'/p\mathrm{C}'$ *déduit de u par passage aux quotients.*

a) On a $l(\mathrm{C}) \geqslant l(\mathrm{C}')$ *et u est injectif si et seulement si l'on a* $l(\mathrm{C}) = l(\mathrm{C}')$.

b) Pour que u soit surjectif, il faut et il suffit que v soit un isomorphisme.

c) Pour que u soit un isomorphisme, il faut et il suffit que v soit un isomorphisme et qu'on ait $l(\mathrm{C}) = l(\mathrm{C}')$.

Soit $n \geqslant 1$ un entier. On a $u(p^{n-1}1_{\mathrm{C}}) = p^{n-1}1_{\mathrm{C}'}$, donc la relation $p^{n-1}1_{\mathrm{C}'} \neq 0$ entraîne $p^{n-1}1_{\mathrm{C}} \neq 0$ et lui est équivalente si u est injectif. On a donc $l(\mathrm{C}') \leqslant l(\mathrm{C})$ avec égalité si u est injectif. Si u n'est pas injectif, il existe un entier $i < l(\mathrm{C})$ tel que le noyau de u soit l'idéal $p^i\mathrm{C}$ de C ; on a alors $p^i 1_{\mathrm{C}'} = 0$, d'où $l(\mathrm{C}') \leqslant i$. Ceci prouve *a*).

Comme κ_{C} et $\kappa_{\mathrm{C}'}$ sont des corps, l'homomorphisme v est injectif. Si u est surjectif, il en est de même de v qui est donc un isomorphisme. Réciproquement, supposons v surjectif. Alors pour tout entier $n \geqslant 0$, l'application $v_n : p^n\mathrm{C}/p^{n+1}\mathrm{C} \to p^n\mathrm{C}'/p^{n+1}\mathrm{C}'$ déduite de u est surjective. Comme C est complet pour la filtration pC-adique et C′ séparé pour la filtration pC′-adique, u est surjectif d'après le cor. 2 du th. 1 de III, § 2, n° 8. Ceci prouve *b*).

Enfin, *c*) résulte de *a*) et *b*).

PROPOSITION 3. — *Soit* $(\mathrm{C}_n, \pi_{n,m})$ *un système projectif d'anneaux relatif à l'ensemble d'indices* N. *On suppose que* C_n *est un p-anneau pour tout* $n \in \mathbf{N}$ *et que les homomorphismes* $\pi_{n,m}$ *sont surjectifs. Alors* $\mathrm{C} = \varprojlim \mathrm{C}_n$ *est un p-anneau, et pour tout* $n \in \mathbf{N}$, *l'homomorphisme canonique* $\pi_n : \mathrm{C} \to \mathrm{C}_n$ *est surjectif et induit un isomorphisme de* κ_{C} *sur* κ_{C_n}.

Comme les applications $\pi_{n,m}$ sont surjectives, il en est de même des applications π_n (E, III, p. 58, prop. 5). Montrons que C est un p-anneau. Soit d_n la longueur de C_n. D'après la prop. 2, *a*), la suite des éléments d_n de $\mathbf{N} \cup \{+\infty\}$ est croissante ; si elle est stationnaire, il existe un entier n_0 tel que $\pi_{n,m}$ soit un isomorphisme de C_m sur C_n lorsque $n_0 \leqslant n \leqslant m$, de sorte que C, isomorphe à C_{n_0}, est un p-anneau.

Il suffit donc de considérer le cas où chaque d_n est fini, et où la suite (d_n) tend vers $+\infty$. Munissons l'anneau C de la filtration triviale (III, § 2, n° 1, exemple 5). Pour $n \in \mathbf{N}$, soit I_n le noyau de π_n ; posons $\mathrm{I}_n = \mathrm{C}$ si $n < 0$. Notons E le C-module C muni de la filtration $(\mathrm{I}_n)_{n\in\mathbf{Z}}$. Il est séparé et complet, car la topologie $\mathfrak{T}$ définie par la filtration $(\mathrm{I}_n)_{n\in\mathbf{Z}}$ est la topologie limite projective des topologies discrètes sur les C_n.

Soit k un entier $\geqslant 1$. On a $p^k C \subset \varprojlim(p^k C_n)$ (E, III, p. 55, formule (9)). Réciproquement, si $x = (x_n)_{n\in\mathbf{N}} \in \varprojlim(p^k C_n)$ et si on pose $X_n = \{y \in C | \pi_n(p^k y) = x_n\}$, la suite $(X_n)_{n\in\mathbf{N}}$ est une suite décroissante de parties affines fermées non vides de E. Comme E/I_n est un C-module artinien, l'intersection des X_n est non vide (III, § 2, n° 7, prop. 7); pour tout $z \in \bigcap_{n\in\mathbf{N}} X_n$, on a $p^k z = x$. Nous avons donc prouvé qu'on a $p^k C = \varprojlim p^k C_n$ pour tout entier $k \geqslant 1$. En particulier l'idéal $p^k C$ de C est fermé pour la topologie $\mathfrak{C}$. Sur C, la topologie p-adique est plus fine que la topologie $\mathfrak{C}$ car on a $p^{d_n} C \subset I_n$. Il résulte alors de TG, III, p. 26, cor. 1 à la prop. 10, que C est séparé et complet pour la topologie pC-adique. En outre on a $pC = \varprojlim pC_n = \pi_0^{-1}(pC_0)$ et donc l'homomorphisme surjectif de C/pC dans C_0/pC_0 déduit de π_0 est un isomorphisme. Ceci montre que l'idéal pC de C est maximal et par suite que C est un p-anneau. La dernière assertion de la prop. 3 résulte de la prop. 2, *b*).

2. Anneaux de Cohen

DÉFINITION 2. — *Soit* A *un anneau local séparé et complet, dont le corps résiduel est de caractéristique p. On appelle sous-anneau de Cohen de* A *un sous-anneau* C *de* A *qui est un p-anneau tel que* $A = \mathfrak{m}_A + C$ (i.e. $A/\mathfrak{m}_A = C/(\mathfrak{m}_A \cap C)$).

Si C est un sous-anneau de Cohen de A, l'idéal $\mathfrak{m}_A \cap C$ de C est maximal, donc égal à pC. L'application canonique de $\kappa_C = C/pC$ sur $\kappa_A = A/\mathfrak{m}_A$ est donc un isomorphisme de corps.

Exemple. — Soit C un p-anneau. L'anneau de séries formelles $A = C[[T_1, ..., T_n]]$ est un anneau noethérien, local, séparé et complet, dont l'idéal maximal est engendré par la suite $(p, T_1, ..., T_n)$. Il est immédiat que C est un sous-anneau de Cohen de A. Ceci s'applique en particulier lorsque C est égal à $\mathbf{Z}_p$, à $\mathbf{Z}/p^n\mathbf{Z}$ ou à un corps de caractéristique p.

THÉORÈME 1. — *Soit* A *un anneau local, séparé et complet, dont le corps résiduel k est de caractéristique p. Soit* π *l'application canonique de* A *sur k, et soit* S *une partie de* A, *telle que* π *induise une bijection de* S *sur une p-base de k* (A, V, p. 95).

a) *Il existe un sous-anneau de Cohen* C *de* A *contenant* S, *et un seul.*

b) *Le sous-anneau* C *de* A *est fermé, et la topologie pC-adique de* C *est induite par la topologie* $\mathfrak{m}_A$*-adique de* A.

c) *Tout sous-anneau fermé* A′ *de* A, *contenant* S, *et tel que* $A = A' + \mathfrak{m}_A$, *contient* C.

A) *Cas particulier* : $\mathfrak{m}_A$ *nilpotent*

Soit n un entier positif tel que $\mathfrak{m}_A^{n+1} = \{0\}$. Si Φ_n est le n-ième polynôme de Witt (§ 1, n° 1), l'application $u : [a_0, ..., a_n] \mapsto \Phi_n(a_0, ..., a_n)$ est un homomorphisme d'anneaux de $W_{n+1}(A)$ dans A (§ 1, n° 7). Soit B_n l'image de u et soit C_n le sous-anneau de A engendré par $B_n \cup S$.

Lemme 1. — *Soit* A′ *un sous-anneau de* A *contenant* S. *Pour que* A′ *contienne* C_n, *il faut et il suffit qu'on ait* $A' + \mathfrak{m}_A = A$.

On a $pA \subset \mathfrak{m}_A$ et B_n se compose des éléments de la forme $a_0^{p^n} + pa_1^{p^{n-1}} + \cdots + p^n a_n$ avec $a_0, ..., a_n$ dans A. Par suite, on a $\pi(B_n) = k^{p^n}$, d'où $\pi(C_n) = k^{p^n}[\pi(S)]$. Mais comme $\pi(S)$ est une p-base de k, on a $k = k^{p^n}[\pi(S)]$ (A, V, p. 96), d'où $\pi(C_n) = k$, c'est-à-dire $C_n + \mathfrak{m}_A = A$.

Soit A′ un sous-anneau de A contenant S. Si A′ contient C_n, on a

$$A' + \mathfrak{m}_A \supset C_n + \mathfrak{m}_A = A, \quad \text{d'où} \quad A' + \mathfrak{m}_A = A.$$

Réciproquement, supposons qu'on ait $A' + \mathfrak{m}_A = A$. Soient $a_0, ..., a_n$ des éléments de A ; il existe par hypothèse des éléments $a'_0, ..., a'_n$ de A′ tels que $a_i \equiv a'_i \bmod \mathfrak{m}_A$ pour $0 \leqslant i \leqslant n$. D'après la prop. 1 du § 1, n° 1 et l'hypothèse $\mathfrak{m}_A^{n+1} = \{0\}$, on a donc $\Phi_n(a_0, ..., a_n) = \Phi_n(a'_0, ..., a'_n) \in A'$, d'où $B_n \subset A'$. Comme C_n est l'anneau engendré par $B_n \cup S$, on a $C_n \subset A'$.

Dans l'ensemble $\mathfrak{S}$ des sous-anneaux A′ de A contenant S et tels que $A' + \mathfrak{m}_A = A$, il existe d'après le lemme 1 un plus petit élément C, et l'on a $C_n = C$ pour tout entier $n \geqslant 0$ tel que $\mathfrak{m}_A^{n+1} = \{0\}$.

On a $C + \mathfrak{m}_A = A$ par construction et $p1_C$ est nilpotent. On a évidemment $pC \subset C \cap \mathfrak{m}_A$ et le lemme 2 qui suit montre donc que pC est un idéal maximal de C et par suite que C est un sous-anneau de Cohen de A.

Lemme 2. — *On a* $C \cap \mathfrak{m}_A \subset pC$.

Choisissons un entier $m \geqslant 1$ tel que $\mathfrak{m}_A^m = \{0\}$, d'où $C = C_m = C_{m-1}$. Soit Λ la partie de $\mathbf{N}^{(S)}$ formée des familles à support fini d'entiers $(\alpha_s)_{s \in S}$ satisfaisant à $0 \leqslant \alpha_s < p^m$ pour tout $s \in S$. Comme B_m contient $s^{p^m} = \Phi_m(s, 0, ..., 0)$ pour tout $s \in S$, les monômes $Z_\alpha = \prod_{s \in S} s^{\alpha_s}$, où α parcourt Λ, engendrent C_m comme B_m-module. De plus, d'après la formule

$$\Phi_m(a_0, ..., a_m) = a_0^{p^m} + p\Phi_{m-1}(a_1, ..., a_m),$$

tout élément de B_m est de la forme $a^{p^m} + pb$ avec $a \in A$ et $b \in B_{m-1}$. Par suite tout élément de $C = C_m$ est de la forme

$$x = \sum_{\alpha \in \Lambda} c_\alpha^{p^m} Z_\alpha + py \tag{1}$$

avec $c_\alpha \in A$ pour tout $\alpha \in \Lambda$, et $y \in C_{m-1} = C$. Si x appartient à $C \cap \mathfrak{m}_A$, on a $\pi(x) = 0$ d'où $\sum_{\alpha \in \Lambda} \pi(c_\alpha)^{p^m} \pi(Z_\alpha) = 0$. Comme $\pi(S)$ est une p-base de k, on a $\pi(c_\alpha) = 0$ pour tout $\alpha \in \Lambda$ d'après A, V, p. 96. On a alors $c_\alpha \in \mathfrak{m}_A$, d'où $c_\alpha^m = 0$ et *a fortiori* $c_\alpha^{p^m} = 0$. D'après (1), on a $x = py$, d'où le lemme 2.

On a $p^m C = \mathfrak{m}_A^m = \{0\}$ pour m assez grand et l'assertion *b*) est donc triviale. L'assertion *c*) résulte du lemme 1. Si C′ est un sous-anneau de Cohen de A contenant S, on a $C' \supset C$ d'après le lemme 1. Mais comme l'inclusion de C dans C′ induit un

isomorphisme de κ_C sur $\kappa_{C'}$, on a $C = C'$ (n° 1, prop. 2, *b*)), et ceci achève de prouver *a*).

B) *Cas général*

Pour tout entier $n \geqslant 0$, notons A_n l'anneau local $A/\mathfrak{m}_A^{n+1}$, $\mathfrak{m}_n = \mathfrak{m}_A/\mathfrak{m}_A^{n+1}$ son idéal maximal et π_n l'homomorphisme canonique de A sur A_n. D'après A), il existe un unique sous-anneau de Cohen C_n de A_n contenant $\pi_n(S)$. Lorsque $0 \leqslant n \leqslant m$, on note $\pi_{n,m}$ l'homomorphisme canonique de A_m sur A_n. D'après le cor. 2 de la prop. 1 du n° 1, $\pi_{n,m}(C_m)$ est un *p*-anneau ; on a $\pi_{n,m}(C_m) + \mathfrak{m}_n = A_n$, donc $\pi_{n,m}(C_m)$ est égal au sous-anneau de Cohen C_n de A_n. D'après la prop. 3 du n° 1, le sous-anneau $\varprojlim C_n$ de $\varprojlim A_n$ est un *p*-anneau. Posons $C = \bigcap_{n\in\mathbf{N}} \pi_n^{-1}(C_n)$. Comme C est l'image réciproque de $\varprojlim C_n$ par l'isomorphisme $a \mapsto (\pi_n(a))_{n\in\mathbf{N}}$ de A sur $\varprojlim A_n$, c'est un sous-anneau fermé de A, et un *p*-anneau. On a $\pi_n(C) = C_n$ pour tout $n \in \mathbf{N}$ (n° 1, prop. 3), et en particulier $\pi_0(C) = A_0$, c'est-à-dire $\pi(C) = k$. Donc C est un sous-anneau de Cohen de A.

Pour tout entier $n \geqslant 0$, posons $J_n = C \cap \mathfrak{m}_A^n$. Comme l'anneau local A est séparé, on a $\bigcap_{n\in\mathbf{N}} J_n = \{0\}$, et vu la structure des idéaux d'un *p*-anneau (n° 1, prop. 1), tout idéal de C de la forme p^kC contient l'un des J_n. Réciproquement, J_n contient p^nC. Par suite, la topologie *p*C-adique de C est induite par la topologie $\mathfrak{m}_A$-adique de A. Ceci prouve *b*).

Soit A' un sous-anneau fermé de A, contenant S et tel que $A' + \mathfrak{m}_A = A$. Comme A' est fermé, on a $A' = \bigcap_{n\in\mathbf{N}} \pi_n^{-1}(\pi_n(A'))$. On a $\pi_n(A') \supset \pi_n(S)$ et $\pi_n(A') + \mathfrak{m}_n = A_n$, d'où $\pi_n(A') \supset C_n$ d'après ce qu'on a vu en A). Finalement, on a $\pi_n^{-1}(\pi_n(A')) \supset \pi_n^{-1}(C_n)$ d'où $A' \supset C$. Ceci prouve *c*). On en déduit l'unicité d'un sous-anneau de Cohen comme en A).

Remarque. — Supposons que $p1_A$ ne soit pas nilpotent (ceci a lieu en particulier lorsque A est un anneau intègre dont le corps des fractions est de caractéristique 0). Alors C est un anneau de valuation discrète dont le corps des fractions est de caractéristique 0.

3. Existence et unicité des *p*-anneaux

PROPOSITION 4. — *Soient* C *et* C' *deux p-anneaux tels que* $l(C) \geqslant l(C')$, π (resp. π') *l'homomorphisme canonique de* C (resp. C') *sur* κ_C (resp. $\kappa_{C'}$). *Soit* $(x_\lambda)_{\lambda\in\Lambda}$ (resp. $(x'_\lambda)_{\lambda\in\Lambda}$) *une famille d'éléments de* C (resp. C') *dont l'image par* π (resp. π') *soit une p-base de* κ_C (resp. $\kappa_{C'}$). *Soit v un isomorphisme de* κ_C *sur* $\kappa_{C'}$ *tel que* $v(\pi(x_\lambda)) = \pi'(x'_\lambda)$ *pour tout* $\lambda \in \Lambda$. *Il existe alors un unique homomorphisme u de* C *dans* C', *tel que* $v \circ \pi = \pi' \circ u$ *et* $u(x_\lambda) = x'_\lambda$ *pour tout* $\lambda \in \Lambda$. *Il est surjectif. Si* $l(C) = l(C')$, *c'est un isomorphisme.*

Prouvons l'*existence* de *u*. Soit A le sous-anneau de $C \times C'$ formé des couples (x, x') tels que $v(\pi(x)) = \pi'(x')$. L'application $(x, x') \mapsto \pi(x)$ est un homomorphisme

surjectif d'anneaux de A sur κ_C. Son noyau $\mathfrak{m}$, égal à $pC \times pC'$ est donc un idéal maximal de A. Le sous-espace topologique A de $C \times C'$ est fermé dans $C \times C'$, donc complet, et la topologie induite sur A par celle de $C \times C'$ est la topologie $\mathfrak{m}$-adique. Par suite A est un anneau local séparé et complet d'idéal maximal $\mathfrak{m}$ (III, § 2, n° 13, prop. 19). Pour tout $\lambda \in \Lambda$, on a $(x_\lambda, x'_\lambda) \in A$ par hypothèse ; si ξ_λ est la classe de (x_λ, x'_λ) modulo $\mathfrak{m}$, la famille $(\xi_\lambda)_{\lambda \in \Lambda}$ est une p-base du corps $A/\mathfrak{m}$. D'après le th. 1 du n° 2, il existe un sous-anneau de Cohen C'' de A, et un seul, contenant (x_λ, x'_λ) pour tout $\lambda \in \Lambda$. On a $l(C'') = l(C) \geqslant l(C')$. La restriction à C'' de la projection de $C \times C'$ sur C est un homomorphisme $h : C'' \to C$ qui induit un isomorphisme de $\kappa_{C''}$ sur κ_C. D'après la prop. 2, *c*) du n° 2, h est un isomorphisme de C'' sur C. On voit de même que la restriction h' à C'' de la projection de $C \times C'$ sur C' est un homomorphisme surjectif de C'' dans C'. Par suite, C'' est le graphe d'un homomorphisme surjectif $u = h' \circ h^{-1}$ de C sur C', et l'on a évidemment $v \circ \pi = \pi' \circ u$, $u(x_\lambda) = x'_\lambda$ pour tout $\lambda \in \Lambda$. En outre, si $l(C) = l(C')$, u est un isomorphisme.

Prouvons l'*unicité* de u. Soit u_1 un homomorphisme de C dans C' tel que $v \circ \pi = \pi' \circ u_1$ et $u_1(x_\lambda) = x'_\lambda$ pour tout $\lambda \in \Lambda$, et soit C_1 le graphe de u_1. Il est immédiat que C_1 est un sous-anneau de Cohen de A, contenant (x_λ, x'_λ) pour tout $\lambda \in \Lambda$, d'où $C_1 = C''$ (th. 1 du n° 2) et finalement $u_1 = u$.

PROPOSITION 5. — *Soit k un corps de caractéristique p, et soit n un entier $\geqslant 1$, ou $+\infty$. Il existe un p-anneau de longueur n dont le corps résiduel est isomorphe à k.*

L'anneau $W(k)$ des vecteurs de Witt à coefficients dans k est un anneau local intègre séparé et complet, dont le corps résiduel est isomorphe à k (§ 1, n° 8, prop. 8), et on a $p.1_{W(k)} \neq 0$ (*loc. cit.*, formule (52)). Soit C un sous-anneau de Cohen de $W(k)$ (n° 2, th. 1). Alors C est un p-anneau de longueur $+\infty$ dont le corps résiduel est isomorphe à k, et, si n est un entier $\geqslant 1$, le quotient C/p^nC est un p-anneau de longueur n dont le corps résiduel est isomorphe à k.

Remarques. — 1) Soient n un entier $\geqslant 1$ et S une p-base de k. On peut montrer que le sous-anneau de $W_n(k)$ engendré par $W_n(k^{p^n})$ et par les éléments $[\xi, 0, ..., 0]$ $(\xi \in S)$, est un p-anneau de longueur n dont le corps résiduel est isomorphe à k (*cf.* p. 72, exerc. 10).

2) Le lecteur trouvera en Appendice une démonstration de la prop. 5 qui n'utilise ni les résultats du § 1, ni le théorème d'existence de sous-anneaux de Cohen (n° 2, th. 1).

COROLLAIRE. — *Soit C un p-anneau de longueur finie n. Il existe un p-anneau C' de longueur infinie tel que C soit isomorphe à C'/p^nC'.*

D'après la prop. 5, il existe un p-anneau C' de longueur infinie tel que $\kappa_{C'}$ soit isomorphe à κ_C. Alors $C'/p^nC' = C'_n$ est un p-anneau de longueur n, et le corps $\kappa_{C'_n}$ est isomorphe à $\kappa_{C'}$, donc à κ_C. D'après la prop. 4, les anneaux C et C'_n sont donc isomorphes.

4. Représentants multiplicatifs

PROPOSITION 6. — *Soit* C *un p-anneau, dont le corps résiduel k soit parfait. Supposons* C *de longueur finie n* (resp. infinie). *Il existe un unique isomorphisme* $u : \mathrm{W}_n(k) \to \mathrm{C}$ (resp. $u : \mathrm{W}(k) \to \mathrm{C}$) *qui induise par passage aux quotients l'application identique de k.*

Comme $\mathrm{W}_n(k)$ (resp. $\mathrm{W}(k)$) est un p-anneau de corps résiduel k, et de longueur n (resp. de longueur infinie) (n° 1, exemple 2), et que $\varnothing$ est une p-base du corps parfait k, la prop. 6 est un cas particulier de la prop. 4 du n° 3.

THÉORÈME 2. — *Soient* A *un anneau local séparé et complet, k son corps résiduel et* π *l'homomorphisme canonique de* A *sur k. On suppose que k est un corps* parfait *de caractéristique p.*

a) Il existe un unique homomorphisme d'anneaux $u : \mathrm{W}(k) \to \mathrm{A}$ *tel que* $\pi(u(\boldsymbol{a})) = a_0$ *pour* $\boldsymbol{a} = (a_n)_{n \in \mathbf{N}}$ *dans* $\mathrm{W}(k)$.

b) L'homomorphisme u est continu lorsqu'on munit $\mathrm{W}(k)$ *de la topologie* $p\mathrm{W}(k)$*-adique, et l'image de u est l'unique sous-anneau de Cohen de* A.

D'après le th. 1 du n° 2, il existe un unique sous-anneau de Cohen de A ; notons-le C. Soit u un homomorphisme de $\mathrm{W}(k)$ dans A tel que $\pi(u(\boldsymbol{a})) = a_0$ pour tout $\boldsymbol{a} = (a_n)_{n \in \mathbf{N}}$ dans $\mathrm{W}(k)$; il est immédiat que l'image de u est un sous-anneau de Cohen de A, donc égal à C. L'existence et l'unicité de u résultent alors de la prop. 6. La topologie pC-adique de C est induite par la topologie $\mathfrak{m}_\mathrm{A}$-adique de A (n° 2, th. 1, *b*)), d'où la continuité de u.

Pour une construction directe de u, voir p. 70, exerc. 6.

PROPOSITION 7. — *Conservons les hypothèses et notations du th. 2. Il existe une unique partie multiplicative* S *de* A *telle que* π *induise une bijection de* S *sur k. Pour qu'un élément a de* A *appartienne à* S, *il faut et il suffit que pour tout* $n \in \mathbf{N}$, *il existe un élément* a_n *de* A *tel que* $a = a_n^{p^n}$. *L'ensemble* S *est l'ensemble des éléments de la forme* $u(x, 0, 0, \ldots)$.

Prouvons tout d'abord l'unicité de S. Soit S une partie multiplicative de A, telle que π induise une bijection de S sur k. Soit T l'ensemble des éléments de A qui sont des puissances p^n-ièmes pour tout $n \in \mathbf{N}$.

a) On a $\mathrm{S} \subset \mathrm{T}$: Soient $a \in \mathrm{S}$ et $n \in \mathbf{N}$; comme le corps k est parfait, il existe un élément x_n de k tel que $x_n^{p^n} = \pi(a)$; comme on a $\pi(\mathrm{S}) = k$, il existe un élément a_n de S tel que $x_n = \pi(a_n)$. On a alors $\pi(a_n^{p^n}) = \pi(a)$ d'où $a_n^{p^n} = a$ puisque la restriction de π à S est injective.

b) La restriction de π *à* T *est injective* : soient a et b deux éléments de T tels que $\pi(a) = \pi(b)$. Soit $n \in \mathbf{N}$; il existe deux éléments a_n et b_n de A tels que $a = a_n^{p^n}$, $b = b_n^{p^n}$. On a alors $\pi(a_n)^{p^n} = \pi(b_n)^{p^n}$, d'où $\pi(a_n) = \pi(b_n)$, c'est-à-dire $a_n \equiv b_n \bmod \mathfrak{m}_\mathrm{A}$. D'après le lemme 1 du § 1, n° 1, on a $a_n^{p^n} \equiv b_n^{p^n} \bmod \mathfrak{m}_\mathrm{A}^{n+1}$ c'est-à-dire $a \equiv b \bmod \mathfrak{m}_\mathrm{A}^{n+1}$. Comme n est arbitraire, on a $a = b$.

Les propriétés *a*) et *b*) ci-dessus, jointes à la formule $\pi(S) = k$, entraînent la relation S = T, d'où l'unicité.

Prouvons maintenant l'existence de S. Avec les notations du th. 2, posons $\varphi = u \circ \tau_k$, c'est-à-dire (§ 1, n° 6)

$$\varphi(x) = u(x, 0, 0, \ldots) \tag{2}$$

pour tout $x \in k$. D'après la prop. 4 de *loc. cit.*, on a

$$\varphi(1) = 1\,, \quad \varphi(xy) = \varphi(x)\,\varphi(y) \quad \text{pour} \quad x, y \text{ dans } k\,. \tag{3}$$

Il est clair que l'application $\pi \circ \varphi$ est l'application identique de k. Donc l'image S de φ satisfait aux conditions de la prop. 7.

Les éléments de S sont souvent appelés les *représentants multiplicatifs* (ou de Teichmüller) *de* A.

Remarques. — 1) Conservons les hypothèses et notations précédentes. On a

$$\boldsymbol{a} = \sum_{n=0}^{\infty} p^n \tau_k(a_n^{p^{-n}}) \quad (\boldsymbol{a} = (a_n)_{n \in \mathbf{N}} \in \mathrm{W}(k))$$

d'après la prop. 7 du § 1, n° 8. On a donc

$$u(\boldsymbol{a}) = \sum_{n=0}^{\infty} p^n \varphi(a_n^{p^{-n}}) \tag{4}$$

pour tout $\boldsymbol{a} = (a_n)_{n \in \mathbf{N}}$ dans $\mathrm{W}(k)$, car u est continu (th. 2, *b*)). D'après la formule (4), l'unique sous-anneau de Cohen de A se compose des éléments de la forme $\sum_{n=0}^{\infty} p^n s_n$ avec $s_n \in \mathrm{S}$ pour tout entier $n \geqslant 0$.

2) Soient A un anneau local séparé et complet, k son corps résiduel et π l'homomorphisme canonique de A sur k. On peut montrer qu'il existe une partie multiplicative S de A (non unique en général) telle que π induise une bijection de S sur k (*cf.* p. 72, exerc. 11).

Exemples. — 1) Soit k un corps parfait de caractéristique p. Les représentants multiplicatifs de l'anneau $\mathrm{W}(k)$ sont les vecteurs de Witt $\tau(x) = (x, 0, 0, \ldots)$ pour $x \in k$.

2) Soit A un anneau local intègre, séparé et complet. On suppose que le corps résiduel k de A est fini, à $q = p^f$ éléments, donc parfait de caractéristique p. On a $x^q = x$ pour tout $x \in k$, d'où $s^q = s$ pour tout représentant multiplicatif s. Il en résulte que l'ensemble des représentants multiplicatifs se compose de 0 et des $q - 1$ racines $(q-1)$-ièmes de l'unité dans le corps des fractions de A. Si le corps des fractions de A est localement compact, l'existence des représentants multiplicatifs découle aussi de VI, § 9, n° 2, prop. 3 (*cf.* aussi VI, § 9, exerc. 5).

3) Plus particulièrement, considérons le cas $\mathrm{A} = \mathbf{Z}_p$. Alors les représentants

multiplicatifs sont 0 et les racines $(p-1)$-ièmes de l'unité dans le corps des fractions $\mathbf{Q}_p$ de $\mathbf{Z}_p$.

5. Structure des anneaux locaux noethériens et complets

Soient A et C des anneaux locaux noethériens *complets* et soit u un homomorphisme local de C dans A, induisant par passage aux quotients un *isomorphisme de* κ_C *sur* κ_A. Soit $(p_1, ..., p_m)$ une suite engendrant l'idéal $\mathfrak{m}_C$ de C, et soient $t_1, ..., t_n$ des éléments de $\mathfrak{m}_A$. Posons $B = C[[T_1, ..., T_n]]$.

Lemme 3. — *a) Il existe un unique homomorphisme* $v : B \to A$ *qui prolonge* u *et applique* T_i *sur* t_i *pour* $1 \leqslant i \leqslant n$.

b) Pour que v *soit surjectif, il faut et il suffit que la suite* $(u(p_1), ..., u(p_m), t_1, ..., t_n)$ *engendre l'idéal* $\mathfrak{m}_A$ *de* A, *ou encore que les classes de ces éléments modulo* $\mathfrak{m}_A^2$ *engendrent* $\mathfrak{m}_A/\mathfrak{m}_A^2$ *comme espace vectoriel sur le corps* κ_A.

c) Pour que v *fasse de* A *une* B*-algèbre finie, il faut et il suffit que la suite* $(u(p_1), ..., u(p_m), t_1, ..., t_n)$ *engendre un idéal de définition de* (*la topologie* $\mathfrak{m}_A$*-adique de*) A.

Notons $\mathfrak{n}$ l'idéal de l'anneau B engendré par $T_1, ..., T_n$. Tout homomorphisme v de B dans A qui prolonge u et tel que $v(T_i) = t_i$ applique $\mathfrak{n}$ dans $\mathfrak{m}_A$, donc est continu lorsqu'on munit B de la topologie $\mathfrak{n}$-adique. L'existence et l'unicité de v résultent alors de A, IV, p. 26, prop. 4.

L'anneau $B = C[[T_1, ..., T_n]]$ est un anneau local noethérien complet (III, § 2, n° 10, cor. 6 du th. 2 et n° 6, prop. 6), dont l'idéal maximal $\mathfrak{m}_B$ est engendré par $p_1, ..., p_m, T_1, ..., T_n$. On a donc $v(\mathfrak{m}_B) \subset \mathfrak{m}_A$ et v définit un homomorphisme $\mathrm{gr}(v)$ de $\mathrm{gr}(B) = \bigoplus_{n=0}^{\infty} \mathfrak{m}_B^n/\mathfrak{m}_B^{n+1}$ dans $\mathrm{gr}(A) = \bigoplus_{n=0}^{\infty} \mathfrak{m}_A^n/\mathfrak{m}_A^{n+1}$. Or l'anneau $\mathrm{gr}(A)$ est engendré par $A/\mathfrak{m}_A = \kappa_A$ et $\mathfrak{m}_A/\mathfrak{m}_A^2$, $\mathrm{gr}(v)$ induit un isomorphisme de $\kappa_B = \kappa_C$ sur κ_A, et les classes modulo $\mathfrak{m}_B^2$ des éléments $p_1, ..., p_m, T_1, ..., T_n$ engendrent $\mathfrak{m}_B/\mathfrak{m}_B^2$ comme espace vectoriel sur κ_B ; de plus v est surjectif si et seulement si $\mathrm{gr}(v)$ est surjectif (III, § 2, n° 8, cor. 2 du th. 1). Ceci prouve *b)*.

L'idéal de A engendré par la suite $(u(p_1), ..., u(p_m), t_1, ..., t_n)$ n'est autre que $v(\mathfrak{m}_B)$ A. Puisque $\mathfrak{m}_A$ contient $v(\mathfrak{m}_B)$, A est un anneau de Zariski pour la topologie $v(\mathfrak{m}_B)$ A-adique. L'anneau $A/v(\mathfrak{m}_B)$ A est artinien si et seulement si sa longueur en tant que A-module est finie. Mais comme tout module simple sur A est annulé par $\mathfrak{m}_A$ et que, par hypothèse, $A/\mathfrak{m}_A$ et $B/\mathfrak{m}_B$ sont isomorphes, cela se produit si et seulement si la dimension sur le corps $B/\mathfrak{m}_B$ de l'espace vectoriel $A/v(\mathfrak{m}_B)$ A est finie. Par IV, § 2, n° 5, cor. 2 de la prop. 9, on voit donc que $v(\mathfrak{m}_B)$ A est un idéal de définition de A si et seulement si la dimension de $A/v(\mathfrak{m}_B)$ A sur $B/\mathfrak{m}_B$ est finie. C'est bien le cas si A est une B-algèbre finie.

Supposons que $v(\mathfrak{m}_B)$ A soit un idéal de définition de A. La topologie $\mathfrak{m}_B$-adique du B-module A coïncide alors avec la topologie $\mathfrak{m}_A$-adique de l'anneau A, donc est séparée. Comme $A/v(\mathfrak{m}_B)$ A est un module de type fini sur $B/\mathfrak{m}_B$, A est un B-module de type fini (III, § 2, n° 3, exemple 3 et n° 9, cor. 1 de la prop. 12). Ceci prouve *c)*.

Lemme 4. — *Supposons que l'anneau local noethérien* C *soit régulier, et que* $(p_1, ..., p_m)$ *soit un système de coordonnées de* C (VIII, § 5, n° 1, déf. 1).

a) Si la suite $(u(p_1), ..., u(p_m), t_1, ..., t_n)$ *est sécante pour* A (VIII, § 3, n° 2, déf. 1), *l'homomorphisme* $v : B \to A$ *est injectif.*

b) Pour que v soit injectif et fasse de A *une algèbre finie sur* B, *il faut et il suffit que* $(u(p_1), ..., u(p_m), t_1, ..., t_n)$ *soit une suite sécante maximale pour* A. *Alors* A *est de dimension* $m + n$.

Pour que la suite $(u(p_1), ..., u(p_m), t_1, ..., t_n)$ soit une suite sécante maximale pour A, il faut et il suffit qu'elle engendre un idéal de définition de A, et que A soit de dimension $m + n$ (VIII, § 3, n° 2, th. 1). D'après le lemme 3, *c*), il revient au même de dire que A est une B-algèbre finie, et un anneau de dimension $m + n$. Or C est un anneau intègre noethérien de dimension m, donc $B = C[[T_1, ..., T_n]]$ est un anneau intègre noethérien de dimension $m + n$ (VIII, § 3, n° 4, cor. 3 de la prop. 8). Si A est une B-algèbre finie, et si $\mathfrak{a}$ est le noyau de v, on a $\dim(A) = \dim(B/\mathfrak{a})$ (VIII, § 2, n° 3, th. 1, *c*)) ; comme B est un anneau intègre de dimension finie, on a $\dim(B/\mathfrak{a}) < \dim(B)$ si $\mathfrak{a} \neq \{0\}$ (VIII, § 1, n° 3, prop. 6, *e*)). Donc, si A est une B-algèbre finie, v est injectif si et seulement si A est de dimension $m + n$. Ceci prouve *b*).

Supposons que la suite $(u(p_1), ..., u(p_m), t_1, ..., t_n)$ d'éléments de $\mathfrak{m}_A$ soit sécante. On peut lui adjoindre (VIII, § 3, n° 2, th. 1) des éléments $t_{n+1}, ..., t_{n+r}$ de $\mathfrak{m}_A$ pour en faire une suite sécante maximale. D'après ce qui précède, il existe alors un homomorphisme *injectif* w de $C[[T_1, ..., T_n, T_{n+1}, ..., T_{n+r}]] = B[[T_{n+1}, ..., T_{n+r}]]$ qui prolonge v et applique T_{n+j} sur t_{n+j} pour $1 \leqslant j \leqslant r$. Donc v est injectif. Ceci prouve *a*).

THÉORÈME 3. — *Soit* A *un anneau local, noethérien et complet dont le corps résiduel k soit de caractéristique p. Soit* C *un p-anneau de longueur infinie, dont le corps résiduel soit isomorphe à k* (n° 3, prop. 5).

a) Soit m la dimension de l'espace vectoriel $\mathfrak{m}_A/(\mathfrak{m}_A^2 + pA)$ *sur le corps k. Il existe un idéal* $\mathfrak{a}$ *de l'anneau* $C[[T_1, ..., T_m]]$ *tel que* A *soit isomorphe à* $C[[T_1, ..., T_m]]/\mathfrak{a}$.

b) Soit d la dimension de A. *Supposons que* $p1_A$ *ne soit pas diviseur de* 0 *dans* A. *Alors il existe un sous-anneau* A′ *de* A *isomorphe à* $C[[T_1, ..., T_{d-1}]]$ *et tel que* A *soit une algèbre finie sur* A′.

Soit C′ un sous-anneau de Cohen de A (n° 2, th. 1). Comme C est de longueur infinie, il existe un homomorphisme de C sur C′ (n° 3, prop. 4). Par suite, il existe un homomorphisme local $u : C \to A$. Choisissons des éléments $t_1, ..., t_m$ de $\mathfrak{m}_A$ dont les classes forment une base de l'espace vectoriel $\mathfrak{m}_A/(\mathfrak{m}_A^2 + pA)$ sur le corps k. On a $u(p1_C) = p1_A$, et le lemme 3, *b*) prouve l'existence d'un homomorphisme surjectif de $C[[T_1, ..., T_m]]$ dans A, prolongeant u et appliquant T_i sur t_i pour $1 \leqslant i \leqslant m$. Ceci prouve *a*).

Supposons que $p1_A$ ne soit pas diviseur de 0 dans A donc sécant pour A (VIII, § 3, n° 2, prop. 3). Il existe alors (VIII, § 3, n° 2, th. 1) des éléments $t_1, ..., t_{d-1}$ de $\mathfrak{m}_A$ tels que la suite $(p1_A, t_1, ..., t_{d-1})$ soit sécante maximale pour A. L'anneau local noethérien C est régulier, et $(p1_C)$ est un système de coordonnées de C. L'assertion *b*) du th. 3 résulte alors du lemme 4, *b*).

§ 3. CORPS DE REPRÉSENTANTS

1. Anneaux locaux d'égales caractéristiques

Soit A un anneau. Rappelons (A, V, p. 2) que la caractéristique de A est définie lorsque A contient un sous-corps. Elle est égale à 0 si et seulement si A contient un sous-corps isomorphe à $\mathbf{Q}$, et égale à un nombre premier p si et seulement si on a $p1_A = 0$. Si la caractéristique de A est définie, et si $f: A \to B$ est un homomorphisme non nul d'anneaux, la caractéristique de B est définie et elle est égale à celle de A.

Soit A un anneau local, d'idéal maximal $\mathfrak{m}$, et de corps résiduel k.

a) Supposons k de caractéristique 0. Alors A contient un corps et la caractéristique de A est égale à 0. En effet, l'homomorphisme canonique de $\mathbf{Z}$ dans A est injectif, et pour tout entier n non nul, $n1_A$ est inversible dans A, car il n'appartient pas à $\mathfrak{m}$.

b) Supposons k de caractéristique $p \neq 0$. Alors A contient un corps si et seulement si $p1_A = 0$. Dans ce cas la caractéristique de A est égale à p.

Supposons que A soit un anneau local intègre, de corps des fractions K et de corps résiduel k.

a') L'anneau A contient un sous-corps si et seulement si les caractéristiques de k et K sont égales. Dans ce cas, la caractéristique de A est égale à celle de k et de K, et on dit que A est un anneau local d'égales caractéristiques.

b') Supposons que les corps k et K n'aient pas même caractéristique. Alors il existe un nombre premier p tel que k soit de caractéristique p. Comme on a $q1_A \neq 0$ pour tout nombre premier $q \neq p$, le corps K est de caractéristique 0. On dit alors que A est un anneau local d'inégales caractéristiques.

2. Un théorème de relèvement

PROPOSITION 1. — *Soient k_0 un corps,* A *une k_0-algèbre qui est un anneau local séparé et complet,* K *une sous-k_0-extension de κ_A qui possède une base de transcendance séparante $(\xi_\lambda)_{\lambda\in\Lambda}$ sur k_0* (A, V, p. 130, déf. 1). *Pour tout $\lambda \in \Lambda$, soit x_λ un représentant de ξ_λ dans* A. *Il existe un unique sous-corps* L *de* A, *contenant k_0 et les éléments x_λ, et tel que l'homomorphisme canonique π de* A *sur κ_A induise un isomorphisme de* L *sur* K.

Soit φ le k_0-homomorphisme de l'anneau de polynômes $k_0[(X_\lambda)_{\lambda\in\Lambda}]$ dans A qui applique X_λ sur x_λ pour tout $\lambda \in \Lambda$. Soit u un élément non nul de $k_0[(X_\lambda)_{\lambda\in\Lambda}]$; on a $\pi(\varphi(u)) \neq 0$, car la famille $(\xi_\lambda)_{\lambda\in\Lambda}$ est algébriquement libre sur k_0 dans κ_A ; par suite, $\varphi(u)$ est inversible dans l'anneau local A. Il en résulte que φ se prolonge en un homomorphisme ψ du corps $k_1 = k_0((X_\lambda)_{\lambda\in\Lambda})$ dans A. Alors A est une k_1-algèbre, κ_A est une extension de k_1 et K une sous-extension de κ_A qui est *algébrique et séparable*

sur k_1. Il s'agit de prouver qu'il existe un unique sous-corps L de A contenant $\psi(k_1)$ et tel que $\pi(L) = K$.

a) Existence de L : Soit $\mathcal{S}$ l'ensemble des sous-corps L de A, contenant $\psi(k_1)$ et tels que $\pi(L) \subset K$; il est inductif pour la relation d'inclusion. Soit L un élément maximal de $\mathcal{S}$; on considère K comme une extension (algébrique et séparable, d'après A, V, p. 40, prop. 9) de L. Soit $\xi \in K$ et soit $P \in L[X]$ son polynôme minimal sur L. Comme ξ est racine simple de P, le lemme de Hensel (III, § 4, n° 5, cor. 1 du th. 2) assure l'existence d'un élément x de A tel que $\pi(x) = \xi$ et $P(x) = 0$. Le sous-anneau L[X] de A appartient à $\mathcal{S}$; d'après le caractère maximal de L, on a donc $x \in L$, d'où $\xi \in \pi(L)$. Finalement on a $\pi(L) = K$.

b) Unicité de L : Soient L et L′ deux sous-corps de A contenant $\psi(k_1)$ et tels que $\pi(L) = \pi(L') = K$. Soit $\xi \in K$, et soient $x \in L$ et $x' \in L'$ les éléments tels que $\pi(x) = \pi(x') = \xi$. Si $P \in k_1[X]$ est le polynôme minimal de ξ sur k_1, alors ξ est racine simple de P, et l'on a $P(x) = P(x') = 0$. D'après le lemme de Hensel (*loc. cit.*) on a $x = x'$. On a donc $L = L'$.

Remarque. — * La démonstration précédente s'applique plus généralement au cas où on suppose seulement que A est un anneau local hensélien$_*$. La démonstration d'unicité utilise l'hypothèse que l'anneau local A est séparé, mais non qu'il est complet.

3. Corps de représentants

DÉFINITION 1. — *Soit* A *un anneau local. On appelle corps de représentants de* A *tout sous-corps* K *de* A *tel que l'homomorphisme canonique de* A *sur* κ_A *induise un isomorphisme de* K *sur* κ_A *(autrement dit, tel que* $A = K + \mathfrak{m}_A$*).*

Il ne peut exister de corps de représentants de A que si A admet une caractéristique. Cette condition est suffisante lorsque A est séparé et complet. Plus précisément, on a le théorème suivant :

THÉORÈME 1. — *Soit* A *un anneau local séparé et complet de caractéristique p.*

a) Supposons $p = 0$ *et soit* $(x_\lambda)_{\lambda \in \Lambda}$ *une famille d'éléments de* A *dont les classes modulo* $\mathfrak{m}_A$ *forment une base de transcendance de* κ_A *sur* **Q**. *Il existe un unique corps de représentants de* A *contenant les éléments* x_λ.

b) Supposons $p \neq 0$. *Soit* $(x_\lambda)_{\lambda \in \Lambda}$ *une famille d'éléments de* A *dont les classes modulo* $\mathfrak{m}_A$ *forment une p-base de* κ_A (A, V, p. 95). *Il existe un unique corps de représentants de* A *contenant les éléments* x_λ. *C'est un sous-anneau de Cohen de* A.

Supposons qu'on ait $p = 0$ de sorte que A est une **Q**-algèbre. Toute base de transcendance de κ_A sur **Q** étant séparante, l'assertion *a)* résulte de la prop. 1 du n° 1 appliquée au cas $k_0 = \mathbf{Q}$, $K = \kappa_A$.

Supposons maintenant qu'on ait $p \neq 0$. Alors on a $p1_A = 0$, et tout sous-anneau de Cohen C de A satisfait à $pC = 0$. Autrement dit, il y a identité entre les notions de corps de représentants et de sous-anneau de Cohen de A. L'assertion *b)* résulte alors du § 2, n° 2, th. 1.

COROLLAIRE 1. — *Soit* A *un anneau local séparé et complet, dont le corps résiduel est une extension algébrique de* **Q**. *Il existe alors un unique corps de représentants de* A.

En effet l'anneau A est de caractéristique 0 (n° 1).

COROLLAIRE 2. — *Soit* A *un anneau local séparé et complet de caractéristique* $p \neq 0$. *Supposons que le corps résiduel* κ_A *soit parfait. Alors il existe un unique corps de représentants de* A, *à savoir l'ensemble des représentants multiplicatifs.*

Le cor. 2 résulte aussitôt du th. 1 et de la prop. 7 du § 2, n° 4.

THÉORÈME 2. — *Soit* A *un anneau local noethérien complet de dimension d contenant un corps. Soit* K *un corps de représentants de* A, *et soit m la dimension de l'espace vectoriel* $\mathfrak{m}_A/\mathfrak{m}_A^2$ *sur le corps* K.

a) *Il existe un idéal* $\mathfrak{a}$ *de* $K[[T_1, ..., T_m]]$ *tel que la* K*-algèbre* A *soit isomorphe à* $K[[T_1, ..., T_m]]/\mathfrak{a}$.

b) *Il existe une sous-*K*-algèbre* A′ *de* A, *isomorphe à* $K[[T_1, ..., T_d]]$ *et telle que* A *soit une algèbre finie sur* A′.

c) *Supposons que l'anneau local noethérien* A *soit régulier*, i.e. $d = m$. *Alors il existe un* K*-isomorphisme de* A *sur* $K[[T_1, ..., T_d]]$.

Soient $t_1, ..., t_m$ des éléments de $\mathfrak{m}_A$ dont les classes modulo $\mathfrak{m}_A^2$ engendrent le K-espace vectoriel $\mathfrak{m}_A/\mathfrak{m}_A^2$. D'après le lemme 3 du § 2, n° 5, il existe un K-homomorphisme surjectif de $K[[T_1, ..., T_m]]$ dans A, transformant T_i en t_i pour $1 \leqslant i \leqslant m$. Ceci prouve *a*).

De même, l'assertion *b*) résulte du lemme 4 de *loc. cit.* et de l'existence d'une suite sécante maximale pour A (VIII, § 3, n° 2, th. 1).

Enfin, l'assertion *c*) n'est autre que le cor. 3 du th. 1 de VIII, § 5, n° 2.

§ 4. FERMETURE INTÉGRALE D'UN ANNEAU LOCAL COMPLET

1. Anneaux japonais

DÉFINITION 1. — *Soit* A *un anneau noethérien intègre. On dit que* A *est japonais si la fermeture intégrale de* A *dans toute extension finie de son corps des fractions est une* A*-algèbre finie.*

Remarques. — 1) Il revient au même de dire que A satisfait à la condition suivante : toute A-algèbre intègre B entière sur A, contenue dans une extension de type fini du corps des fractions K de A, est une A-algèbre finie. En effet, le corps des fractions L de B est une extension algébrique de K, donc est de degré fini sur K (A, V, p. 112, cor. 1 de la prop. 17). La A-algèbre B est contenue dans la fermeture intégrale de A dans L, et est donc finie si cette dernière est finie.

2) Soient A un anneau noethérien intègre japonais et S une partie multiplicative de A ne contenant pas 0. L'anneau de fractions $S^{-1}A$ est japonais. Soient en effet L une extension finie du corps des fractions de A et B la fermeture intégrale de A dans L ; alors la fermeture intégrale de $S^{-1}A$ dans L est $S^{-1}B$ (V, § 1, n° 5, prop. 16), donc est une $S^{-1}A$-algèbre finie.

Exemple. — Toute algèbre intègre de type fini sur un corps est un anneau japonais (V, § 3, n° 2, th. 2).

PROPOSITION 1. — *Soient* A *un anneau noethérien intègre,* K *son corps des fractions. Supposons que pour toute extension finie* radicielle L *de* K, *la fermeture intégrale de* A *dans* L *soit une* A*-algèbre finie. Alors l'anneau* A *est japonais.*

Soit E une extension finie de K. Soient N une extension finie quasi-galoisienne de K contenant E (A, V, p. 54, cor. 1), et L le corps des invariants du groupe des K-automorphismes de N. Alors (A, V, p. 73, prop. 13), L est une extension radicielle de K et N est une extension séparable de L. La fermeture intégrale B de A dans L est donc par hypothèse une A-algèbre finie ; la fermeture intégrale C de B dans N est une B-algèbre finie (V, § 1, n° 6, cor. 1 à la prop. 18), donc une A-algèbre finie. La fermeture intégrale de A dans E est contenue dans C, donc est une A-algèbre finie puisque A est noethérien.

COROLLAIRE. — *Supposons le corps* K *parfait (par exemple de caractéristique* 0). *Alors* A *est japonais si et seulement si sa clôture intégrale est une* A*-algèbre finie.*

PROPOSITION 2. — *Soient* B *un anneau noethérien intègre et* A *un sous-anneau noethérien de* B, *tel que* B *soit une* A*-algèbre finie. Pour que* A *soit japonais, il faut et il suffit que* B *soit japonais.*

Notons K (resp. L) le corps des fractions de A (resp. B). Supposons d'abord A japonais, et soit M une extension finie de L. Notons C la fermeture intégrale de B dans M. D'après V, § 1, n° 1, prop. 6, C est la fermeture intégrale de A dans M, donc est une A-algèbre finie puisque M est une extension finie de K et que A est japonais. *A fortiori,* C est une B-algèbre finie. Ceci prouve que B est japonais.

Inversement, supposons B japonais et soit N une extension finie de K. Notons D la fermeture intégrale de A dans N. Soit E une extension de K composée de L et N ; comme B est japonais, la fermeture intégrale D′ de B dans E est une B-algèbre finie, donc une A-algèbre finie ; le A-module D qui est un sous-module de D′ est donc de type fini, ce qui entraîne que A est japonais.

2. Théorème de Nagata

THÉORÈME 1 (Tate). — *Soient* A *un anneau noethérien intégralement clos, a un élément de* A. *On suppose que l'idéal* aA *est premier, que l'anneau* A/aA *est japonais et que* A *est complet pour la topologie* aA*-adique. Alors l'anneau* A *est japonais.*

a) Soit K le corps des fractions de A. L'assertion étant triviale lorsque K est de caractéristique 0 (n° 1, corollaire de la prop. 1), on peut supposer K de caractéristique $p > 0$. On peut aussi supposer $a \neq 0$.

Soient L une extension finie radicielle de K et q une puissance de p telle que $L \subset K^{1/q}$. Posons $x = a^{1/q}$ et $M = L(x)$. D'après la prop. 1 du n° 1, il suffit de démontrer que la fermeture intégrale B de A dans M est une A-algèbre finie.

b) Démontrons d'abord que l'idéal xB est l'unique idéal premier de B au-dessus de aA. Il existe en effet au moins un idéal premier de B au-dessus de aA (V, § 2, n° 1, th. 1). Soit q l'un de ces idéaux. On a $x^q = a \in \mathfrak{q}$, d'où xB $\subset$ q puisque q est premier. Inversement, soit y un élément de q ; l'élément y^q de K est entier sur A, donc appartient à A puisque A est intégralement clos. Puisque $\mathfrak{q} \cap A = aA$, il existe un élément α de A tel que $y^q = a\alpha = x^q\alpha$. Par conséquent l'élément y/x de M est entier sur A, donc appartient à B ; ainsi on a $y \in x$B, d'où q $= x$B, ce qui démontre notre assertion.

c) Il en résulte que l'anneau B_{xB} est la fermeture intégrale dans M de l'anneau A_{aA} (V, § 1, n° 5, prop. 16 et § 2, n° 1, prop. 2). D'après VI, § 3, n° 6, prop. 9, A_{aA} est un anneau de valuation discrète ; on déduit alors du théorème de Krull-Akizuki (VII, § 2, n° 5, prop. 5) que le corps $\kappa(x\text{B})$ est une extension finie de $\kappa(a\text{A})$ et que B_{xB} est noethérien.

d) L'anneau B/xB est entier sur l'anneau japonais A/aA et son corps des fractions est une extension finie du corps des fractions de ce dernier. Par conséquent, B/xB est un (A/aA)-module de type fini. Pour tout entier $i \geqslant 0$, il en est de même du module $x^i\text{B}/x^{i+1}\text{B}$; par suite le (A/aA)-module B/aB possède une suite de composition de longueur q dont les quotients sont des (A/aA)-modules de type fini, donc est lui-même un (A/aA)-module de type fini.

e) Munissons l'anneau A de la filtration (aA)-adique et l'anneau B de la filtration (aB)-adique. Alors A est complet par hypothèse ; comme B_{xB} est intègre et noethérien, la filtration $a\text{B}_{xB}$-adique de B_{xB} est séparée (III, § 3, n° 2, corollaire à la prop. 5) ; par suite on a $\bigcap a^n\text{B} \subset \bigcap a^n\text{B}_{xB} = \{0\}$, et la filtration aB-adique de B est séparée ; le gr(A)-module gr(B) est engendré par $\text{gr}_0(\text{B})$, donc est de type fini d'après *d*). Il résulte alors de III, § 2, n° 9, cor. 1 à la prop. 12, que B est un A-module de type fini, ce qui achève la démonstration.

COROLLAIRE. — *Soient* R *un anneau noethérien intègre et n un entier. Si* R *est japonais, l'anneau* $\text{R}[[\text{T}_1, ..., \text{T}_n]]$ *est japonais.*

Raisonnant par récurrence, on peut supposer $n = 1$. Notons S la clôture intégrale de R ; si R est japonais, S est une algèbre finie sur R, donc un anneau japonais (n° 1, prop. 2). L'anneau S[[T]] est noethérien et intégralement clos (V, § 1, n° 4, prop. 14) ; appliquant le th. 1 à A = S[[T]] et a = T, on en déduit que S[[T]] est japonais. Par conséquent R[[T]] est japonais (n° 1, prop. 2).

THÉORÈME 2 (Nagata). — *Tout anneau* A *local noethérien intègre et complet est japonais.*

D'après le th. 3 du § 2, n° 5 et le th. 2 du § 3, n° 3, il existe un entier $n \geqslant 0$, un anneau R qui est un corps ou un anneau de valuation discrète de corps des fractions de

caractéristique 0, et un sous-anneau B de A, isomorphe à $R[[T_1, ..., T_n]]$ et tel que A soit une B-algèbre finie. Alors R est japonais (n° 1, exemple et corollaire de la prop. 1), donc B est japonais (corollaire au th. 1), et A est japonais (n° 1, prop. 2).

COROLLAIRE. — *Soit* A *un anneau semi-local noethérien dont le complété est réduit. Alors la fermeture intégrale* A′ *de* A *dans son anneau total des fractions* R *est une* A*-algèbre finie.*

Supposons d'abord A local et complet, et soient $\mathfrak{p}_1, ..., \mathfrak{p}_n$ les idéaux premiers minimaux (distincts) de A ; pour $i = 1, ..., n$, notons K_i le corps des fractions de $A/\mathfrak{p}_i$ et A'_i la clôture intégrale de $A/\mathfrak{p}_i$. Comme A est réduit, R est le produit des anneaux K_i et A′ le produit des anneaux A'_i (V, § 1, n° 2, cor. 1 à la prop. 9). Puisque les anneaux locaux $A/\mathfrak{p}_i$ sont intègres et complets, ils sont japonais (th. 2), de sorte que chaque A'_i est une A-algèbre finie, et A′ est une A-algèbre finie.

Si A est semi-local et complet, il est isomorphe à un produit fini d'anneaux locaux complets (III, § 2, n° 13, corollaire à la prop. 19), et on conclut aussitôt d'après ce qui précède.

Passons au cas général et notons que le complété $\hat{A}$ de A est un anneau semi-local, complet, noethérien et fidèlement plat sur A (III, *loc. cit.*, § 3, n° 4, corollaire de la prop. 8 et § 3, n° 5, prop. 9). Soit S l'ensemble des éléments non diviseurs de zéro de A ; on a $R = S^{-1}A$. Puisque $\hat{A}$ est plat sur A, les éléments de S sont non diviseurs de zéro dans $\hat{A}$, et $S^{-1}\hat{A}$ s'identifie à un sous-anneau de l'anneau total des fractions T de $\hat{A}$. Toujours puisque $\hat{A}$ est plat sur A, l'anneau $A' \otimes_A \hat{A}$ s'identifie à un sous-anneau de $R \otimes_A \hat{A} = S^{-1}\hat{A}$, donc aussi à un sous-anneau de T entier sur $\hat{A}$. D'après la première partie de la démonstration, $A' \otimes_A \hat{A}$ est donc un $\hat{A}$-module de type fini ; par suite, A′ est un A-module de type fini (I, § 3, n° 6, prop. 11).

Rappelons (A, V, p. 114, déf. 1) qu'une algèbre E sur un corps K est dite *séparable* si l'anneau $L \otimes_K E$ est réduit pour toute extension L de K ; il suffit qu'il en soit ainsi pour toute extension finie de K. La proposition suivante généralise le th. 2 :

PROPOSITION 3. — *Soient* A *un anneau semi-local noethérien intègre,* K *son corps des fractions. Si la* K*-algèbre* $K \otimes_A \hat{A}$ *est séparable, l'anneau* A *est japonais.*

Soient L une extension finie de K et B la fermeture intégrale de A dans L. Soit F une partie finie de B telle que $L = K[F]$ (V, § 1, n° 5, cor. 2 à la prop. 16) ; notons C la A-algèbre (finie) engendrée par F. Puisque L est le corps des fractions de C, l'anneau B est la clôture intégrale de C (V, § 1, n° 1, prop. 6) et il suffit de prouver que B est une C-algèbre finie. Or, C est un anneau semi-local noethérien (IV, § 2, n° 5, cor. 3 à la prop. 9) ; son complété s'identifie à $C \otimes_A \hat{A}$ (III, § 3, n° 4, th. 3 (ii)), donc aussi à un sous-anneau de l'anneau réduit $L \otimes_A \hat{A} = L \otimes_K (K \otimes_A \hat{A})$ et par suite est réduit. La prop. 3 résulte donc du corollaire au th. 2.

3. Quelques lemmes

Lemme 1. — *Soient* A *un anneau semi-local noethérien et* B *une* A*-algèbre finie. Alors l'anneau* B *est semi-local et noethérien ; soient* $\mathfrak{m}_1, ..., \mathfrak{m}_n$ *ses idéaux maximaux.*

L'homomorphisme canonique de B *dans* $\prod_{i=1}^{n} \hat{B}_{m_i}$ *se prolonge en un isomorphisme de* $\hat{A} \otimes_A B$ *sur* $\prod_{i=1}^{n} \hat{B}_{m_i}$.

D'après IV, § 2, n° 5, cor. 3 à la prop. 9, l'anneau B est semi-local et $m_A B$ en est un idéal de définition. D'après III, § 3, n° 4, th. 3, (ii), l'anneau $\hat{A} \otimes_A B$ est le complété de B pour la topologie définie par son radical ; on applique alors III, § 2, n° 13, corollaire à la prop. 19.

Lemme 2. — *Soient* A *un anneau noethérien et* M *un* A*-module. L'application canonique de* M *dans le produit* $\prod_{p \in Ass(M)} M_p$ *est injective.*

Soit en effet m un élément non nul de M ; alors $\mathrm{Ann}(m)$ est contenu dans un idéal premier $\mathfrak{p}$ de A associé à M (IV, § 1, n° 1, prop. 2), et l'image de m dans $M_\mathfrak{p}$ est non nulle (II, § 2, n° 2, prop. 4).

Lemme 3. — *Soient* A *un anneau noethérien,* x *un élément de* A, M *un* A*-module de type fini, et* $\mathfrak{p}$ *un idéal premier de* A *associé à* M. *On suppose que l'homothétie* x_M *est injective. Soit* $\mathfrak{q}$ *un idéal premier de* A, *minimal parmi ceux qui contiennent* $\mathfrak{p} + x\mathrm{A}$. *Alors* $\mathfrak{q}$ *est associé au* A*-module* $\mathrm{M}/x\mathrm{M}$.

Notons N le sous-module de M formé des éléments m tels que $\mathfrak{p}m = 0$. On a $\mathrm{N} \cap x\mathrm{M} = x\mathrm{N}$; en effet, si un élément m de M est tel que $\mathfrak{p}xm = 0$, on a $\mathfrak{p}m = 0$ puisque x_M est injective, donc $m \in \mathrm{N}$. Par conséquent, le A-module $\mathrm{N}/x\mathrm{N}$ est isomorphe au sous-module $(\mathrm{N} + x\mathrm{M})/x\mathrm{M}$ de $\mathrm{M}/x\mathrm{M}$, et il suffit de démontrer que $\mathfrak{q}$ est associé à $\mathrm{N}/x\mathrm{N}$. Puisque $\mathfrak{p}$ est associé à M, il existe un élément m de M tel que $\mathfrak{p} = \mathrm{Ann}(m)$; on a $m \in \mathrm{N}$ d'où $\mathfrak{p} = \mathrm{Ann}(\mathrm{N})$ et par suite $\mathrm{Supp}(\mathrm{N}/x\mathrm{N}) = \mathrm{V}(\mathfrak{p} + x\mathrm{A})$ d'après II, § 4, n° 4, corollaire à la prop. 18 ; par conséquent, $\mathfrak{q}$ est associé à $\mathrm{N}/x\mathrm{N}$ (IV, § 1, n° 4, th. 2).

Lemme 4. — *Soient* A *un anneau de valuation discrète,* B *un anneau local noethérien, et* $\rho : \mathrm{A} \to \mathrm{B}$ *un homomorphisme local et plat. Si l'anneau* $\kappa_A \otimes_A B$ *est réduit, alors* B *est réduit.*

Supposons qu'il existe un élément nilpotent non nul x de B, et soit π une uniformisante de A. Puisqu'on a $\pi\mathrm{B} \subset \mathfrak{m}_\mathrm{B}$, l'anneau B est séparé pour la topologie πB-adique. Il existe donc $n \in \mathbf{N}$ et $y \in \mathrm{B}$ avec $x = \pi^n y$ et $y \notin \pi\mathrm{B}$. Puisque B est plat sur A, la multiplication par π est injective dans B. La classe de y dans $\mathrm{B}/\pi\mathrm{B}$ est donc un élément nilpotent non nul, ce qui contredit l'hypothèse.

4. Anneaux de Nagata

DÉFINITION 2. — *On dit qu'un anneau* A *est un anneau de Nagata s'il est noethérien et si, pour tout idéal premier* $\mathfrak{p}$ *de* A, *l'anneau noethérien intègre* $\mathrm{A}/\mathfrak{p}$ *est japonais* (n° 1, déf. 1).

Exemples. — 1) Toute algèbre de type fini sur un corps est un anneau de Nagata (n° 1, exemple).

2) Tout anneau noethérien local complet est un anneau de Nagata (n° 2, th. 2).

3) L'anneau **Z** est un anneau de Nagata (n° 1, exemple et corollaire de la prop. 1).

4) On peut montrer (exerc. 30) que toute algèbre de type fini sur un anneau de Nagata est un anneau de Nagata.

PROPOSITION 4. — *Soit* A *un anneau de Nagata.*

a) *Toute* A*-algèbre finie est un anneau de Nagata.*

b) *Pour toute partie multiplicative* S *de* A, *l'anneau* $S^{-1}A$ *est un anneau de Nagata.*

a) Soit B une A-algèbre finie, $\rho : A \to B$ l'homomorphisme canonique. Pour tout idéal premier $\mathfrak{p}$ de B, l'anneau $B/\mathfrak{p}$ qui est une algèbre finie sur l'anneau japonais $A/\rho^{-1}(\mathfrak{p})$, est japonais (n° 1, prop. 2).

b) Soit $\mathfrak{q}$ un idéal premier de $S^{-1}A$; alors il existe un idéal premier $\mathfrak{p}$ de A tel que $\mathfrak{q} = S^{-1}\mathfrak{p}$. L'anneau $(S^{-1}A)/\mathfrak{q}$ est un anneau de fractions de l'anneau japonais $A/\mathfrak{p}$, donc est japonais (n° 1, remarque 2).

THÉORÈME 3 (Zariski-Nagata). — *Soit* A *un anneau semi-local noethérien. Les conditions suivantes sont équivalentes* :

(i) A *est un anneau de Nagata* ;

(ii) *pour tout idéal premier* $\mathfrak{p}$ *de* A, *la* $\kappa(\mathfrak{p})$*-algèbre* $\kappa(\mathfrak{p}) \otimes_A \hat{A}$ *est séparable* ;

(iii) *pour toute* A*-algèbre réduite* R, *l'anneau* $R \otimes_A \hat{A}$ *est réduit.*

Démontrons d'abord l'équivalence des conditions (ii) et (iii). L'implication (iii) $\Rightarrow$ (ii) est triviale ; supposons inversement que A satisfasse à la condition (ii). Alors, pour toute A-algèbre K qui est un corps, l'anneau $K \otimes_A \hat{A}$ est réduit. Soit maintenant C une A-algèbre réduite de type fini ; l'anneau C, étant noethérien, est isomorphe à un sous-anneau d'un produit fini $K_1 \times \cdots \times K_n$ de corps (IV, § 2, n° 5, prop. 10) ; puisque $\hat{A}$ est plat sur A, l'anneau $C \otimes_A \hat{A}$ est isomorphe à un sous-anneau de l'anneau réduit $\prod_i (K_i \otimes_A \hat{A})$, donc est réduit. Soit enfin R une A-algèbre réduite quelconque ; alors R est réunion de la famille filtrante (C_α) de ses sous-algèbres de type fini, et $R \otimes_A \hat{A}$ est limite inductive de la famille filtrante $(C_\alpha \otimes_A \hat{A})$ d'anneaux réduits, donc est réduit.

Montrons que (ii) implique (i). Soit $\mathfrak{p}$ un idéal premier de A ; le corps des fractions K de l'anneau $A/\mathfrak{p}$ s'identifie à $\kappa(\mathfrak{p})$, et la K-algèbre $K \otimes_{A/\mathfrak{p}} \widehat{(A/\mathfrak{p})}$ s'identifie à $\kappa(\mathfrak{p}) \otimes_{A/\mathfrak{p}} \hat{A}/\mathfrak{p}\hat{A}$, donc à $\kappa(\mathfrak{p}) \otimes_A \hat{A}$. Si $\kappa(\mathfrak{p}) \otimes_A \hat{A}$ est une $\kappa(\mathfrak{p})$-algèbre séparable, l'anneau $A/\mathfrak{p}$ est japonais (n° 2, prop. 3).

Démontrons l'implication (i) $\Rightarrow$ (ii) par récurrence sur dim(A). Elle est évidente si dim(A) = 0 puisqu'alors A est artinien, donc complet. Soit n un entier > 0 ; considérons l'hypothèse suivante :

(R_n) { *pour tout anneau local noethérien de Nagata* C *de dimension* $< n$ *et tout idéal premier* $\mathfrak{r}$ *de* C, *l'anneau* $\kappa(\mathfrak{r}) \otimes_C \hat{C}$ *est réduit.*

Soit A un anneau semi-local noethérien de Nagata de dimension n, soient $\mathfrak{p}$ un idéal premier de A et L une extension finie du corps $\kappa(\mathfrak{p})$; il suffit de démontrer,

sous l'hypothèse (R_n), que l'anneau $L \otimes_A \hat{A}$ est réduit. Notons B la fermeture intégrale de A/p dans L ; puisque A/p est japonais, B est une A-algèbre finie donc un anneau de Nagata semi-local (prop. 4). Notons $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ les idéaux maximaux de B ; l'anneau $L \otimes_A \hat{A}$ s'identifie à un anneau de fractions de $B \otimes_A \hat{A}$, et ce dernier s'identifie au produit des complétés des anneaux locaux $B_{\mathfrak{m}_i}$ (n° 3, lemme 1). Il suffit donc de prouver que, pour tout idéal maximal $\mathfrak{m}$ de B, l'anneau $\hat{B}_{\mathfrak{m}}$ est réduit (II, § 2, n° 6, prop. 17). L'anneau $B_{\mathfrak{m}}$ est local, intégralement clos, de Nagata (prop. 4), et l'on a $\dim(B_{\mathfrak{m}}) \leqslant \dim(B) \leqslant \dim(A) = n$ (VIII, § 1, n° 3, prop. 6 et § 2, n° 3, th. 1). Changeant de notations, on est ramené à prouver, *sous l'hypothèse* (R_n), *que pour tout anneau local noethérien* A *intégralement clos, de Nagata et de dimension* $\leqslant n$, *l'anneau* $\hat{A}$ *est réduit*, c'est-à-dire (n° 3, lemme 2) que $\hat{A}_{\mathfrak{p}'}$ est réduit pour tout idéal premier $\mathfrak{p}' \in \mathrm{Ass}(\hat{A})$. Comme cela est immédiat si $\dim(A) = 0$, on peut supposer $\dim(A) > 0$. Soient alors x un élément non nul de $\mathfrak{m}_A$, et $\mathfrak{q}'$ un idéal premier de $\hat{A}$, minimal parmi ceux qui contiennent $x\hat{A} + \mathfrak{p}'$; puisque $\hat{A}_{\mathfrak{p}'}$ s'identifie à un anneau de fractions de l'anneau $\hat{A}_{\mathfrak{q}'}$, il suffit de prouver que ce dernier est réduit (II, § 2, n° 6, prop. 17). D'après le lemme 3, l'idéal $\mathfrak{q}'$ est associé au $\hat{A}$-module $\hat{A}/x\hat{A}$; puisque $\hat{A}$ est plat sur A, l'image réciproque $\mathfrak{q}$ de $\mathfrak{q}'$ dans A est associée au A-module A/xA (IV, § 2, n° 6, cor. 1 au th. 2). L'anneau A étant supposé intégralement clos, cela implique que $\mathfrak{q}$ est de hauteur 1 (VII, § 1, n° 6, prop. 10), donc que l'anneau $A_{\mathfrak{q}}$ est de valuation discrète (*loc. cit.*, n° 3, corollaire au th. 2 et n° 6, th. 4). Puisque $A/\mathfrak{q}$ est un anneau de Nagata de dimension $< n$, l'anneau $\kappa(\mathfrak{q}) \otimes_{A/\mathfrak{q}} \widehat{A/\mathfrak{q}}$ est réduit d'après l'hypothèse (R_n). L'anneau $\kappa(\mathfrak{q}) \otimes_A \hat{A}$, qui lui est isomorphe, est réduit, ainsi par conséquent que l'anneau $\kappa(\mathfrak{q}) \otimes_{A_{\mathfrak{q}}} \hat{A}_{\mathfrak{q}'}$, qui en est un anneau de fractions. On peut donc appliquer à l'homomorphisme canonique de $A_{\mathfrak{q}}$ dans $\hat{A}_{\mathfrak{q}'}$ le lemme 4 du n° 3 et on en conclut que l'anneau $\hat{A}_{\mathfrak{q}'}$ est réduit, ce qu'on voulait prouver. Le th. 3 est ainsi démontré.

COROLLAIRE 1. — *Le complété d'un anneau de Nagata local et réduit est réduit.*

Il suffit en effet de poser R = A dans le th. 3, (iii).

COROLLAIRE 2 (Chevalley). — *Soient* A *une algèbre réduite de type fini sur un corps, et* p *un idéal premier de* A. *Le complété de l'anneau local* $A_{\mathfrak{p}}$ *est réduit.*

Comme A est réduit, l'anneau local $A_{\mathfrak{p}}$ est réduit ; de plus A est un anneau de Nagata (exemple 1), donc $A_{\mathfrak{p}}$ est un anneau de Nagata (prop. 4), et le cor. 2 résulte du cor. 1, appliqué à l'anneau $A_{\mathfrak{p}}$.

COROLLAIRE 3. — *Soient k un corps de caractéristique* 0, *et* A *une k-algèbre locale et noethérienne. Pour que* A *soit un anneau de Nagata, il faut et il suffit que, pour tout idéal premier* p *de* A, *l'anneau* $\widehat{(A/\mathfrak{p})}$ *soit réduit.*

En effet, puisque les corps $\kappa(\mathfrak{p})$ sont de caractéristique 0, il est équivalent de dire que les algèbres $\kappa(\mathfrak{p}) \otimes_A \hat{A} = \kappa(\mathfrak{p}) \otimes_{A/\mathfrak{p}} \widehat{(A/\mathfrak{p})}$ sont réduites ou qu'elles sont séparables (A, V, p. 117, th. 1), ce qui montre que la condition énoncée est suffisante (th. 3, (ii) $\Rightarrow$ (i)) ; elle est par ailleurs nécessaire (th. 3, (i) $\Rightarrow$ (iii) avec R = A/p).

APPENDICE

1. Limite inductive d'anneaux locaux

Soit I un ensemble préordonné non vide filtrant à droite et soit $(A_\alpha, \varphi_{\beta\alpha})$ un système inductif d'anneaux relatif à I. On suppose que, pour tout $\alpha \in I$, l'anneau A_α est *local*, d'idéal maximal $\mathfrak{m}_\alpha$, que les homomorphismes $\varphi_{\beta\alpha}$ sont *locaux* et *plats*, et qu'on a $\varphi_{\beta\alpha}(\mathfrak{m}_\alpha) A_\beta = \mathfrak{m}_\beta$ pour $\beta \geqslant \alpha$. Notons A la limite inductive des A_α, et pour tout $\alpha \in I$, soit $\varphi_\alpha : A_\alpha \to A$ l'homomorphisme canonique.

PROPOSITION 1. — *a) L'anneau* A *est local, d'idéal maximal* $\mathfrak{m} = \varinjlim \mathfrak{m}_\alpha$. *Pour tout* $\alpha \in I$, *l'homomorphisme* φ_α *est local et plat, et on a* $\varphi_\alpha(\mathfrak{m}_\alpha) A = \mathfrak{m}$.

b) Si A_α *est noethérien pour tout* $\alpha \in A$, *alors* A *est noethérien.*

a) Posons $\mathfrak{m} = \varinjlim \mathfrak{m}_\alpha$; c'est un idéal de A. L'anneau quotient $A/\mathfrak{m}$ est limite inductive des corps $A_\alpha/\mathfrak{m}_\alpha$, donc est un corps (A, I, p. 116, prop. 3). Par ailleurs, tout élément de $A - \mathfrak{m}$ est inversible dans A : en effet, soit $x \in A - \mathfrak{m}$; il existe $\alpha \in I$ et $\xi \in A_\alpha$ tels que $x = \varphi_\alpha(\xi)$; on a $\xi \notin \mathfrak{m}_\alpha$, donc ξ est inversible dans A_α et x est inversible dans A. Par conséquent, A est un anneau local, d'idéal maximal $\mathfrak{m}$. Soit $\alpha \in I$. Des relations $\varphi_{\beta\alpha}(\mathfrak{m}_\alpha) A_\beta = \mathfrak{m}_\beta$ pour $\beta \geqslant \alpha$, on déduit, par passage à la limite inductive, $\varphi_\alpha(\mathfrak{m}_\alpha) A = \mathfrak{m}$; enfin, l'homomorphisme φ_α est plat d'après I, § 2, n° 7, prop. 9.

b) Soient $\hat{A}$ l'anneau séparé complété de A pour la topologie $\mathfrak{m}$-adique et π l'application canonique de A dans $\hat{A}$. Supposons les anneaux A_α noethériens. Fixons $\alpha \in I$ et prouvons que l'anneau $\hat{A}$ est noethérien et plat sur A_α. Par hypothèse, $\mathfrak{m}_\alpha$ est un idéal de type fini de A_α, donc $\mathfrak{m} = \varphi_\alpha(\mathfrak{m}_\alpha)$. A est un idéal de type fini de A. Il s'ensuit que l'idéal maximal $\hat{\mathfrak{m}}$ de $\hat{A}$ est égal à $\mathfrak{m}\hat{A}$ (III, § 2, n° 12, cor. 2 à la prop. 16 et n° 13, prop. 19), donc est de type fini. Par conséquent, l'anneau $\hat{A}$ est noethérien (*loc. cit.*, n° 10, cor. 5 au th. 2). D'autre part, pour tout $n \in \mathbf{N}$, le quotient $\hat{A}/\hat{\mathfrak{m}}^n$ est isomorphe à $A/\mathfrak{m}^n$ (*loc. cit.*, n° 12, cor. 2 à la prop. 16 et formule (21)), ce qui signifie que $\hat{A}/\pi \circ \varphi_\alpha(\mathfrak{m}_\alpha^n)\hat{A}$ est isomorphe à $A \otimes_A (A_\alpha/\mathfrak{m}_\alpha^n)$; puisque A est un A_α-module plat, le $(A_\alpha/\mathfrak{m}_\alpha^n)$-module $\hat{A}/\pi \circ \varphi_\alpha(\mathfrak{m}_\alpha^n)\hat{A}$ est plat pour tout $n \in \mathbf{N}$. D'après III, § 5, n° 4, prop. 2, le A_α-module $\hat{A}$ est idéalement séparé pour $\mathfrak{m}_\alpha$; d'après *loc. cit.*, n° 2, th. 1, le A_α-module $\hat{A}$ est donc plat. Il en résulte par passage à la limite inductive que $\hat{A}$ est (fidèlement) plat sur A (I, § 2, n° 7, prop. 9), donc que A est noethérien (I, § 3, n° 5, corollaire à la prop. 8).

2. Gonflement d'un anneau local

Soit A un anneau local.

On note A]X[l'anneau local de l'anneau de polynômes A[X] en l'idéal premier $\mathfrak{m}_A A[X]$. C'est un anneau local d'idéal maximal $\mathfrak{m}_A A]X[$, l'homomorphisme cano-

nique $A \to A]X[$ est local et plat, et le corps résiduel de $A]X[$ est l'extension pure de κ_A engendrée par la classe de X.

Lemme 1. — *Soit* $P \in A[X]$ *un polynôme unitaire dont l'image* $\overline{P}$ *dans* $\kappa_A[X]$ *est irréductible. Alors la* A*-algèbre* $B = A[X]/(P)$ *est locale et finie sur* A, *d'idéal maximal* $\mathfrak{m}_A B$, *l'homomorphisme canonique* $\rho : A \to B$ *est local et plat, l'extension résiduelle* $\kappa_A \to \kappa_B$ *est algébrique et engendrée par la classe* x *de* X, *et le polynôme minimal de* x *sur* κ_A *est* $\overline{P}$.

Comme le polynôme P est unitaire, le A-module B est libre de type fini (A, IV, p. 10). L'anneau $B/\mathfrak{m}_A B$ s'identifie à $\kappa_A[X]/(\overline{P})$, donc est un corps ; l'idéal $\mathfrak{m}_A B$ est donc maximal. Soit q un idéal maximal de B ; alors l'idéal $\rho^{-1}(q)$ est maximal (V, § 2, n° 1, prop. 1) ; on a donc $\rho^{-1}(q) = \mathfrak{m}_A$, d'où $q \supset \mathfrak{m}_A B$ et enfin $q = \mathfrak{m}_A B$. Ainsi l'anneau B est local. Le lemme 1 en résulte aussitôt.

DÉFINITION 1. — *Soit* A *un anneau local. On dit qu'une* A*-algèbre* B *est un gonflement élémentaire de* A *si* B *est isomorphe à la* A*-algèbre* $A]X[$, *ou bien s'il existe un polynôme unitaire* P *de* $A[X]$, *d'image irréductible dans* $\kappa_A[X]$, *tel que* B *soit isomorphe à la* A*-algèbre* $A[X]/(P)$.

Soit B un gonflement élémentaire de A. De ce qui précède résultent les propriétés suivantes :

a) L'anneau B est local et l'homomorphisme canonique de A dans B est local et plat, et en particulier injectif (I, § 3, n° 5, prop. 8).

b) Le corps résiduel κ_B de B est une extension monogène du corps résiduel κ_A de A. Si κ_A est de degré fini d sur κ_A, alors B est un A-module libre de rang d.

c) On a $\mathfrak{m}_B = \mathfrak{m}_A B$. En particulier, si A est un corps, il en est de même de B. Une extension de corps est un gonflement élémentaire si et seulement si elle est monogène.

d) Si A est noethérien, il en est de même de B.

DÉFINITION 2. — *Soit* A *un anneau local. On dit qu'une* A*-algèbre* B *est un gonflement de* A *s'il existe un ensemble bien ordonné* Λ *ayant un plus grand élément* ω, *et une famille croissante* $(B_\lambda)_{\lambda \in \Lambda}$ *de sous-algèbres de* B *satisfaisant aux conditions suivantes* :

a) *On a* $B_\omega = B$ *et l'anneau* B_λ *est local pour tout* $\lambda \in \Lambda$.

b) *Si* α *est le plus petit élément de* Λ, *la* A*-algèbre* B_α *est isomorphe à* A.

c) *Soit* $\nu \neq \alpha$ *dans* Λ *et soit* S_ν *l'ensemble des* $\lambda \in \Lambda$ *tels que* $\lambda < \nu$. *Si* S_ν *n'a pas de plus grand élément, on a* $B_\nu = \bigcup_{\lambda \in S_\nu} B_\lambda$; *si* S_ν *a un plus grand élément* μ, *alors* B_ν *est un gonflement élémentaire de* B_μ.

Soient B un anneau et $\rho : A \to B$ un homomorphisme d'anneaux. On dit que ρ est un gonflement (resp. un gonflement élémentaire) si la A-algèbre définie par ρ a cette propriété. S'il en est ainsi, ρ est injectif.

Exemples. — 1) *Toute extension de corps est un gonflement.* Soit en effet K une extension d'un corps k. Munissons K d'un bon ordre pour lequel 0 est le plus grand élément, et pour $\lambda \in K$, soit K_λ la sous-k-extension de K engendrée par les éléments β de K tels que $\beta < \lambda$. La vérification des conditions *a*), *b*), *c*), pour k, K et la famille $(K_\lambda)_{\lambda \in K}$, est immédiate.

2) Soient A un anneau local, et I un ensemble d'indices. Notons $A](X_i)_{i\in I}[$ l'anneau local de l'anneau de polynômes $A[(X_i)_{i\in I}]$ en l'idéal premier $\mathfrak{m}_A A[(X_i)_{i\in I}]$. La A-algèbre $A](X_i)_{i\in I}[$ est un gonflement de A. En effet, munissons l'ensemble I d'un bon ordre ; soit Λ l'ensemble bien ordonné obtenu en adjoignant à I un plus grand élément ω. Pour $i \in I$, identifions $A](X_j)_{j<i}[$ à une sous-algèbre B_i de $B = A](X_i)_{i\in I}[$, et posons $B_\omega = B$. La famille $(B_\lambda)_{\lambda\in\Lambda}$ satisfait aux conditions *a*), *b*), *c*).

Remarque. — Avec les notations de la déf. 2, l'anneau B_μ est un gonflement de B_λ lorsque $\lambda \leqslant \mu$.

PROPOSITION 2. — *Soient* A *un anneau local et* B *un gonflement de* A.

a) *L'anneau* B *est local et l'on a* $\mathfrak{m}_A B = \mathfrak{m}_B$.

b) *La* A*-algèbre* B *est fidèlement plate.*

c) *L'homomorphisme canonique*

$$\gamma_B : \mathrm{gr}(A) \otimes_{\kappa_A} \kappa_B \to \mathrm{gr}(B)$$

est bijectif.

d) *Si* A *est noethérien, il en est de même de* B *et les séries de Hilbert-Samuel* (VIII, § 4, n° 3) *de* A *et* B *sont égales.*

Soit $(B_\lambda)_{\lambda\in\Lambda}$ une famille de sous-algèbres de B satisfaisant aux conditions *a*), *b*) et *c*) de la déf. 2.

Soit Λ' l'ensemble des indices $\lambda \in \Lambda$ tels que, pour tout $\mu \leqslant \lambda$ dans Λ, la A-algèbre B_μ soit locale et fidèlement plate, et qu'on ait $\mathfrak{m}_{B_\mu} = \mathfrak{m}_A B_\mu$. Supposons qu'on ait $\Lambda' \neq \Lambda$ et soit ν le plus petit élément de $\Lambda - \Lambda'$. On a $\alpha \in \Lambda'$, d'où $\nu \neq \alpha$. Or S_ν est contenu dans Λ'. Si S_ν n'a pas de plus grand élément, on a $B_\nu = \bigcup_{\lambda\in S_\nu} B_\lambda$ et ν appartient à Λ' d'après la prop. 1 du n° 1. Si S_ν a un plus grand élément μ, on a $\mu \in \Lambda'$ et B_ν est un gonflement élémentaire de B_μ : on a encore $\nu \in \Lambda'$ d'après les remarques qui suivent la déf. 1, d'où une contradiction.

Lorsque A est noethérien, on prouve de manière analogue que l'ensemble Λ'' des indices $\lambda \in \Lambda$ tels que l'anneau B_λ soit noethérien est égal à Λ.

On a donc $\omega \in \Lambda'$, d'où les assertions *a*) et *b*). Lorsque A est noethérien, on a $\omega \in \Lambda''$, donc $B = B_\omega$ est noethérien.

L'assertion *c*) résulte de *a*), *b*), et du th. 1 de III, § 5, n° 2. Supposons A (donc B) noethérien ; comme on a

$$[\mathfrak{m}_B^n/\mathfrak{m}_B^{n+1} : \kappa_B] = [\mathfrak{m}_A^n/\mathfrak{m}_A^{n+1} : \kappa_A]$$

pour tout $n \in \mathbf{N}$, les séries de Hilbert-Samuel de A et B sont égales.

COROLLAIRE. — *Supposons* A *noethérien.*

a) *On a* $\dim(A) = \dim(B)$.

b) *Supposons* A *régulier, et soit* $(x_1, ..., x_n)$ *un système de coordonnées de* A. *Alors* B *est régulier et la suite* $(x_1 1_B, ..., x_n 1_B)$ *est un système de coordonnées de* B.

Cela résulte de la prop. 1 de VIII, § 5, n° 1.

PROPOSITION 3. — *Soient* A, B, C *trois anneaux locaux et* $u : A \to B$, $v : B \to C$ *deux gonflements. Alors* $v \circ u$ *est un gonflement.*

Soient $(B_\lambda)_{\lambda \in \Lambda}$ et $(C_\mu)_{\mu \in M}$ des familles de sous-A-algèbres de B et de sous-B-algèbres de C respectivement, ayant les propriétés *a*), *b*), *c*) de la déf. 2. Sur l'ensemble N somme de Λ et M, considérons la relation d'ordre induisant sur Λ et M les ordres donnés et telle qu'on ait $\lambda < \mu$ pour $\lambda \in \Lambda$, $\mu \in M$. C'est une relation de bon ordre. Pour $\lambda \in \Lambda \subset N$, posons $C_\lambda = v(B_\lambda)$. Alors la famille $(C_\nu)_{\nu \in N}$ satisfait aux conditions *a*), *b*), *c*) de la déf. 1 relativement à la A-algèbre C.

THÉORÈME 1. — *Soient* $f : A \to A'$ *un homomorphisme local surjectif d'anneaux locaux et* B′ *un gonflement de* A′. *Il existe un gonflement* B *de* A *et un isomorphisme de* A*-algèbres de* $B \otimes_A A'$ *sur* B′.

A) *Supposons que* B′ *soit un gonflement élémentaire de* A′. Distinguons deux cas :

1) Si B′ est finie sur A′, choisissons un isomorphisme de A′-algèbres $\varphi : A'[X]/(P') \to B'$, où $P' \in A'[X]$ est un polynôme unitaire d'image irréductible dans $\kappa_{A'}[X]$. Choisissons un polynôme unitaire $P \in A[X]$ dont l'image dans $A'[X]$ est P′. Il est nécessairement irréductible modulo l'idéal maximal de A. Posons alors $B = A[X]/(P)$. La A-algèbre B est un gonflement élémentaire de A et φ induit un isomorphisme de A-algèbres de $B \otimes_A A'$ sur B′.

2) Si B′ n'est pas finie sur A′, choisissons un isomorphisme de A′-algèbres $\psi : A'[X[\to B'$. Posons $B = A]X[$. La A-algèbre B est un gonflement élémentaire de A, et $B \otimes_A A'$ est canoniquement isomorphe à $A']X[$. Par suite ψ induit un isomorphisme de A-algèbres de $B \otimes_A A'$ sur B′.

B) *Passons au cas général.* Soit $(B'_\lambda)_{\lambda \in \Lambda}$ une famille de sous-A′-algèbres de B′ ayant relativement à A′ et B′ les propriétés *a*), *b*), *c*) de la déf. 2. Nous allons définir par récurrence transfinie un système inductif $(\tilde{B}_\lambda, i_{\mu\lambda})$ relatif à Λ d'anneaux locaux et d'homomorphismes locaux injectifs, et des isomorphismes $u_\lambda : \tilde{B}_\lambda \otimes_A A' \to B'_\lambda$ tels que, pour $\lambda \leqslant \mu$, $u_\mu \circ (i_{\mu\lambda} \otimes \mathrm{Id}_{A'}) \circ u_\lambda^{-1}$ soit l'injection canonique de B'_λ dans B'_μ.

Si α est le plus petit élément de Λ, on pose $\tilde{B}_\alpha = A$, $i_{\alpha\alpha} = \mathrm{Id}_A$ et on prend pour u_α l'isomorphisme canonique $A \otimes_A A' \to A'$.

Soit $\nu \in \Lambda$, et supposons $\tilde{B}_\lambda$, u_λ et $i_{\mu\lambda}$ construits lorsque $\lambda \leqslant \mu < \nu$. Soit S_ν l'ensemble des éléments ε de Λ tels que $\varepsilon < \nu$. Si S_ν n'a pas de plus grand élément, on prend pour $\tilde{B}_\nu$ la limite inductive des $\tilde{B}_\lambda$ pour $\lambda \in S_\nu$, pour u_ν l'isomorphisme composé $\tilde{B}_\nu \otimes_A A' \to \varinjlim(\tilde{B}_\lambda \otimes_A A') \to \varinjlim B'_\lambda \to B'_\nu$, et pour $i_{\nu\lambda}$, lorsque $\lambda \in S_\nu$, l'application canonique de $\tilde{B}_\lambda$ dans $\tilde{B}_\nu$. Si S_ν a un plus grand élément μ, alors B'_ν est un gonflement élémentaire de B'_μ. D'après A), il existe un gonflement élémentaire

$i_{\nu\mu} : \tilde{B}_\mu \to \tilde{B}_\nu$ et un isomorphisme de $\tilde{B}_\mu$-algèbres de $\tilde{B}_\nu \otimes_{\tilde{B}_\mu} B'_\mu$ sur B'_ν. Prenons pour u_ν l'isomorphisme de A-algèbres composé

$$\tilde{B}_\nu \otimes_A A' \to \tilde{B}_\nu \otimes_{\tilde{B}_\mu} (\tilde{B}_\mu \otimes_A A') \to \tilde{B}_\nu \otimes_{\tilde{B}_\mu} B'_\mu \to B'_\nu$$

et pour $i_{\nu\lambda}$, lorsque $\lambda \in S_\nu$, l'homomorphisme $i_{\nu\mu} \circ i_{\mu\lambda}$.

Posons alors $B = \tilde{B}_\omega$ et, pour tout $\lambda \in \Lambda$, notons B_λ l'image de $\tilde{B}_\lambda$ par l'injection canonique $\tilde{B}_\lambda \to B$. La famille $(B_\lambda)_{\lambda \in \Lambda}$ satisfait aux conditions *a*), *b*), *c*) de la déf. 2, et B est un gonflement de A. D'autre part, l'homomorphisme u_ω est un A'-isomorphisme de $B \otimes_A A'$ dans B'.

COROLLAIRE. — *Soient* A *un anneau local et* K *une extension de son corps résiduel* κ_A. *Il existe un anneau local* B *et un gonflement* $A \to B$ *tels que la* κ_A*-algèbre* κ_B *soit isomorphe à* K.

En effet, l'homomorphisme $\kappa_A \to K$ est un gonflement (exemple 1). Appliquant le th. 1 avec $A' = \kappa_A$ et $B' = K$, on obtient l'existence d'un gonflement B de A et d'un A-isomorphisme de $B/\mathfrak{m}_A B$ sur K, d'où le corollaire.

3. Existence des *p*-anneaux

PROPOSITION 4. — *Soient p un nombre premier, k un corps de caractéristique p, et soit n un entier* $\geqslant 1$, *ou* $+\infty$. *Il existe un p-anneau* (§ 2, n° 1, déf. 1) *de longueur n dont le corps résiduel est isomorphe à k.*

On peut considérer k comme une extension du corps résiduel $\mathbf{Z}/p\mathbf{Z}$ de l'anneau local $\mathbf{Z}_{(p)}$. D'après le corollaire du th. 1, il existe un anneau local B, gonflement de $\mathbf{Z}_{(p)}$, tel que κ_B soit isomorphe à k. L'anneau local $\mathbf{Z}_{(p)}$ est régulier et $\{p\}$ est un système de coordonnées de $\mathbf{Z}_{(p)}$. D'après le corollaire de la prop. 2 du n° 2, l'anneau B est régulier et $\{p1_B\}$ est un système de coordonnées de B. Autrement dit, B est un anneau de valuation discrète, d'idéal maximal pB. Le complété C de B est alors un p-anneau de longueur infinie et le corps résiduel κ_C est isomorphe à κ_B, donc à k. De plus, pour tout entier $n \geqslant 1$, C/p^nC est un p-anneau de longueur n, de corps résiduel isomorphe à κ_C, donc à k.

Exercices

§ 1

Dans les exercices 1 à 27, p est un nombre premier fixé. Si A est un anneau, l'anneau des vecteurs de Witt W(A) est celui attaché au nombre premier p.

1) Soit A un anneau. L'endomorphisme V du groupe additif W(A) peut-il être compatible à la multiplication de W(A) ?

2) Notons A l'anneau $\mathbf{Z}[(X_n)_{n\in\mathbf{N}}, (Y_n)_{n\in\mathbf{N}}]$ des polynômes en les deux familles d'indéterminées (X_n) et (Y_n), et B l'anneau $\mathbf{Z}[X, Y]$ des polynômes en deux indéterminées X et Y. Pour tout polynôme R de B, il existe une suite unique de polynômes $(R_n)_{n\in\mathbf{N}}$ de A telle que l'on ait, pour tout $n \in \mathbf{N}$,

$$R(\Phi_n(X_0, ..., X_n), \Phi_n(Y_0, ..., Y_n)) = \Phi_n(R_0, ..., R_n) .$$

On a $R_0 = R(X_0, Y_0)$ et R_n ne dépend pas des X_i et Y_i pour $i > n$. Si R est homogène de degré r par rapport à X (resp. Y, resp. (X, Y)) et qu'on attribue pour tout $i \in \mathbf{N}$, le poids p^i à X_i et Y_i, alors R_n est isobare de poids rp^n par rapport à $(X_i)_{i\in\mathbf{N}}$ (resp. $(Y_i)_{i\in\mathbf{N}}$, resp. $((X_i)_{i\in\mathbf{N}}, (Y_i)_{i\in\mathbf{N}})$). Si R est constant, R_n est constant. Examiner les cas $R = 0, 1, -1, X + Y, XY, -X$.

3) *a*) Il existe une unique suite de polynômes $(R_n)_{n\in\mathbf{N}}$ de $\mathbf{Z}[X, Y]$ telle que, pour tout entier $n \geqslant 0$, on ait

$$X^{p^n} + Y^{p^n} = \sum_{i=0}^{n} p^i R_i(X, Y)^{p^{n-i}} .$$

b) Si p est impair, on a, pour tout $n \in \mathbf{N}$,

$$R_n(X, -X) = 0 .$$

Si $p = 2$, on a

$$R_1(X, Y) = -XY$$

et

$$R_n(X, X) \equiv 0 \bmod 2 \quad \text{pour} \quad n \geqslant 2 .$$

4) Soient A un anneau, $\boldsymbol{a} = (a_n)_{n\in\mathbf{N}}$ un élément de W(A), $\boldsymbol{a}^{(p)}$ l'élément $(a_n^p)_{n\in\mathbf{N}}$ de W(A). Posons

$$\boldsymbol{b} = (b_n)_{n\in\mathbf{N}} = p.\boldsymbol{a} - V\boldsymbol{a}^{(p)} .$$

Prouver que l'on a $b_n - pa_n \in p^{p-1}A$ pour tout $n \in \mathbf{N}$. (Se ramener au cas où $A = \mathbf{Z}[(X_n)_{n\in\mathbf{N}}]$ et $\boldsymbol{a} = (X_n)_{n\in\mathbf{N}}$ et utiliser la prop. 1 du § 1, n° 1.)

5) Soit A un anneau de caractéristique p.
a) L'anneau W(A) est intègre si et seulement si A est intègre.
b) W(A) est réduit si et seulement si A est réduit.
c) Les conditions suivantes sont équivalentes :
(i) A est un anneau parfait de caractéristique p.
(ii) $W(A)/pW(A)$ est réduit.

6) Soit A une $\mathbf{Z}_{(p)}$-algèbre. Soient n un entier, $n \geqslant 1$, $\boldsymbol{g} = (g_0, ..., g_{n-1})$ un élément de $W_n(A)$, et $f = g_0$. Alors notant A_f (resp. $W_n(A)_{\boldsymbol{g}}$) le localisé de A (resp. $W_n(A)$) par rapport au système multiplicatif des puissances de f (resp. $\boldsymbol{g}$), on a $W_n(A_f) = W_n(A)_{\boldsymbol{g}}$.

7) Soit A un anneau de caractéristique p. Prouver que les topologies $\mathcal{C}$ et p-adique de W(A) coïncident si et seulement si A est parfait.

8) Soient A un anneau, et ξ un élément de A vérifiant $\sum_{i=0}^{p-1} \xi^i = 0$. On a alors, dans W(A), l'équation

$$V_A(\mathbf{1}) = \sum_{i=0}^{p-1} \tau_A(\xi^i).$$

En déduire que si A est de caractéristique p, on a

$$V_A \circ F_A(\boldsymbol{a}) = p.\boldsymbol{a} \quad \text{pour tout} \quad \boldsymbol{a} \in W(A).$$

9) Soit A un corps de caractéristique p. Montrer que l'anneau W(A) est noethérien si et seulement si A est parfait. (Calculer la dimension sur A de l'espace vectoriel $V_1(A)/V_1(A)^2$.)

10) Soit k un corps de caractéristique p, possédant une p-base finie. Soient A un anneau et φ un homomorphisme de k dans A, qui fasse de A une k-algèbre de type fini.
a) Pour tout entier $n \geqslant 1$, A est un module de type fini sur A^{p^n}.
b) Pour tout entier $n \geqslant 1$, $W_n(A)$ est une $W_n(k)$-algèbre de type fini.
(Si $a_1, ..., a_N$ engendrent A comme k-algèbre et comme $A^{p^{n-1}}$-module, prouver que les éléments $V^j\tau(a_i)$, $1 \leqslant i \leqslant N$, $0 \leqslant j \leqslant n-1$, engendrent la $W_n(k)$-algèbre $W_n(A)$.)

11) Soit A un anneau de caractéristique p.
a) Soit $n \in \mathbf{N}$; prouver qu'on a $p^{n-1}/n\,! \in \mathbf{Z}_{(p)}$. Prouver que $(nm)\,!/n\,!(m\,!)^n$ est un entier pour n, m dans $\mathbf{N}$.
b) Pour $n \in \mathbf{N}$, soit $\gamma_n : V_1(A) \to W(A)$ l'application définie par

$$\gamma_n(Vx) = 1 \qquad \text{si } n = 0,$$
$$\gamma_n(Vx) = (p^{n-1}/n\,!)\,V(x^n) \qquad \text{si } n \geqslant 1.$$

(i) Prouver qu'on a $\gamma_n(x) \in V_1(A)$ si $n \geqslant 1$ et $x \in V_1(A)$.
(ii) Pour $x, y \in V_1(A)$ et $n \in \mathbf{N}$, on a

$$\gamma_n(x + y) = \sum_{i=0}^{n} \gamma_i(x)\,\gamma_{n-i}(y).$$

(iii) Pour $\lambda \in W(A)$, $x \in V_1(A)$, $n \in \mathbf{N}$, on a

$$\gamma_n(\lambda x) = \lambda^n \gamma_n(x).$$

(iv) Pour $x \in V_1(A)$ et n, m dans $\mathbf{N}$, on a

$$\gamma_n(x)\,\gamma_m(x) = \binom{m+n}{n} \gamma_{n+m}(x)$$

et

$$\gamma_n(\gamma_m(x)) = \frac{(nm)\,!}{n\,!(m\,!)^n}\,\gamma_{nm}(x).$$

(v) On a $F\gamma_n(Vx) = (p^n/n\,!)\,x^n$ et $\gamma_n(px) = (p^n/n\,!)\,x^n$, pour $x \in W(A)$.

12) Soit A un anneau de caractéristique p. Pour tout élément $\boldsymbol{a} = (a_n)_{n\in\mathbf{N}}$ de W(A) et tout entier $n \in \mathbf{N}$, posons $\boldsymbol{a}_+ = (a_{n+1})_{n\in\mathbf{N}}$.
a) On a $\boldsymbol{a} = \tau(a_0) + \mathrm{V}\boldsymbol{a}_+$.
b) Notons $\alpha : \mathrm{W(A)} \to \mathrm{W(A)}$ l'application qui à $\boldsymbol{a} = (a_n)_{n\in\mathbf{N}}$ associe

$$\alpha(\boldsymbol{a}) = \boldsymbol{a}_+ - \sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} \tau(\alpha_0)^{p-i}(\mathrm{V}\boldsymbol{a}_+)^i - (p-1)!\,\gamma_p(\mathrm{V}\boldsymbol{a}_+),$$

où (*cf.* exercice précédent) on a posé $\gamma_p(\mathrm{V}\boldsymbol{a}_+) = (p^{p-1}/p!)\,\mathrm{V}(\boldsymbol{a}_+^p)$. Prouver que l'on a, dans W(A), l'égalité $\mathrm{F}\boldsymbol{a} = \boldsymbol{a}^p + p\alpha(\boldsymbol{a})$.
c) Prouver que, pour tout entier $n \geqslant 1$, α définit, par passage aux quotients, une application α_n de $\mathrm{W}_{n+1}(\mathrm{A})$ dans $\mathrm{W}_n(\mathrm{A})$.

13) Soit A un anneau de caractéristique p. La filtration de W(A) par les idéaux $\mathrm{V}_n(\mathrm{A})$ est compatible à la structure d'anneau de W(A) et on note $\mathrm{gr}_{\mathrm{V}}(\mathrm{W(A)})$ l'anneau gradué associé. Pour tout entier $n \geqslant 0$, on notera $\varphi^n_*\mathrm{A}$ l'anneau A muni de la structure de A-algèbre donnée par l'homomorphisme $\varphi^n : \mathrm{A} \to \mathrm{A}$, où φ désigne l'élévation à la puissance p-ième. Prouver que, pour tout entier $n \geqslant 0$, l'application de A dans $\mathrm{V}_n(\mathrm{A})/\mathrm{V}_{n+1}(\mathrm{A})$ qui à $x \in \mathrm{A}$ associe la classe de $\mathrm{V}^n\tau(x)$, est un isomorphisme du A-module $\varphi^n_*\mathrm{A}$ sur le A-module $\mathrm{gr}^n_{\mathrm{V}}(\mathrm{W(A)})$.

Munissons le A-module $\bigoplus_{n\in\mathbf{N}} \varphi^n_*\mathrm{A}$ de la structure d'anneau gradué donnée par les applications $(x, y) \mapsto \varphi^n x.\varphi^m y$ de $\varphi^m_*\mathrm{A} \times \varphi^n_*\mathrm{A}$ dans $\varphi^{m+n}_*\mathrm{A}$ (pour tout couple d'entiers positifs (m, n)). Montrer que les isomorphismes précédents définissent un isomorphisme de A-algèbres graduées de $\bigoplus_{n\in\mathbf{N}} \varphi^n_*\mathrm{A}$ sur $\mathrm{gr}_{\mathrm{V}}(\mathrm{W(A)})$.

14) Soit A un anneau. On suppose que la multiplication par $p.1_{\mathrm{A}}$ est injective dans A. Soit σ un endomorphisme de A tel que $\sigma(x) \equiv x^p \bmod p\mathrm{A}$, pour tout $x \in \mathrm{A}$.
a) Il existe un unique homomorphisme d'anneaux s_σ de A dans W(A) qui vérifie

$$s_\sigma \circ \sigma = \mathrm{F}_{\mathrm{A}} \circ s_\sigma$$

et

$$\Phi_0 \circ s_\sigma = \mathrm{Id}_{\mathrm{A}}.$$

C'est aussi l'unique homomorphisme s_σ de A dans W(A) qui vérifie, pour tout entier n positif, $\Phi_n \circ s_\sigma = \sigma^n$.
b) Soit B un anneau. On suppose que la multiplication par $p.1_{\mathrm{B}}$ est injective dans B. Soit σ' un endomorphisme de B tel que $\sigma'(x) \equiv x^p \bmod p\mathrm{B}$ pour tout $x \in \mathrm{B}$. Soit u un homomorphisme de A dans B vérifiant $u \circ \sigma = \sigma' \circ u$. Alors on a $\mathrm{W}(u) \circ s_\sigma = s_{\sigma'} \circ u$.
c) Si t_σ désigne le composé de s_σ et de la projection canonique de W(A) sur $\mathrm{W(A}/p\mathrm{A)}$, prouver que t_σ induit, pour tout entier $n \geqslant 1$, un homomorphisme $t_{\sigma,n}$ de $\mathrm{A}/p^n\mathrm{A}$ dans $\mathrm{W}_n(\mathrm{A}/p\mathrm{A})$.
d) Si $\mathrm{A}/p\mathrm{A}$ est parfait, prouver que $t_{\sigma,n}$ est un isomorphisme. (Munissant A de la filtration par les puissances de l'idéal $p\mathrm{A}$ et notant $\mathrm{gr}_p(\mathrm{A})$ l'anneau gradué associé, on montrera que l'homomorphisme de $\mathrm{gr}_p(\mathrm{A})$ dans $\mathrm{gr}_{\mathrm{V}}(\mathrm{W}(\mathrm{A}/p\mathrm{A}))$ (*cf.* exerc. 13) induit par t_σ est un isomorphisme.)
e) Si $\mathrm{A}/p\mathrm{A}$ est parfait, et que A est séparé et complet pour la topologie p-adique, t_σ est un isomorphisme de A sur $\mathrm{W(A}/p\mathrm{A)}$.

15) *a*) Soit A un anneau tel que la multiplication par $p.1_{\mathrm{A}}$ dans A soit injective. Alors il existe un unique homomorphisme d'anneaux s_{A} de W(A) dans W(W(A)) qui vérifie

$$s_{\mathrm{A}} \circ \mathrm{F}_{\mathrm{A}} = \mathrm{F}_{\mathrm{W(A)}} \circ s_{\mathrm{A}}$$

et

$$\Phi_0 \circ s_{\mathrm{A}} = \mathrm{Id}_{\mathrm{W(A)}}$$

(où Φ_0 est la projection de W(W(A)) sur W(A)). C'est aussi l'unique homomorphisme d'anneaux qui vérifie $\Phi_n \circ s_{\mathrm{A}} = \mathrm{F}^n_{\mathrm{A}}$ pour tout entier $n \in \mathbf{N}$ (où $\Phi_n : \mathrm{W(W(A))} \to \mathrm{W(A)}$ est la n-ième composante fantôme dans W(W(A))).
b) Considérons l'anneau $\mathcal{A} = \mathbf{Z}[(\mathrm{X}_n)_{n\in\mathbf{N}}]$ des polynômes en une famille d'indéterminées $(\mathrm{X}_n)_{n\in\mathbf{N}}$. Soit $\mathbf{X}$ l'élément $(\mathrm{X}_n)_{n\in\mathbf{N}}$ de $\mathrm{W}(\mathcal{A})$. Posons $s_{\mathcal{A}}(\mathbf{X}) = (s_n(\mathbf{X}))_{n\in\mathbf{N}}$, où $s_n(\mathbf{X}) \in \mathrm{W}(\mathcal{A})$. Pour

tout anneau A, définissons l'application s_A de W(A) dans W(W(A)) par la formule $s_A(a) = (s_n(a))_{n\in\mathbf{N}}$. Prouver que s_A est un homomorphisme d'anneaux vérifiant

$$s_A \circ F_A = F_{W(A)} \circ s_A$$

et

$$\Phi_0 \circ s_A = \mathrm{Id}_{W(A)}.$$

c) Pour tout homomorphisme d'anneaux $u : B \to A$, on a

$$s_A \circ W(u) = W(W(u)) \circ s_B.$$

d) Les applications $W(s_A) \circ s_A$ et $s_{W(A)} \circ s_A$ de W(A) dans W(W(W(A))) sont égales.
e) Pour tout $x \in A$, on a $s_A(\tau_A(x)) = \tau_{W(A)}(\tau_A(x))$.
f) On a $s_A \circ V_A = V_{W(A)} \circ s_A$, et l'application s_A est continue quand on munit W(A) et W(W(A)) des topologies $\mathfrak{C}$.

16) *a*) Soient A, B deux anneaux et φ un homomorphisme de A dans B. Alors l'application $W(\varphi)$ permet de munir l'ensemble W(B) et, pour tout $m \in \mathbf{N}$, l'ensemble $W_m(B)$, d'une structure de W(A)-module. Si m et n sont deux entiers $\geqslant 0$, tels que $n \geqslant m$, l'application canonique de $W_n(B)$ sur $W_m(B)$ est W(A)-linéaire. En outre, W(B) est le W(A)-module limite projective des $W_m(B)$.
b) Soient A, B deux anneaux et ψ un homomorphisme de W(A) dans B. Posons $\tilde{\psi} = W(\psi) \circ s_A$ (*cf.* exerc. 15). L'application $\tilde{\psi}$ de W(A) dans W(B) permet de munir l'ensemble W(B) et, pour tout $m \in \mathbf{N}$, l'ensemble $W_m(B)$, d'une structure de W(A)-module, et les deux dernières assertions de *a*) sont encore vraies. Si φ est un homomorphisme de A dans B tel que $\psi = \varphi \circ \Phi_0$, on a $\tilde{\psi} = W(\varphi)$.

17) Soit A l'anneau $\mathbf{Q}[X]$. Soit $\boldsymbol{\Omega} = (\Omega_n)_{n\in\mathbf{N}}$ l'élément de A qui vérifie $\Phi_A(\boldsymbol{\Omega}) = (X, X, ..., X, ...)$. Pour tout élément a de $\mathbf{Z}_p$, posons

$$\boldsymbol{\Omega}(a) = (\Omega_n(a))_{n\in\mathbf{N}}.$$

a) Pour tout $a \in \mathbf{Z}_p$, et tout entier $n \in \mathbf{N}$, on a $\Omega_n(a) \in \mathbf{Z}_p$.
b) Pour tout $a \in \mathbf{Z}$ et tout entier $n \in \mathbf{N}$, on a $\Omega_n(a) \in \mathbf{Z}$, et, si $a \in \mathbf{N}$, $\boldsymbol{\Omega}(a)$ est l'élément de $W(\mathbf{Z})$ somme de a termes égaux à l'élément unité de $W(\mathbf{Z})$.
c) L'application $a \mapsto \boldsymbol{\Omega}(a)$ définit un homomorphisme de $\mathbf{Z}_p$ dans $W(\mathbf{Z}_p)$ qui, quand on identifie $\mathbf{Z}_p$ avec $W(\mathbf{F}_p)$ (§ 1, n° 7, exemple 3), coïncide avec l'homomorphisme $s_{\mathbf{F}_p}$ défini dans l'exerc. 15.

18) *a*) Soit L un corps (commutatif). Soient G un groupe d'automorphismes de L et K le corps des invariants de G. Alors tout élément g de G agit sur W(L) (par $W(g)$) et, pour tout entier $n \geqslant 1$, sur $W_n(L)$. L'ensemble des éléments de W(L) (resp. $W_n(L)$) invariants sous l'action de G est W(K) (resp. $W_n(K)$).
b) Supposons que L soit une extension galoisienne finie de K, et notons $\mathbf{Z}[G]$ l'algèbre sur $\mathbf{Z}$ du groupe (fini) G. Pour tout $\mathbf{Z}$-module M, notons M^G le $\mathbf{Z}[G]$-module $\mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}[G], M)$ (muni de sa structure naturelle de $\mathbf{Z}[G]$-module à gauche). Prouver que le $\mathbf{Z}[G]$-module W(L) (resp. $W_n(L)$) est isomorphe à $W(K)^G$ (resp. $W_n(K)^G$). En déduire qu'on a

$$H^i(G, W(L)) = 0 \quad (\text{resp. } H^i(G, W_n(L)) = 0)$$

pour tout entier $i > 0$. (Utiliser le théorème de la base normale A, V, p. 70, th. 6 et A, X, p. 111 à 113.)

19) Soient K un corps de caractéristique p, P son sous-corps premier, Ω une clôture algébrique de K. On note $\wp$ l'endomorphisme $x \mapsto Fx - x$ du groupe $W(\Omega)$, et aussi, pour tout entier $n \geqslant 1$, l'endomorphisme de $W_n(\Omega)$ qu'il induit par passage aux quotients.
a) Fixons un entier $n \geqslant 1$. L'endomorphisme $\wp$ de $W(\Omega)$ (resp. $W_n(\Omega)$) laisse stable W(K) (resp. $W_n(K)$) et son noyau est W(P) (resp. $W_n(P)$).
On identifiera, dans la suite de cet exercice, W(P) et $\mathbf{Z}_p$, $W_n(P)$ et $\mathbf{Z}/p^n\mathbf{Z}$ (§ 1, n° 7, exemple 3).

b) Soit $\boldsymbol{a} \in W_n(K)$. Notant V l'homomorphisme de décalage $W_n(K) \to W_{n+1}(K)$, prouver que l'on a $\boldsymbol{a} \in \wp W_n(K)$ si et seulement si l'on a $V\boldsymbol{a} \in \wp W_{n+1}(K)$. Si K est séparablement clos, on a $\wp W_n(K) = W_n(K)$.

c) Soit $\boldsymbol{a} \in W_n(\Omega)$ tel que $\wp \boldsymbol{a} \in W_n(K)$. On note $K(\boldsymbol{a})$ le sous-corps de Ω engendré par K et les composantes $a_0, \ldots, a_{n-1}$ de $\boldsymbol{a}$. Si A est une partie de $W_n(K)$, on note $K(\wp^{-1}(A))$ la sous-extension de Ω engendrée par les corps $K(\boldsymbol{a})$, pour tous les éléments $\boldsymbol{a}$ de $W_n(\Omega)$ vérifiant $\wp \boldsymbol{a} \in A$.

Raisonnant comme dans A, V, p. 87 et utilisant l'exercice précédent, prouver les assertions suivantes :

(i) Soit L une extension galoisienne de K dans Ω. Il existe une unique application $(\sigma, a) \mapsto [\sigma, a\rangle$ de $\mathrm{Gal}(L/K) \times (\wp W_n(L) \cap W_n(K))/\wp W_n(K)$ dans $\mathbf{Z}/p^n\mathbf{Z}$ telle que pour tout $\sigma \in \mathrm{Gal}(L/K)$ et tout $x \in W_n(L)$ tel que $\wp(x) \in W_n(K)$, on ait, en notant $\overline{\wp(x)}$ la classe de $\wp(x)$ modulo $\wp W_n(K)$

$$[\sigma, \overline{\wp(x)}\rangle = \sigma x - x .$$

Si $\sigma, \sigma' \in \mathrm{Gal}(L/K)$ et $a, a' \in (\wp W_n(L) \cap W_n(K))/\wp W_n(K)$, on a

$$[\sigma\sigma', a\rangle = [\sigma, a\rangle + [\sigma', a\rangle$$

et

$$[\sigma, a + a'\rangle = [\sigma, a\rangle + [\sigma, a'\rangle .$$

(ii) Notons, pour toute extension galoisienne L de K dans Ω,

$$a_L : (\wp W_n(L) \cap W_n(K))/\wp W_n(K) \to \mathrm{Hom}(\mathrm{Gal}(L/K), \mathbf{Z}/p^n\mathbf{Z})$$

et

$$a'_L : \mathrm{Gal}(L/K) \to \mathrm{Hom}((\wp W_n(L) \cap W_n(K))/\wp W_n(K), \mathbf{Z}/p^n\mathbf{Z})$$

les homomorphismes déduits de l'application $(\sigma, a) \mapsto [\sigma, a\rangle$ construite en (i). Pour toute extension galoisienne L de K dans Ω, l'homomorphisme a_L est injectif, et son image est le groupe des homomorphismes continus du groupe topologique $\mathrm{Gal}(L/K)$ dans le groupe discret $\mathbf{Z}/p^n\mathbf{Z}$.

(iii) L'application $A \mapsto K(\wp^{-1}(A))$ est une bijection de l'ensemble des sous-groupes de $W_n(K)$ contenant $\wp W_n(K)$ sur l'ensemble des extensions de K dans Ω, abéliennes sur K et d'exposant divisant p^n. L'application réciproque est $L \mapsto \wp W_n(L) \cap W_n(K)$.

(iv) Pour tout sous-groupe A de $W_n(K)$ contenant $\wp W_n(K)$, l'homomorphisme

$$a'_{K(\wp^{-1}(A))} : \mathrm{Gal}(K(\wp^{-1}(A))/K) \to \mathrm{Hom}(A/\wp W_n(K), \mathbf{Z}/p^n\mathbf{Z})$$

est bijectif. Lorsqu'on munit $\mathrm{Hom}(A/\wp W_n(K), \mathbf{Z}/p^n\mathbf{Z})$ de la topologie de la convergence simple, c'est un homéomorphisme.

20) Conservons les hypothèses et notations de l'exercice précédent.

a) Pour chaque extension L de K dans Ω, considérons le $\mathbf{Z}_p$-module

$$\mathfrak{W}(L) = (W(L)/\wp W(L)) \otimes_{\mathbf{Z}_p} (\mathbf{Q}_p/\mathbf{Z}_p)$$

et pour chaque entier $n \geqslant 0$ son sous-module

$$\mathfrak{W}_n(L) = (W(L)/\wp W(L)) \otimes_{\mathbf{Z}_p} (p^{-n}\mathbf{Z}_p/\mathbf{Z}_p) .$$

Prouver que $\mathfrak{W}(L)$ s'identifie à la limite inductive de ses sous-modules $\mathfrak{W}_n(L)$ selon les applications d'inclusion

$$i_n : \mathfrak{W}_n(L) \to \mathfrak{W}_{n+1}(L) .$$

b) Pour tout entier $n \geqslant 0$, soit ψ_n l'application de $\mathfrak{W}_n(L)$ dans $W_n(L)/\wp W_n(L)$ qui à $x \otimes p^{-n}$ associe la classe de x. Prouver que ψ_n est un isomorphisme et qu'on a

$$V_n \circ \psi_n = \psi_{n+1} \circ i_n ,$$

où V_n est l'application de $W_n(L)/\wp W_n(L)$ dans $W_{n+1}(L)/\wp W_{n+1}(L)$ induite par le décalage V. En déduire que $\mathfrak{W}(L)$ s'identifie à la limite inductive des groupes $W_n(L)/\wp W_n(L)$ selon les applications V_n.

c) Soit $a \in \mathfrak{W}(K)$. Si n est un entier tel que a appartienne à $\mathfrak{W}_n(K)$, on a construit à l'exerc. 19, *c*) l'extension $K(\wp^{-1}(\psi_n(a)))$. Cette extension ne dépend pas du choix de l'entier n ; on la note $K(\wp^{-1}(a))$. Si A est une partie de $\mathfrak{W}(K)$, on notera $K(\wp^{-1}(A))$ l'extension engendrée par les corps $K(\wp^{-1}(a))$ pour a parcourant A. Prouver que $K(\wp^{-1}(A))$ est une extension abélienne de K. Prouver dans cette situation des assertions analogues aux assertions (i) à (iv) de l'exerc. 19, *c*).

21) Conservons les hypothèses et notations des deux exercices précédents.
a) La multiplication par p dans $W(K)/\wp W(K)$ est injective.
b) Soit $\boldsymbol{a}$ un élément de $W(\Omega)$ tel que $\boldsymbol{a} \notin W(K)$ et $\wp \boldsymbol{a} \in W(K)$. On note $K(\boldsymbol{a})$ le sous-corps de Ω engendré sur K par les composantes $(a_n)_{n\in\mathbf{N}}$ de $\boldsymbol{a}$. Prouver que $K(\boldsymbol{a})$ est une extension abélienne de K, dont le groupe de Galois est isomorphe au groupe topologique $\mathbf{Z}_p$.
c) Si A est une partie de W(K), on note $K(\wp^{-1}(A))$ la sous-extension de Ω engendrée par les corps $K(\boldsymbol{a})$ pour tous les éléments $\boldsymbol{a}$ de $W(\Omega)$ tels que $\wp \boldsymbol{a} \in A$. Prouver dans cette situation des assertions analogues aux assertions (i) à (iv) de l'exerc. 19, *c*).
d) Soit Γ le groupe des automorphismes de Ω sur K. Soient n un entier $\geqslant 1$ et φ_n un homomorphisme continu de Γ dans $\mathbf{Z}/p^n\mathbf{Z}$. Prouver qu'il existe un homomorphisme continu φ de Γ dans $\mathbf{Z}_p$ qui induise φ_n par passage au quotient. Désignant par $\mathrm{Hom}_c(\Gamma, \Gamma')$ le groupe des homomorphismes continus de Γ dans Γ', Γ' étant un groupe topologique, prouver que l'application canonique

$$\mathrm{Hom}_c(\Gamma, \mathbf{Z}_p) \otimes_{\mathbf{Z}_p} (\mathbf{Q}_p/\mathbf{Z}_p) \to \mathrm{Hom}_c(\Gamma, \mathbf{Q}_p/\mathbf{Z}_p)$$

est un isomorphisme.

22) Soit A une $\mathbf{Z}_{(p)}$-algèbre. On note $\mathfrak{D}_A$ l'algèbre sur W(A) engendrée par deux indéterminées **F** et **V** soumises aux relations

$$\begin{aligned} \mathbf{F}a &= (\mathrm{F}a).\mathbf{F} && \text{pour} \quad a \in \mathrm{W}(\mathrm{A}) \\ a\mathbf{V} &= \mathbf{V}(\mathrm{F}a) && \text{pour} \quad a \in \mathrm{W}(\mathrm{A}) \\ \mathbf{FV} &= p \\ \mathbf{V}a\mathbf{F} &= \mathbf{V}a && \text{pour} \quad a \in \mathrm{W}(\mathrm{A}), \end{aligned}$$

où F et V désignent respectivement les homomorphismes de Frobenius et de décalage de W(A).
a) Soit B une A-algèbre. Faisant agir **F** et **V** sur W(B) par les homomorphismes de Frobenius et de décalage de W(B), on munit W(B) d'une structure de $\mathfrak{D}_A$-module. De même pour chaque entier $n \geqslant 1$, $W_n(B)$ est un $\mathfrak{D}_A$-module.
b) Pour tout élément x de $\mathfrak{D}_A$, il existe une famille $(a_i)_{i\in\mathbf{Z}}$, à support fini, d'éléments de W(A), caractérisée par l'égalité

$$x = \sum_{n\geqslant 1} a_{-n}\, \mathbf{F}^n + a_0 + \sum_{n\geqslant 1} \mathbf{V}^n a_n .$$

c) Supposons W(A) intègre. Soit $x \in \mathfrak{D}_A$. On note $\delta(x)$ le plus grand entier n tel que a_n soit non nul. Si x et y sont deux éléments non nuls de $\mathfrak{D}_A$, on a $\delta(xy) = \delta(x) + \delta(y)$. En déduire que $\mathfrak{D}_A$ est intègre.
d) Si A est un anneau parfait de caractéristique p, on peut remplacer la condition $\mathbf{V}a\mathbf{F} = \mathbf{V}a$ pour $a \in W(A)$ par la condition $\mathbf{VF} = p$. L'idéal à gauche $\mathfrak{D}_A\mathbf{V}$ de $\mathfrak{D}_A$ est bilatère.
e) Si k est un corps parfait de caractéristique p, $\mathfrak{D}_k$ est noethérien. (Considérer $\mathfrak{D}_k$ comme quotient de l'anneau engendré sur $W(k)$ par deux indéterminées X et Y soumises aux relations $XY = YX$ et $Xa = (Fa)\,X$, $aY = Y(Fa)$ pour $a \in W(k)$. Appliquer ensuite, III, § 2, n° 8, corollaire 2 au th. 1 et exerc. 10.)

23) Soient A un anneau et I l'ensemble des entiers négatifs. Soient m un entier $\geqslant 1$ et $[a_0, \ldots, a_{m-1}]$ un élément de $W_m(A)$. Associons-lui l'élément $(b_i)_{i\in\mathrm{I}}$ de A^{I} défini par

$$\begin{cases} b_i = a_{i+m-1} & \text{pour} \quad 1 - m \leqslant i \leqslant 0 \\ b_i = 0 & \text{pour} \quad i \leqslant -m . \end{cases}$$

On identifie ainsi $W_m(A)$ à un sous-ensemble de A^I.

a) Pour tout entier $n \geqslant 0$, l'application $V_n : W_n(A) \to W_{n+1}(A)$ induite par le décalage est un homomorphisme de groupes. Les identifications des groupes $W_n(A)$ à des sous-ensembles de A^I sont compatibles aux applications V_n et permettent d'identifier le groupe $\varinjlim W_n(A)$, limite inductive des groupes $W_n(A)$ suivant les V_n, au sous-ensemble $CW^u(A)$ de A^I formé des éléments dont les composantes sont nulles sauf un nombre fini, éléments qu'on appellera *covecteurs de Witt unipotents*. Par transport de structure, on obtient sur ce sous-ensemble une structure de groupe.

b) Pour $\boldsymbol{a} = (a_i)_{i\in I}$ et $\boldsymbol{b} = (b_i)_{i\in I}$ dans $CW^u(A)$, on a

$$\boldsymbol{a} + \boldsymbol{b} = (c_i)_{i\in I} \quad \text{où} \quad c_{-n} = S_m(a_{-m-n}, \ldots, a_{-n-1}, a_{-n}; b_{-m-n}, \ldots, b_{-n-1}, b_{-n})$$

pour tout entier m suffisamment grand.

c) Pour tout homomorphisme d'anneaux $\varphi : A \to B$, l'application $CW^u(\varphi) : CW^u(A) \to CW^u(B)$ définie par $CW^u(\varphi)(a_i)_{i\in I} = (\varphi(a_i))_{i\in I}$ est un homomorphisme de groupes.

24) Soit I l'ensemble des entiers négatifs. Pour tout anneau A, tout idéal nilpotent $\mathfrak{n}$ de A, et tout entier $r \geqslant 0$, soit $CW(A, \mathfrak{n}, r)$ le sous-ensemble de A^I formé des éléments $(a_i)_{i\in I}$ tels que $a_{-n} \in \mathfrak{n}$ si $n \geqslant r$. Autrement dit, on a

$$CW(A, \mathfrak{n}, r) = A^{\{0,-1,\ldots,1-r\}} \times \mathfrak{n}^{\{-r,-r-1,\ldots\}}.$$

On munit $CW(A, \mathfrak{n}, r)$ de la topologie produit, chaque facteur A ou $\mathfrak{n}$ étant muni de la topologie discrète. On note CW(A) la réunion des $CW(A, \mathfrak{n}, r)$ et on munit CW(A) de la topologie limite inductive. Pour cette topologie, CW(A) est séparé et $CW^u(A)$ (*cf.* exerc. 23) est dense dans CW(A). Les éléments de CW(A) sont appelés *covecteurs de Witt de* A.

a) Soit t un entier positif, et soient $\omega_0, \ldots, \omega_t$ des entiers positifs tels que ω_0 soit non nul et que p^{t+1} divise $\sum_{i=0}^{t} p^i\omega_i$. Alors on a $\sum_{i=0}^{t} \omega_i \geqslant t(p-1) + p$.

b) Soit $\mathcal{A}$ l'anneau $\mathbf{Z}[X, Y]$ des polynômes en deux familles d'indéterminées $\mathbf{X} = (X_i)_{i\in I}$ et $\mathbf{Y} = (Y_i)_{i\in I}$. Pour tout entier $r \geqslant 0$, soit $\mathfrak{n}_r$ l'idéal de $\mathcal{A}$ engendré par les X_{-n} et Y_{-n} pour $n \geqslant r$. Soient r et s deux entiers $\geqslant 1$. Alors on a

$$S_m(X_{-m}, \ldots, X_0; Y_{-m}, \ldots, Y_0) \equiv S_{m+1}(X_{-m-1}, X_{-m}, \ldots, X_0; Y_{-m-1}, \ldots, Y_0)$$

modulo $\mathfrak{n}_r^s$ pour tout entier $m \geqslant r-1$ si $s < p$ et pour tout entier $m \geqslant r-1+(s-p)/(p-1)$ si $s \geqslant p$. (Par des arguments de poids, montrer que la différence des deux membres est combinaison linéaire à coefficients entiers de termes de la forme $X_{-m-1}^{u_0} Y_{-m-1}^{v_0} X_{-m}^{u_1} Y_{-m}^{v_1} \ldots X_0^{u_{m+1}} Y_0^{v_{m+1}}$ où, si l'on pose $\omega_i = u_i + v_i$ pour $0 \leqslant i \leqslant m+1$, on a $\omega_0 \neq 0$ et $\sum_{i=0}^{m+1} p^i\omega_i = p^{m+1}$. Utiliser alors *a*).)

c) Soient A un anneau, $\mathfrak{n}$ un idéal nilpotent de A, r un entier positif et $\boldsymbol{a}$, $\boldsymbol{b}$ deux éléments de $CW(A, \mathfrak{n}, r)$. Alors :

(i) Pour tout entier $n \geqslant 0$, la suite des éléments

$$d_m = S_m(a_{-n-m}, \ldots, a_{-n-1}, a_{-n}; b_{-n-m}, \ldots, b_{-n-1}, b_{-n})$$

de A est stationnaire.

(ii) Pour tout entier $n \geqslant 0$, soit c_{-n} la limite de la suite précédente. Alors l'élément $\boldsymbol{c} = (c_i)_{i\in I}$ appartient à $CW(A, \mathfrak{n}, r)$. On posera $\boldsymbol{a} + \boldsymbol{b} = \boldsymbol{c}$.

(iii) La loi d'addition précédente munit CW(A) d'une structure de groupe commutatif, compatible avec sa topologie. Pour tout idéal nilpotent $\mathfrak{n}$ de A et tout entier $r \geqslant 0$, le sous-ensemble $CW(A, \mathfrak{n}, r)$ de CW(A) en est un sous-groupe topologique. Il en est de même de $CW^u(A)$.

d) Soient A et B deux anneaux, φ un homomorphisme d'anneaux de A dans B. Notons $CW(\varphi)$ l'application de CW(A) dans CW(B) qui à $(a_i)_{i\in I}$ associe $(\varphi(a_i))_{i\in I}$. Alors $CW(\varphi)$ est un homomorphisme de groupes et une application continue.

25) Soit A un anneau parfait de caractéristique p.
a) Soient B une A-algèbre et $\varphi : A \to B$ l'homomorphisme structural. Pour tout entier $n \geqslant 1$, munissons le groupe $W_n(B)$ de la structure de W(A)-module définie par

$$(a, b) \mapsto \varphi(F^{1-n}a).b \quad \text{pour} \quad (a, b) \in W(A) \times W_n(B).$$

Muni de l'action de F par l'homomorphisme de Frobenius F et de V par l'homomorphisme de décalage V, $W_n(B)$ est alors un $\mathfrak{D}_A$-module (exerc. 22). L'application $V_n : W_n(B) \to W_{n+1}(B)$ induite par le décalage est un homomorphisme de $\mathfrak{D}_A$-modules.

Par transport de structure, on munit le groupe $CW^u(B)$ d'une structure de $\mathfrak{D}_A$-module.
b) Soit $\mathcal{A}$ l'anneau de polynômes A[X] en une famille $\mathbf{X} = (X_i)_{i \in I}$ d'indéterminées. Pour tout entier $r \geqslant 0$, soit $\mathfrak{b}_r$ l'idéal de $\mathcal{A}$ engendré par les X_{-n}, pour $n \geqslant r$. Soient r et s des entiers $\geqslant 1$. Alors, pour tout élément $\boldsymbol{a} = (a_n)_{n \in \mathbf{N}}$ de W(A), on a

$$P_m(a_0^{p^{-m}}, ..., a_m^{p^{-m}}; X_{-m}, ..., X_0) \equiv P_{m+1}(a_0^{p^{-m-1}}, ..., a_{m+1}^{p^{-m-1}}; X_{-m-1}, ..., X_0) \bmod \mathfrak{b}_r^s,$$

pour tout entier $m \geqslant r - 1$ si $s < p$, et pour tout entier $m \geqslant r - 1 + (s - p)/(p - 1)$ si $s \geqslant p$.
c) Soient B une A-algèbre et $\varphi : A \to B$ l'homomorphisme structural. Soient $\boldsymbol{a} = (a_n)_{n \in \mathbf{N}}$ un élément de W(A), et $\boldsymbol{b} = (b_i)_{i \in I}$ un élément de CW(B). Pour tout entier $n \geqslant 0$, la suite des éléments $P_m(\varphi(a_0^{p^{-n-m}}), ..., \varphi(a_m^{p^{-n-m}}); b_{-m-n}, ..., b_{-n})$ est stationnaire.

Notant c_{-n} la limite de cette suite, l'élément $\boldsymbol{c} = (c_i)_{i \in I}$ appartient à CW(B). Posons $\boldsymbol{c} = \boldsymbol{a}.\boldsymbol{b}$. L'application de W(A) × CW(B) dans CW(B) qui à $(\boldsymbol{a}, \boldsymbol{b})$ associe $\boldsymbol{c}$, munit CW(B) d'une structure de W(A)-module, qui prolonge la structure de W(A)-module de $CW^u(A)$.

Pour tout $a \in A$ et tout $\boldsymbol{b} \in CW(B)$, on a

$$\tau(a).\boldsymbol{b} = (c_i)_{i \in I} \quad \text{avec} \quad c_i = a^{p^i} b_i \quad \text{pour tout} \quad i \in I$$

et

$$p.\boldsymbol{b} = (b_{i-1}^p)_{i \in I}.$$

Si pour tout $\boldsymbol{b} \in CW(B)$, on pose

$$F\boldsymbol{b} = (b_i^p)_{i \in I}$$
$$V\boldsymbol{b} = (b_{i-1})_{i \in I}, .$$

alors F et V sont des endomorphismes continus de CW(B) et permettent de munir CW(B) d'une structure de $\mathfrak{D}_A$-module. Le $\mathfrak{D}_A$-module $CW^u(B)$ est un sous-$\mathfrak{D}_A$-module de CW(B).

26) Soit M l'ensemble des nombres rationnels positifs dont le dénominateur est une puissance de p, muni de la structure de monoïde donnée par l'addition. Soit k un corps parfait de caractéristique p. On munit W(k) et son corps de fractions K de la topologie donnée par la valuation de W(k). Soit n un entier positif. Soit C l'algèbre sur K du monoïde produit M^n. Pour $1 \leqslant i \leqslant n$, on notera T_i l'image dans C de l'élément de M ayant pour i-ième composante 1 et pour autres composantes 0, et pour $\alpha \in M^n$ on notera T^α l'image de α. Pour $\alpha \in M^n$, on posera

$$\operatorname{den}(\alpha) = \sup_{1 \leqslant i \leqslant n} (p^{-\inf(0, w_p(\alpha_i))})$$

où w_p désigne la valuation p-adique de **Q**. On note A l'anneau $k[T_1, ..., T_n]$, B l'anneau $W(k)[T_1, ..., T_n]$, $\overline{B}$ l'algèbre de M^n sur W(k), $\overline{A}$ l'algèbre de M^n sur k. On considère A comme un sous-anneau de $\overline{A}$, B comme un sous-anneau de $\overline{B}$, $\overline{B}$ comme un sous-anneau de C.

Soit E l'ensemble des éléments de C de la forme $\sum_{\alpha \in M^n} \operatorname{den}(\alpha)\, a_\alpha T^\alpha$ où la famille à support fini (a_α) est formée d'éléments de W(k).

Soient F l'automorphisme de C coïncidant avec l'automorphisme de Frobenius sur W(k) et vérifiant $F(T_i^\alpha) = T_i^{p\alpha}$ pour tout i ($1 \leqslant i \leqslant n$) et tout $\alpha \in M$, et V l'automorphisme du groupe additif de C défini par $V = pF^{-1}$.
a) E est un sous-anneau de C, contenant B et stable par F et V.
b) E est un W(k)-module, et est somme de ses sous-modules V^iB, pour $i \in \mathbf{N}$.
c) On a $\bigcap_{i \in \mathbf{N}} V^iE = 0$.
d) Pour tout $i \in \mathbf{N}$, on a $B \cap V^iE = p^iB$.

e) Notons $\rho : \overline{B} \to \overline{A}$ l'application obtenue en réduisant les coefficients des éléments de M^n modulo $pW(k)$. Alors on a $\rho(E) = A$, et ρ induit un isomorphisme ρ' de E/VE sur A.
f) Pour tout entier $r \geqslant 0$, $V^rE/V^{r+1}E$ est un module sur E/VE. Par ρ'^{-1}, on peut le considérer comme un A-module. L'application de A dans $V^rE/V^{r+1}E$, qui à $a \in A$ associe la classe de V^re, pour tout élément $e \in E$ vérifiant $\rho(e) = a$, est un isomorphisme du A-module φ'^r_*A (p. 44, exerc. 13) sur le A-module $V^rE/V^{r+1}E$.
g) Il existe un unique homomorphisme de W(*k*)-algèbres $\sigma : \overline{B} \to W(\overline{A})$ tel que pour $1 \leqslant i \leqslant n$ et $r \in M$, on ait $\sigma(T_i^r) = \tau_{\overline{A}}(T_i^r)$. On a $\sigma \circ F = F_{\overline{A}}$ et $\sigma \circ V = V_{\overline{A}} \circ \sigma$ (s'inspirer de l'exerc. 14, p. 44).
h) L'homomorphisme σ induit un homomorphisme de W(*k*)-algèbres $\tilde{\sigma} : E \to W(A)$, qui est le seul W(*k*)-homomorphisme de E dans W(A) vérifiant $\tilde{\sigma}(T_i) = \tau_A(T_i)$ pour $1 \leqslant i \leqslant n$ et $\tilde{\sigma} \circ V = V_A \circ \tilde{\sigma}$.
i) Pour tout entier $r \geqslant 1$, $\tilde{\sigma}$ induit un isomorphisme de E/V^rE et $W_r(A)$ (utiliser l'exerc. 13, p. 44) ; $\tilde{\sigma}$ est injectif.
j) Soit $\hat{C}$ le complété de C pour la topologie *p*-adique. Pour tout $x \in \hat{C}$, il existe une unique famille $(a_\alpha)_{\alpha \in M^n}$ d'éléments de K, telle que a_α tende vers 0 quand α tend vers l'infini suivant le filtre des complémentaires des parties finies de M^n, et que x soit la somme de la famille $a_\alpha T^\alpha$.
k) Soit $\hat{E}$ l'ensemble des éléments $x = \sum_{\alpha \in M^n} \mathrm{den}(\alpha)\, \alpha_\alpha T^\alpha$ de $\hat{C}$ tels qu'on ait $a_\alpha \in W(k)$ pour tout $\alpha \in M^n$. Prouver que $\tilde{\sigma} : E \to W(A)$ se prolonge en un isomorphisme de $\hat{E}$ sur W(A).

27) Soient r_1, r_2, n des entiers vérifiant

$$1 \leqslant r_1 \leqslant r_2 \leqslant n .$$

Soient $T_1, \ldots, T_n$ des indéterminées. Par des arguments analogues à ceux de l'exercice précédent, donner une description de l'anneau des vecteurs de Witt sur l'anneau

$$k[T_1, \ldots, T_{r_1}, T_1^{-1}, \ldots, T_{r_1}^{-1}, T_{r_1+1}, \ldots, T_{r_2}][[T_{r_2+1}, \ldots, T_n]] .$$

28) Soit **J** l'ensemble des entiers $\geqslant 1$. Pour tout $n \in \mathbf{J}$, notons $\mathbf{J}_n$ l'ensemble des entiers $d \geqslant 1$ qui divisent n. Soit A un anneau. On munit $A^{\mathbf{J}}$ de sa structure d'anneau produit. On définit les applications Φ, f_n, v_n ($n \in \mathbf{J}$) de $A^{\mathbf{J}}$ dans lui-même par les formules suivantes. Pour $\boldsymbol{a} = (a_j)_{j \in \mathbf{J}}$, on pose

$$\Phi(\boldsymbol{a}) = (\Phi_n(\boldsymbol{a}))_{n \in \mathbf{J}}, \quad \text{où} \quad \Phi_n(\boldsymbol{a}) = \sum_{d \in \mathbf{J}_n} d a_d^{n/d} ,$$

$$v_n(\boldsymbol{a}) = (n a_{m/n})_{m \in \mathbf{J}} , \quad f_n(\boldsymbol{a}) = (a_{mn})_{m \in \mathbf{J}} ;$$

on convient que $a_{m/n} = 0$ si $m/n \notin \mathbf{J}$. Remarquons que Φ_n ne dépend que des a_d ($d \in \mathbf{J}_n$). On écrira parfois $\Phi_n((a_d)_{d \in \mathbf{J}_n})$ au lieu de $\Phi_n(\boldsymbol{a})$.

Pour tout nombre premier p, on note w_p la valuation *p*-adique de **Q**. *Ces notations seront conservées dans la suite des exercices du* § 1.
a) f_n est un endomorphisme de l'anneau $A^{\mathbf{J}}$, et $f_n \circ f_m = f_{nm}$ quels que soient n, m dans **J**.
b) v_n est un endomorphisme du groupe additif de $A^{\mathbf{J}}$, et $v_n \circ v_m = v_{nm}$ quels que soient n, m dans **J**.

Soient n, m dans **J** et $d = \mathrm{pgcd}(m, n)$
c) On a $f_n \circ v_m = d.v_{m/d} \circ f_{n/d}$. En particulier $f_n \circ v_n = n.\mathrm{Id}$, et $f_n \circ v_m = v_m \circ f_n$ si $d = 1$.
d) Quels que soient $\boldsymbol{a}$, $\boldsymbol{b}$ dans $A^{\mathbf{J}}$ on a

$$v_n(\boldsymbol{a}).v_m(\boldsymbol{b}) = d.v_{nm/d}(f_{m/d}(\boldsymbol{a}).f_{n/d}(\boldsymbol{b}))$$

$$((\boldsymbol{q})^{p/u}f)^{p/u}a \cdot (\boldsymbol{v})^u a = ((\boldsymbol{q})^u f \cdot \boldsymbol{v})^u a \frac{p}{u}$$

$$\frac{n}{d} v_n(f_m(\boldsymbol{b})) = v_n(\mathbf{1}).v_{n/d}(f_{m/d}(\boldsymbol{b})) .$$

(La seconde formule résulte de la première, et la troisième de la seconde en prenant $\boldsymbol{a} = 1$.) En particulier, on a

$$v_n(\boldsymbol{a}).v_n(\boldsymbol{b}) = n v_n(\boldsymbol{a}.\boldsymbol{b}) ,$$

et

$$v_n(\boldsymbol{a}).v_m(\boldsymbol{b}) = v_{nm}(f_m(\boldsymbol{a}).f_n(\boldsymbol{b}))$$

si $d = 1$.

29) Soit A un anneau. Soient $n \in \mathbf{J}$, p un nombre premier, et $\boldsymbol{a} \in \mathrm{A}^{\mathbf{J}}$. Établir la relation $\Phi_{pn}(\boldsymbol{a}) = \Phi_n(\boldsymbol{a}^p) + p^w\Phi_m(f_{p^w}(\boldsymbol{a}))$, où $w = w_p(pn)$ et $pn = p^w m$. On a donc

$$\Phi_{pn}(\boldsymbol{a}) \equiv \Phi_n(\boldsymbol{a}^p) \bmod. p^{w_p(pn)}\mathrm{A}\,, \quad \text{et en particulier} \quad \Phi_{pn}(\boldsymbol{a}) \equiv \Phi_n(\boldsymbol{a})^p \bmod. p\mathrm{A}\,.$$

30) Soit p un nombre premier. Soient A un anneau filtré et $(\mathrm{J}_r)_{r\in\mathbf{Z}}$ sa filtration. On suppose que l'on a $\mathrm{J}_0 = \mathrm{A}$ et $p.1_\mathrm{A} \in \mathrm{J}_1$. Soient $\boldsymbol{a}$ et $\boldsymbol{b}$ des éléments de $\mathrm{A}^{\mathbf{J}}$ et $r \in \mathbf{N}$.
a) Si l'on a $a_d \equiv b_d \bmod. \mathrm{J}_r$ pour tout $d \in \mathbf{J}_n$, alors on a $\Phi_n(\boldsymbol{a}) \equiv \Phi_n(\boldsymbol{b}) \bmod. \mathrm{J}_{r+k}$ où $k = w_p(n)$.
b) Supposons que, pour tout entier $m \geqslant 1$ et tout $x \in \mathrm{A}$, la relation $p.x \in \mathrm{J}_{m+1}$ entraîne $x \in \mathrm{J}_m$. Si l'on a $\Phi_d(\boldsymbol{a}) \equiv \Phi_d(\boldsymbol{b}) \bmod. \mathrm{J}_{r+w_p(d)}$, pour tout $d \in \mathbf{J}_n$, alors $a_d \equiv b_d \bmod. \mathrm{J}_r$ pour tout $d \in \mathbf{J}_n$.

31) Soit A un anneau. Soit $n \in \mathbf{J}$. Soit $(a_d)_{d\in\mathbf{J}_n-\{n\}}$ une famille d'éléments de A. Posons $u_d = \Phi_d((a_e)_{e\in\mathbf{J}_d})$ pour $d \in \mathbf{J}_n - \{n\}$, et soit u_n un élément de A. Pour tout nombre premier $p \in \mathbf{J}_n$, supposons donné de plus un endomorphisme σ_p de A tel que $\sigma_p(a) \equiv a^p \bmod. p\mathrm{A}$ pour tout $a \in \mathrm{A}$. Alors les conditions suivantes sont équivalentes :
a) Il existe un élément a_n de A tel que $u_n = \Phi_n((a_d)_{d\in\mathbf{J}_n})$.
b) Pour tout nombre premier $p \in \mathbf{J}_n$, on a $u_n \equiv \sigma_p(u_{n/p}) \bmod. p^{w_p(n)}\mathrm{A}$.

32) Soit A un anneau.
a) Le noyau de $\Phi : \mathrm{A}^{\mathbf{J}} \to \mathrm{A}^{\mathbf{J}}$ est formé des éléments $\boldsymbol{a}$ tels que $da_d = 0$ pour tout $d \in \mathbf{J}$.
b) Supposons donné pour tout nombre premier p un endomorphisme σ_p de A tel que $\sigma_p(a) \equiv a^p \bmod. p\mathrm{A}$ pour tout $a \in \mathrm{A}$. Alors l'image de Φ est formée des éléments $\boldsymbol{u}$ tels que $u_{np} \equiv \sigma_p(u_n) \bmod. p^{w_p(np)}\mathrm{A}$ pour tout $n \in \mathbf{J}$. Cette image est un sous-anneau de $\mathrm{A}^{\mathbf{J}}$ stable par f_n et v_n pour tout $n \in \mathbf{J}$.
c) Soit $q \in \mathbf{J}$. Si la multiplication par q dans A est bijective, alors la multiplication par q est encore bijective dans $\mathrm{Ker}(\Phi)$ et dans $\mathrm{Im}(\Phi)$.

33) *a*) Soit J' une partie de $\mathbf{J}$. Soient R un anneau commutatif et $\mathrm{R}[\mathbf{X}]$ la R-algèbre de polynômes en une famille $\mathbf{X} = (\mathrm{X}_n)_{n\in\mathrm{J}'}$ d'indéterminées, munie de la graduation de type $\mathbf{Z}$ telle que X_n soit de degré n pour tout $n \in \mathrm{J}'$. Soit, pour tout $n \in \mathrm{J}'$, $\varphi_n(\mathbf{X})$ un élément de $\mathrm{R}[\mathbf{X}]$ homogène de degré n où le coefficient de X_n soit inversible dans R. Alors l'endomorphisme φ de $\mathrm{R}[\mathbf{X}]$ tel que $\varphi(\mathrm{X}_n) = \varphi_n(\mathbf{X})$ est un automorphisme de la R-algèbre graduée $\mathrm{R}[\mathbf{X}]$.
b) Soient $\mathrm{J}' = \mathbf{J}$, $\mathrm{R} = \mathbf{Q}$, et $\varphi_n(\mathbf{X}) = \Phi_n(\mathbf{X})$. Il existe, pour tout $n \in \mathbf{J}$, un et un seul élément $\Psi_n(\mathbf{X})$ de $\mathbf{Q}[\mathbf{X}]$, homogène de degré n, qui ne dépend que des indéterminées $(\mathrm{X}_d)_{d\in\mathbf{J}_n}$, et tel que $\Psi_n(\Phi(\mathbf{X})) = \mathrm{X}_n$. (Appliquer *a*) avec $\mathrm{J}' = \mathbf{J}_n$.)
c) Si A est une $\mathbf{Q}$-algèbre, $\Phi : \mathrm{A}^{\mathbf{J}} \to \mathrm{A}^{\mathbf{J}}$ est bijectif, son inverse étant donné par $\boldsymbol{a} \mapsto (\Psi_n(\boldsymbol{a}))_{n\in\mathbf{J}}$.
d) Si A est un anneau dont le groupe additif est sans $\mathbf{Z}$-torsion, $\Phi : \mathrm{A}^{\mathbf{J}} \to \mathrm{A}^{\mathbf{J}}$ est injectif. (Plonger $\mathrm{A}^{\mathbf{J}}$ dans $(\mathbf{Q} \otimes \mathrm{A})^{\mathbf{J}}$.)

34) Soit $\mathrm{R} = \mathbf{Z}[\mathbf{X}, \mathbf{Y}]$ la $\mathbf{Z}$-algèbre des polynômes en deux familles d'indéterminées $\mathbf{X} = (\mathrm{X}_n)_{n\in\mathbf{J}}$ et $\mathbf{Y} = (\mathrm{Y}_n)_{n\in\mathbf{J}}$. Pour tout nombre premier p, soit σ_p l'endomorphisme de R défini par $\sigma_p(\mathrm{X}_n) = \mathrm{X}_n^p$ et $\sigma_p(\mathrm{Y}_n) = \mathrm{Y}_n^p$ pour tout $n \in \mathbf{J}$; on a alors $\sigma_p(a) \equiv a^p \bmod. p\mathrm{R}$ pour tout $a \in \mathrm{R}$. De plus, R est sans $\mathbf{Z}$-torsion.
a) Il existe dans $\mathrm{R}^{\mathbf{J}}$ des éléments $\mathbf{S} = (\mathrm{S}_n)_{n\in\mathbf{J}}$, $\mathbf{P} = (\mathrm{P}_n)_{n\in\mathbf{J}}$, $\mathbf{I} = (\mathrm{I}_n)_{n\in\mathbf{J}}$, et, pour tout $q \in \mathbf{J}$, $\mathbf{F}_q = (\mathrm{F}_{q,n})_{n\in\mathbf{J}}$ et $\mathbf{V}_q = (\mathrm{V}_{q,n})_{n\in\mathbf{J}}$, caractérisés respectivement par les égalités

$$\begin{aligned}
\Phi(\mathbf{S}) &= \Phi(\mathbf{X}) + \Phi(\mathbf{Y})\,,\\
\Phi(\mathbf{P}) &= \Phi(\mathbf{X}).\Phi(\mathbf{Y})\,,\\
\Phi(\mathbf{I}) &= -\Phi(\mathbf{X})\,,\\
\Phi(\mathbf{F}_q) &= f_q(\Phi(\mathbf{X}))\,,\\
\Phi(\mathbf{V}_q) &= v_q(\Phi(\mathbf{X}))\,.
\end{aligned}$$

(En plongeant R dans $\mathbf{Q} \otimes \mathrm{R}$, on a, avec les notations de l'exerc. 33,

$$S_n(X, Y) = \Psi_n(\Phi(X) + \Phi(Y)), \quad P_n(X, Y) = \Psi_n(\Phi(X).\Phi(Y)), \quad I_n(X) = \Psi_n(-\Phi(X)),$$
$$F_{q,n}(X) = \Psi_n(f_q(\Phi(X))), \quad \text{et} \quad V_{q,n}(X) = \Psi_n(v_q(\Phi(X))).)$$

b) Pour tout $n \in \mathbf{J}$, affectons X_n et Y_n du poids n. Alors S_n, P_n et I_n ne dépendent que des familles $(X_d)_{d\in\mathbf{J}_n}$ et $(Y_d)_{d\in\mathbf{J}_n}$. De plus :

α) S_n est isobare de poids n.

β) P_n est isobare de poids $2n$, et isobare de poids n en chacune des familles $(X_d)_{d\in\mathbf{J}_n}$ et $(Y_d)_{d\in\mathbf{J}_n}$.

γ) I_n est isobare de poids n.

c) $F_{q,n}$ est isobare de poids qn, et ne dépend que de la famille $(X_d)_{d\in\mathbf{J}_{qn}}$.

d) On a $V_{q,n}(X) = X_{n/q}$, où on convient que $X_{n/q} = 0$ si $n/q \notin \mathbf{J}$. (Il suffit de vérifier qu'avec cette définition de $\mathbf{V}_q$, on a $v_q(\Phi(X)) = \Phi(\mathbf{V}_q(X))$.)

35) Soit A un anneau.

a) L'ensemble $A^{\mathbf{J}}$, muni de l'addition

$$\boldsymbol{a} + \boldsymbol{b} = \mathbf{S}(\boldsymbol{a}, \boldsymbol{b})$$

et de la multiplication

$$\boldsymbol{a} \times \boldsymbol{b} = \mathbf{P}(\boldsymbol{a}, \boldsymbol{b}),$$

est un anneau commutatif, noté U(A). L'élément neutre pour l'addition est la suite $\mathbf{0}$ dont tous les termes sont nuls ; l'élément neutre pour la multiplication est la suite $\mathbf{1}$ dont tous les termes sont nuls sauf celui d'indice 1, qui vaut 1_A. L'opposé d'un élément $\boldsymbol{a}$ de U(A) est $\mathbf{I}(\boldsymbol{a})$.

b) Soit $\rho : B \to A$ un homomorphisme d'anneaux. Alors $U(\rho) : U(B) \to U(A)$ défini par $U(\rho)(b_n)_{n\in\mathbf{J}} = (\rho(b_n))_{n\in\mathbf{J}}$ est un homomorphisme d'anneaux.

c) L'application $\Phi : U(A) \to A^{\mathbf{J}}$ est un homomorphisme d'anneaux. En d'autres termes $\Phi_n : U(A) \to A$ est un homomorphisme d'anneaux pour tout $n \in \mathbf{J}$.

d) Si le groupe additif de A est sans **Z**-torsion, le groupe additif de U(A) l'est aussi.

e) Soit $q \in \mathbf{J}$. Si la multiplication par q est bijective dans A, elle est encore bijective dans U(A). (Utiliser l'exerc. 32, *c*), p. 51.)

36) Soit A un anneau. Soient n, m dans $\mathbf{J}$ et $d = \mathrm{pgcd}(n, m)$.

a) L'application $\boldsymbol{a} \mapsto \mathbf{F}_n(\boldsymbol{a}) = (\mathbf{F}_{n,r}(\boldsymbol{a}))_{r\in\mathbf{J}}$ est un endomorphisme de l'anneau U(A), et l'on a $\mathbf{F}_n \circ \mathbf{F}_m = \mathbf{F}_{mn}$, $\Phi_n \circ \mathbf{F}_m = \Phi_{nm}$.

b) L'application $\boldsymbol{a} \mapsto \mathbf{V}_n(\boldsymbol{a}) = (\mathbf{V}_{n,r}(\boldsymbol{a}))_{r\in\mathbf{J}}$ est un endomorphisme du groupe additif de U(A), et l'on a $\mathbf{V}_n \circ \mathbf{V}_m = \mathbf{V}_{nm}$. De plus, $\Phi_n \circ \mathbf{V}_q$ est égal à 0 si q ne divise pas n et à $q\Phi_{n/q}$ si q divise n.

c) On a $\mathbf{F}_n \circ \mathbf{V}_m = d \times \mathbf{V}_{m/d} \circ \mathbf{F}_{n/d}$; autrement dit $\mathbf{F}_n(\mathbf{V}_m(\boldsymbol{a}))$ (pour $\boldsymbol{a} \in \mathrm{U(A)}$) est somme dans U(A) de d termes égaux à $\mathbf{V}_{m/d}(\mathbf{F}_{n/d}(\boldsymbol{a}))$. En particulier, on a $\mathbf{F}_n(\mathbf{V}_n(\boldsymbol{a})) = n \times \boldsymbol{a}$ et $\mathbf{F}_n \circ \mathbf{V}_m = \mathbf{V}_m \circ \mathbf{F}_n$ si $d = 1$.

d) Quels que soient $\boldsymbol{a}$, $\boldsymbol{b}$ dans U(A), on a

$$\mathbf{V}_n(\boldsymbol{a}) \times \mathbf{V}_m(\boldsymbol{b}) = d \times \mathbf{V}_{nm/d}(\mathbf{F}_{m/d}(\boldsymbol{a}) \times \mathbf{F}_{n/d}(\boldsymbol{b}))$$

$$\frac{n}{d} \times \mathbf{V}_n(\boldsymbol{a} \times \mathbf{F}_m(\boldsymbol{b})) = \mathbf{V}_n(\boldsymbol{a}) \times \mathbf{V}_{n/d}(\mathbf{F}_{m/d}(\boldsymbol{b}))$$

$$\frac{n}{d} \times \mathbf{V}_n(\mathbf{F}_m(\boldsymbol{b})) = \mathbf{V}_n(\mathbf{1}) \times \mathbf{V}_{n/d}(\mathbf{F}_{m/d}(\boldsymbol{b})).$$

En particulier, on a

$$\mathbf{V}_n(\boldsymbol{a}) \times \mathbf{V}_n(\boldsymbol{b}) = n \times \mathbf{V}_n(\boldsymbol{a} \times \boldsymbol{b}),$$

et

$$\mathbf{V}_n(\boldsymbol{a}) \times \mathbf{V}_m(\boldsymbol{b}) = \mathbf{V}_{nm}(\mathbf{F}_m(\boldsymbol{a}) \times \mathbf{F}_n(\boldsymbol{b}))$$

si $d = 1$. (Se ramener au cas où $A = \mathbf{Z}[X, Y]$, $\boldsymbol{a} = X$, $\boldsymbol{b} = Y$ et utiliser l'exerc. 33, *d*), p. 51 et l'exerc. 28, p. 50.)

37) Soit A un anneau.
a) Soit $m \in \mathbf{J}$. Pour tout élément $\boldsymbol{a} = (a_n)_{n\in\mathbf{J}}$ de U(A), on a

$$\boldsymbol{a} = (a_1, ..., a_m, 0, ..., 0, ...) + (\underbrace{0, ..., 0}_{m \text{ termes}}, a_{m+1}, a_{m+2}, ...) .$$

b) On munit U(A) de la topologie produit sur $A^{\mathbf{J}}$ de la topologie discrète sur chacun des facteurs. Elle fait de U(A) un anneau topologique séparé et complet.
c) On note τ_A (ou τ) l'application de A dans U(A) qui à $a \in A$ associe $(a, 0, ..., 0) \in U(A)$. Soient a, b deux éléments de A, $\boldsymbol{x} = (x_n)_{n\in\mathbf{J}}$ un élément de U(A).
(i) On a les formules

$$\tau(ab) = \tau(a) \times \tau(b), \quad \tau(a) \times \boldsymbol{x} = (a^n x_n)_{n\in\mathbf{J}},$$
$$\Phi(\tau(a)) = (a^n)_{n\in\mathbf{J}},$$
$$F_n(\tau(a)) = \tau(a^n) \quad \text{pour tout} \quad n \in \mathbf{J}.$$

(ii) La série de terme général $V_n\tau(x_n)$ est convergente dans U(A), de somme $\boldsymbol{x}$.

38) Soient p un nombre premier, A un anneau et $\boldsymbol{a} \in U(A)$.
a) On a $\mathbf{F}_p(\boldsymbol{a}) \equiv \boldsymbol{a}^p \bmod. pA^{\mathbf{J}}$; autrement dit, on a $F_{p,n}(\boldsymbol{a}) \equiv a_n^p \bmod. pA$ pour tout $n \in \mathbf{J}$.
b) On a $\mathbf{F}_p(\boldsymbol{a}) \equiv \boldsymbol{a}^{*p} \bmod. p \times U(A)$, où $\boldsymbol{a}^{*p}$ désigne le produit dans U(A) de p termes égaux à $\boldsymbol{a}$, et où $p \times U(A)$ désigne l'idéal de U(A) engendré par $p \times 1_{U(A)}$, somme dans U(A) de p termes égaux à $1_{U(A)}$. (Il suffit de traiter le cas où $A = \mathbf{Z}[X]$ et $\boldsymbol{a} = \mathbf{X}$. Alors A est sans Z-torsion et $\Phi : U(A) \to A^{\mathbf{J}}$ est injectif. Pour *a*) il suffit (p. 51, exerc. 30, *b*)) de montrer que, pour tout $n \in \mathbf{J}$, $\Phi_n(\mathbf{F}_p(\mathbf{X})) = \Phi_{pn}(\mathbf{X})$ est congru à $\Phi_n(\mathbf{X}^p)$ modulo $p^{w_p(pn)}A$, ce qui résulte de l'exerc. 29, p. 51. Pour *b*) il suffit de montrer que $\Phi(\mathbf{F}_p(\mathbf{X})) = f_p(\Phi(\mathbf{X}))$ est congru à $\Phi(\mathbf{X}^{*p}) = \Phi(\mathbf{X})^p$ modulo $p.\Phi(U(A))$. Or il existe un élément $\boldsymbol{u} \in A^{\mathbf{J}}$ tel que

$$f_p(\Phi(\mathbf{X})) - \Phi(\mathbf{X})^p = (\Phi_{np}(\mathbf{X}) - \Phi_n(\mathbf{X})^p)_{n\in\mathbf{J}} = p.\boldsymbol{u} \quad \text{(p. 51, exerc. 29)}$$

et il s'agit de montrer que $\boldsymbol{u} \in \Phi(U(A))$. Pour tout nombre premier q, soit σ_q l'endomorphisme de l'anneau $A = \mathbf{Z}[X]$ tel que $\sigma_q(X_n) = X_n^q$ pour tout $n \in \mathbf{J}$. D'après l'exerc. 32, p. 51, il suffit de montrer que, pour tout nombre premier q et pour tout $n \in \mathbf{J}$, on a $u_{qn} \equiv \sigma_q(u_n) \bmod. q^{w_q(qn)}A$, ce qui équivaut à prouver la congruence suivante

$$\Phi_{pqn}(\mathbf{X}) - \Phi_{qn}(\mathbf{X})^p \equiv \sigma_q(\Phi_{pn}(\mathbf{X}) - \Phi_n(\mathbf{X})^p) \bmod. pq^{w_q(qn)}A . \tag{1}$$

Or le terme de droite est égal à $\Phi_{pn}(\mathbf{X}^q) - \Phi_n(\mathbf{X}^q)^p$. D'après l'exerc. 29, p. 51, on a

$$\Phi_{pqn}(\mathbf{X}) \equiv \Phi_{pn}(\mathbf{X}^q) \bmod. q^{w_q(pqn)}A \tag{2}$$

et

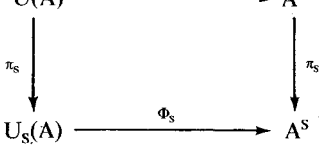
$$\Phi_{qn}(\mathbf{X}) \equiv \Phi_n(\mathbf{X}^q) \bmod. q^{w_q(qn)}A . \tag{3}$$

Les termes de droite et de gauche de (1) sont tous deux congrus à zéro modulo pA (p. 51, exerc. 29), donc (1) résulte de (2) et (3) si $q \neq p$. Supposons que l'on ait $q = p$. Alors il résulte de (3) et du lemme 1 qu'on a

$$\Phi_{pn}(\mathbf{X})^p \equiv \Phi_n(\mathbf{X}^p)^p \bmod. p^{w_p(pn)+1}A , \tag{4}$$

et (1) résulte de (2) et (4).)

39) Soit S une partie non vide de **J** telle que pour tout n dans S, S contienne $\mathbf{J}_n$. Notons π_S la projection canonique de $A^{\mathbf{J}}$ sur A^S.
a) Le noyau de π_S est un idéal de A. On notera $U_S(A)$ l'anneau obtenu en munissant A^S de la structure d'anneau quotient. On a un diagramme commutatif d'homomorphismes d'anneaux



où $\Phi_S((a_n)_{n\in S}) = (\Phi_n((a_d)_{d\in\mathbf{J}_n}))_{n\in S}$.

b) Pour tout $n \in \mathbf{J}$, $\mathrm{Ker}(\pi_S)$ est stable par $\mathbf{V}_n$, et $\mathrm{Ker}(\pi_S)$ contient $\mathbf{V}_n(\mathrm{U}(\mathrm{A}))$ si $n \notin \mathrm{S}$. Par passage au quotient $\mathbf{V}_n$ définit un endomorphisme, encore noté $\mathbf{V}_n$, du groupe additif de $\mathrm{U}_S(\mathrm{A})$.
c) Si $n \in \mathbf{J}$ et si $n\mathrm{S} \subset \mathrm{S}$ alors $\mathrm{Ker}(\pi_S)$ est stable par $\mathbf{F}_n$, qui définit, par passage au quotient, un endomorphisme, encore noté $\mathbf{F}_n$, de l'anneau $\mathrm{U}_S(\mathrm{A})$.
d) Soit $n \in \mathbf{J}$. L'anneau $\mathrm{U}_S(\mathrm{A})$ se notera aussi $\mathrm{U}_n(\mathrm{A})$ si $S = \mathbf{J}_n$, et $\mathrm{U}_{n\infty}(\mathrm{A})$ si $\mathrm{S} = \bigcup_{r \geqslant 1} \mathbf{J}_{n^r}$.
Soit p un nombre premier. Montrer que $\mathrm{U}_{p\infty}(\mathrm{A})$ s'identifie à l'anneau de Witt $\mathrm{W}(\mathrm{A})$, et que, pour tout $n \in \mathbf{N}$, $\mathrm{U}_{p^n}(\mathrm{A})$ s'identifie à l'anneau $\mathrm{W}_{n+1}(\mathrm{A})$ (on identifiera l'élément $(u_1, u_p, u_{p^2}, \ldots, u_{p^{n-1}}, u_{p^n})$ de $\mathrm{U}_{p^n}(\mathrm{A})$ au vecteur de Witt $[a_0, \ldots, a_n]$ avec $a_i = u_{p^i}$ pour $0 \leqslant i \leqslant n$). Les endomorphismes de groupes $\mathbf{V}_p$ et $\mathbf{F}_p$ de $\mathrm{U}_{p\infty}(\mathrm{A})$ correspondent respectivement, par cette identification, au décalage et à l'endomorphisme de Frobenius de $\mathrm{W}(\mathrm{A})$.

40) Soit A un anneau. Soit $\mathbf{J} = \mathrm{P} \times \mathrm{Q}$ une décomposition du monoïde J en produit de sous-monoïdes P et Q (qui sont donc engendrés par les nombres premiers qu'ils contiennent). On suppose que tout $q \in \mathrm{Q}$ est inversible dans A, donc aussi dans U(A) (p. 52, exerc. 35, *e*)).
a) Pour tout $\boldsymbol{a} \in \mathrm{U}(\mathrm{A})$, la série

$$\varepsilon_{\mathrm{Q}}(\boldsymbol{a}) = \sum_{q \in \mathrm{Q}} \frac{\mu(q)}{q} \mathbf{V}_q \mathbf{F}_q(a),$$

où μ désigne la fonction de Möbius (Lie, II, p. 71), est convergente pour la topologie produit de $\mathrm{U}(\mathrm{A}) = \mathrm{A}^{\mathbf{J}}$. On définit ainsi l'endomorphisme additif $\varepsilon_{\mathrm{Q}} = \sum_{q \in \mathrm{Q}} \frac{\mu(q)}{q} \mathbf{V}_q \mathbf{F}_q$ de U(A). Pour tout $n \in \mathbf{J}$, l'application $\Phi_n \circ \varepsilon_{\mathrm{Q}}$ de U(A) dans A est égale à 0 si $n \notin \mathrm{P}$ et à Φ_n si $n \in \mathrm{P}$.
b) Pour tout $q \in \mathrm{Q}$, $q \neq 1$, on a

$$\varepsilon_{\mathrm{Q}} \mathbf{V}_q = 0 = \mathbf{F}_q \varepsilon_{\mathrm{Q}}.$$

(Utiliser l'exerc. 36, *c*), p. 52.)
c) Montrer que ε_{Q} est un idempotent ayant pour image l'intersection des noyaux des $\mathbf{F}_q$ ($q \in \mathrm{Q}$, $q \neq 1$).

Pour $m \in \mathbf{J}$ et $a \in \mathrm{A}$, calculer $\varepsilon_{\mathrm{Q}} \mathbf{V}_m \tau(a)$. En déduire que le noyau de ε_{Q} est l'ensemble des éléments de la forme $\sum_{n \in \mathrm{Q}} \mathbf{V}_n \tau(a_n)$, avec $a_n \in \mathrm{A}$. Le sous-ensemble $\varepsilon_{\mathrm{Q}}\mathrm{U}(\mathrm{A})$ de U(A) est stable par addition et multiplication. Muni de ces deux opérations, c'est un anneau commutatif, d'unité $\varepsilon_{\mathrm{Q}}(1_{\mathrm{U}(\mathrm{A})})$, et l'application $\varepsilon_{\mathrm{Q}} : \mathrm{U}(\mathrm{A}) \to \varepsilon_{\mathrm{Q}}\mathrm{U}(\mathrm{A})$ est un homomorphisme d'anneaux.
d) Pour tout $q \in \mathrm{Q}$, posons $e_q = \frac{1}{q} \mathbf{V}_q \varepsilon_{\mathrm{Q}} \mathbf{F}_q$. Montrer que l'on a $e_q^2 = e_q$ et $e_q e_{q'} = 0$ si $q \neq q'$, et que, pour tout $\boldsymbol{a} \in \mathrm{U}(\mathrm{A})$ on a

$$(*) \quad \boldsymbol{a} = \sum_{q \in \mathrm{Q}} e_q(\boldsymbol{a}),$$

où la somme est convergente pour la topologie produit de U(A). (Pour (*) se ramener au cas où $\boldsymbol{a} = \mathbf{X} \in \mathrm{U}(\mathrm{R}[\mathbf{X}])$, R étant le sous-anneau de $\mathbf{Q}$ formé des nombres rationnels à dénominateur dans Q. Il suffit alors d'appliquer Φ et de vérifier l'analogue de (*) dans $\mathrm{R}[\mathbf{X}]^{\mathbf{J}}$ ce qui résulte de la formule $\Phi_{pq} \circ e_{q'} = \Phi_{pq} \delta_{qq'}$ si $p \in \mathrm{P}$, $q \in \mathrm{Q}$, $q' \in \mathrm{Q}$.

Le sous-ensemble $e_q\mathrm{U}(\mathrm{A})$ de U(A) est stable par addition et multiplication. Muni de ces deux opérations, c'est un anneau commutatif, d'unité $e_q(1_{\mathrm{U}(\mathrm{A})})$ et l'application $e_q : \mathrm{U}(\mathrm{A}) \to e_q\mathrm{U}(\mathrm{A})$ est un homomorphisme d'anneaux.
e) Pour tout $q \in \mathrm{Q}$, on a $\mathbf{F}_q e_q = \varepsilon_{\mathrm{Q}} \mathbf{F}_q$ et $\left(\frac{1}{q} \mathbf{V}_q\right) \varepsilon_{\mathrm{Q}} = e_q\left(\frac{1}{q} \mathbf{V}_q\right)$. En conclure que $\boldsymbol{a} \mapsto \mathbf{F}_q(\boldsymbol{a})$ est un isomorphisme d'anneaux $e_q\mathrm{U}(\mathrm{A}) \to \varepsilon_{\mathrm{Q}}\mathrm{U}(\mathrm{A})$, d'inverse $\boldsymbol{a} \mapsto \frac{1}{q} \mathbf{V}_q(\boldsymbol{a})$.

f) Montrer que la projection canonique $\pi_{\mathrm{P}} : \mathrm{U}(\mathrm{A}) \to \mathrm{U}_{\mathrm{P}}(\mathrm{A})$ (exerc. 39) définit un isomorphisme d'anneaux $\varepsilon_{\mathrm{Q}}\mathrm{U}(\mathrm{A}) \to \mathrm{U}_{\mathrm{P}}(\mathrm{A})$. En déduire un isomorphisme d'anneaux de U(A) sur $\mathrm{U}_{\mathrm{P}}(\mathrm{A})^{\mathrm{Q}}$ transformant $\boldsymbol{a}$ en $(\pi_{\mathrm{P}} \varepsilon_{\mathrm{Q}} \mathbf{F}_q(\boldsymbol{a}))_{q \in \mathrm{Q}}$ pour tout $\boldsymbol{a} \in \mathrm{U}(\mathrm{A})$.
g) Si A est une $\mathbf{Q}$-algèbre, on peut prendre $\mathrm{P} = \{1\}$ et $\mathrm{Q} = \mathbf{J}$. On déduit un isomorphisme d'anneaux $\mathrm{U}(\mathrm{A}) \to \mathrm{A}^{\mathbf{J}}$, qui n'est autre que Φ.

h) Supposons que $P = \{p^n | n \in \mathbf{N}\}$, où p est un nombre premier. Ainsi tout nombre premier $q \neq p$ est inversible dans A. On obtient un isomorphisme d'anneaux $U(A) \to W(A)^Q$ (*cf.* exerc. 39, *d*)).

On notera ω_A l'application de W(A) dans U(A), qui, par l'isomorphisme de U(A) et $W(A)^Q$, correspond à l'inclusion de W(A) dans $W(A)^Q$ selon la première composante.

41) Soit A un anneau.

a) Soit $\mu : A \to U(A)$ un homomorphisme d'anneaux tel que $\Phi_1 \circ \mu = Id_A$. Posons $\sigma = \Phi \circ \mu$ et $\sigma(a) = (\sigma_n(a))_{n \in \mathbf{J}}$ pour $a \in A$. Les applications $\sigma_n : A \to A$ ($n \in \mathbf{J}$) satisfont aux conditions suivantes :

(1) σ_n est un homomorphisme d'anneaux pour tout $n \in \mathbf{J}$, et $\sigma_1 = Id_A$.

(2) Pour tout nombre premier p et pour tout $a \in A$, on a $\sigma_p(a) \equiv a^p$ mod. pA et

$$\sigma_p(\sigma_n(a)) \equiv \sigma_{pn}(a) \text{ mod. } p^{w_p(pn)}A \quad \text{pour tout} \quad n \in \mathbf{J}\ .$$

b) Supposons que le groupe additif de A soit sans **Z**-torsion. Soit $\sigma = (\sigma_n)_{n \in \mathbf{J}}$ une famille d'applications $\sigma_n : A \to A$ satisfaisant aux conditions (1) et (2) de *a*). Il existe un unique homomorphisme d'anneaux $\mu : A \to U(A)$ tel que $\Phi_1 \circ \mu = Id_A$ et $\Phi \circ \mu = \sigma$. (Appliquer les exerc. 32 et 33, *d*), p. 51.)

c) Supposons que le groupe additif de A soit sans **Z**-torsion. Il existe un unique homomorphisme d'anneaux

$$\mu^A : U(A) \to U(U(A))$$

tel que $\Phi^{U(A)} \circ \mu^A$ soit l'application

$$\mathbf{F}^A : U(A) \to U(A)^{\mathbf{J}}$$

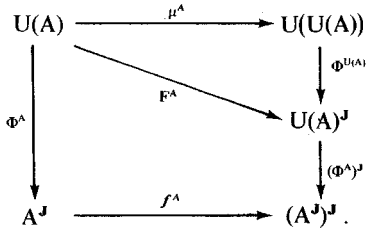
définie par $\mathbf{F}^A(\boldsymbol{a}) = (\mathbf{F}_n(\boldsymbol{a}))_{n \in \mathbf{J}}$. (Se ramener au cas où $A = \mathbf{Z}[\mathbf{X}]$. Appliquer *b*) et les exerc. 36 et 38, *b*), p. 52 et 53.)

d) Soit $\mathbf{X} = (X_n)_{n \in \mathbf{J}}$ une famille d'indéterminées considérée comme élément de $U(\mathbf{Z}[\mathbf{X}])$. Posons

$$\mu^{\mathbf{Z}[\mathbf{X}]}(\mathbf{X}) = (\mu_n(\mathbf{X}))_{n \in \mathbf{J}} = ((\mu_{n,m}(\mathbf{X}))_{m \in \mathbf{J}})_{n \in \mathbf{J}}$$

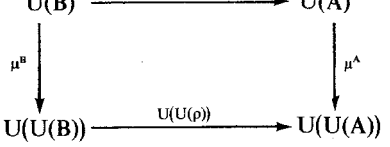
où $\mu_{n,m}(\mathbf{X}) \in \mathbf{Z}[\mathbf{X}]$ pour n, m dans **J**. Pour tout anneau A définissons $\mu^A : U(A) \to U(U(A))$ par $\mu^A(\boldsymbol{a}) = ((\mu_{n,m}(\boldsymbol{a}))_{m \in \mathbf{J}})_{n \in \mathbf{J}}$. Montrer que μ^A est un homomorphisme d'anneaux tel que le diagramme suivant soit commutatif

(1)



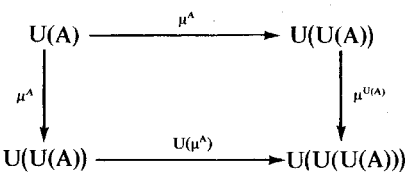
Ici par définition, $f^A(\boldsymbol{a}) = (f_n(\boldsymbol{a}))_{n \in \mathbf{J}}$ pour $\boldsymbol{a} \in A^{\mathbf{J}}$, et Φ^A (resp. $\Phi^{U(A)}$) est l'homomorphisme Φ associé à l'anneau A (resp. U(A)).

e) Pour tout homomorphisme d'anneaux $\rho : B \to A$ le diagramme

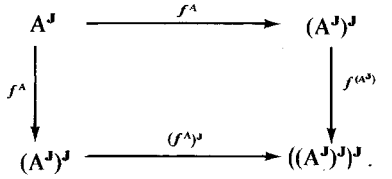


est commutatif.

f) Montrer que le diagramme suivant est commutatif



(Se ramener au cas où A = **Q**[X]. Alors A est une **Q**-algèbre, donc $\Phi^A : U(A) \to A^J$ est un isomorphisme et U(A) est également une **Q**-algèbre. Si, à l'aide du diagramme (1) et par transport de structure, on remplace μ^A par f^A lorsque A est une **Q**-algèbre, on est ramené à démontrer la commutativité du diagramme



On a

$$f^{(A^J)}(f^A(X)) = f^{(A^J)}((f_n(X))_{n\in J}) = ((f_m(f_n(X)))_{n\in J})_{m\in J} = ((f_{mn}(X))_{n\in J})_{m\in J},$$

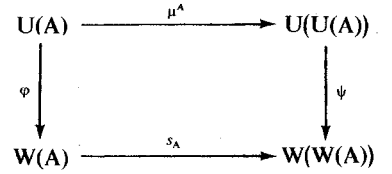
et

$$(f^A)^J(f^A(X)) = (f^A)^J((f_n(X))_{n\in J}) = (f^A(f_n(X)))_{n\in J} = ((f_{mn}(X))_{m\in J})_{n\in J}.)$$

g) Pour tout $a \in A$, on a

$$\mu_n^A(\tau(a)) = 0 \quad \text{pour} \quad n \geqslant 2.$$

h) On a le diagramme commutatif suivant



où l'application s_A est celle définie à l'exerc. 15, p. 44, où l'application φ de U(A) dans W(A) est obtenue par identification de W(A) et $U_{p^\infty}(A)$ (p. 53, exerc. 39), et l'application ψ est composée de U(φ) et de l'application de U(W(A)) dans W(W(A)) obtenue par identification de W(W(A)) à $U_{p^\infty}(W(A))$.

42) Soient A un anneau et T une indéterminée. On note $\Lambda(A)$ (ou $\Lambda_T(A)$) l'ensemble $1 + TA[[T]]$ des séries formelles à coefficients dans A de terme constant égal à 1 ; c'est un sous-groupe du groupe multiplicatif de A[[T]]. On définit

$$L : \Lambda(A) \to A^J, \quad L(f) = (L_n(f))_{n\in J},$$

par

$$-T\frac{df}{dT}/f = \sum_{n\in J} L_n(f)(-T)^n.$$

a) Montrer que l'on a $L(fg) = L(f) + L(g)$ quels que soient $f, g \in \Lambda(A)$.

b) Si A est une **Q**-algèbre, alors L est bijectif, son inverse ε étant donné par

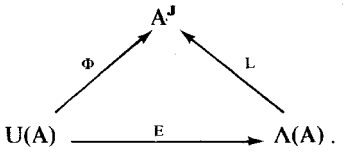
$$\varepsilon(\boldsymbol{a}) = \exp(-\sum_{n\in\mathbf{J}} \frac{a_n}{n}(-\mathrm{T})^n)$$

pour $\boldsymbol{a} \in \mathrm{A}^{\mathbf{J}}$.

43) Soit $\mathrm{E}:\mathrm{U}(\mathrm{A}) \to \Lambda(\mathrm{A})$ l'application définie par

$$\mathrm{E}(\boldsymbol{a}) = \prod_{n\in\mathbf{J}} (1 - a_n(-\mathrm{T})^n)$$

pour $\boldsymbol{a} \in \mathrm{U}(\mathrm{A})$.
a) Démontrer la commutativité du diagramme



En déduire que si A est une **Q**-algèbre, on a

$$\prod_{n\in\mathbf{J}} (1 - a_n\mathrm{T}^n) = \exp(-\sum_{n\in\mathbf{J}} (\Phi_n(\boldsymbol{a})/n)\,\mathrm{T}^n)$$

quel que soit $\boldsymbol{a} \in \mathrm{U}(\mathrm{A})$.
b) Montrer que E est bijectif. (Si l'on pose $\prod_{n\in\mathbf{J}} (1 - a_n(-\mathrm{T})^n) = \sum_{n\geqslant 0} c_n(\boldsymbol{a})(-\mathrm{T})^n$, il suffit d'appliquer l'exerc. 33, *a*), p. 51 à la famille de polynômes $c_n(\mathrm{X})$ de $\mathbf{Z}[\mathrm{X}]$.)
c) On munit Λ(A) de l'unique structure d'anneau telle que E soit un isomorphisme d'anneaux. Montrer que l'addition de Λ(A) est la multiplication des séries, d'élément neutre 1. La multiplication de l'anneau Λ(A) notée $(f, g) \mapsto f * g$, est définie par la formule

$$\mathrm{E}(\boldsymbol{a} \times \boldsymbol{b}) = \mathrm{E}(\boldsymbol{a}) * \mathrm{E}(\boldsymbol{b})$$

quels que soient $\boldsymbol{a}, \boldsymbol{b} \in \mathrm{U}(\mathrm{A})$; son élément neutre est $1 + \mathrm{T}$.
d) Soit $\tau:\mathrm{A} \to \mathrm{U}(\mathrm{A})$ l'application définie dans l'exerc. 37, *c*), p. 53. On a

$$\mathrm{E}(\tau(a)) = 1 + a\mathrm{T}$$
$$(1 + a\mathrm{T}) * (1 + b\mathrm{T}) = 1 + ab\mathrm{T}$$
$$(1 + a\mathrm{T}) * f(\mathrm{T}) = f(a\mathrm{T})$$
$$\mathrm{L}(1 + a\mathrm{T}) = (a^n)_{n\in\mathbf{J}}$$

quels que soient a, b dans A et $f(\mathrm{T})$ dans Λ(A).
e) Soient f et g deux éléments de Λ(A) qui soient des polynômes en T, et soit m le degré de f. Posons

$$\varphi(\mathrm{X}) = \mathrm{X}^m f(\mathrm{T}/\mathrm{X})$$

et

$$\gamma(\mathrm{X}) = g(-\mathrm{X}).$$

Ce sont des polynômes en X à coefficients dans A[T]; φ est unitaire et $f * g$ est le résultant $\mathrm{res}(\varphi, \gamma)$ des polynômes φ et γ (*cf.* A, IV, p. 75).
(On pourra partir de la formule

$$(1 + a\mathrm{T}) * g = g(a\mathrm{T}),$$

en déduire le résultat si $\mathrm{A} = \mathbf{Z}[\mathrm{X}_1, \ldots, \mathrm{X}_m]$ et $f = \prod_{i=1}^{m} (1 + \mathrm{X}_i\mathrm{T})$, et passer de là au cas général.)

44) Soit A un anneau.
a) L'ensemble $\hat{U}(A)$ des éléments de U(A) à coordonnées nilpotentes, nulles sauf un nombre fini d'entre elles, est un idéal de l'anneau U(A). Pour tout $n \in \mathbf{J}$, il est stable par F_n et V_n.
b) Soit $\boldsymbol{a} \in \hat{U}(A)$. Alors l'élément $E(\boldsymbol{a})$ de $\Lambda(A)$ est un polynôme en T. Sa valeur en -1 est un élément inversible de A, qui est aussi, pour tout $n \in \mathbf{J}$, la valeur en -1 du polynôme $E(V_n\boldsymbol{a})$.
c) Si $\boldsymbol{a} \in U(A)$ et $\boldsymbol{b} \in \hat{U}(A)$, on note $\langle \boldsymbol{a}, \boldsymbol{b} \rangle$ la valeur en -1 du polynôme $E(\boldsymbol{ab})$. On définit ainsi une application $\mathbf{Z}$-bilinéaire de $U(A) \times \hat{U}(A)$ dans A^* et on a

$$\langle F_n\boldsymbol{a}, \boldsymbol{b} \rangle = \langle \boldsymbol{a}, V_n\boldsymbol{b} \rangle$$
$$\langle V_n\boldsymbol{a}, \boldsymbol{b} \rangle = \langle \boldsymbol{a}, F_n\boldsymbol{b} \rangle \quad \text{pour tout } n \in \mathbf{J}.$$

45) Par *pré-λ-anneau* on entend un anneau A muni d'applications $\lambda_n : A \to A$ ($n \in \mathbf{N}$) telles que
(i) $\lambda_0(a) = 1$,
(ii) $\lambda_1(a) = a$,
(iii) $\lambda_n(a + b) = \sum_{p=0}^{n} \lambda_p(a)\,\lambda_{n-p}(b)$,
quels que soient a, b dans A. Les conditions (i) et (iii) s'expriment également en disant que

$$\lambda(a) = \sum_{n \geqslant 0} \lambda_n(a)\,T^n$$

définit un homomorphisme du groupe additif de A dans le groupe multiplicatif $\Lambda(A)$.

Par *λ-morphisme* d'un pré-λ-anneau A dans un autre B, on entend un homomorphisme $\rho : A \to B$ d'anneaux tel que $\rho(\lambda_n(a)) = \lambda_n(\rho(a))$ quels que soient $a \in A$, $n \in \mathbf{N}$, autrement dit tel que le diagramme

$$\begin{array}{ccc} \Lambda(A) & \xrightarrow{\Lambda(\rho)} & \Lambda(B) \\ {\scriptstyle\lambda}\uparrow & & \uparrow{\scriptstyle\lambda} \\ A & \xrightarrow{\rho} & B \end{array}$$

soit commutatif (l'application $\Lambda(\rho)$ transforme la série $1 + \sum_{n \geqslant 1} a_n T^n$ en la série $1 + \sum_{n \geqslant 1} \rho(a_n)\,T^n$).

Soit A un anneau. Nous nous proposons de munir $\Lambda(A)$ d'une structure de pré-λ-anneau. Notons $E^A : U(A) \to \Lambda_T(A)$ l'isomorphisme d'anneaux défini dans l'exerc. 43. Soit S une autre indéterminée.
a) Montrer que les deux isomorphismes composés

$$U(U(A)) \xrightarrow{U(E^A)} U(\Lambda_T(A)) \xrightarrow{E^{\Lambda_T(A)}} \Lambda_S(\Lambda_T(A))$$

et

$$U(U(A)) \xrightarrow{E^{U(A)}} \Lambda_S(U(A)) \xrightarrow{\Lambda_S(E^A)} \Lambda_S(\Lambda_T(A))$$

coïncident ; on les notera $\tilde{E}^A$.

On définit l'application λ^A par la commutativité du diagramme

$$\begin{array}{ccc} U(U(A)) & \xrightarrow{\tilde{E}^A} & \Lambda_S(\Lambda_T(A)) \\ {\scriptstyle\mu^A}\uparrow & & \uparrow{\scriptstyle\lambda^A} \\ U(A) & \xrightarrow{E^A} & \Lambda_T(A) \end{array}$$

où μ^A désigne l'homomorphisme défini dans l'exerc. 41, *d*), p. 55.

b) L'anneau $\Lambda(A)$, muni de λ^A, est un pré-λ-anneau. Pour tout homomorphisme d'anneaux $\rho : A \to B$, $\Lambda(\rho) : \Lambda(A) \to \Lambda(B)$ est un λ-morphisme.
c) Un pré-λ-anneau A s'appelle un *λ-anneau* si $\lambda : A \to \Lambda(A)$ est un λ-morphisme (pour la structure de pré-λ-anneau sur $\Lambda(A)$ qu'on vient de définir).

Soit A un anneau. Montrer que $(\Lambda(A), \lambda^A)$ est un λ-anneau. (Utiliser l'exerc. 41, *f*), p. 56.)

46) *a*) Soient A un pré-λ-anneau et $a \in A$. On appelle *λ-rang de a* la borne supérieure dans $\overline{\mathbf{R}}$ de l'ensemble des entiers $n \in \mathbf{N}$ tels que $\lambda_n(a) \neq 0$. Soit P une partie multiplicative de A formée d'éléments de λ-rang $\leqslant 1$. Soit $a = \sum_{i \in I} a_i$ la somme d'une famille finie d'éléments de P. On a $\lambda(a) = \prod_{i \in I} (1 + a_i T)$, donc $\lambda_n(a) = s_n((a_i)_{i \in I})$, où s_n désigne le polynôme symétrique élémentaire de degré n (A, IV, p. 63).
b) Soient A un anneau et a, b des éléments de A. Alors dans $\Lambda(A)$ les éléments $1 + aT$ et $(1 + aT) * (1 + bT) = 1 + abT$ sont de λ-rang $\leqslant 1$.
c) Soit A un pré-λ-anneau. Supposons qu'il existe un sous-monoïde multiplicatif de A, formé d'éléments de λ-rang $\leqslant 1$, qui engendre le groupe additif de A. Montrer que A est alors un λ-anneau. Plus généralement, A est un λ-anneau s'il existe un λ-morphisme injectif de A dans un pré-λ-anneau satisfaisant à la propriété précédente (« Principe de scindage »). (Il s'agit de montrer que l'application $\mathbf{Z}$-bilinéaire $(a, b) \mapsto \lambda(a) * \lambda(b)\, \lambda(ab)^{-1}$ est nulle et que les applications $\mathbf{Z}$-linéaires $a \mapsto \Lambda_S(\lambda_T)[\lambda_S(a)]$ et $a \mapsto \lambda_S^{\Lambda}(\lambda_T(a))$ de A dans $\Lambda_S(\Lambda_T(A))$ coïncident. Il suffit de vérifier ces propriétés pour $a, b \in P$.)
d) Soit $A = \mathbf{Z}[(X_i)_{i \in I}, (X'_{i'})_{i' \in I'}]$ l'anneau des polynômes en deux familles finies d'indéterminées. On a

$$\prod_{i \in I} (1 + X_i T) = \sum_{n \geqslant 0} s_n((X_i)_{i \in I})\, T^n$$

où

$$s_n((X_i)_{i \in I}) = \sum_{H \in \binom{I}{n}} X_H,$$

$\binom{I}{n}$ désignant l'ensemble des parties à n éléments de I, et où $X_H = \prod_{h \in H} X_h$. En affectant les X_i (et $X'_{i'}$) du poids 1, s_n est homogène de poids n. Tout polynôme symétrique en $(X_i)_{i \in I}$ s'exprime de façon unique comme polynôme en les s_n ($n \geqslant 1$) (A, IV, p. 58). En particulier, pour tout $m \geqslant 0$, on a

$$s_m((X_H)_{H \in \binom{I}{n}}) = Q_{n,m}(s_1, \ldots, s_{nm})$$

où $Q_{n,m}$ est homogène de poids nm en les $s_r = s_r((X_i)_{i \in I})$ ($r = 1, \ldots, nm$). C'est le coefficient de T^m dans $\prod_{H \in \binom{I}{n}} (1 + X_H T)$, et il est bien défini et indépendant de I, pourvu que $\mathrm{Card}(I) \geqslant nm$.
Le coefficient de T^n dans $\prod_{(i,i') \in I \times I'} (1 + X_i X'_{i'} T)$ est

$$s_n((X_i X'_{i'})_{(i,i') \in I \times I'}) = P_n(s_1, \ldots, s_n, s'_1, \ldots, s'_n)$$

où $s'_r = s_r((X'_{i'})_{i' \in I'})$, et où P_n est homogène de poids n en chacune des familles de variables (s_r) et (s'_r). Il est bien défini et indépendant de I et I' pourvu que I et I' soient de cardinaux $\geqslant n$.

Montrer que dans le λ-anneau $\Lambda(A)$ on a

$$\Big(\sum_{r \geqslant 0} s_r T^r\Big) * \Big(\sum_{r \geqslant 0} s'_r T^r\Big) = \sum_{n \geqslant 0} P_n(s_1, \ldots, s_n, s'_1, \ldots, s'_n)\, T^n$$

et

$$\lambda_n^A\Big(\sum_{r \geqslant 0} s_r T^r\Big) = \sum_{m \geqslant 0} Q_{n,m}(s_1, \ldots, s_{nm})\, T^m.$$

D'après *a*) et *b*), on a

$$\Big(\sum_r s_r T^r\Big) * \Big(\sum_r s'_r T^r\Big) = \Big(\prod_i (1 + X_i T)\Big) * \Big(\prod_{i'} (1 + X'_{i'} T)\Big) = \prod_{i,i'} (1 + X_i X'_{i'} T)$$

et

$$\lambda(\sum_r s_r T^r) = \lambda(\prod_i (1 + X_i T)) = \prod_i (1 + (1 + X_i T)S) = \sum_n s_n((1 + X_i T)_{i\in\mathbf{I}})\, S^n$$

et

$$s_n((1 + X_i T)_{i\in\mathbf{I}}) = \prod_{H\in\binom{\mathbf{I}}{n}} \ast_{h\in H} (1 + X_h T) = \prod_{H\in\binom{\mathbf{I}}{n}} (1 + X_H T).$$

e) Soit A un pré-λ-anneau. Pour que A soit un λ-anneau, il faut et il suffit que les conditions suivantes soient satisfaites, quels que soient a, b dans A, et n, m dans **N**.

(i) $\lambda(1) = 1 + T$,

(ii) $\lambda_n(ab) = P_n(\lambda_1(a), \ldots, \lambda_n(a), \lambda_1(b), \ldots, \lambda_n(b))$,

(iii) $\lambda_m(\lambda_n(a)) = Q_{n,m}(\lambda_1(a), \ldots, \lambda_{nm}(a))$.

f) Soit $\rho : A \to B$ un λ-morphisme de pré-λ-anneaux. Si A est un λ-anneau et ρ surjectif, alors B est un λ-anneau. Si B est un λ-anneau et si ρ est injectif, alors A est un λ-anneau.

47) Soit A un anneau. On définit des applications F_n, V_n ($n \in \mathbf{J}$) de Λ(A) dans lui-même par les formules

$$F_n(E(a)) = E(F_n(a)), \quad V_n(E(a)) = E(V_n(a))$$

quel que soit $a \in U(A)$.

a) On a $L(F_n(f)) = f_n(L(f))$ et $L(V_n(f)) = v_n(L(f))$ quel que soit $f \in \Lambda(A)$.

Soient n, m dans **J** et posons $d = \text{pgcd}(n, m)$.

b) Montrer que F_n est un endomorphisme de l'anneau Λ(A), et que l'on a $F_n \circ F_m = F_{nm}$. Pour tout nombre premier p et pour tout $f \in \Lambda(A)$, on a $F_p(f) \equiv f^{*p} \bmod p * \Lambda(A)$, où f^{*p} désigne le produit dans l'anneau Λ(A) de p termes égaux à f, et où $p * \Lambda(A)$ désigne l'idéal principal de Λ(A) engendré par la somme dans Λ(A) de p termes égaux à l'élément neutre $1 + T$, autrement dit par $(1 + T)^p$.

c) Prouver que V_n est un endomorphisme du groupe additif de Λ(A), et que l'on a $V_n \circ V_m = V_{nm}$.

d) Pour tout $f \in \Lambda(A)$, on a $F_n(V_m(f)) = V_{m/d}(F_{n/d}(f))^d$. En particulier $F_n(V_n(f)) = f^n$, et $F_n \circ V_m = V_m \circ F_n$ si $d = 1$.

e) Quels que soient f, g dans Λ(A), on a

$$V_n(f) * V_m(g) = V_{nm/d}(F_{m/d}(f) * F_{n/d}(g))^d,$$
$$V_n(f * F_m(g))^{n/d} = V_n(f) * V_{n/d}(F_{m/d}(g)),$$
$$V_n(F_m(g))^{n/d} = V_n(1 + T) * V_{n/d}(F_{m/d}(g)).$$

En particulier, on a

$$V_n(f) * V_n(g) = V_n(f * g)^n$$

et

$$V_n(f) * V_m(g) = V_{nm}(F_m(f) * F_n(g)) \quad \text{si} \quad d = 1.$$

f) On a

$$V_n(f)(T) = f(-(-T)^n)$$

quel que soit $f \in \Lambda(A)$. En particulier

$$V_n(1 + aT) = 1 - a(-T)^n$$

pour tout $a \in A$.

g) Pour tout $a \in A$, on a

$$F_n(1 + aT) = 1 + a^n T.$$

Pour tout $f \in \Lambda(A)$, on a

$$F_n(f)(-(-T)^n) = N(f(T))$$

où N désigne la norme dans l'extension $A[[T^n]] \subset A[[T]]$. (Il suffit de traiter le cas où $f \in A[T]$, puis de plonger A dans un anneau B où f se décompose en produit de facteurs linéaires, auxquels on peut appliquer la première formule.)

Pour tout $a \in A$, on a

$$F_n(1 - a(-T)^m) = (1 - a^{n/d}(-T)^{m/d})^d .$$

(Observer que $1 - a(-T)^m = V_m(1 + aT)$ et utiliser *c*) et *f*).)
h) Quels que soient $a, b \in A$, on a

$$(1 - a(-T)^n) * (1 - b(-T)^m) = (1 - a^{m/d}b^{n/d}(-T)^{mn/d})^d .$$

(Utiliser la première formule de *e*).)

48) Soit A un pré-λ-anneau. Notons Ψ le composé $A \xrightarrow{\lambda} \Lambda(A) \xrightarrow{L} A^{\mathbf{J}}$, de sorte que $\Psi(a) = (\psi_n(a))_{n\in\mathbf{J}}$, où

$$-T\frac{d}{dT}\lambda(a)/\lambda(a) = \sum_{n\in\mathbf{J}} \psi_n(a)(-T)^n .$$

Plus explicitement,

$$-n\lambda_n(a) = (-1)^n\psi_n(a) + (-1)^{n-1}\psi_{n-1}(a).\lambda_1(a) + \cdots + (-\psi_1(a)).\lambda_{n-1}(a)$$

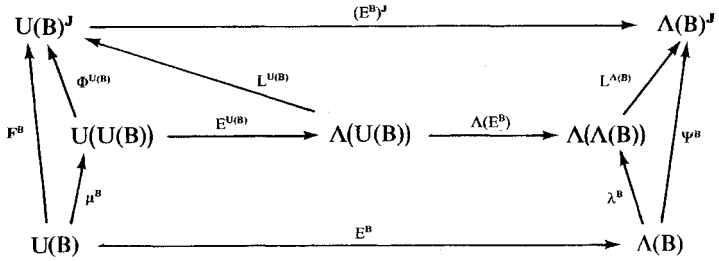
quel que soit $n \in \mathbf{J}$. En particulier,

$$\psi_1(a) = \lambda_1(a) = a$$
$$\psi_2(a) = \lambda_1(a)^2 - 2\lambda_2(a)$$
$$\psi_3(a) = \lambda_1(a)^3 - 3\lambda_1(a)\lambda_2(a) + 3\lambda_3(a) .$$

Les applications $\psi_n : A \to A$ s'appellent *opérations d'Adams*.
Lorsque $(A, \lambda) = (\Lambda(B), \lambda^B)$, B étant un anneau, on écrira aussi Ψ^B pour Ψ.
a) Soit B un anneau. Montrer que pour tout $n \in \mathbf{J}$, on a

$$\psi_n^B = F_n : \Lambda(B) \to \Lambda(B) .$$

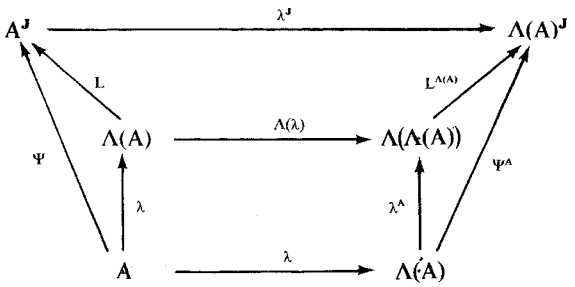
(Utiliser le diagramme commutatif



où toutes les applications horizontales sont bijectives.)
b) Soit A un pré-λ-anneau. Pour tout $n \in \mathbf{J}$, ψ_n est un endomorphisme du groupe additif de A, et $\psi_1 = \mathrm{Id}_A$. Si A est un λ-anneau, ψ_n est un endomorphisme de l'anneau A, et $\psi_n \circ \psi_m = \psi_{nm}$ quels que soient *n*, *m* dans **J**. De plus, pour tout nombre premier *p* on a $\psi_p(a) \equiv a^p \bmod. pA$ quel que soit $a \in A$. (Utiliser l'injectivité de $\lambda : A \to \Lambda(A)$, et les propriétés analogues des $\psi_n^A = F_n$.)
c) Soit A un pré-λ-anneau dont le groupe additif soit sans **Z**-torsion. Pour que A soit un λ-anneau, il faut et il suffit que les conditions suivantes soient satisfaites pour tous les entiers $n \geqslant 2$ et $m \geqslant 2$:

(i) $\psi_n(1) = 1$;
(ii) $\psi_n(ab) = \psi_n(a)\,\psi_n(b)$ quels que soient *a*, *b* dans A ;
(iii) $\psi_n \circ \psi_m = \psi_{nm}$.

(Puisque $L : \Lambda(A) \to A^J$ est un homomorphisme *injectif* d'anneaux, $\Psi = L \circ \lambda$ est un homomorphisme d'anneaux si et seulement si λ en est un. De même du diagramme



on déduit que

$$\Lambda(\lambda) \circ \lambda = \lambda^A \circ \lambda \quad (\lambda \text{ est un } \lambda\text{-morphisme})$$
$$\Leftrightarrow \lambda^J \circ \Psi = \Psi^A \circ \lambda \Leftrightarrow \lambda \circ \psi_n = \psi_n^A \circ \lambda \text{ pour tout } n$$
$$\Leftrightarrow L \circ \lambda \circ \psi_n = L \circ \psi_n^A \circ \lambda \text{ pour tout } n.$$

Or $L \circ \lambda = \Psi$ et $L \circ \psi_n^A = L \circ F_n = f_n \circ L$. Donc

$$\Lambda(\lambda) \circ \lambda = \lambda^A \circ \lambda \Leftrightarrow \Psi \circ \psi_n = f_n \circ \Psi \text{ pour tout } n$$
$$\Leftrightarrow \psi_m \circ \psi_n = \psi_{nm} \text{ quels que soient } m \text{ et } n.)$$

d) Soit A un λ-anneau. Soit $a \in A$ un élément de λ-rang $\leqslant 1$ (i.e. $\lambda(a) = 1 + aT$). Alors $\psi_n(a) = a^n$ quel que soit $n \in \mathbf{J}$. Si P est une partie multiplicative de A formée d'éléments de λ-rang $\leqslant 1$ et si $a_1, ..., a_r$ appartiennent à P, on a $\psi_n(a_1 + \cdots + a_r) = a_1^n + \cdots + a_r^n$.

Dans l'algèbre de polynômes $\mathbf{Z}[(X_i)_{i\in I}]$, notons (s_n) les polynômes symétriques élémentaires, $\sum_{n\geqslant 0} s_n T^n = \prod_i (1 + X_i T)$, et

$$v_n(s_1, ..., s_n) = \sum_i X_i^n$$

le n-ième polynôme de Newton. Montrer que, quel que soit $a \in A$, on a

$$\psi_n(a) = v_n(\lambda_1(a), ..., \lambda_n(a)).$$

(Vérifier d'abord cette relation lorsque a est de la forme $a_1 + \cdots + a_r$ comme ci-dessus. Passer de là au cas où $a = 1 + \sum_{h\geqslant 1} s_h T^h \in \Lambda(\mathbf{Z}[(X_i)_{i\in I}])$. Ensuite déduire le cas général en plongeant A dans le λ-anneau $\Lambda(A)$ et en utilisant l'homomorphisme $\mathbf{Z}[(s_h)_{h=1,...,n}] \to A$ qui envoie s_h sur $\lambda_h(a)$.)

49) Soient A un anneau, E un A-module projectif de type fini, et $u \in \mathrm{End}_A(E)$. Si E est un A-module libre, on note $\det_E(u)$ le déterminant de u. En général, on peut choisir un A-module F tel que $E \oplus F$ soit un A-module libre de type fini, et on pose

$$\det_E(u) = \det_{E\oplus F}(u \oplus 1_F).$$

a) Montrer que $\det_E(u)$ est indépendant du choix de F, que $\det(1_E) = 1$, et que $\det_F(u \circ v) = \det_E(u).\det_E(v)$ quels que soient u, v dans $\mathrm{End}_A(E)$.

b) Supposons que L soit un sous-module facteur direct de E stable par u, et notons $u_L \in \mathrm{End}_A(L)$ et $u_{E/L} \in \mathrm{End}_A(E/L)$ les endomorphismes définis par u. Alors on a $\det_E(u) = \det_L(u_L).\det_{E/L}(u_{E/L})$.

Soient T une indéterminée, $E[T] = A[T] \otimes_A E$, et identifions u à $1_{A[T]} \otimes_A u \in \mathrm{End}_{A[T]}(E[T])$. Posons

$$\chi_E(u) = \det(T.1 - u)$$

(polynôme caractéristique de u) et

$$\overline{\chi}_E(u) = \det(1 + uT) = \sum_{n \geqslant 0} \mathrm{Tr}(\Lambda^n(u))\, T^n$$

où 1 désigne $1_{E[T]}$ (*cf.* A, III, p. 107).
c) On a $\overline{\chi}_E(0) = 1$. Supposons que E soit localement libre de rang constant r. On a $\overline{\chi}_E(1_E) = (1 + T)^r$. Si $\sigma_r : A[T, T^{-1}] \to A[T, T^{-1}]$ désigne l'application $(\sigma_r f)(T) = T^r . f((-T)^{-1})$ on a $\sigma_r(\sigma_r(f)) = (-1)^r f$ et $\sigma_r(\overline{\chi}_E(u)) = \chi_E(u)$.
d) Soit $\alpha : A \to A'$ un homomorphisme d'anneaux. On a $\overline{\chi}_{A' \otimes_A E}(\mathrm{Id}_{A'} \otimes_A u) = \alpha(\overline{\chi}_E(u))$, où on note α aussi l'homomorphisme $A[T] \to A'[T]$ défini par α.
e) On a $\overline{\chi}_E(u) \in \Lambda(A)$. Pour tout $n \in \mathbf{J}$, on a

$$\lambda_n^A(\overline{\chi}_E(u)) = \overline{\chi}_{\Lambda^n(E)}(\Lambda^n(u)),$$
$$\psi_n^A(\overline{\chi}_E(u)) = \overline{\chi}_E(u^n).$$

(Il suffit de vérifier les formules localement sur le spectre de A, donc on peut supposer E égal à A^r. Soit $(u_{ij})_{1 \leqslant i,j \leqslant r}$ la matrice de u, soit $(X_{ij})_{1 \leqslant i,j \leqslant r}$ une famille d'indéterminées, posons $B = Z[(X_{ij})]$, et soit v l'endomorphisme de B^r de matrice $X = (X_{ij})_{1 \leqslant i,j \leqslant r}$. Il suffit de vérifier les formules pour B^r et $v \in \mathrm{End}_B(B^r)$. On peut plonger B dans un corps C algébriquement clos, et il suffit de vérifier les formules pour C^r et $w = \mathrm{Id}_C \otimes_B v$. Soient $a_1, \ldots, a_r$ les valeurs propres de w, de sorte que $\overline{\chi}_{C^r}(w^n) = \prod_i (1 + a_i T)$. On a $\psi_n^C(\overline{\chi}_{C^r}(w)) = \prod_{i=1}^r (1 + a_i^n T) = \overline{\chi}_{C^r}(w^n)$. De plus $\chi_{\Lambda^n(C^r)}(\Lambda^n(w)) = \prod_H (1 + a_H T)$, où H parcourt l'ensemble des parties à n éléments de $\{1, \ldots, r\}$, et où $a_H = \prod_{h \in H} a_h$. On peut maintenant appliquer l'exerc. 46, *d*), p. 59, pour montrer que $\lambda_n^C(\overline{\chi}_{C^r}(w)) = \overline{\chi}_{\Lambda^n(C^r)}(\Lambda^n(w))$.)
f) On a

$$-T\left[\frac{d}{dT}\overline{\chi}_E(u)\right] \Big/ \overline{\chi}_E(u) = \sum_{n \in \mathbf{J}} \mathrm{Tr}(u^n)(-T)^n,$$

autrement dit $L_n(\overline{\chi}_E(u)) = \mathrm{Tr}(u^n)$ pour $n \in \mathbf{J}$. (Raisonner comme dans *e*).)
g) Soient E' un A-module projectif de type fini, et $u' \in \mathrm{End}_A(E')$. On a, dans l'anneau $\Lambda(A)$,

$$\overline{\chi}_{E \otimes_A E'}(u \otimes_A u') = \overline{\chi}_E(u) * \overline{\chi}_{E'}(u').$$

(Raisonner comme dans *e*).)
h) Soient k un corps algébriquement clos de caractéristique p non nulle, E un espace vectoriel sur k de dimension finie n, u un endomorphisme de E. On notera $\tilde{\chi}_E(u)$ l'image de $\overline{\chi}_E(u)$ dans $W(k)$ par les homomorphismes canoniques (exerc. 43, p. 57 et exerc. 39, p. 53) :

$$\Lambda(k) \xrightarrow{E^{-1}} U(k) \longrightarrow U_{p^\infty}(k) \longrightarrow W(k).$$

Prouver que si $\alpha_1, \ldots, \alpha_n$ sont les valeurs propres de l'endomorphisme u, on a

$$\tilde{\chi}_E(u) = \sum_{i=1}^n \tau(\alpha_i) \quad \text{dans} \quad W(k).$$

50) Soit A un pré-λ-anneau. Par λ-*idéal* de A on entend un idéal $\mathfrak{a}$ de A tel que $\lambda_n(\mathfrak{a}) \subset \mathfrak{a}$ pour tout $n \in \mathbf{J}$.
a) Soit $\mathfrak{a}$ un λ-idéal de A. Montrer qu'il existe une unique structure $\lambda : A/\mathfrak{a} \to \Lambda(A/\mathfrak{a})$ de pré-λ-anneau sur $A/\mathfrak{a}$ telle que la projection canonique $A \to A/\mathfrak{a}$ soit un λ-morphisme.
b) Les λ-idéaux de A sont précisément les noyaux des λ-morphismes de A dans d'autres pré-λ-anneaux.
c) Soit $(\mathfrak{a}_i)_{i \in I}$ une famille de λ-idéaux de A. Alors $\bigcap_i \mathfrak{a}_i$ et $\sum_i \mathfrak{a}_i$ sont des λ-idéaux de A.
d) Soit A un λ-anneau. Si $\mathfrak{a}$ et $\mathfrak{a}'$ sont des λ-idéaux de A, alors $\mathfrak{a}\mathfrak{a}'$ est un λ-idéal.
e) Soit A un λ-anneau et soit $a \in A$. L'idéal $\mathfrak{a}$ de A engendré par $a, \lambda_2(a), \lambda_3(a), \ldots$ est un λ-idéal.

51) Soit A un λ-anneau et soit $(X_i)_{i\in I}$ une famille d'indéterminées. Introduisons la famille d'indéterminées $(\lambda_n X_i)_{(n,i)\in \mathbf{J}\times I}$ telle que $\lambda_1 X_i = X_i$ quel que soit $i \in I$. Considérons l'algèbre de polynômes $B = A[(\lambda_n X_i)_{(n,i)\in \mathbf{J}\times I}]$.

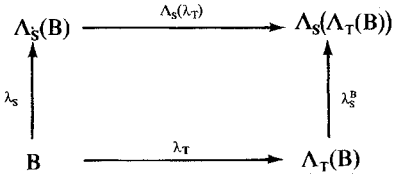
L'homomorphisme d'anneaux $\lambda : A \to \Lambda(A) \subset \Lambda(B)$ se prolonge de façon unique en un homomorphisme d'anneaux $\lambda : B \to \Lambda(B)$ tel que

$$\lambda(X_i) = 1 + \sum_{n\in\mathbf{J}} (\lambda_n X_i)\, T^n$$

et, pour $q \geqslant 2$,

$$\lambda(\lambda_q X_i) = \lambda_q^B(\lambda(X_i)).$$

a) Montrer que (B, λ) est un λ-anneau. (Il s'agit de montrer que le diagramme d'*homomorphismes d'anneaux*



est commutatif. Il suffit de le vérifier sur un système générateur de l'anneau B.)
b) Soient C un λ-anneau, $\rho : A \to C$ un λ-morphisme, et $(c_i)_{i\in I}$ une famille d'éléments de C. Il existe un et un seul λ-morphisme $\rho' : B \to C$ prolongeant ρ et tel que $\rho'(X_i) = c_i$ pour tout $i \in I$.

52) Soient $(A_i)_{i\in I}$ une famille d'anneaux, $A = \prod_i A_i$, et $p_i : A \to A_i$ la projection canonique pour tout $i \in I$.
a) L'application $\alpha : A[[T]] \to \prod_i A_i[[T]]$, qui applique $\sum a_n T^n$ sur $(\sum_n p_i(a_n)\, T^n)_{i\in I}$ est un isomorphisme d'anneaux. Elle définit, par restriction, un isomorphisme d'anneaux $\alpha : \Lambda(A) \to \prod_i \Lambda(A_i)$. De plus on a, pour tout $n \in \mathbf{J}$, $\alpha \circ \lambda_n^A = (\prod_i \lambda_n^{A_i}) \circ \alpha$. (Utiliser les « polynômes universels » de l'exerc. 46, *d*), p. 59.)
b) Supposons que, pour tout $i \in I$, A_i soit muni d'une structure $\lambda_i : A_i \to \Lambda(A_i)$ de pré-λ-anneau. En identifiant $\Lambda(A)$ à $\prod_i \Lambda(A_i)$ au moyen de α, on définit $\lambda = \prod_i \lambda_i : A \to \Lambda(A)$. Alors (A, λ) est un pré-λ-anneau, appelé produit de la famille $((A_i, \lambda_i))_{i\in I}$. Pour que (A, λ) soit un λ-anneau, il faut et il suffit que (A_i, λ_i) en soit un pour tout $i \in I$.

53) Soit $u = 1 + T + \sum_{n=2}^{\infty} a_n T^n$ un élément de $\Lambda(\mathbf{Z})$. Il existe un et un seul homomorphisme de groupes $\lambda^u : \mathbf{Z} \to \Lambda(\mathbf{Z})$ tel que $\lambda^u(1) = u$, et $(\mathbf{Z}, \lambda^u)$ est un pré-λ-anneau. On a $\lambda^u(n) = u^n$ quel que soit $n \in \mathbf{Z}$. Pour que $(\mathbf{Z}, \lambda^u)$ soit un λ-anneau, il faut et il suffit que $u = 1 + T$, auquel cas on a

$$\lambda_m^{1+T}(n) = \binom{n}{m} = \frac{n(n-1)\ldots(n-m+1)}{m!}$$

quels que soient $n \in \mathbf{Z}$ et $m \in \mathbf{N}$.

54) Soient C un anneau et A une C-algèbre (non nécessairement commutative). On note $\mathrm{Rep}_C(A)$ l'ensemble additif des classes des A-modules qui sont des C-modules projectifs de type fini, et on note $R_C(A)$ le groupe de Grothendieck $K(\mathrm{Rep}_C(A))$ (*cf.* A, VIII, § 10, n° 6).
a) Soit $\alpha : A' \to A$ un homomorphisme de C-algèbres. Si E est un A-module de type $\mathrm{Rep}_C(A)$, alors le module $\alpha_* E$ obtenu par restriction à A' de l'anneau des scalaires A (A, II, p. 30) est un A'-module de type $\mathrm{Rep}_C(A')$, et $[E] \mapsto [\alpha_* E]$ définit un homomorphisme $\alpha_* : R_C(A) \to R_C(A')$.

Si $\alpha_1 : A_1 \to A'$ est un homomorphisme de C-algèbres, on a $(\alpha \circ \alpha_1)_* = \alpha_{1*} \circ \alpha_*$.
b) On pose $K_0(C) = R_C(C)$. L'homomorphisme structural $\varepsilon : C \to A$ définit un homomorphisme $\varepsilon_* : R_C(A) \to K_0(C)$. S'il existe un homomorphisme $\gamma : A \to C$ de C-algèbres, alors $\gamma_* : K_0(C) \to R_C(A)$ est un inverse à droite de ε_*.
c) Soit $\gamma : C \to C'$ un homomorphisme d'anneaux. Si E est un A-module de type $\mathrm{Rep}_C(A)$, alors $\gamma^*E = C' \otimes_C E$ est un $A_{C'}$-module de type $\mathrm{Rep}_{C'}(A_{C'})$, où $A_{C'} = C' \otimes_C A$, et $[E] \mapsto [\gamma^*E]$ définit un homomorphisme $\gamma^* : R_C(A) \to R_{C'}(A_{C'})$. Si $\gamma'_1 : C' \to C_1$ est un autre homomorphisme d'anneaux, on a $(\gamma_1 \circ \gamma)^* = \gamma_1^* \circ \gamma^*$.
d) Soient $E \xrightarrow{f} F \xrightarrow{g} G$ des homomorphismes de A-modules, et posons $h = g \circ f$. Construire une suite exacte de A-modules

$$(*) \quad 0 \to \mathrm{Ker}(f) \to \mathrm{Ker}(h) \to \mathrm{Ker}(g) \to \mathrm{Coker}(f) \to \mathrm{Coker}(h) \to \mathrm{Coker}(g) \to 0 .$$

Déduire de là que si f et g sont injectifs, et si $\mathrm{Coker}(f)$ et $\mathrm{Coker}(g)$ sont de type $\mathrm{Rep}_C(A)$, alors $\mathrm{Coker}(h)$ est de type $\mathrm{Rep}_C(A)$, et on a

$$[\mathrm{Coker}(h)] = [\mathrm{Coker}(f)] + [\mathrm{Coker}(g)]$$

dans $R_C(A)$.

55) Soit C un anneau. Soit G un monoïde et soit $C^{(G)}$ son algèbre sur C. Au lieu de $\mathrm{Rep}_C(C^{(G)})$ et $R_C(C^{(G)})$, on écrira $\mathrm{Rep}_C(G)$ et $R_C(G)$. Si $\alpha : G' \to G$ est un homomorphisme de monoïdes, on notera aussi α l'homomorphisme de C-algèbres $C^{(G')} \to C^{(G)}$ qu'il définit, et $\alpha_* : R_C(G) \to R_C(G')$ l'homomorphisme correspondant.
D'après A, VIII, § 10, n° 5, il existe sur $R_C(G)$ une structure d'anneau (commutatif) telle que

$$[E].[F] = [E \otimes_C F]$$

si E et F sont des modules de type $\mathrm{Rep}_C(G)$. L'élément neutre pour cette multiplication est la classe du module C_1, égal à C avec opération triviale de G.
a) L'anneau $R_C(G)$ admet une unique structure de pré-λ-anneau telle que

$$\lambda[E] = \sum_{n \geqslant 0} [\mathbf{\Lambda}^n(E)]\, T^n$$

pour tout module E de type $\mathrm{Rep}_C(G)$. (Observer tout d'abord que $\mathbf{\Lambda}^n(E)$ est encore un module de type $\mathrm{Rep}_C(G)$. Ensuite, si F est un sous-module tel que F et E/F sont de type $\mathrm{Rep}_C(G)$, montrer que

$$[\mathbf{\Lambda}^n(E)] = \sum_{p=0}^{n} [\mathbf{\Lambda}^p(F) \otimes_C \mathbf{\Lambda}^{n-p}(E/F)] .$$

dans $R_C(G)$. Pour cela notons L_p l'image de $\mathbf{\Lambda}^p(F) \otimes_C \mathbf{\Lambda}^{n-p}(E)$, par la multiplication, dans $\mathbf{\Lambda}^n(E)$. On a $\mathbf{\Lambda}^n(E) = L_0 \supset L_1 \supset \ldots \supset L_n = \mathbf{\Lambda}^n(F) \supset L_{n+1} = 0$, et il existe un isomorphisme canonique de $C^{(G)}$-modules de L_p/L_{p+1} sur $\mathbf{\Lambda}^p(F) \otimes \mathbf{\Lambda}^{n-p}(E/F)$.)
b) Pour tout homomorphisme $\alpha : G' \to G$ de monoïdes, l'application $\alpha_* : R_C(G) \to R_C(G')$ est un λ-morphisme. En particulier $K_0(C)$ est un pré-λ-anneau et $\varepsilon_* : R_C(G) \to K_0(C)$ est un λ-morphisme. L'homomorphisme $G \to \{1\}$ en fournit un inverse à droite.
c) Soient G un monoïde et R un ensemble. Une fonction $f : G \to R$ sera dite *centrale* si $f(st) = f(ts)$ quels que soient $s, t \in G$. Notons FC(G, R) l'ensemble de ces fonctions. Si R est un λ-anneau, FC(G, R) est canoniquement muni d'une structure de λ-anneau telle que

$$(f + f')(s) = f(s) + f'(s)$$
$$(f.f')(s) = f(s).f'(s)$$
$$(\lambda_n f)(s) = \lambda_n(f(s))$$

quels que soient f, f' dans FC(G, R) et s dans G. Ceci s'applique notamment lorsque $R = \Lambda(C)$.

d) Soit E un module de type $\mathrm{Rep}_C(G)$. Pour tout $s \in G$, notons s_E l'homothétie de rapport s dans E, et posons

$$\overline{\chi}_E(s) = \det_{E[T]}(1 + s_E T) \in \Lambda(C)$$

(*cf.* p. 62, exerc. 49). Montrer que

$$\overline{\chi} : [E] \mapsto \overline{\chi}_E$$

définit un λ-morphisme

$$\overline{\chi} : R_C(G) \to FC(G, \Lambda(C)) .$$

e) Si C est un corps, alors $\overline{\chi}$ est injectif (A, VIII, § 10, n° 6, prop. 10). En déduire dans ce cas que $R_C(G)$ est un λ-anneau.

56) Soit G le monoïde libre engendré par un élément T, de sorte que $C^{(G)}$ s'identifie à C[T]. Notons C_0 le module C[T]/TC[T]. Alors $[C_0]$ est un élément idempotent de $R_C(C[T])$. Le noyau du λ-morphisme canonique $R_C(C[T]) \to K_0(C)$ est l'idéal engendré par $1 - [C_0]$. Posons

$$\tilde{R}_C(C[T]) = R_C(C[T])/[C_0].R_C(C[T]) .$$

a) Montrer que $[C_0].R_C(C[T])$ est un λ-idéal, donc que $\tilde{R}_C(C[T])$ admet une structure quotient de pré-λ-anneau.
b) Pour tout module E de type $\mathrm{Rep}_C(C[T])$, notons T_E l'homothétie de rapport T dans E. On a

$$\overline{\chi}_E(T) = \det_{E[T]}(1 + T_E T) \in \Lambda(C)$$

et

$$\chi_E(T) = \det_{E[T]}(T - T_E)$$

est le polynôme caractéristique de T_E (*cf.* exerc. 49, p. 62). Montrer que $[E] \mapsto \overline{\chi}_E(T)$ définit un λ-morphisme $R_C(C[T]) \to \Lambda(C)$ dont le noyau contient $[C_0]$. Par passage au quotient, on obtient un λ-morphisme

$$\overline{\chi} : \tilde{R}_C(C[T]) \to \Lambda(C) .$$

c) Notons $\Lambda_{rat}(C)$ le sous-groupe de $\Lambda(C)$ engendré par les éléments de $\Lambda(C)$ qui sont des polynômes en T. Montrer que l'image de $\overline{\chi}$ est $\Lambda_{rat}(C)$. En conclure que $\Lambda_{rat}(C)$ est un sous-λ-anneau de $\Lambda(C)$.
d) Pour tout $r \in \mathbf{Z}$, définissons $\sigma_r : C[T, T^{-1}] \to C[T, T^{-1}]$ par $(\sigma_r f)(T) = T^r f((-T)^{-1})$. On a $(\sigma_r(\sigma_s f))(T) = (-1)^s T^{r-s} f(T)$, en particulier $\sigma_r(\sigma_r f) = (-1)^r f$, et $(\sigma_r f).(\sigma_s g) = \sigma_{r+s}(f.g)$, quels que soient r, s dans $\mathbf{Z}$ et f, g dans $C[T, T^{-1}]$. Si f est un polynôme en T de degré $\leqslant r$ ($r \geqslant 0$), alors $\sigma_r f$ en est un aussi. Si de plus $f \in \Lambda(C)$ (i.e. $f(0) = 1$), alors $\sigma_r f$ est unitaire de degré r. Si E est un C[T]-module qui est un C-module libre de rang r, on a $\sigma_r(\overline{\chi}_E(T)) = \chi_E(T)$.
e) Si $f \in \Lambda(C)$ est un polynôme en T de degré $\leqslant r$, posons $E_{r,f} = C[T]/\sigma_r f.C[T]$; c'est un C-module libre de rang r. Si $f = 1$ on a $E_{r,1} = C[T]/T^r C[T]$. Si $g \in \Lambda(C)$ est un polynôme en T de degré $\leqslant s$, on a une suite exacte de C[T]-modules

$$(*) \quad 0 \to E_{s,g} \to E_{r+s,fg} \to E_{r,f} \to 0$$

(utiliser *d*)). Montrer que la classe $\tau(f)$ de $E_{r,f}$ dans $\tilde{R}_C(C[T])$ est indépendante de r ($\geqslant \deg(f)$). (En effet $\sigma_{r+s} f = (\sigma_s 1).(\sigma_r f) = T^s.(\sigma_r f)$, et la classe du module $C[T]/T^s C[T]$ dans $\tilde{R}_C(C[T])$ est nulle.) Montrer que si g est un polynôme dans $\Lambda(C)$, on a $\tau(fg) = \tau(f) + \tau(g)$. (Utiliser encore la suite exacte (*).) Déduire de là que τ s'étend en un homomorphisme de groupes

$$\tau : \Lambda_{rat}(C) \to \tilde{R}_C(C[T]) .$$

f) Montrer que $\overline{\chi} \circ \tau$ est l'application identique de $\Lambda_{rat}(C)$. (Utiliser le fait que si $f \in \Lambda(C)$ est un polynôme de degré $\leqslant r$, alors le polynôme caractéristique de $T_{E_{r,f}}$ est $\sigma_r f$.)
g) Montrer que tout élément de $\tilde{R}_C(C[T])$ est la classe d'un C[T]-module E qui est un C-module libre.

h) Soit E un C[T]-module, et notons $u \in \mathrm{End}_C(E)$ l'homothétie de rapport T dans E ; soit $\overline{u} = \mathrm{Id}_{C[T]} \otimes_C u \in \mathrm{End}_{C[T]}(E[T])$. On a une suite exacte de C[T]-modules

$$0 \longrightarrow E[T] \xrightarrow{T-\overline{u}} E[T] \longrightarrow E \longrightarrow 0$$

(A, III, p. 106). Supposons que E soit un C-module libre de base $(e_1, ..., e_r)$. Alors E[T] est un C[T]-module libre de base $(1 \otimes e_i)$. Si la matrice de u pour la base (e_i) est (a_{ij}), la matrice de $T - \overline{u}$ pour la base $(1 \otimes e_i)$ est $(T\delta_{ij} - a_{ij})$.
i) Soit $f = (f_{ij})_{1 \leqslant i,j \leqslant r}$ une matrice à coefficients dans C[T]. On dira que f est *spéciale* si, quels que soient i, j dans $\{1, ..., r\}$, $i \neq j$, f_{ii} est un polynôme unitaire et $\deg(f_{ii}) > \deg(f_{ij})$. Montrer alors que $\det(f)$ est un polynôme unitaire (de degré $\deg(f_{11}) + \cdots + \deg(f_{rr})$) et que f définit un endomorphisme injectif de $C[T]^r$. Déduire de *h*) que tout C[T]-module qui est un C-module libre de rang r est isomorphe au conoyau d'un tel endomorphisme de $C[T]^r$.

j) Soit f une matrice spéciale comme dans *i*). Posons $f = \begin{pmatrix} f_{11} & f_+ \\ f_- & f' \end{pmatrix}$ où f_+, f_-, f' sont des matrices de types $(1, r-1)$, $(r-1, 1)$ et $(r-1, r-1)$ respectivement. Posons

$$g = \begin{pmatrix} 1 & 0 \\ -f_- & f_{11}\mathrm{I} \end{pmatrix} \quad \text{et} \quad h = gf = \begin{pmatrix} f_{11} & f_+ \\ 0 & \overline{f} \end{pmatrix} \quad \text{où} \quad \overline{f} = f_{11}f' - f_-f_+ .$$

Montrer que h est une matrice spéciale. De plus, en identifiant les matrices carrées aux endomorphismes correspondants, on obtient des suites exactes de C[T]-modules

$$0 \to \mathrm{Coker}(f) \to \mathrm{Coker}(h) \to \mathrm{Coker}(g) \to 0 ,$$

(où $\mathrm{Coker}(g)$ est isomorphe à $C[T]^{r-1}/f_{11}C[T]^{r-1}$) et

$$0 \to C[T]/f_{11}C[T] \to \mathrm{Coker}(h) \to \mathrm{Coker}(\overline{f}) \to 0 .$$

Déduire de là, par récurrence sur r, que $\mathrm{Coker}(f)$ est un C-module projectif dont la classe dans $R_C(C[T])$ est combinaison **Z**-linéaire d'éléments de la forme $[C[T]/pC[T]]$ où p est un polynôme unitaire.
k) Utiliser les parties *f*), *g*), *i*) et *j*) précédentes pour montrer que $\tau : \Lambda_{\mathrm{rat}}(C) \to \tilde{R}_C(C[T])$ est surjectif, donc que $\overline{\chi} : \tilde{R}_C(C[T]) \to \Lambda_{\mathrm{rat}}(C)$ est un isomorphisme.
l) Montrer que $\Lambda_{\mathrm{rat}}(C)$ est stable par V_n et F_n pour chaque $n \in \mathbf{J}$. Il leur correspond donc des endomorphismes V_n et F_n de $\tilde{R}_C(C[T])$, par l'isomorphisme précédent. Soit φ_n l'homomorphisme de C-algèbres de C[T] dans lui-même qui applique T sur T^n. Montrer que V_n (resp. F_n) se déduit de l'endomorphisme φ_n^* (resp. $(\varphi_n)_*$) de $R_C(C[T])$ par passage aux quotients.

Dans les exercices ci-après, p est un nombre premier fixé, et les anneaux de vecteurs de Witt sont relatifs à ce nombre premier.

57) Soient m, n deux entiers $\geqslant 1$. Pour tout anneau A de caractéristique p, notons ${}_mW_n(A)$ le noyau de l'endomorphisme F^m de $W_n(A)$.
a) Pour $m \geqslant 2$ et $n \geqslant 1$, le diagramme suivant est commutatif

$$\begin{array}{ccc} {}_mW_n(A) & \xrightarrow{V} & {}_mW_{n+1}(A) \\ \downarrow{\scriptstyle pI} & & \downarrow{\scriptstyle F} \\ {}_{m-1}W_n(A) & \xleftarrow{R} & {}_{m-1}W_{n+1}(A) \end{array}$$

où les applications V, F sont induites par les homomorphismes de décalage et de Frobenius respectivement, I est l'injection naturelle et R la projection naturelle.
b) Pour $n \geqslant 1$ et $\boldsymbol{a} = [a_0, ..., a_{n-1}]$ dans $W_n(A)$, on note $\tilde{\boldsymbol{a}}$ l'élément $(a_0, ..., a_{n-1}, 0, ...)$ de W(A).

Soient $\boldsymbol{a} \in {}_m\mathrm{W}_n(\mathrm{A})$, $\boldsymbol{b} \in {}_n\mathrm{W}_m(\mathrm{A})$. On pose alors

$$\langle \boldsymbol{a}, \boldsymbol{b} \rangle = \mathrm{E}(\omega_\mathrm{A}(\tilde{\boldsymbol{a}})\, \omega_\mathrm{A}(\tilde{\boldsymbol{b}}), 1)$$

(*cf.* p. 57, exerc. 43 pour la notation E, et p. 54, exerc. 40 pour la notation ω_A). Prouver que l'application $(\boldsymbol{a}, \boldsymbol{b}) \mapsto \langle \boldsymbol{a}, \boldsymbol{b} \rangle$ de ${}_m\mathrm{W}_n(\mathrm{A}) \times {}_n\mathrm{W}_m(\mathrm{A})$ dans A* est Z-bilinéaire.

c) Avec les notations de *a*), on a

$$\langle \boldsymbol{a}, \mathrm{V}\boldsymbol{b} \rangle = \langle \mathrm{F}\boldsymbol{a}, \boldsymbol{b} \rangle \quad \text{pour} \quad \boldsymbol{a} \in {}_m\mathrm{W}_n(\mathrm{A}) \quad \text{et} \quad \boldsymbol{b} \in {}_n\mathrm{W}_{m-1}(\mathrm{A})$$

et

$$\langle \mathrm{R}\boldsymbol{a}, \boldsymbol{b} \rangle = \langle \boldsymbol{a}, \mathrm{I}\boldsymbol{b} \rangle \quad \text{pour} \quad \boldsymbol{a} \in {}_m\mathrm{W}_n(\mathrm{A}) \quad \text{et} \quad \boldsymbol{b} \in {}_{n-1}\mathrm{W}_m(\mathrm{A}).$$

58) *a*) Soit $\mathfrak{E}(\mathrm{T})$ la série formelle $\exp(-\sum_{n=0}^{\infty} \mathrm{T}^{p^n}/p^n)$ de $\mathbf{Q}[[\mathrm{T}]]$. On a

$$\mathfrak{E}(\mathrm{T}) = \prod_{\substack{(n,p)=1 \\ n \text{ entier} \geqslant 1}} (1 - \mathrm{T}^n)^{\mu(n)/n}$$

où μ est la fonction de Möbius. Les coefficients de $\mathfrak{E}(\mathrm{T})$ appartiennent à $\mathbf{Z}_{(p)}$.

b) Soit $\mathrm{X} = (\mathrm{X}_n)_{n\in\mathbf{N}}$ une famille d'indéterminées. Dans l'algèbre $\mathbf{Q}[(\mathrm{X}_n)_{n\in\mathbf{N}}]$, on a l'égalité

$$\prod_{n=0}^{\infty} \mathfrak{E}(\mathrm{X}_n \mathrm{T}^{p^n}) = \exp(-\sum_{n=0}^{\infty} \Phi_n(\mathbf{X})\, \mathrm{T}^{p^n}/p^n).$$

c) Soit A une $\mathbf{Z}_{(p)}$-algèbre. On suppose que la multiplication par $p.1_\mathrm{A}$ est injective dans A. Soit $\boldsymbol{a} = (a_n)_{n\in\mathbf{N}} \in \mathrm{A}^\mathbf{N}$. Pour que la série $\exp(\sum_{n=0}^{\infty} a_n \mathrm{T}^{p^n}/p^n)$ de $\mathrm{A}\left[\frac{1}{p}\right][[\mathrm{T}]]$ ait ses coefficients dans A, il faut et il suffit que $\boldsymbol{a}$ appartienne à $\Phi_\mathrm{A}(\mathrm{W}(\mathrm{A}))$.

d) Soit A une $\mathbf{Z}_{(p)}$-algèbre. L'application $\mathrm{E} \circ \omega_\mathrm{A}$ de W(A) dans $\Lambda(\mathrm{A})$ (*cf.* p. 54, exerc. 40 et p. 57, exerc. 43) associe à $\boldsymbol{a} = (a_n)_{n\in\mathbf{N}}$ l'élément $\prod_{n=0}^{\infty} \mathfrak{E}(a_n(-\mathrm{T})^{p^n})$ de $\Lambda(\mathrm{A})$.

e) Soit A une $\mathbf{Z}_{(p)}$-algèbre. Supposons que la multiplication par $p.1_\mathrm{A}$ soit injective dans A. Soit σ un endomorphisme de A vérifiant $\sigma a \equiv a^p$ mod. pA. Soit $s_\sigma : \mathrm{A} \to \mathrm{W}(\mathrm{A})$ l'homomorphisme associé à σ (p. 44, exerc. 14). Alors, pour tout $a \in \mathrm{A}$, la série formelle

$$\mathrm{E}_\sigma(a, \mathrm{T}) = \exp(\sum_{i=0}^{\infty} \sigma^i(a)\, \mathrm{T}^{p^i}/p^i)$$

a ses coefficients dans A, et on a

$$\mathrm{E} \circ \omega_\mathrm{A} \circ s_\sigma(a^{-1}) = \exp(\sum_{i=0}^{\infty} \sigma^i(a)\,(-\mathrm{T})^{p^i}/p^i) = \mathrm{E}_\sigma(a, -\mathrm{T}).$$

f) Soit $\mathcal{A}$ l'anneau $\mathbf{Z}_{(p)}[(\mathrm{X}_n)_{n\in\mathbf{N}}]$ et soit $\mathbf{X} = (\mathrm{X}_n)_{n\in\mathbf{N}} \in \mathrm{W}(\mathcal{A})$. La série $\mathrm{E}_{\mathrm{F}_\mathcal{A}}(\mathbf{X}, \mathrm{T})$ a ses coefficients dans $\mathrm{W}(\mathcal{A})$. Pour toute $\mathbf{Z}_{(p)}$-algèbre A et tout élément $\boldsymbol{a} = (a_n)_{n\in\mathbf{N}}$ de W(A), on notera $\mathrm{E}_\mathrm{F}(\boldsymbol{a}, \mathrm{T})$ la série obtenue en appliquant $\mathrm{W}(\varphi)$ aux coefficients de $\mathrm{E}_{\mathrm{F}_\mathcal{A}}(\mathbf{X}, \mathrm{T})$ où $\varphi : \mathcal{A} \to \mathrm{A}$ est l'application qui à X_n associe a_n. Alors $\mathrm{E}_\mathrm{F}(\boldsymbol{a}, \mathrm{T})$ a ses coefficients dans W(A) et si s_A désigne l'homomorphisme $\mathrm{W}(\mathrm{A}) \to \mathrm{W}(\mathrm{W}(\mathrm{A}))$ défini à l'exerc. 15, p. 44, on a

$$\mathrm{E} \circ \omega_{\mathrm{W}(\mathrm{A})} \circ s_\mathrm{A}(\boldsymbol{a}^{-1}) = \mathrm{E}_\mathrm{F}(\boldsymbol{a}, -\mathrm{T}) \quad \text{pour tout} \quad \boldsymbol{a} \in \mathrm{W}(\mathrm{A}).$$

§ 2

Dans les exercices du § 2, p est un nombre premier fixé. Si $\mathfrak{a}$ est un idéal d'un anneau A, on note $\mathfrak{a}^p$ l'idéal engendré par les éléments a^p, où a parcourt $\mathfrak{a}$.

1) Soit $(\mathrm{C}_n, \pi_{n,m})$ un système projectif d'anneaux relatif à l'ensemble d'indices N. On suppose que C_n est artinien pour tout $n \in \mathbf{N}$ et que les homomorphismes $\pi_{n,m}$ sont surjectifs. Soit π_n l'homomorphisme canonique de $\mathrm{C} = \varprojlim \mathrm{C}_n$ dans C_n. Montrer que pour tout $x \in \mathrm{C}$, on a $x\mathrm{C} = \varprojlim \pi_n(x)\,\mathrm{C}_n$. (Raisonner comme dans la démonstration de la prop. 3 du § 2, n° 1.)

2) Soient A un anneau et $(J_n)_{n\in\mathbf{N}}$ une suite décroissante d'idéaux de A, telle que $pJ_n + J_n^p \subset J_{n+1}$ pour tout $n \in \mathbf{N}$.
a) Prouver que les assertions du lemme 1 et de la prop. 1 du § 1, n° 1 sont encore vraies sous cette hypothèse.
b) Soient i et n deux entiers positifs. Lorsque $i \leqslant n$ l'application $x \mapsto p^i x^{p^{n-i}}$ de A dans A définit, par passage aux quotients, une application

$$\rho_{n,i}^{A} : A/J_0 \to A/J_n .$$

Pour $i > n$, on pose $\rho_{n,i}^{A} = 0$. Pour $x \in A/J_n$ et $a \in A/J_0$, on a $x^{p^{n-i}}\rho_{n,i}^{A}(a) = \rho_{n,i}^{A}(\overline{x}a)$, où $\overline{x}$ est l'image de x dans A/J_0. Si j est un entier positif et que a, b sont deux éléments de A/J_n, on a

$$\rho_{n,i}^{A}(a)\,\rho_{n,j}^{A}(b) = \rho_{n,i+j}^{A}(a^{p^j}b^{p^i}) .$$

c) Soit $(R_n)_{n\in\mathbf{N}}$ la suite de polynômes construite dans l'exerc. 3, p. 42. Soient n et i deux entiers positifs, a et b deux éléments de A/J_0. On a alors, dans A/J_n, l'égalité

$$\rho_{n,i}^{A}(a) + \rho_{n,i}^{A}(b) = \sum_{m=0}^{n-i} \rho_{n,i+m}^{A}(R_m(a, b)) .$$

3) Soit n un entier positif. Soit C un p-anneau de Cohen, de corps résiduel k, et de longueur $n + 1$. Soit $(x_\lambda)_{\lambda\in\Lambda}$ une famille d'éléments de C relevant une p-base $(\xi_\lambda)_{\lambda\in\Lambda}$ de k. On notera $\rho_i : k \to C$ pour tout $i \in \mathbf{N}$, l'application $\rho_{n,i}^{C}$ définie à l'exerc. 2, où l'on prend pour J_m l'idéal $p^{m+1}C$.
a) Pour $r \in \mathbf{N}$, soit M_r l'ensemble des multi-indices $\boldsymbol{m} \in \mathbf{N}^{(\Lambda)}$ tels que, pour tout $\lambda \in \Lambda$, on ait $0 \leqslant m_\lambda < p^r$. Alors, pour tout élément α de C, il existe une unique famille à support fini $(a_{i,\boldsymbol{m}})$ $(0 \leqslant i \leqslant n,\ \boldsymbol{m} \in M_{n-i})$ d'éléments de k, telle que

$$\alpha = \sum_{i=0}^{n} \sum_{\boldsymbol{m}\in M_{n-i}} \rho_i(a_{i,\boldsymbol{m}})\, \boldsymbol{x}^{\boldsymbol{m}} ,$$

où la notation $\boldsymbol{x}^{\boldsymbol{m}}$ désigne le produit $\prod_{\lambda\in\Lambda} x_\lambda^{m_\lambda}$.
b) Considérons l'anneau U engendré par des générateurs $[x_\lambda]$, λ parcourant Λ, et $[\rho_i(a)]$, i parcourant $\mathbf{N}$ et a parcourant k, et soumis aux seules relations suivantes (où les polynômes R_i sont ceux introduits dans l'exerc. 3, p. 42).
(i) $[\rho_i(a)] = 0$ pour $a \in k$, $i > n$,
(ii) $[\rho_0(1)] = 1$ et $[\rho_0(0)] = 0$,
(iii) $[\rho_i(a)]\,[\rho_j(b)] = [\rho_{i+j}(a^{p^j}b^{p^i})]$ pour i, j dans $\mathbf{N}$ et a, b dans k,
(iv) $[\rho_i(a)] + [\rho_i(b)] = \sum_{m=0}^{n-i} [\rho_{i+m}(R_m(a, b))]$ pour $i \in \mathbf{N}$ et a, b dans k,
(v) $[x_\lambda]^{p^{n-i}}[\rho_i(a)] = [\rho_i(\xi_\lambda a)]$ pour $0 \leqslant i \leqslant n$, $\lambda \in \Lambda$, $a \in k$.
Prouver qu'on a $[\rho_i(0)] = 0$ pour tout $i \in \mathbf{N}$.
Prouver, grâce à l'exerc. 3, *b*), p. 42, que si p est impair, on a $[\rho_0(-1)] = -1$; si p est pair, on a $\sum_{i=0}^{n} [\rho_i(1)] = -1$.

c) Il existe une seule application de U dans C, qui, pour toute famille à support fini $(a_{i,\boldsymbol{m}})_{0\leqslant i\leqslant n,\, \boldsymbol{m}\in M_{n-i}}$ d'éléments de k, associe à l'élément

$$\langle (a_{i,\boldsymbol{m}}) \rangle = \sum_{i=0}^{n} \sum_{\boldsymbol{m}\in M_{n-i}} [\rho_i(a_{i,\boldsymbol{m}})] \prod_{\lambda\in\Lambda} [x_\lambda]^{m_\lambda}$$

de U l'élément $\sum_{i=0}^{n} \sum_{\boldsymbol{m}\in M_{n-i}} \rho_i(a_{i,\boldsymbol{m}})\, \boldsymbol{x}^{\boldsymbol{m}}$ de C ; c'est un isomorphisme d'anneaux.
d) Déduire de ce qui précède une autre démonstration des résultats du § 2, n° 3.

4) Soient C un p-anneau de Cohen de longueur infinie, et k son corps résiduel. Soient A un anneau, et $(J_n)_{n\in\mathbf{N}}$ une suite décroissante d'idéaux de A vérifiant $pJ_n + J_n^p \subset J_{n+1}$ pour tout $n \in \mathbf{N}$. Soient enfin $\overline{\varphi} : k \to A/J_0$ un homomorphisme d'anneaux, $(\xi_\lambda)_{\lambda\in\Lambda}$ une p-base de k, $(x_\lambda)_{\lambda\in\Lambda}$ une famille d'éléments de C, relevant cette p-base, $(a_\lambda)_{\lambda\in\Lambda}$ une famille d'éléments de A, telle que l'image de a_λ dans A/J_0 soit $\overline{\varphi}(\xi_\lambda)$.
a) Pour tout $n \in \mathbf{N}$, il existe un unique homomorphisme φ_n de $C/p^{n+1}C$ dans A/J_n tel que $\varphi_n \circ \rho^C_{n,i} = \rho^A_{n,i} \circ \overline{\varphi}$ et que l'image par φ_n de la classe de x_λ soit la classe de a_λ. (Utiliser les exerc. 2 et 3.)
b) Supposons que A soit séparé et complet pour la topologie définie par la filtration $(J_n)_{n\in\mathbf{N}}$. Alors il existe un unique homomorphisme d'anneaux φ de C dans A, tel que $\varphi(x_\lambda) = a_\lambda$ pour $\lambda \in \Lambda$, et que φ induise $\overline{\varphi}$ par passage aux quotients. Cet homomorphisme est continu.
c) Supposons que l'anneau A soit local, séparé et complet, qu'on ait $J_n = \mathfrak{m}_A^{n+1}$ pour tout $n \in \mathbf{N}$, qu'on ait $A/J_0 = k$ et que $\overline{\varphi}$ soit l'application identique. Prouver que l'image par φ de C dans A est l'unique sous-anneau de Cohen de A contenant chacun des éléments a_λ, et donner ainsi une autre démonstration de la partie *a*) du th. 1 du § 2, n° 2 ; si k est parfait et que C est l'anneau $W(k)$, on obtient une autre démonstration du th. 2 du § 2, n° 4.

5) Soient A un anneau et $(J_n)_{n\in\mathbf{N}}$ une suite décroissante d'idéaux de A, vérifiant $pJ_n + J_n^p \subset J_{n+1}$ pour tout entier $n \geqslant 0$. Soient R un anneau de caractéristique p et $\overline{\varphi}$ un homomorphisme d'anneaux de R dans A/J_0. On appelle relèvement de $\overline{\varphi}$ à A/J_n une application $\varphi_n : R \to A/J_n$ telle que $\varphi_n(x^p) = \varphi_n(x)^p$ pour $x \in R$, et qui redonne $\overline{\varphi}$ par passage au quotient.
a) Soient φ_n, $\tilde{\varphi}_n$ deux relèvements de $\overline{\varphi}$ à A/J_n. Alors φ_n et $\tilde{\varphi}_n$ coïncident sur R^{p^n}.
b) Si R est parfait, il existe un unique relèvement φ_n de $\overline{\varphi}$ à A/J_n. On a $\varphi_n(1) = 1$ et $\varphi_n(xy) = \varphi_n(x)\,\varphi_n(y)$ pour $x, y \in R$.

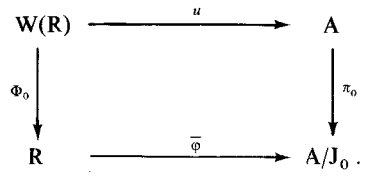
6) Soient A un anneau et $(J_n)_{n\in\mathbf{N}}$ une suite décroissante d'idéaux de A. On suppose que A est séparé et complet pour la topologie définie par la filtration $(J_n)_{n\in\mathbf{N}}$ et qu'on a $pJ_n + J_n^p \subset J_{n+1}$ pour tout entier $n \geqslant 0$. On note π_n l'application canonique de A sur A/J_n. Soient R un anneau parfait de caractéristique p et $\overline{\varphi}$ un homomorphisme d'anneaux de R dans A/J_0.
a) Il existe une application φ de R dans A, et une seule, telle que l'on ait $\overline{\varphi} = \pi_0 \circ \varphi$ et $\varphi(x^p) = \varphi(x)^p$ pour tout $x \in R$. De plus, on a $\varphi(1) = 1$ et $\varphi(xy) = \varphi(x)\,\varphi(y)$ pour x et y dans R. Lorsque A est un anneau de caractéristique p, φ est un homomorphisme d'anneaux. (On pourra utiliser l'exercice précédent.)
b) Pour tout $n \in \mathbf{N}$, il existe un unique homomorphisme d'anneaux $v_n : W_{n+1}(A/J_0) \to A/J_n$ rendant commutatif le diagramme

$$\begin{array}{ccc} W_{n+1}(A) & \xrightarrow{\Phi_n} & A \\ \downarrow{\scriptstyle W_{n+1}(\pi_0)} & & \downarrow{\scriptstyle \pi_n} \\ W_{n+1}(A/J_0) & \xrightarrow{v_n} & A/J_n\,. \end{array}$$

c) Posons $u_n = v_n \circ W_{n+1}(\overline{\varphi}) \circ F^{-n}$. Alors, pour tout $n \in \mathbf{N}$, le diagramme suivant, où les flèches verticales désignent les projections canoniques, est commutatif

$$\begin{array}{ccc} W_{n+2}(R) & \xrightarrow{u_{n+1}} & A/J_{n+1} \\ \downarrow & & \downarrow \\ W_{n+1}(R) & \xrightarrow{u_n} & A/J_n\,. \end{array}$$

d) Il existe un unique homomorphisme d'anneaux u rendant commutatif le diagramme suivant

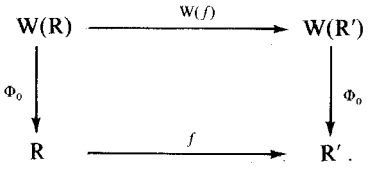


L'homomorphisme u est continu quand on munit W(R) de la topologie p-adique, et pour tout $\boldsymbol{a} = (a_n)_{n\in\mathbf{N}} \in \mathrm{W}(\mathrm{R})$, on a $u(\boldsymbol{a}) = \sum_{n=0}^{\infty} p^n \varphi(a_n^{p^{-n}})$.

(L'existence de u découle de ce qui précède. Pour prouver l'unicité de u, sa continuité et son expression explicite, utiliser l'égalité $\varphi = u \circ \tau$ où φ est l'application de R dans A construite en *a*) et $\tau : \mathrm{R} \to \mathrm{W}(\mathrm{R})$ l'application définie au § 1, n° 5.)

e) Donner du th. 2 du § 2, n° 4, une démonstration autre que celle du texte et que celle de l'exerc. 4, *c*).

7) *a*) Soient R un anneau parfait de caractéristique p, et R′ un anneau de caractéristique p. Soit f un homomorphisme de R dans R′. Alors l'homomorphisme $\mathrm{W}(f) : \mathrm{W}(\mathrm{R}) \to \mathrm{W}(\mathrm{R}')$ est l'unique homomorphisme rendant commutatif le diagramme suivant



(Utiliser l'exercice précédent.)

En particulier, prenant pour f l'élévation à la puissance p-ième dans R, prouver que $\mathrm{F_R}$ est l'unique endomorphisme de W(R) tel que $\Phi_0 \circ \mathrm{F_R} = f \circ \Phi_0$. Il est caractérisé par les égalités

$$\mathrm{F_R}(\tau(x)) = \tau(x^p) \quad \text{pour tout} \quad x \in \mathrm{R}\,.$$

b) Soit A un anneau séparé et complet pour la topologie p-adique. On suppose que la multiplication par $p.1_\mathrm{A}$ dans A est injective et que A/pA est un anneau parfait. Alors il existe un unique endomorphisme σ de A tel que $\sigma(x) \equiv x^p$ mod. pA pour $x \in$ A, et l'inverse de l'isomorphisme $t_\sigma : \mathrm{A} \to \mathrm{W}(\mathrm{A}/p\mathrm{A})$ décrit dans l'exerc. 14, p. 44 est donné par

$$(a_i)_{i\in\mathbf{N}} \mapsto \sum_{i=0}^{\infty} \varphi(a_i)^{p^{-i}} p^i\,,$$

où $\varphi : \mathrm{A}/p\mathrm{A} \to \mathrm{A}$ est l'unique application qui donne l'identité de A/pA par passage au quotient et vérifie $\varphi(x^p) = \varphi(x)^p$ pour $x \in$ R (*cf.* exerc. 6, *a*)).

8) Soit C un p-anneau de longueur infinie, de corps résiduel k. Tout automorphisme de k se prolonge en un automorphisme de C. Pour que tout automorphisme de C induisant par passage aux quotients l'identité sur k soit l'identité, il faut et il suffit que k soit parfait.

9) Soient k un corps de caractéristique p, C_k un p-anneau de longueur infinie, et de corps résiduel k. Soient A un anneau local séparé et complet et $u : \mathrm{C}_k \to \mathrm{A}$ un homomorphisme local tel que l'homomorphisme déduit de u par passage aux quotients fasse du corps résiduel K de A une extension séparable de k. Soit $\mathrm{C_K}$ un p-anneau de longueur infinie, de corps résiduel K. Prouver qu'il existe des homomorphismes locaux $i : \mathrm{C}_k \to \mathrm{C_K}$ et $v : \mathrm{C_K} \to \mathrm{A}$ tels que $u = v \circ i$ et que v induise l'identité sur K par passage aux quotients.

10) Soient k un corps de caractéristique p, $(\xi_\lambda)_{\lambda\in\Lambda}$ une p-base de k, et pour chaque entier $n \geqslant 1$, soit C_n le sous-anneau de $W_n(k)$ engendré par $W_n(k^{p^{n-1}})$ et les éléments $\tau(\xi_\lambda) = [\xi_\lambda, 0, ..., 0]$, pour $\lambda \in \Lambda$. Pour tout entier $n \geqslant 1$, la projection de $W_{n+1}(k)$ sur $W_n(k)$ applique C_{n+1} dans C_n. On note C le sous-anneau de $W(k)$ limite projective des C_n.
a) Soit n un entier $\geqslant 0$. Posons $A = W_{n+1}(k)$ et pour tout entier $i \geqslant 0$ soit $\rho_i = \rho_{n,i}^{A}$ l'application de k dans A définie à l'exerc. 2, p. 69. Prouver qu'on a, pour $a \in k$, $\rho_i(a) = V^i\tau(a^{p^n})$. En déduire que les éléments $\rho_i(a)$ pour $a \in k$, engendrent le sous-anneau $W_{n+1}(k^{p^n})$ de A.
b) Soit $\tilde{C}$ un p-anneau de corps résiduel k et de longueur infinie, et soit $(x_\lambda)_{\lambda\in\Lambda}$ une famille d'éléments de $\tilde{C}$ relevant la p-base $(\xi_\lambda)_{\lambda\in\Lambda}$. Utilisant l'exerc. 4, p. 70, prouver qu'il existe, pour chaque entier $n \geqslant 1$, un unique homomorphisme d'anneaux $\varphi_n : \tilde{C} \to W_n(k)$ induisant l'identité sur k par passage aux quotients, et envoyant x_λ sur $\tau(\xi_\lambda)$ pour tout $\lambda \in \Lambda$. Déduire de l'exerc. 3, p. 69 que l'image de φ_n est C_n.
c) Les applications $(\varphi_n)_{n\geqslant 1}$ forment un système projectif d'applications de $\tilde{C}$ dans les C_n et $\varphi = \varprojlim \varphi_n$ est un isomorphisme de $\tilde{C}$ sur C. Pour chaque $n \geqslant 1$, la projection canonique $C \to C_n$ identifie C_n à C/p^nC.

11) Soient k un corps de caractéristique p, $(\xi_\lambda)_{\lambda\in\Lambda}$ une p-base de k, C le sous-anneau de Cohen de $W(k)$ contenant $\tau(\xi_\lambda)$ pour tout $\lambda \in \Lambda$. Soit $(\varepsilon_j)_{j\in J}$ une base de $k^*/(k^{*p})$ comme $\mathbf{F}_p$-espace vectoriel. Soient n un entier $\geqslant 0$ et $(x_j)_{j\in J}$ une famille d'éléments de k^* telle que l'image de x_j dans k^*/k^{*p} soit ε_j, pour tout $j \in J$.
a) Le groupe k^*/k^{*p^n} est un $(\mathbf{Z}/p^n\mathbf{Z})$-module libre de base $(\overline{x}_j)_{j\in J}$, où $\overline{x}_j$ est la classe de x_j dans k^*/k^{*p^n}.
b) Pour tout $j \in J$, écrivons la décomposition de x_j suivant la base $(\xi^{\boldsymbol{m}})_{\boldsymbol{m}\in M_n}$ de k sur k^{p^n} (avec les notations de l'exerc. 3, p. 69) :

$$x_j = \sum_{\boldsymbol{m}\in M_n} a_{j,\boldsymbol{m}}^{p^n} \xi^{\boldsymbol{m}}, \quad a_{j,\boldsymbol{m}} \in k .$$

Posons

$$\sigma_n(x_j) = \sum_{\boldsymbol{m}\in M_n} \tau(a_{j,\boldsymbol{m}}^{p^n} \xi^{\boldsymbol{m}}) \quad \text{pour tout} \quad j \in J$$

et

$$\sigma_n(x) = \tau(x) \quad \text{pour} \quad x \in k^{*p^n} .$$

Alors σ_n s'étend, de façon unique, en une application multiplicative de k^* dans $C/p^{n+1}C$, encore notée σ_n, et qui par passage au quotient, détermine l'inclusion de k^* dans $k = C/pC$.
c) Soit σ'_n une autre application multiplicative de k^* dans $C/p^{n+1}C$ définissant l'inclusion de k^* dans k par passage au quotient. Alors pour tout $x \in k^*$, on a $\sigma_n(x) = v(x)\,\sigma'_n(x)$, où v est un homomorphisme de k^* dans le groupe multiplicatif $(1 + pC)/(1 + p^{n+1}C)$ trivial sur k^{*p^n}. Une famille quelconque $(\beta_j)_{j\in J}$ d'éléments de C/p^nC définit un tel homomorphisme par la formule

$$v(x_j) = 1 + p\beta_j \quad \text{pour tout} \quad j \in J .$$

d) Pour tout entier $n \geqslant 0$ et toute application multiplicative $s_n : k^* \to C/p^{n+1}C$ définissant l'inclusion de k^* dans k par passage au quotient, il existe une application multiplicative $s_{n+1} : k^* \to C/p^{n+2}C$ qui détermine s_n par passage au quotient.
e) Prouver qu'il existe une section multiplicative $s : k \to C$. On peut imposer à s de vérifier $s(\xi_\lambda) = \tau(\xi_\lambda)$ pour tout $\lambda \in \Lambda$.
f) Soit A un anneau local, séparé et complet. Soient k son corps résiduel, $(\xi_\lambda)_{\lambda\in\Lambda}$ une p-base de k, et pour $\lambda \in \Lambda$, a_λ un relèvement de ξ_λ dans A. Montrer qu'il existe une section multiplicative $k^* \to A$ qui vérifie $s(\xi_\lambda) = a_\lambda$.

12) Soit A un anneau local complet dont le corps résiduel soit de caractéristique p.
a) Soit $x \in \mathfrak{m}_A$. L'application $n \mapsto (1 + x)^n$ de $\mathbf{Z}$ dans $1 + \mathfrak{m}_A$ se prolonge de façon unique en une application continue de $\mathbf{Z}_p$ dans $1 + \mathfrak{m}_A$, notée $\alpha \mapsto (1 + x)^\alpha$. On définit ainsi une structure de $\mathbf{Z}_p$-module sur le groupe multiplicatif $1 + \mathfrak{m}_A$.
b) Soit $\mathcal{E}$ la série formelle $\exp(-\sum_{n=0}^{\infty} T^{p^n}/p^n)$ de l'exerc. 58, p. 68. L'application $x \mapsto \mathcal{E}(x)$ de $\mathfrak{m}_A$ dans $1 + \mathfrak{m}_A$ est bijective.

c) Soient k un corps parfait de caractéristique p, et φ un homomorphisme local de $W(k)$ dans A. Pour $\alpha \in W(k)$, considérons la série $\varphi E_F(\alpha, T)$ obtenue en appliquant φ aux coefficients de la série $E_F(\alpha, T)$ de l'exerc. 58, *f*), p. 68. Pour $\alpha \in W(k)$, $x \in 1 + \mathfrak{m}_A$, posons $x^\alpha = \varphi E_F(\alpha, \varepsilon^{-1}(x))$. Montrer qu'on définit ainsi une action du groupe additif $W(k)$ sur l'ensemble $1 + \mathfrak{m}_A$, qui prolonge l'action de $W(\mathbf{F}_p)$ (identifié à $\mathbf{Z}_p$) définie en *a*). Montrer qu'on a en outre, pour $a \in \mathbf{Z}_p$ et $\alpha \in W(k)$, $x \in 1 + \mathfrak{m}_A$, la relation $(x^\alpha)^a = x^{a\alpha}$.
d) Utilisant l'exerc. 15, p. 44, prouver qu'on n'a pas toujours, pour $a \in \mathbf{Z}_p$ et $\alpha \in W(k)$, $x \in 1 + \mathfrak{m}_A$, la relation $(x^a)^\alpha = x^{a\alpha}$. On n'a pas non plus toujours, pour $\alpha \in W(k)$ et x, y dans $1 + \mathfrak{m}_A$, la relation $(xy)^\alpha = x^\alpha y^\alpha$.

13) Soit A un anneau de valuation discrète complet de caractéristique nulle, dont le corps résiduel soit de caractéristique p. Soient K le corps de fractions de A, $\overline{K}$ une clôture algébrique de K, munie de l'unique valuation v prolongeant celle de K (VI, § 8, n° 7), $\hat{K}$ le complété de $\overline{K}$, $\hat{A}$ l'anneau de valuation de $\hat{K}$. Posons $e = v(p)$.

a) La série $\log(1 + x) = \sum_{i=1}^{\infty} (-1)^{i-1} x^i / i$ converge pour $v(x) > 0$ et définit des homomorphismes de $\mathbf{Z}_p$-modules (*cf.* exerc. 12)

$$\log : 1 + \mathfrak{m}_{\hat{A}} \to \hat{K},$$
$$\log : 1 + \mathfrak{m}_A \to K.$$

b) La série $\exp(x) = \sum_{i=0}^{\infty} x^i / i!$ converge sur l'idéal $\mathfrak{a}$ de $\hat{K}$ des éléments de valuation $> e/(p-1)$, et définit des homomorphismes de $\mathbf{Z}_p$-modules

$$\exp : \mathfrak{a} \to 1 + \mathfrak{m}_{\hat{A}}$$
$$\exp : \mathfrak{a} \cap K \to 1 + \mathfrak{m}_A.$$

c) Pour $x \in \mathfrak{a}$, on a $\log(\exp(x)) = x$, $\log(1 + x) \in \mathfrak{a}$ et $\exp(\log(1 + x)) = 1 + x$. Ainsi exp définit des isomorphismes de $\mathbf{Z}_p$-modules

$$\mathfrak{a} \to 1 + \mathfrak{a}$$
$$\mathfrak{a} \cap K \to 1 + (\mathfrak{a} \cap K)$$

d'inverses définis par log.
d) Le noyau de log sur $1 + \mathfrak{m}_{\hat{A}}$ est formé des racines de l'unité dont l'ordre est une puissance de p. L'image $\log(1 + \mathfrak{m}_{\hat{A}})$ est égale à $\mathfrak{m}_{\hat{A}}$.

14) Soit A un anneau de valuation discrète complet, de caractéristique nulle, dont le corps résiduel k soit parfait de caractéristique p. Soit K le corps des fractions de A. Soient n un entier $\geqslant 1$ et ζ une racine primitive p^n-ième de l'unité dans K. Soit $\overline{K}$ une clôture algébrique de K, munie de l'unique valuation v prolongeant celle de K.
a) Soit C le sous-anneau de Cohen de A, T son corps de fractions ; c'est un sous-corps de K. L'isomorphisme canonique de $W(k)$ sur C induit un isomorphisme de $W(k) \otimes_{\mathbf{Z}} \mathbf{Q}$ sur T. Pour toute extension l de degré fini de k, le corps $W(l) \otimes_{\mathbf{Z}} \mathbf{Q}$ est une extension de degré fini de $W(k) \otimes_{\mathbf{Z}} \mathbf{Q}$, galoisienne si l l'est. Si l est galoisienne, l'unique extension T_l de T dans $\overline{K}$ isomorphe à $W(l) \otimes_{\mathbf{Z}} \mathbf{Q}$ a un corps résiduel isomorphe à l. En particulier le corps T^∞, réunion des corps T_l quand l parcourt les extensions galoisiennes de degré fini de k (dans une clôture algébrique fixée de k), a pour corps résiduel une clôture algébrique $\bar{k}$ de k. Il en est de même de $\overline{K}$. Pour chaque extension l de k dans $\bar{k}$, on notera T_l l'unique extension de T dans T^∞ dont le corps résiduel soit le sous-corps l de k, et K_l l'extension composée de K et T_l. Alors, si l est galoisienne sur k, K_l est galoisienne sur K et son groupe de Galois s'identifie canoniquement au groupe de Galois de l sur k.
b) Soit k_n la plus grande extension abélienne de k dans $\bar{k}$ dont le groupe de Galois est annulé par p^n. Grâce à l'exerc. 19, p. 45, on a un isomorphisme canonique

$$\mathrm{Gal}(k_n/k) \to \mathrm{Hom}(W_n(k)/\wp W_n(k), \mathbf{Z}/p^n\mathbf{Z}).$$

Par A, V, p. 85, th. 4, on a un isomorphisme canonique

$$\mathrm{Gal}(K_{k_n}/K) \to \mathrm{Hom}(H_n/K^{*p^n}, \mu_{p_n}(K))$$

où $H_n = (K^*_{k_n})^{p^n} \cap K^*$.

Prouver qu'il existe une unique application

$$E^* : W_n(k)/\wp W_n(k) \to H_n/K^{*p^n}$$

telle que le diagramme suivant soit commutatif :

$$\begin{array}{ccc} \mathrm{Gal}(K_{k_n}/K) & \longrightarrow & \mathrm{Hom}(H_n/K^{*p^n}, \mu_{p^n}(K)) \\ \downarrow & & \downarrow \\ \mathrm{Gal}(k_n/k) & \longrightarrow & \mathrm{Hom}(W_n(k)/\wp W_n(k), \mathbf{Z}/p^n\mathbf{Z}), \end{array}$$

où la flèche verticale de droite désigne l'application qui à l'homomorphisme φ de H_n/K^{*p^n} dans $\mu_{p^n}(K)$ associe l'homomorphisme ψ de $W_n(k)/\wp W_n(k)$ dans $\mathbf{Z}/p^n\mathbf{Z}$ défini par $\zeta^{\psi(\alpha)} = \varphi(E^*(\alpha))$ pour $\alpha \in W_n(k)/\wp W_n(k)$. L'application E^* est un isomorphisme.

15) Conservons les hypothèses et notations de l'exercice précédent.

a) Soient $\alpha \in W(k)$ et $\bar{\alpha} \in W(\bar{k})$ vérifiant $\wp(\bar{\alpha}) = \alpha$ (*cf.* p. 45, exerc. 19). Alors l'élément $\zeta^{p^n\bar{\alpha}}$ (p. 72, exerc. 12) du complété $\hat{K}$ de $\bar{K}$ ne dépend que de α, il appartient à K, et on a

$$v(\zeta^{p^n\bar{\alpha}} - 1) \geqslant ep/(p-1) \quad (\text{avec } e = v(p)).$$

(On pourra prouver l'égalité

$$\log(\zeta^{p^n\bar{\alpha}}) = -p^n \sum_{j=1}^{\infty} \sum_{\sigma=0}^{j-1} (F^\sigma\alpha)\frac{\pi^{p^j}}{p^j}$$

où $\pi = \mathcal{E}^{-1}(\zeta)$ (*loc. cit.*) et où F désigne l'automorphisme de Frobenius de $W(k)$.)

b) Pour $\alpha \in W(k)$, notons $E^{**}(\alpha)$ la classe dans K^*/K^{*p^n} de $\zeta^{p^n\bar{\alpha}}$. Alors $E^{**}(\alpha)$ vaut 1 si $\alpha \in \wp W(k)$ ou si $\alpha \in p^n W(k)$. L'application de $W_n(k)/\wp W_n(k)$ dans K^*/K^{*p^n} qui associe à la classe de $\alpha \in W(k)$ l'élément $E^{**}(\alpha)$, prend ses valeurs dans $H_n/(K^*)^{p^n}$ et vérifie les conditions de l'exerc. 14, *b*).

16) Soit A un anneau de valuation discrète complet, de corps résiduel k.

a) Prouver qu'il existe une section multiplicative $\varphi : k^* \to A$. (Si A contient un corps, utiliser le § 3. Sinon, utiliser l'exerc. 11, p. 72.)

b) Soient t une uniformisante de A, $\mathcal{C}$ le groupe engendré par t, et $\varphi : k^* \to A$ une section multiplicative. Le groupe multiplicatif du corps des fractions de A se décompose en un produit direct $\mathcal{C} \times \varphi(k^*) \times (1 + \mathfrak{m}_A)$.

c) Supposons A d'égales caractéristiques et soit K un corps de représentants. Alors A s'identifie à l'anneau $K[[T]]$ des séries formelles à coefficients dans K, et le groupe $1 + \mathfrak{m}_A$ s'identifie au groupe $\Lambda(K) = 1 + TK[[T]]$ (*cf.* p. 56, exerc. 42). Si K est de caractéristique nulle, l'application $\varphi \mapsto \frac{1}{T}\log\varphi$ du groupe $\Lambda(K)$ dans le groupe additif $K[[T]]$ est un isomorphisme. Si A est de caractéristique p, $1 + \mathfrak{m}_A$ s'identifie au groupe $W(A)^L$ où L est l'ensemble des entiers positifs premiers à p (utiliser les exerc. 40, *h*) p. 54 et 43, *b*), p. 57).

17) Soit A un anneau de valuation discrète complet, dont le corps résiduel k est parfait de caractéristique p et dont le corps des fractions est de caractéristique 0. Soit f l'unique homomorphisme de $W(k)$ dans A qui induise l'identité sur le corps résiduel k. Soit enfin π une uniformisante de A.

a) Il existe un polynôme d'Eisenstein P à coefficients dans $f(W(k))$ tel que $P(\pi) = 0$ (utiliser VIII, § 5, n° 4).
b) Soit e la valuation de p. Pour tout entier $n \geqslant 0$, notons U_n le groupe multiplicatif $1 + \mathfrak{m}_A^n$, et posons $\lambda(n) = \inf(np, n + e)$, $e_1 = e/(p-1)$. Soit u la classe dans k^* de $p\pi^{-e}$. Soit φ l'endomorphisme de U_1 qui à x associe x^p. On a alors pour tout entier $n \geqslant 1$, $\varphi(U_n) \subset U_{\lambda(n)}$, $\varphi(U_{n+1}) \subset U_{\lambda(n)+1}$ et l'homomorphisme induit $\varphi_n : U_n/U_{n+1} \to U_{\lambda(n)}/U_{\lambda(n)+1}$ est un isomorphisme si $n \neq e_1$. Si $n = e_1$, φ_n est injective si et seulement si l'équation $x^{p-1} + u = 0$ n'a pas de solution dans k, et surjective si et seulement si l'équation $x^p + ux = y$ a une solution dans k pour tout $y \in k$.
c) Les deux conditions suivantes sont équivalentes :
(i) A contient p racines p-ièmes de l'unité ;
(ii) e_1 est un entier et l'équation $x^{p-1} + u = 0$ a une solution dans k.
d) La topologie induite sur U_1 par celle de A coïncide avec la topologie p-adique de U_1.
e) Soit S l'ensemble des entiers $n \geqslant 1$ tels que A contienne p^n racines p^n-ièmes de l'unité. Alors $s = \mathrm{Card}(S)$ est fini.
f) Soit I l'ensemble des entiers i étrangers à p et vérifiant $1 \leqslant i < e + e_1$. Alors on a $\mathrm{Card}(I) = e$ et l'image de $\mathbf{N} - \{0\}$ par λ est $\mathbf{N} - (I \cup \{0\})$.
g) Si e_1 est entier et que φ_{e_1} n'est pas surjective, posons $I' = I \cup \{e + e_1\}$; sinon, posons $I' = I$. Pour chaque entier $i \in I'$, soit π_i un élément de A de valuation i. Alors l'application de $W(k)^{I'}$ dans U_1 qui à $(a_i)_{i \in I'}$ associe $\prod_{i \in I'} (1 + \pi_i)^{a_i}$ est surjective ; c'est un homomorphisme de $\mathbf{Z}_p$-modules.
h) Soient n un entier $> e_1$ et $I(n)$ l'intervalle $[n, \lambda(n) - 1]$ de $\mathbf{N}$. Pour tout entier $i \in I(n)$, soit π_i un élément de A de valuation i. Alors l'application de $W(k)^{I(n)}$ dans U_n qui à $(a_i)_{i \in I(n)}$ associe $\prod_{i \in I(n)} (1 + \pi_i)^{a_i}$ est un isomorphisme de $\mathbf{Z}_p$-modules.
i) Supposons que k soit fini et notons d le degré sur $\mathbf{Q}_p$ du corps des fractions de A. Alors le $\mathbf{Z}_p$-module $1 + \mathfrak{m}_A$ est isomorphe à $(\mathbf{Z}/p^s\mathbf{Z}) \times \mathbf{Z}_p^d$. (On pourra utiliser les questions précédentes, ou bien utiliser l'exerc. 13, p. 73.)

§ 3

1) Soient p un nombre premier, G le groupe libre à deux générateurs X et Y, $\mathbf{F}_p[G]$ l'algèbre du groupe G sur $\mathbf{F}_p$. On pose $Z = XY - YX$ et on note $\mathfrak{a}$ l'idéal bilatère de $\mathbf{F}_p[G]$ engendré par les éléments $ZX - XZ$, $ZY - YZ$ et Z^2. Posant $A = \mathbf{F}_p[G]/\mathfrak{a}$, on note $\mathfrak{z}$ l'idéal bilatère de A engendré par l'image de Z dans A (on notera encore X, Y, Z les images dans A de X, Y et Z).
a) Soit a un élément de A. Prouver qu'il existe deux familles à support fini d'éléments de $\mathbf{F}_p$, soient $(p_{\alpha,\beta})_{(\alpha,\beta) \in \mathbf{Z}^2}$ et $(q_{\alpha,\beta})_{(\alpha,\beta) \in \mathbf{Z}^2}$, déterminées de manière unique par la condition

$$a = \sum_{(\alpha,\beta) \in \mathbf{Z}^2} (p_{\alpha,\beta} + q_{\alpha,\beta} Z)\, X^\alpha Y^\beta .$$

En déduire que l'algèbre quotient $A/\mathfrak{z}$ est commutative et intègre, et que l'idéal $\mathfrak{z}$ est contenu dans le centre de A.
b) Pour tout couple (a, b) d'éléments de A, il existe un élément c de A tel qu'on ait

$$a^k b - b a^k = k a^{k-1} c Z \quad \text{pour tout entier } k \geqslant 0 .$$

En déduire que l'ensemble A^p des puissances p-ièmes des éléments de A est contenu dans le centre de A.
c) La partie multiplicative $S = A - \mathfrak{z}$ de A permet un calcul de fractions à droite et à gauche (II, § 2, exerc. 22). On notera B l'anneau de fractions de A ainsi construit.
(Pour vérifier par exemple que pour tout a dans A et tout s dans S, il existe $b \in A$ et $t \in S$ tels que $at = sb$, prendre $b = s^{p-1}a$, $t = s^p$ et utiliser *b*).)
d) Prouver que l'application canonique de A dans B est injective. (Remarquer que le noyau de cette application est contenu dans $\mathfrak{z}$ et raisonner comme dans *a*).)

e) Le centre de B contient Z. Si $\mathfrak{m}$ est l'idéal bilatère de B engendré par Z, on a $\mathfrak{m}^2 = 0$.
f) L'idéal $\mathfrak{m}$ est l'ensemble des éléments non-inversibles de B, et le corps $B/\mathfrak{m}$ est isomorphe au corps $\mathbf{F}_p(X, Y)$.
g) Prouver qu'il n'existe pas de sous-corps de B dont l'image dans $B/\mathfrak{m}$ soit tout $B/\mathfrak{m}$.

Dans les exerc. 2 à 5, les anneaux topologiques (commutatifs) sont supposés linéairement topologisés. Si A et B sont deux anneaux topologiques et que B est une A-algèbre, on dit que B est une A-algèbre topologique si l'homomorphisme de A dans B qui définit la structure d'algèbre est continu.

2) Soient A un anneau topologique, B une A-algèbre topologique. On dit que B est une A-algèbre *formellement lisse* [1] si, pour toute A-algèbre topologique discrète C, tout idéal j de C, de carré nul, et tout A-homomorphisme continu $u : B \to C/j$, il existe un A-homomorphisme continu $v : B \to C$ qui, par passage au quotient, induise u.

Soient A un anneau, B une A-algèbre. On dit que B est une A-algèbre *lisse* si B est une A-algèbre formellement lisse quand on munit A et B des topologies discrètes.
a) Soient A un anneau topologique et B une A-algèbre *formellement lisse*. Soient C un anneau et j un idéal de C. Munissons C de la topologie j-adique, et supposons C séparé et complet pour cette topologie. Alors, pour tout A-homomorphisme continu $u : B \to C/j$, il existe un A-homomorphisme continu $v : B \to C$ qui, par passage au quotient, induise u.
b) Soit A un anneau. Toute algèbre de polynômes sur A est une A-algèbre lisse.
c) Soit A un anneau topologique. Si B est une A-algèbre formellement lisse et C une B-algèbre formellement lisse, alors C est une A-algèbre formellement lisse.
d) Soient A un anneau topologique, B une A-algèbre formellement lisse, A′ une A-algèbre topologique. Alors la A′-algèbre topologique $B \otimes_A A'$ (III, § 2, exerc. 28) est une A′-algèbre formellement lisse.
e) Soient A un anneau topologique, B une A-algèbre formellement lisse. Soit S (resp. T) une partie multiplicative de A (resp. B) telle que l'image de S dans B soit contenue dans T. Alors $T^{-1}B$ est une $S^{-1}A$-algèbre formellement lisse (voir III, § 2, exerc. 27 pour la topologie de $T^{-1}B$ et $S^{-1}A$).
f) Soient n un entier $\geqslant 1$, A un anneau topologique, $(B_i)_{1 \leqslant i \leqslant n}$ une famille de A-algèbres topologiques. Pour que $\prod_{i=1}^{n} B_i$ soit une A-algèbre formellement lisse, il faut et il suffit que B_i soit une A-algèbre formellement lisse pour $1 \leqslant i \leqslant n$.
g) Soient A un anneau topologique, B une A-algèbre topologique, $\hat{A}$ et $\hat{B}$ les séparés complétés respectifs de A et B. Alors les trois conditions suivantes sont équivalentes :
(i) B est une A-algèbre formellement lisse ;
(ii) $\hat{B}$ est une A-algèbre formellement lisse ;
(iii) $\hat{B}$ est une $\hat{A}$-algèbre formellement lisse.
h) Reprenons les notations et hypothèses de *e*). Alors $B\{T^{-1}\}$ est une $A\{S^{-1}\}$-algèbre formellement lisse.

3) Soient k un corps et A une k-algèbre commutative. Pour tout entier $i \geqslant 1$ posons $B_i = \underbrace{A \otimes_k A \otimes_k \cdots \otimes_k A}_{i \text{ termes}}$ et munissons B_i de la structure de A-algèbre obtenue en faisant agir A sur la première composante. Posons $C_1 = B_2$, $C_2 = B_3$, $C_3 = B_4 \oplus B_3$, et définissons des applications A-linéaires $d_2 : C_2 \to C_1$ et $d_3 : C_3 \to C_2$ par les formules

$$d_3((1 \otimes x \otimes y \otimes z, 1 \otimes \alpha \otimes \beta)) = x \otimes y \otimes z - 1 \otimes xy \otimes z + 1 \otimes x \otimes yz - z \otimes x \otimes y + \\ + 1 \otimes \alpha \otimes \beta - 1 \otimes \beta \otimes \alpha$$

$$d_2(1 \otimes \alpha \otimes \beta) = \alpha \otimes \beta - 1 \otimes \alpha\beta + \beta \otimes \alpha,$$

[1] Si A est une algèbre locale, noethérienne et complète sur un corps (discret) k, cette définition coïncide avec celle donnée en VIII, p. 98, exerc. 30, d'après l'exerc. 5 ci-après.

pour tout choix d'éléments x, y, z, α, β de A. On obtient ainsi un complexe de A-modules

$$C_k(A) : C_3 \xrightarrow{d_3} C_2 \xrightarrow{d_2} C_1 .$$

Si N est un A-module, on dira qu'une application k-bilinéaire $f : A \times A \to N$ est un 2-cocycle si l'on a l'identité $xf(y, z) - f(xy, z) + f(x, yz) - zf(x, y) = 0$ pour x, y et z dans A, et qu'elle est symétrique si l'on a $f(x, y) = f(y, x)$ pour tout couple $(x, y) \in A \times A$.

a) Les conditions suivantes sont équivalentes :

(i) le complexe $\mathrm{Hom}_A(C_k(A), N)$ est acyclique pour tout A-module N ;

(ii) quel que soit le A-module N, tout 2-cocycle symétrique $f : A \times A \to N$ est un 1-cobord, c'est-à-dire de la forme $f(a, b) = ag(b) + bg(a) - g(ab)$ avec $g \in \mathrm{Hom}_k(A, N)$;

(iii) A est une algèbre lisse sur k.

b) Si A est un corps, les conditions précédentes sont aussi équivalentes à la condition que le complexe $C_k(A)$ soit acyclique.

4) *a*) Soient k un corps et K une extension de k. Si K est séparable sur k, alors K est une k-algèbre lisse. (Si K est une extension de type fini de k, utiliser la prop. 1 du § 3, n° 2. Dans le cas général, écrire K comme réunion d'extensions de type fini de k et utiliser l'exercice précédent.)

b) Soit A un anneau local séparé et complet contenant un corps k. Utilisant *a*), prouver que A possède un corps de représentants. Si le corps résiduel de A est une extension séparable de k, alors A possède un corps de représentants contenant k.

5) Soient A un anneau local noethérien contenant un corps k, et $\mathfrak{m}$ l'idéal maximal de A. On suppose que A est une k-algèbre formellement lisse (le corps k étant discret).

a) Soient K un corps de représentants de l'anneau $A/\mathfrak{m}^2$ (exerc. 4, *b*)), et $x_1, ..., x_d$ des éléments de $\mathfrak{m}$ dont les images forment une base du K-espace vectoriel $\mathfrak{m}/\mathfrak{m}^2$. Soient $K[X_1, ..., X_d]$ l'anneau des polynômes en d variables $X_1, ..., X_d$, $\mathfrak{n}$ son idéal engendré par $X_1, ..., X_d$, et φ l'homomorphisme de $K[X_1, ..., X_d]$ dans $A/\mathfrak{m}^2$ qui à X_i associe x_i pour $1 \leqslant i \leqslant d$ et induit l'identité sur K. Alors φ induit un isomorphisme $\overline{\varphi}$ de $K[X_1, ..., X_d]/\mathfrak{n}^2$ sur $A/\mathfrak{m}^2$.

b) Pour tout entier $n \geqslant 1$, il existe un homomorphisme $\psi_n : A \to K[X_1, ..., X_d]/\mathfrak{n}^{n+1}$ qui, par passage aux quotients induise $\overline{\varphi}^{-1}$. Un tel homomorphisme ψ_n est surjectif.

c) Pour tout entier $n \geqslant 1$, la longueur du A-module $A/\mathfrak{m}^{n+1}$ vaut au moins $\binom{d+n}{d}$ et l'on a $\dim(A) \geqslant d$.

d) Pour toute extension k' de degré fini de k, et tout idéal maximal $\mathfrak{m}'$ de l'anneau semi-local $A \otimes_k k'$, l'anneau local $(A \otimes_k k')_{\mathfrak{m}'}$ est régulier.

6) Soient k un corps et K une extension de k. On suppose que K est une k-algèbre lisse. Soit k' une extension algébrique de degré fini de k.

a) L'anneau $K \otimes_k k'$ est produit d'un nombre fini d'anneaux locaux artiniens, qui sont des k'-algèbres lisses (utiliser l'exerc. 2, p. 76).

b) L'anneau $K \otimes_k k'$ est réduit (utiliser l'exercice précédent).

c) Le corps K est séparable sur k.

7) Soient k un corps, P son sous-corps premier, K une extension de k. Alors les conditions suivantes sont équivalentes :

a) Toute dérivation de k dans un K-module M s'étend de façon unique en une dérivation de K dans M.

b) On a $\Omega_P(K) = \Omega_P(k) \otimes_k K$.

c) Le corps K est séparable sur k et $\Omega_k(K) = 0$.

Si k est de caractéristique 0, ces conditions sont aussi équivalentes à la condition :

d) Le corps K est une extension algébrique de k.

Si k est de caractéristique non nulle p, elles sont aussi équivalentes aux conditions :

e) $K = k \otimes_{k^p} K^p$.

f) Toute p-base de k est aussi une p-base de K.

8) Soient k un corps et K une extension de k. On dit que K est *formellement étale* sur k si, pour toute k-algèbre A, tout idéal $\mathfrak{a}$ de A, de carré nul, et tout k-homomorphisme u de K dans $A/\mathfrak{a}$, il existe un *unique* k-homomorphisme v de K dans A qui donne u par passage au quotient.
a) Si K est formellement étale sur k, les conditions équivalentes de l'exercice précédent sont vérifiées. (Si M est un K-module, considérer la k-algèbre dont le k-espace vectoriel sous-jacent est $K \oplus M$, M en étant un idéal de carré nul.)
b) Inversement, si les conditions équivalentes de l'exercice précédent sont vérifiées, alors K est formellement étale sur k. (Le corps K étant séparable sur k, l'exerc. 4 permet de prouver l'existence de v.)
c) Soit $B = (b_i)_{i\in I}$ une famille d'éléments de K telle que $(db_i)_{i\in I}$ soit une base de $\Omega_k(K)$ sur K. Si K est séparable sur k, alors $k(B)$ est une extension transcendante pure de k (utiliser le th. 2 de A, V, p. 125, le th. 1 de A, V, p. 97 et l'exerc. 6 de A, V, p. 165) et K est formellement étale sur $k(B)$.

9) Soient A un anneau local d'égales caractéristiques, $\mathfrak{m}_A$ son idéal maximal et k un sous-corps de A. Alors le corps résiduel κ_A est une k-algèbre. On dit que k est un *corps de représentants faible* de A si κ_A est formellement étale sur k (exerc. 8).
a) Si A possède un corps de représentants faible k, alors le séparé complété $\hat{A}$ de A possède un unique corps de représentants contenant l'image de k dans $\hat{A}$.
b) Soit B un anneau local inclus dans A, d'idéal maximal $\mathfrak{m}_B = \mathfrak{m}_A \cap B$. Si κ_A est une extension séparable du corps résiduel κ_B de B, tout corps de représentants faible de B est contenu dans un corps de représentants faible de A (utiliser l'exerc. 8, *c*)).
c) Soit B un anneau local inclus dans A, d'idéal maximal $\mathfrak{m}_B = \mathfrak{m}_A \cap B$. Supposons en outre que A soit de caractéristique p non nulle et contienne B^p. Alors il existe un corps de représentants faible de A qui contienne un corps de représentants faible de B.

§ 4

1) Soit A un anneau semi-local noethérien intègre de dimension 1.
a) La clôture intégrale de A est une A-algèbre finie si et seulement si le complété $\hat{A}$ de A est réduit. (Si $\hat{A}$ est réduit, utiliser le corollaire du th. 2 du § 4, n° 2. Pour l'implication dans l'autre sens, se ramener au cas où A est intégralement clos, et raisonner comme dans la démonstration du th. 3 du § 4, n° 4).
b) Les trois conditions suivantes sont équivalentes :
(i) A est un anneau japonais ;
(ii) A est un anneau de Nagata ;
(iii) $\hat{A}$ est réduit et si $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ sont les idéaux premiers minimaux de $\hat{A}$, alors les corps $\kappa(\mathfrak{q}_i)$ sont des extensions séparables du corps des fractions de A.

2) Soit A un anneau local noethérien de dimension 1. Alors les conditions suivantes sont équivalentes :
a) A est régulier ;
b) A est intégralement clos ;
c) A est un anneau de valuation discrète.

3) On dit qu'un anneau A est *normal* si l'anneau $A_\mathfrak{p}$ est intégralement clos pour tout idéal premier $\mathfrak{p}$ de A.
a) Un anneau normal A est réduit et tout idéal premier $\mathfrak{p}$ de A contient un seul idéal premier minimal de A. Pour tout idéal premier minimal $\mathfrak{p}$ de A, l'anneau $A/\mathfrak{p}$ est intégralement clos.
b) Un anneau noethérien normal A est isomorphe à un produit d'un nombre fini d'anneaux noethériens intégralement clos.
c) Soient A un anneau noethérien normal et a un élément de A. Alors $\mathrm{Ass}_A(A/aA)$ ne contient pas d'idéal premier immergé (IV, § 2, n° 3, remarque).

4) Soit A un anneau. On considère sur A les deux conditions suivantes :
(R1) Pour tout idéal premier p de A de hauteur $\leqslant 1$, l'anneau A_p est régulier.
(S2) L'ensemble $\mathrm{Ass}_A(A)$ et, pour tout élément simplifiable a de A, l'ensemble $\mathrm{Ass}_A(A/aA)$ ne contiennent pas d'idéal premier immergé.
Un anneau noethérien normal (exerc. 3) vérifie (R1) et (S2). (Utiliser les exerc. 2 et 3, *c*).)

5) Soit A un anneau noethérien vérifiant les conditions (R1) et (S2).
a) Montrer que A est réduit.
b) Soit a un élément simplifiable de A. Si un élément x de A est tel que son image dans A_p appartienne à aA_p pour tout $p \in \mathrm{Ass}_A(A/aA)$, alors x appartient à aA. (Utiliser IV, § 2, n° 3, prop. 5.)
c) Prouver que A est intégralement fermé dans son anneau total des fractions R. (Si $a, b, c_1, \ldots, c_n$ sont des éléments de A vérifiant
(i) b est simplifiable dans A,
(ii) $(b^{-1}a)^n + c_1(b^{-1}a)^{n-1} + \cdots + c_n = 0$ dans R,
alors prouver successivement qu'on a $a \in bA_p$ pour tout idéal premier p de hauteur 1 de A, puis qu'on a $a \in bA$.)
d) Prouver que A est normal. (Remarquer qu'un idempotent de R est entier sur A.)

6) *a*) Soient A un anneau, M un A-module fidèle et noethérien. Montrer que A est un anneau noethérien.
b) Soient A un anneau et M un A-module fidèle de type fini. On suppose que pour toute suite croissante d'idéaux $(\mathfrak{a}_i)_{i\in\mathbf{N}}$ de A, la suite des sous-modules $(\mathfrak{a}_i M)_{i\in\mathbf{N}}$ de M est stationnaire. Alors A est un anneau noethérien. (Par *a*), il suffit de prouver que M est un A-module noethérien. Se ramener au cas où pour tout idéal non nul $\mathfrak{a}$ de A, le A-module $M/\mathfrak{a}M$ est noethérien et où, pour tout sous-module non nul N de M, le A-module M/N n'est pas fidèle.)
c) Soient B un anneau noethérien et A un sous-anneau de B tel que B soit une A-algèbre finie. Alors A est un anneau noethérien. (Ceci permet de supprimer l'hypothèse que A soit noethérien dans la prop. 2 du § 4, n° 1.)

7) Soient A un anneau de Krull et P l'ensemble de ses idéaux premiers de hauteur 1. On suppose que pour tout idéal premier $p \in P$, l'anneau A/p est noethérien, et on note K le corps des fractions de A. Prouver que A est noethérien.
(Soient $p \in P$ et $x \in K$ tels que $v_p(x) = 1$ et $v_q(x) \leqslant 0$ pour $q \in P - \{p\}$. Posons $B = A[x]$. Alors on a les propriétés suivantes :
(i) $p = xB \cap A$;
(ii) l'inclusion de A dans B induit, par passage aux quotients, un isomorphisme de A/p sur B/xB ;
(iii) pour tout entier $n \geqslant 0$, l'anneau B/x^nB est noethérien ;
(iv) pour tout entier $n \geqslant 0$, l'anneau $A/(x^nB \cap A)$ est noethérien (utiliser l'exerc. 6) ;
(v) pour tout entier $n \geqslant 0$, le A-module $A/p^{(n)}$ est noethérien. On rappelle qu'on pose $p^{(n)} = A \cap p^nA_p$, *cf.* IV, § 2, exerc. 18.)

8) Soient A un anneau intègre, K son corps des fractions. Soient B un anneau et $\varphi : A \to B$ un homomorphisme d'anneaux qui fasse de B un A-module fidèlement plat. On suppose que B n'a qu'un nombre fini d'idéaux premiers minimaux $p_1, \ldots, p_n$. Pour $1 \leqslant i \leqslant n$, on pose $B_i = B/p_i$, on note L_i le corps des fractions de B_i et L l'anneau produit des L_i. Enfin, on note $\overline{A}$ la clôture intégrale de A, $\overline{B}_i$ celle de B_i.
a) L'homomorphisme de A dans L déduit de φ est injectif, et se prolonge en un homomorphisme injectif ψ de K dans L.
b) On a $\overline{A} = \psi^{-1}(\prod_{i=1}^{n} \overline{B}_i)$. (On pourra prouver que si $x \in \psi^{-1}(\prod_{i=1}^{n} \overline{B}_i)$ et si x' est son image dans $K \otimes_A B$, il existe un polynôme unitaire P à coefficients dans B tel que $P(x')$ soit nilpotent dans $K \otimes_A B$.)

9) Soient A un anneau noethérien intègre, K son corps des fractions, E une extension finie de K, et $\overline{A}$ la fermeture intégrale de A dans E.
a) Si A est un anneau local de complété $\hat{A}$, alors $(\hat{A} \otimes_A \overline{A})_{red}$ est une $\hat{A}$-algèbre finie [1]. (Se ramener au cas où K = E. Utilisant III, § 3, n° 4, cor. 2 du th. 3, prouver que les éléments non nuls de A ne sont pas diviseurs de zéro dans $\hat{A}_{red}$. Prouver alors qu'il existe un $\hat{A}_{red}$-homomorphisme injectif de $(\hat{A} \otimes_A \overline{A})_{red}$ dans l'anneau total des fractions de $\hat{A}_{red}$. Conclure.)
b) Pour tout idéal premier $\mathfrak{p}$ de A, la $\kappa(\mathfrak{p})$-algèbre $(\overline{A} \otimes_A \kappa(\mathfrak{p}))_{red}$ est finie. (Se ramener au cas où A est local, d'idéal maximal $\mathfrak{p}$. Remarquer alors que $(\overline{A} \otimes_A \kappa(\mathfrak{p}))_{red}$ est un quotient de $(\overline{A} \otimes_A \hat{A})_{red} \otimes \kappa(\mathfrak{p})$.)

10) Soient A un anneau noethérien local intègre, $\hat{A}$ son complété, $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ les idéaux premiers minimaux de $\hat{A}$, et pour $1 \leqslant i \leqslant n$, posons $B_i = \hat{A}/\mathfrak{p}_i$.
a) L'anneau B_i est japonais.
b) La clôture intégrale $\overline{B}_i$ de B_i est un anneau de Krull.
c) La clôture intégrale $\overline{A}$ de A est un anneau de Krull. (Utiliser l'exerc. 8 et VII, § 1, n° 3, exemples 3 et 4.)
d) $\overline{A}$ n'a qu'un nombre fini d'idéaux maximaux et leurs corps résiduels sont des extensions finies de celui de A. (Utiliser l'exerc. 9, *b*).)
e) Pour tout idéal premier $\mathfrak{p}$ de A, il n'y a qu'un nombre fini d'idéaux premiers $\mathfrak{P}$ de $\overline{A}$ au-dessus de $\mathfrak{p}$, et les corps $\kappa(\mathfrak{P})$ sont des extensions finies de $\kappa(\mathfrak{p})$. (Se ramener au cas où A est local d'idéal maximal $\mathfrak{p}$.)

11) Soient A un anneau noethérien intègre, K son corps des fractions, E une extension finie de K, $\overline{A}$ la fermeture intégrale de A dans E.
a) Pour tout idéal premier $\mathfrak{p}$ de A, il n'y a qu'un nombre fini d'idéaux premiers $\mathfrak{P}$ de $\overline{A}$ au-dessus de $\mathfrak{p}$ et les corps $\kappa(\mathfrak{P})$ sont des extensions finies de $\kappa(\mathfrak{p})$. (Se ramener au cas où A est local d'idéal maximal $\mathfrak{p}$ et où E = K, et utiliser l'exerc. 10.)
b) Soit P l'ensemble des idéaux premiers de hauteur 1 de $\overline{A}$. Si $\mathfrak{p} \in P$, alors $\overline{A}_\mathfrak{p}$ est un anneau de valuation discrète.
c) On a $\overline{A} = \bigcap_{\mathfrak{p} \in P} \overline{A}_\mathfrak{p}$ (dans E).

12) Soient A un anneau intègre, $\overline{A}$ sa clôture intégrale. Soient $a_1, \ldots, a_r$ des éléments non nuls de $\overline{A}$, $\mathfrak{b}$ l'idéal fractionnaire $\sum_{i=1}^{r} Aa_i$ de A.
a) Il existe un idéal fractionnaire $\mathfrak{a}$ de A tel que $\mathfrak{a}a_i \subset \mathfrak{a}$ pour $1 \leqslant i \leqslant r$. On a aussi $\tilde{\mathfrak{a}}a_i \subset \tilde{\mathfrak{a}}$ pour $1 \leqslant i \leqslant r$; on rappelle (VII, § 1, n° 1) que $\tilde{\mathfrak{a}}$ est l'intersection des idéaux principaux fractionnaires contenant $\mathfrak{a}$.
b) Soit y un élément non nul de $\tilde{\mathfrak{b}}$. Alors

$$Ay^{-1} \supset \bigcap_{i=1}^{r} Aa_i^{-1} \quad \text{et} \quad \tilde{\mathfrak{a}} \subset \tilde{\mathfrak{a}}y^{-1}.$$

c) On a $\tilde{\mathfrak{b}} \subset \overline{A}$.
d) Soit z un élément de $\overline{A} : \overline{A}\mathfrak{b}$. Alors $\overline{A}$ contient $\tilde{\mathfrak{b}}z$.
e) On a $\mathfrak{b} \subset \overline{A} : (\overline{A} : \overline{A}\mathfrak{b})$.
f) Soient $\mathfrak{P}$ un idéal divisoriel de $\overline{A}$ et $\mathfrak{p} = \mathfrak{P} \cap A$. Alors $\mathfrak{p}$ est divisoriel dans A. (Par *e*), on obtient $\tilde{\mathfrak{p}} \subset \mathfrak{P}$. Mais on a aussi $\tilde{\mathfrak{p}} \subset A$.)

13) Soient A un anneau noethérien intègre, K son corps des fractions, $\overline{A}$ sa clôture intégrale, f un élément non nul de A, $\mathfrak{P}$ un idéal premier de hauteur 1 de $\overline{A}$ contenant f, $\mathfrak{p}$ l'idéal premier

[1] Pour tout anneau B, on note B_{red} le quotient de B par l'idéal des éléments nilpotents de B.

$A \cap \mathfrak{B}$ de A. Prouver qu'on a $\mathfrak{p} \in \mathrm{Ass}_A(A/fA)$ en se ramenant au cas où A est local, d'idéal maximal $\mathfrak{p}$ et en établissant successivement sous cette hypothèse les assertions suivantes :
a) $\mathfrak{B}$ est divisoriel (utiliser l'exerc. 10, *c*)).
b) $\mathfrak{p}$ est divisoriel (utiliser l'exerc. 12, *f*)).
c) Si $a_1, \ldots, a_r$ sont des éléments non nuls de K tels que

$$A : \mathfrak{p} = A + \sum_{i=1}^{r} Aa_i, \quad \text{on a} \quad \mathfrak{p} = \bigcap_{i=1}^{r} (A \cap a_i^{-1}A)$$

et il existe un indice i tel que $\mathfrak{p} = A \cap a_i^{-1}A$.
d) Il existe un élément non nul g de A tel que $\mathfrak{p} \in \mathrm{Ass}_A(A/gA)$.
e) $\mathfrak{p} \in \mathrm{Ass}_A(A/fA)$.

14) Soient A un anneau noethérien intègre, K son corps des fractions, $\overline{A}$ sa fermeture intégrale dans une extension finie E de K. Alors $\overline{A}$ est un anneau de Krull. (Utiliser l'exerc. 11, *c*) et, pour prouver que tout élément f de $\overline{A}$, non nul, n'appartient qu'à un nombre fini d'idéaux premiers de hauteur 1, se ramener au cas où $f \in A$, $E = K$, et utiliser les exerc. 13, *b*) et 11, *a*).)

15) Soient A un anneau noethérien, B une A-algèbre entière n'ayant qu'un nombre fini d'idéaux premiers minimaux $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$. Pour $1 \leqslant i \leqslant n$, notons $\mathfrak{q}_i$ l'image réciproque de $\mathfrak{p}_i$ dans A et supposons que $\kappa(\mathfrak{p}_i)$ soit une extension finie de $\kappa(\mathfrak{q}_i)$. Alors, pour tout élément x de B, le sous-espace topologique $V(x)$ de Spec(B) n'a qu'un nombre fini de composantes irréductibles. (Se ramener au cas où B est intégralement clos et contient A, et utiliser l'exerc. 14.)

16) Soient A un anneau noethérien intègre, $\overline{A}$ sa fermeture intégrale dans une extension finie de son corps des fractions, B un anneau contenant A et contenu dans $\overline{A}$. On pose $Y = \mathrm{Spec}(B)$ et $X = \mathrm{Spec}(A)$. On se propose de prouver que Y est un espace noethérien. Soit $(f_n)_{n \in \mathbf{N}}$ une suite d'éléments de B. Pour $n \in \mathbf{N}$, soit $U_n = \mathrm{Spec}(B_{f_n})$ l'ouvert de Y défini par f_n. Posons $U = \bigcup_{n \in \mathbf{N}} U_n$, $F_n = U - \bigcup_{0 \leqslant m \leqslant n} U_m$. On notera $\overline{F}_n$ l'adhérence de F_n dans Y, G_n l'image de F_n dans X, $\overline{G}_n$ l'adhérence de G_n dans X, B_n l'anneau réduit quotient de B tel que $\mathrm{Spec}(B_n) = \overline{F}_n$, $\overline{f}_n$ l'image de f_n dans B_n.
a) On a $F_n = V(\overline{f}_n B_n) \cap U$ pour tout $n \in \mathbf{N}$.
b) Supposons que pour un entier $n \in \mathbf{N}$, $\overline{F}_n$ n'ait qu'un nombre fini de composantes irréductibles. Alors $V(\overline{f}_n B_n)$ n'a qu'un nombre fini de composantes irréductibles. (Appliquer le résultat de l'exerc. 15 en utilisant aussi l'exerc. 11, *a*).)
c) Pour tout $n \in \mathbf{N}$, F_n n'a qu'un nombre fini de composantes irréductibles.
d) Si A_n est l'anneau réduit quotient de A tel que $\mathrm{Spec}(A_n) = \overline{G}_n$, alors les idéaux premiers minimaux de A_n appartiennent à G_n.
e) Soient $n \in \mathbf{N}$ et x un tel idéal premier minimal de A_n. Alors il existe un entier $n' > n$ tel que $F_{n'}$ ne contienne aucun point de Y au-dessus de x, et x n'appartient pas à $\overline{G}_{n'}$. (Utiliser l'exerc. 11, *a*).)
f) Pour n assez grand, F_n est vide.

17) Soient A un anneau noethérien intègre et $a \neq 0$ un élément du radical de A. On fait les hypothèses suivantes :
(i) $\mathrm{Ass}_A(A/aA)$ contient un seul élément minimal $\mathfrak{p}$;
(ii) $aA_{\mathfrak{p}} = \mathfrak{p}A_{\mathfrak{p}}$;
(iii) $A/\mathfrak{p}$ est intégralement clos ;
(iv) la clôture intégrale $\overline{A}$ de A est une A-algèbre finie ;
(v) si $\mathfrak{q}$ est un idéal premier de hauteur 1 de $\overline{A}$, alors $\mathfrak{q} \cap A$ est un idéal premier de hauteur 1 de A.
Prouver que l'on a $\overline{A} = A$ (A est intégralement clos) et $aA = \mathfrak{p}$ (donc A/aA est intégralement clos). Pour cela, établir successivement les assertions suivantes :
a) $A_{\mathfrak{p}}$ et $\overline{A}_{\mathfrak{p}}$ sont isomorphes et $\overline{\mathfrak{p}} = \mathfrak{p}\overline{A}$ est l'unique idéal premier de $\overline{A}$ au-dessus de $\mathfrak{p}$.
b) De plus $\overline{\mathfrak{p}}$ est l'unique élément minimal de $\mathrm{Ass}_A(\overline{A}/a\overline{A})$.

c) En fait $\overline{\mathfrak{p}}$ est le seul élément de $\mathrm{Ass}_A(\overline{A}/a\overline{A})$.
d) $\overline{A}/a\overline{A}$ est intègre et $a\overline{A} = \overline{\mathfrak{p}}$.
e) A/p et $\overline{A}/\overline{\mathfrak{p}}$ sont isomorphes et l'homomorphisme canonique de A/*a*A dans $\overline{A}/a\overline{A}$ est surjectif.

18) Soient A un anneau noethérien intègre, x un élément non nul de A. On suppose que A est séparé et complet pour la topologie xA-adique et que pour tout idéal premier $\mathfrak{p} \in \mathrm{Ass}_A(A/xA)$, l'anneau A/p est japonais. Prouver que A est japonais. (Soit $\overline{A}$ la fermeture intégrale de A dans une extension finie de son corps des fractions.
a) L'anneau $\overline{A}$ étant de Krull (p. 81, exerc. 14), soient $\mathfrak{P}_1, \ldots, \mathfrak{P}_n$ les idéaux premiers de hauteur 1 de $\overline{A}$ contenant x.
b) Soit $\mathfrak{p}_i = \mathfrak{P}_i \cap A$. Alors on a $\mathfrak{p}_i \in \mathrm{Ass}_A(A/xA)$ et $\kappa(\mathfrak{P}_i)$ est une extension finie de $\kappa(\mathfrak{p}_i)$. (Utiliser les exerc. 11 et 13, p. 80.)
c) $\overline{A}/\mathfrak{P}_i$ est un $A/\mathfrak{p}_i$-module de type fini.
d) $\overline{A}/x\overline{A}$ est un A/xA-module de type fini.
e) $\overline{A}$ est séparé pour la topologie $x\overline{A}$-adique.
Conclure comme dans la démonstration du th. 1 du § 4, n° 2.)

19) Soient A un anneau noethérien, $\mathfrak{a}$ un idéal non nul de A. On suppose que A est séparé et complet pour la topologie $\mathfrak{a}$-adique et que A/$\mathfrak{a}$ est un anneau de Nagata. Prouver que A est un anneau de Nagata. On pourra raisonner comme suit :
a) On suppose que A est intègre et que pour tout idéal premier non nul $\mathfrak{p}$ de A, l'anneau A/$\mathfrak{p}$ est japonais. Soit $\overline{A}$ la fermeture intégrale de A dans une extension finie de son corps des fractions. Alors, pour tout idéal premier non nul $\mathfrak{P}$ de $\overline{A}$, l'anneau $\overline{A}/\mathfrak{P}$ est une algèbre finie sur l'anneau $A/(\mathfrak{P} \cap A)$. (Utiliser l'exerc. 11, *a*), p. 80.)
b) Avec les mêmes hypothèses et notations qu'en *a*), prouver que $\overline{A}$ est noethérien. (Utiliser les exerc. 7, p. 79 et 14, p. 81.) Puis, raisonnant comme dans l'exercice précédent, prouver que $\overline{A}/\mathfrak{a}\overline{A}$ est un A-module de type fini, que $\overline{A}$ est séparé pour la topologie $\mathfrak{a}\overline{A}$-adique et que $\overline{A}$ est un A-module de type fini.

20) Soient A un anneau noethérien, $\mathfrak{a}$ un idéal de A distinct de A, $\hat{A}$ le séparé complété de A pour la topologie $\mathfrak{a}$-adique. Si A/$\mathfrak{a}$ est un anneau de Nagata, alors $\hat{A}$ est un anneau de Nagata. (Utiliser l'exerc. 19.)

21) *a*) Soient A un anneau intègre, K son corps des fractions. Si K est de caractéristique non nulle p et si E est une extension finie radicielle du corps des fractions rationnelles K(X), il existe une extension finie radicielle F de K et une puissance q de p telle que $F(X^{1/q})$ soit une extension de E.
b) Soit A un anneau de Nagata intégralement clos. Alors l'anneau de polynômes A[X] est japonais.
c) Soit A un anneau de Nagata intégralement clos. Alors tout anneau de polynômes $A[X_1, \ldots, X_n]$ en un nombre fini d'indéterminées est un anneau de Nagata.

22) Soient A un anneau noethérien, $\mathfrak{a}$ un idéal de A distinct de A. On suppose que A est séparé et complet pour la topologie $\mathfrak{a}$-adique et que A/$\mathfrak{a}$ est un anneau de Nagata. Alors tout anneau de séries formelles restreintes en un nombre fini d'indéterminées est un anneau de Nagata. (Utiliser III, § 4, exerc. 7, et les exerc. 20 et 21 ci-dessus.)

23) Soient A un anneau semi-local noethérien réduit, R son anneau total des fractions, $\hat{A}$ le complété de A. Pour que $\hat{A}$ soit réduit, il faut et il suffit que $R \otimes_A \hat{A}$ soit réduit.

24) Soient A un anneau semi-local noethérien, $\hat{A}$ son complété, x un élément non nul du radical de A. On suppose que $\mathrm{Ass}_A(A/xA)$ ne contient pas d'idéal premier immergé et que, pour tout $\mathfrak{p} \in \mathrm{Ass}_A(A/xA)$, l'anneau $A_\mathfrak{p}$ est régulier et l'anneau $\kappa(\mathfrak{p}) \otimes_A \hat{A}$ réduit. Alors $\hat{A}$ est réduit. (Raisonner comme dans la démonstration du th. 3, (i) $\Rightarrow$ (ii) du § 4, n° 4.)

25) Soient A un anneau noethérien intègre, X l'espace topologique Spec(A), Nor(X) l'ensemble des points p de A tels que l'anneau local A_p soit intégralement clos. (Si la clôture intégrale de A est une A-algèbre finie, alors Nor(X) est ouvert dans X, *cf.* V, § 1, n° 5, cor. 5.)
Soit f un élément non nul de A tel que l'anneau $A[f^{-1}]$ soit intégralement clos.
a) Si un idéal premier p de A ne contient pas f, alors p appartient à Nor(X).
b) Soit E l'ensemble des idéaux premiers p de A, associés à A/fA, de hauteur > 1 ou bien de hauteur 1 et tels que A_p ne soit pas régulier. Alors on a

$$\mathrm{Nor}(X) = X - \bigcup_{p \in E} V(p).$$

(Utiliser les exerc. 4 et 5, p. 79.)
c) Nor(X) est ouvert dans X.

26) Soient A un anneau noethérien intègre, X l'espace topologique Spec(A), Nor(X) le sous-espace de X introduit à l'exerc. 25, $\overline{A}$ la clôture intégrale de A. On suppose qu'il existe un élément non nul f de A tel que l'anneau $A[f^{-1}]$ soit intégralement clos, et que pour tout idéal maximal m de A, l'anneau $\overline{A}_m$ est une A_m-algèbre finie. Considérons $\overline{A}$ comme limite inductive filtrante croissante de sous-A-algèbres finies, $\overline{A} = \varinjlim(A_j)_{j \in J}$. Posons $X_j = \mathrm{Spec}(A_j)$ et soit G_j l'image dans X de $X_j - \mathrm{Nor}(X_j)$.
a) $\mathrm{Nor}(X_j)$ est ouvert dans X_j. (Utiliser l'exerc. 25.)
b) G_j est fermé dans X.
c) Il existe un indice $j_0 \in J$ tel que l'on ait $G_{j_0} = \bigcap_{j \in J} G_j$.
d) Soit $p \in \mathrm{Spec}(A)$. Alors pour $j \in J$ assez grand, G_j ne contient pas p.
e) $\overline{A}$ est une A-algèbre finie.

27) Soit A un anneau local noethérien intégralement clos. On suppose en outre que A est un anneau de Nagata. Soit x un élément du corps des fractions K de A, n'appartenant pas à A. Soient B l'anneau A[x] et p un idéal maximal de B contenant x. Posons $I = xA \cap A$.
a) Soient X une indéterminée et Q le noyau de l'homomorphisme de A[X] dans B qui applique X sur x. Alors Q est engendré par les polynômes de la forme $aX - b$, où a et b sont des éléments de A tels que $ax = b$, et $I = xA \cap A$ est engendré par les termes constants b de ces polynômes. De plus l'inclusion de A dans B induit un isomorphisme de A/I sur B/xB.
b) L'idéal I de A est divisoriel.
c) $\mathrm{Ass}_B(B/xB)$ ne contient aucun idéal premier immergé.
d) Soit q un idéal premier de B_p associé à B_p/xB_p. Alors $q \cap A$ est associé à A/I et les anneaux $A_{q \cap A}$ et $(B_p)_q$ sont des anneaux de valuation discrète.
e) B_p/q est un anneau de Nagata. (Remarquer que $B/(q \cap B)$ est isomorphe à $A/(q \cap A)$.)
f) Le complété de B_p/q est réduit.
g) Le complété de B_p est réduit et la clôture intégrale de B_p est finie sur B_p. (Utiliser l'exerc. 24.)

28) Soient A un anneau local noethérien intégralement clos, K son corps des fractions, x un élément de K − A, B l'anneau A[x] et p un idéal maximal de B. Soient a, b des éléments non nuls de A tels que $bx = a$.
a) L'anneau $B\left[\frac{1}{b}\right]$ est intégralement clos.
b) Il existe un polynôme unitaire f à coefficients dans A tel que $f(x) \in p$.
c) Soient E le corps obtenu en adjoignant les racines de $f(X)$ à K, A′ la fermeture intégrale de A dans E, B′ l'anneau A′[x]. Soit p′ un idéal maximal de B′ au-dessus de p. Alors la clôture intégrale de $B'_{p'}$ est finie sur $B'_{p'}$. (Utiliser l'exercice précédent.)
d) La clôture intégrale de B'_p est finie sur B'_p. (Utiliser l'exerc. 26.)
e) La clôture intégrale de B_p est finie sur B_p.

29) Soient A un anneau de Nagata intégralement clos, et x un élément du corps des fractions de A, n'appartenant pas à A. Soient B l'anneau A[x] et a, b deux éléments non nuls de A tels que $bx = a$.

a) L'anneau $B\left[\frac{1}{b}\right]$ est intégralement clos.

b) Pour tout idéal maximal $\mathfrak{m}$ de B, la clôture intégrale de $B_{\mathfrak{m}}$ est une $B_{\mathfrak{m}}$-algèbre finie. (Utiliser l'exercice précédent.)
c) La clôture intégrale de B est une B-algèbre finie. (Utiliser l'exerc. 26.)

30) Soit A un anneau de Nagata. Alors toute algèbre de type fini sur A est un anneau de Nagata. (Utiliser les exerc. 21, p. 82 et 29.)

31) Soient A un anneau noethérien intègre et $\overline{A}$ la fermeture intégrale de A dans une extension finie de son corps des fractions. Si A est de dimension au plus 2, alors $\overline{A}$ est un anneau noethérien. (Utiliser l'exerc. 7, p. 79, l'exerc. 14, p. 81 et le théorème de Krull-Akizuki (*cf.* VII, § 2, n° 5).)

32) Soient A un anneau local noethérien intègre et K son corps des fractions. On suppose K de caractéristique p non nulle. On suppose que A est un anneau de Nagata et on note $\hat{A}$ le complété de A. Soient $\mathfrak{p}$ un idéal premier minimal de $\hat{A}$ et L le corps des fractions de $\hat{A}/\mathfrak{p}$. Soient k un corps de représentants faible de A, k' le corps de représentants de $\hat{A}$ contenant l'image de k dans $\hat{A}$ (p. 78, exerc. 9, *a*)). Alors K est séparable sur k si et seulement si L est séparable sur k'. (Remarquer que L est séparable sur K puisque A est un anneau de Nagata. Si K est séparable sur k, prouver que toute dérivation de k' dans L s'étend en une dérivation de L dans L.)

APPENDICE

1) Soit I un ensemble préordonné non vide filtrant à droite et soit $(A_\alpha, \varphi_{\beta\alpha})$ un système inductif d'anneaux relatif à I. Pour chaque indice α dans I, on se donne un idéal $\mathfrak{q}_\alpha$ de A_α. On suppose qu'on a $\varphi_{\beta\alpha}(\mathfrak{q}_\alpha) A_\beta = \mathfrak{q}_\beta$ pour $\beta \geqslant \alpha$. On note A la limite inductive des A_α, et pour $\alpha \in I$, on note $\varphi_\alpha : A_\alpha \to A$ l'homomorphisme canonique. On pose

$$\mathfrak{q} = \varinjlim \mathfrak{q}_\alpha .$$

a) Si pour tout $\alpha \in I$, $\mathfrak{q}_\alpha$ est un idéal maximal de A_α, alors $\mathfrak{q}$ est un idéal maximal de A.
b) Si pour tout $\alpha \in I$, $\mathfrak{q}_\alpha$ est contenu dans le radical de A_α, alors $\mathfrak{q}$ est contenu dans le radical de A.
c) Si pour tout $\alpha \in I$ et tout $\beta \in I$, tels que $\beta \geqslant \alpha$, l'homomorphisme $\varphi_{\beta\alpha}$ est fidèlement plat, alors pour tout $\alpha \in I$, φ_α est fidèlement plat.

Nous supposerons désormais que l'hypothèse de *c*) est vérifiée.
d) Si pour tout $\alpha \in I$, A_α est séparé pour la topologie $\mathfrak{q}_\alpha$-adique, alors A est séparé pour la topologie $\mathfrak{q}$-adique.
e) Si pour tout $\alpha \in I$, A_α est noethérien et si $A/\mathfrak{q}$ est noethérien, alors $(1 + \mathfrak{q})^{-1}A$ est noethérien. (Raisonner comme dans la démonstration de la prop. 1 de l'Appendice en utilisant en outre le résultat suivant, qu'on démontrera :

Soient B un anneau commutatif, $\mathfrak{p}$ un idéal de B, $\hat{B}$ le séparé complété de B pour la topologie $\mathfrak{p}$-adique, et $i : B \to \hat{B}$ l'application canonique. Alors il existe un et un seul homomorphisme d'anneaux $j : (1 + \mathfrak{p})^{-1}B \to \hat{B}$ qui prolonge i. Pour tout idéal maximal $\mathfrak{m}$ de $(1 + \mathfrak{p})^{-1}B$, on a $j(\mathfrak{m})\hat{B} \neq \hat{B}$.)

2) Soient A un anneau local, B un gonflement de A. Si A est séparé (pour la topologie définie par l'idéal maximal $\mathfrak{m}_A$), B est séparé (pour la topologie définie par l'idéal maximal $\mathfrak{m}_B$).

3) Soient k un corps imparfait de caractéristique $p > 0$ et $R = k[T]_{(T)}$. Soit a un élément de k qui n'est pas une puissance p-ième. Montrer que l'anneau $A = R[X]/(X^p - aT^p)$ est local, intègre, et de corps résiduel k. Montrer que l'anneau $B = A[Y]/(Y^p - a)$, qui est un gonflement de A, n'est pas réduit.

4) Soit A un anneau local muni d'une valuation v_A. Soit B un gonflement de A. Montrer que la valuation v_A se prolonge, de manière unique, en une valuation v_B de B, et que les groupes de valeurs $v_A(A)$ et $v_B(B)$ coïncident. Si A est un anneau de valuation discrète, d'uniformisante π, B est aussi un anneau de valuation discrète, dont une uniformisante est l'image de π dans B.

5) Soit A un anneau local, de corps résiduel $\kappa(A)$. Soit B un gonflement de A, de corps résiduel $\kappa(B)$.
a) Si $\kappa(B) = \kappa(A)$, on a A = B.
b) Si $\kappa(B)$ est algébrique sur $\kappa(A)$, la A-algèbre B est entière.
c) Si $\kappa(B)$ est de degré fini sur $\kappa(A)$, B est un A-module libre ayant pour rang le degré de $\kappa(B)$ sur $\kappa(A)$.

6) Soit A un anneau local de corps résiduel *k*. Soit I un ensemble d'indices. Montrer que l'anneau $A]\!(X_i)_{i\in I}[\!$ (*cf.* App., exemple 2) qui est un gonflement de A, a pour corps résiduel l'extension transcendante pure $k((X_i)_{i\in I})$ de *k*.