JACQUES DIXMIER

Sur les algèbres de Weyl

Bulletin de la S. M. F., tome 96 (1968), p. 209-242
<http://www.numdam.org/item?id=BSMF_1968__96__209_0>

Bull. Soc. math. France,
96, 1968, p. 209 à 242.

SUR LES ALGÈBRES DE WEYL

PAR

JACQUES DIXMIER.

Introduction. — Soient k un corps commutatif de caractéristique o, et n un entier $\geqq 0$. On notera $A_n(k)$, ou simplement A_n, l'algèbre associative unifère sur k définie par $2n$ générateurs $p_1, q_1, p_2, q_2, \ldots, p_n, q_n$, et les relations

$$[p_i, q_i] = 1 \qquad (i = 1, 2, \ldots, n),$$
$$[p_i, p_j] = [q_i, q_j] = [p_i, q_j] = 0 \qquad \text{pour} \quad i \neq j.$$

En particulier, $A_0(k) = k$. Suivant une suggestion de SEGAL [11], nous dirons que $A_n(k)$ est l'*algèbre de Weyl d'indice n sur k.* Elle est canoniquement isomorphe à l'algèbre des opérateurs différentiels à coefficients polynomiaux sur k^n.

L'intérêt des algèbres de Weyl s'est accru récemment pour les raisons suivantes. Soit N une algèbre de Lie nilpotente sur $\mathbf{C}$ (corps des nombres complexes). Soit E son algèbre enveloppante. Alors, tout quotient primitif de E est isomorphe à une algèbre de Weyl sur $\mathbf{C}$ (*cf.* [4] pour un résultat plus précis). Ce résultat a été généralisé dans [8] de la manière suivante. Soient N une algèbre de Lie nilpotente sur k, E son algèbre enveloppante, I un idéal bilatère premier de E, Z le centre de E/I (qui est intègre), F le corps des fractions de Z. Alors $(E/I) \otimes_Z F$ est isomorphe à une algèbre de Weyl sur F. (Si I est primitif, et si $k = \mathbf{C}$, on a $Z = F = \mathbf{C}$.) En particulier, soient Z_0 le centre de E, et F_0 le corps des fractions de Z_0. Alors $E \otimes_{Z_0} F_0$ est isomorphe à $A_n(F_0)$ pour un certain n. Comme F_0 est le centre du corps des fractions de E [2], il résulte de [6] que $2n$ est la différence entre la dimension de N et le degré de transcendance de Z_0 sur k; autrement dit, n est le nombre appelé dans [3] défaut de commutativité de N.

D'autres relations entre les algèbres de Lie et les algèbres de Weyl sont démontrées dans [6].

Un certain nombre de propriétés des algèbres de Weyl sont presque immédiates. Les éléments $p_1^{i_1} q_1^{j_1} \ldots p_n^{i_n} q_n^{j_n}$ ($i_1, j_1, \ldots, i_n, j_n$ entiers $\geqq 0$) forment une base sur k de l'espace vectoriel A_n. L'algèbre A_n est intègre, simple, de centre k, noethérienne à gauche et à droite, donc admet un corps des fractions à gauche et à droite. Les seuls éléments inversibles de A_n sont les scalaires. On a $A_n = A_1 \otimes_k A_1 \otimes_k \ldots \otimes_k A_1$ (n facteurs) (*cf.* [4], [6], [7]). Voici quelques propriétés moins immédiates. Toute dérivation de A_n est intérieure [5]. La dimension de Krull de A_n est n [9]. La dimension homologique de A_n est comprise entre n et $2n-1$ [10]. Une certaine dimension définie par I. M. Gelfand et A. A. Kirillov est égale à $2n$ [6]. On trouvera dans [4] quelques résultats sur les représentations irréductibles de A_1, et dans [11] un « lemme de Poincaré » pour A_n.

Le but de ce Mémoire est une étude assez approfondie de A_1 (nous espérons revenir sur A_n plus tard). Nous poserons $p_1 = p$, $q_1 = q$, de sorte que A_1 est engendrée par p et q avec la seule relation $[p, q] = 1$. Voici les principaux résultats obtenus.

1° Toute sous-algèbre commutative maximale de A_1 est intègre de type fini sur k, de degré de transcendance 1 sur k (comme me l'a fait remarquer A. A. Kirillov, ce fait est conséquence facile d'une démonstration de S. A. Amitsur [1]). Il existe des sous-algèbres commutatives maximales de A_1 dont le corps des fractions n'est pas extension transcendante pure de k.

2° Dans l'isomorphisme $A_n(F_0) \to E \otimes_{Z_0} F_0$ rappelé plus haut, les éléments correspondant aux générateurs canoniques de $A_n(F_0)$ n'ont pas de rôle privilégié dans $E \otimes_{Z_0} F_0$. Il est donc intéressant de déterminer les automorphismes de $A_n(F_0)$. Rappelons que toute dérivation de A_1 est intérieure. Comme les seuls éléments inversibles de A_1 sont les scalaires, la propriété analogue pour les automorphismes est, bien entendu, inexacte. Toutefois, on a le résultat suivant. Soient $\lambda \in k$, et n un entier $\geqq 0$; la dérivation $\Delta = \operatorname{ad}\left(\frac{\lambda}{n+1} p^{n+1}\right)$ de A_1 est localement nilpotente, de sorte que $\Phi_{n,\lambda} = \exp \Delta$ est un automorphisme bien défini de A_1, tel que $\Phi_{n,\lambda}(p) = p$, $\Phi_{n,\lambda}(q) = q + \lambda p^n$. On définit de même un automorphisme $\Phi'_{n,\lambda}$ de A_1 tel que $\Phi'_{n,\lambda}(q) = q$, $\Phi'_{n,\lambda}(p) = p + \lambda q^n$. Ceci posé, nous démontrerons que le groupe des automorphismes de A_1 est engendré par les $\Phi_{n,\lambda}$ et les $\Phi'_{n,\lambda}$.

Notations. — On utilisera les notations k, A_1, p, q, $\Phi_{n,\lambda}$, $\Phi'_{n,\lambda}$ de l'introduction. Si k est un corps commutatif, on notera $\bar{k}$ une clôture algébrique de k. Si A est une algèbre sur k, on notera $\bar{A}$ l'algèbre $A \otimes_k \bar{k}$ sur $\bar{k}$. Si $x \in A$, on notera $\operatorname{ad} x$, ou $\operatorname{ad}_A x$, l'application $y \mapsto [x, y]$ de A dans A. Les lettres X, Y désigneront des indéterminées. On notera $\mathbf{Q}$ le corps des nombres rationnels, $\mathbf{Z}$ l'anneau des entiers rationnels.

1. Quelques lemmes sur les polynômes.

1.1. Si $f = \sum \alpha_{ij} X^i Y^j \in k[X, Y]$, on notera $E(f)$ l'ensemble des couples (i, j) tels que $\alpha_{ij} \neq 0$. Si ρ, σ sont deux nombres réels, on posera

$$v_{\rho,\sigma}(f) = \sup_{(i,j) \in E(f)} (\rho i + \sigma j),$$

[on convient que $v_{\rho,\sigma}(0) = -\infty$]. On notera $E(f, \rho, \sigma)$ l'ensemble des couples $(i, j) \in E(f)$ tels que $\rho i + \sigma j = v_{\rho,\sigma}(f)$; si $f \neq 0$, on a $E(f, \rho, \sigma) \neq \emptyset$. Si $E(f) = E(f, \rho, \sigma)$, on dira que f est (ρ, σ)-homogène de (ρ, σ)-degré $v_{\rho,\sigma}(f)$.

1.2. Lemme. — *Soient* $f = \sum \alpha_{ij} X^i Y^j$, $g = \sum \beta_{ij} X^i Y^j$, *et* ρ, σ *des nombres réels. Posons*

$$h = fg = \sum \gamma_{ij} X^i Y^j,$$

$$f_1 = \sum_{(i,j) \in E(f, \rho, \sigma)} \alpha_{ij} X^i Y^j,$$

$$g_1 = \sum_{(i,j) \in E(g, \rho, \sigma)} \beta_{ij} X^i Y^j,$$

$$h_1 = \sum_{(i,j) \in E(h, \rho, \sigma)} \gamma_{ij} X^i Y^j.$$

Alors $h_1 = f_1 g_1$ *et* $v_{\rho,\sigma}(h) = v_{\rho,\sigma}(f) + v_{\rho,\sigma}(g)$.

La démonstration est laissée au lecteur.

1.3. Lemme. — *Soit* $f \in k[X, Y]$ *un polynôme* (ρ, σ)*-homogène de* (ρ, σ)*-degré* v.

(i) *On a* $\rho X \dfrac{\partial f}{\partial X} + \sigma Y \dfrac{\partial f}{\partial Y} = vf$.

(ii) *Si* ρ *et* σ *sont linéairement indépendants sur* $\mathbf{Q}$, f *est un monôme.*

Démonstration. — Soit $g = X^i Y^j$ avec $\rho i + \sigma j = v$. On a

$$\rho X \frac{\partial g}{\partial X} + \sigma Y \frac{\partial g}{\partial Y} = \rho X i X^{i-1} Y^j + \sigma Y j X^i Y^{j-1} = (\rho i + \sigma j)\, g,$$

d'où (i).

Si $(i, j) \in E(f)$ et $(i', j') \in E(f)$, on a $\rho i + \sigma j = \rho i' + \sigma j' = v$, donc $\rho(i - i') = \sigma(j' - j)$. Sous les hypothèses de (ii), on en conclut que f est un monôme.

1.4. LEMME. — *Soient $f, g \in k[X, Y]$ des polynômes (ρ, σ)-homogènes, de (ρ, σ)-degrés v, w.*

(i) *On a*

$$\sigma Y\left(\frac{\partial f}{\partial X}\frac{\partial g}{\partial Y}-\frac{\partial f}{\partial Y}\frac{\partial g}{\partial X}\right)=wg\frac{\partial f}{\partial X}-vf\frac{\partial g}{\partial X}.$$

Si de plus v et w sont des entiers, on a

$$\sigma Y\left(\frac{\partial f}{\partial X}\frac{\partial g}{\partial Y}-\frac{\partial f}{\partial Y}\frac{\partial g}{\partial X}\right)=f^{-w+1}g^{v+1}\frac{\partial}{\partial X}(g^{-v}f^{w}).$$

(ii) *On a*

$$-\rho X\left(\frac{\partial f}{\partial X}\frac{\partial g}{\partial Y}-\frac{\partial f}{\partial Y}\frac{\partial g}{\partial X}\right)=wg\frac{\partial f}{\partial Y}-vf\frac{\partial g}{\partial Y}.$$

Si de plus v et w sont entiers, on a

$$-\rho X\left(\frac{\partial f}{\partial X}\frac{\partial g}{\partial Y}-\frac{\partial f}{\partial Y}\frac{\partial g}{\partial X}\right)=f^{-w+1}g^{v+1}\frac{\partial}{\partial Y}(g^{-v}f^{w}).$$

Démonstration. — Prouvons par exemple (i). D'après le lemme 1.3 (i), on a

$$\sigma Y\left(\frac{\partial f}{\partial X}\frac{\partial g}{\partial Y}-\frac{\partial f}{\partial Y}\frac{\partial g}{\partial X}\right)$$
$$=\frac{\partial f}{\partial X}\left(wg-\rho X\frac{\partial g}{\partial X}\right)-\left(vf-\rho X\frac{\partial f}{\partial X}\right)\frac{\partial g}{\partial X}=wg\frac{\partial f}{\partial X}-vf\frac{\partial g}{\partial X}.$$

Supposons v et w entiers. Alors

$$\frac{\partial}{\partial X}(g^{-v}f^{w})=g^{-v-1}f^{w-1}\left(-v\frac{\partial g}{\partial X}f+gw\frac{\partial f}{\partial X}\right),$$

d'où, compte tenu de ce qui précède,

$$\sigma Y\left(\frac{\partial f}{\partial X}\frac{\partial g}{\partial Y}-\frac{\partial f}{\partial Y}\frac{\partial g}{\partial X}\right)=f^{-w+1}g^{v+1}\frac{\partial}{\partial X}(g^{-v}f^{w}).$$

2. Filtrations de A_1.

2.1. Le lemme suivant se trouve dans [7], théorème XIV.

LEMME. — *Soient i, j, l, m des entiers ≥ 0. On a*

$$(p^i q^j)(p^l q^m)=p^{i+l}q^{j+m}-jlp^{i+l-1}q^{j+m-1}+\frac{1}{2!}j(j-1)l(l-1)p^{i+l-2}q^{j+m-2}$$
$$-\frac{1}{3!}j(j-1)(j-2)l(l-1)(l-2)p^{i+l-3}q^{j+m-3}+\ldots.$$

Démonstration. — En simplifiant par p^i à gauche et q^m à droite, on se ramène aussitôt au cas où $i = m = 0$. Admettons la formule

$$q^j p^l = p^l q^j + \sum_{r \geq 1} (-1)^r r! \binom{j}{r} \binom{l}{r} p^{l-r} q^{j-r}.$$

Alors

$$\begin{aligned}[q^{j+1}, p^l] &= [q, p^l] q^j + q [q^j, p^l] \\ &= -l p^{l-1} q^j + q \sum_{r \geq 1} (-1)^r r! \binom{j}{r} \binom{l}{r} p^{l-r} q^{j-r} \\ &= -l p^{l-1} q^j + \sum_{r \geq 1} (-1)^r r! \binom{j}{r} \binom{l}{r} p^{l-r} q^{j-r+1} \\ &\quad - \sum_{r \geq 1} (-1)^r r! \binom{j}{r} \binom{l}{r} (l-r) p^{l-r-1} q^{j-r},\end{aligned}$$

d'où

$$\begin{aligned}q^{j+1} p^l &= p^l q^{j+1} - l p^{l-1} q^j - j l p^{l-1} q^j + \sum_{r \geq 2} (-1)^r r! \binom{j}{r} \binom{l}{r} p^{l-r} q^{j+1-r} \\ &\quad + \sum_{r \geq 2} (-1)^r (r-1)! \binom{j}{r-1} \binom{l}{r-1} (l-r+1) p^{l-r} q^{j+1-r} \\ &= p^l q^{j+1} - (j+1) l p^{l-1} q^j + \sum_{r \geq 2} (-1)^r r! \, \alpha_r p^{l-r} q^{j+1-r},\end{aligned}$$

avec

$$\alpha_r = \binom{j}{r} \binom{l}{r} + \frac{(r-1)!}{r!} \binom{j}{r-1} \binom{l}{r} \frac{r!}{(r-1)!} = \binom{j+1}{r} \binom{l}{r}.$$

La formule est donc établie pour $q^{j+1} p^l$, et l'on passe de même au cas de $q^j p^{l+1}$.

2.2. Lemme. — *Soient $x, y, z \in A_1$ tels que $z = xy$. Soient*

$$x = \sum \alpha_{ij} p^i q^j, \qquad y = \sum \beta_{ij} p^i q^j, \qquad z = \sum \gamma_{ij} p^i q^j.$$

Posons

$$f = \sum \alpha_{ij} X^i Y^j, \qquad g = \sum \beta_{ij} X^i Y^j, \qquad h = \sum \gamma_{ij} X^i Y^j.$$

Alors

$$h = fg - \frac{\partial f}{\partial Y} \frac{\partial g}{\partial X} + \frac{1}{2!} \frac{\partial^2 f}{\partial Y^2} \frac{\partial^2 g}{\partial X^2} - \frac{1}{3!} \frac{\partial^3 f}{\partial Y^3} \frac{\partial^3 g}{\partial X^3} + \dots$$

Démonstration. — Il suffit de le prouver pour $x = p^i q^j$, $y = p^l q^m$, et alors cela résulte du lemme 2.1.

2.3. Soient $x = \sum \alpha_{ij} p^i q^j \in A_1$, et ρ, σ des nombres réels. Par analogie avec 1.1, on définit de manière évidente $E(x)$, $v_{\rho,\sigma}(x)$, $\mathrm{E}(x, \rho, \sigma)$. Le polynôme $\sum_{(i,j) \in E(x, \rho, \sigma)} \alpha_{ij} X^i Y^j$ sera appelé le polynôme (ρ, σ)-associé à x.

2.4. Lemme. — *Soient $x, y \in A_1$ et ρ, σ des nombres réels tels que $\rho + \sigma > 0$.*

(i) *Le polynôme (ρ, σ)-associé à xy est le produit des polynômes (ρ, σ)-associés à x et y.*

(ii) $v_{\rho,\sigma}(xy) = v_{\rho,\sigma}(x) + v_{\rho,\sigma}(y)$.

Démonstration. — Il suffit d'envisager le cas où $x \neq 0$, $y \neq 0$. Posons $z = xy$ et introduisons les notations f, g, h du lemme 2.2. On a

$$v_{\rho,\sigma}(x) = v_{\rho,\sigma}(f), \qquad v_{\rho,\sigma}(y) = v_{\rho,\sigma}(g), \qquad v_{\rho,\sigma}(z) = v_{\rho,\sigma}(h).$$

D'autre part,

$$v_{\rho,\sigma}\left(\frac{\partial f}{\partial y}\right) \leq v_{\rho,\sigma}(f) - \sigma, \qquad v_{\rho,\sigma}\left(\frac{\partial g}{\partial X}\right) \leq v_{\rho,\sigma}(g) - \rho,$$

donc, compte tenu du lemme 1.2,

$$v_{\rho,\sigma}\left(\frac{\partial^p f}{\partial Y^p} \frac{\partial^p g}{\partial X^p}\right) \leq v_{\rho,\sigma}(f) + v_{\rho,\sigma}(g) - \rho - \sigma$$

pour $p \geq 1$. Comme $\rho + \sigma > 0$, le lemme 2.2 prouve que $h = fg + l$ avec $v_{\rho,\sigma}(l) < v_{\rho,\sigma}(f) + v_{\rho,\sigma}(g)$. Il suffit alors d'appliquer le lemme 1.2.

2.5. Proposition. — *Soit x un élément non scalaire de A_1. L'application $P \mapsto P(x)$ de $k[X]$ dans A_1 est un isomorphisme de $k[X]$ sur $k[x]$.*

Démonstration. — On a $v_{1,1}(x) > 0$ et $v_{1,1}(x^n) = n v_{1,1}(x)$, donc $1, x, x^2, \ldots$ sont linéairement indépendants sur k.

2.6. Lemme. — *Soient $x, y, z \in A_1$, tels que $z = [x, y]$. Soient*

$$x = \sum \alpha_{ij} p^i q^j, \qquad y = \sum \beta_{ij} p^i q^j, \qquad z = \sum \gamma_{ij} p^i q^j.$$

Posons

$$f = \sum \alpha_{ij} X^i Y^j, \qquad g = \sum \beta_{ij} X^i Y^j, \qquad h = \sum \gamma_{ij} X^i Y^j.$$

Alors

$$h = \frac{\partial f}{\partial X} \frac{\partial g}{\partial Y} - \frac{\partial f}{\partial Y} \frac{\partial g}{\partial X} - \frac{1}{2!}\left(\frac{\partial^2 f}{\partial X^2} \frac{\partial^2 g}{\partial Y^2} - \frac{\partial^2 f}{\partial Y^2} \frac{\partial^2 g}{\partial X^2}\right)$$
$$+ \frac{1}{3!}\left(\frac{\partial^3 f}{\partial X^3} \frac{\partial^3 g}{\partial Y^3} - \frac{\partial^3 f}{\partial Y^3} \frac{\partial^3 g}{\partial X^3}\right) - \ldots$$

Démonstration. — Cela résulte du lemme 2.2.

2.7. LEMME. — *Soient x et y des éléments non nuls de A_1, ρ et σ des nombres réels tels que $\rho+\sigma>0$. Posons $v=v_{\rho,\sigma}(x)$, $w=v_{\rho,\sigma}(y)$. Soient f_1 et g_1 les polynômes (ρ, σ)-associés à x et y.*

(i) *Il existe un couple (t, u) d'éléments de A_1, et un seul, possédant les propriétés suivantes :*

(*a*) $[x, y]=t+u$;

(*b*) $E(t)=E(t, \rho, \sigma)$ *et* $v_{\rho,\sigma}(t)=v+w-(\rho+\sigma)$;

(*c*) $v_{\rho,\sigma}(u)<v+w-(\rho+\sigma)$.

(ii) *Les conditions suivantes sont équivalentes* :

(ii_1) $t=0$;

(ii_2) $\dfrac{\partial f_1}{\partial X}\dfrac{\partial g_1}{\partial Y}-\dfrac{\partial f_1}{\partial Y}\dfrac{\partial g_1}{\partial X}=0.$

Si v et w sont des entiers, ces conditions sont encore équivalentes à la suivante :

(ii_3) g_1^v *est proportionnel à* f_1^w.

(iii) *Si $t\neq 0$, le polynôme (ρ, σ)-associé à $[x, y]$ est* $\dfrac{\partial f_1}{\partial X}\dfrac{\partial g_1}{\partial Y}-\dfrac{\partial f_1}{\partial Y}\dfrac{\partial g_1}{\partial X}$.

Démonstration. — Introduisons les notations du lemme 2.6. Alors h est la somme de $\dfrac{\partial f_1}{\partial X}\dfrac{\partial g_1}{\partial Y}-\dfrac{\partial f^1}{\partial Y}\dfrac{\partial g_1}{\partial X}$, qui est (ρ, σ)-homogène de (ρ, σ)-degré $v+w-(\rho+\sigma)$, et d'un polynôme h^* tel que

$$v_{\rho,\sigma}(h^*)<v+w-(\rho+\sigma).$$

Ceci prouve (i), (iii), et l'équivalence $(\text{ii}_1)\Leftrightarrow(\text{ii}_2)$. Si v et w sont des entiers, l'équivalence $(\text{ii}_2)\Leftrightarrow(\text{ii}_3)$ résulte du lemme 1.4.

3. **Graduation de A_1.**

3.1. Quand (ρ, σ) tend vers $(1, -1)$ ou $(-1, 1)$ (avec $\rho+\sigma>0$), la filtration $v_{\rho,\sigma}$ de A_1 tend vers deux filtrations « opposées ». En fait, la situation limite est plus précisément une graduation, comme on va le voir. Pour $n\in\mathbf{Z}$, posons

$$A^n=\sum_{i-j=n} kp^iq^j.$$

Alors A_1 est somme directe des A^n, et il résulte du lemme 2.1 que $A^nA^{n'}\subset A^{n+n'}$. Autrement dit, A_1 est une algèbre graduée par les A^n.

3.2. On a

$$(pq)\,p=p(qp-pq)+p^2q=-p+p^2q=p(pq-1),$$

donc, si $f \in k[X]$,

$$f(pq)\,p = pf(pq - 1),$$

et par suite, si n est un entier $\geqq 0$,

$$f(pq)\,p^n = p^n f(pq - n). \tag{1}$$

De même

$$q^n f(pq) = f(pq - n)\,q^n. \tag{2}$$

En particulier,

$$p^n q^n = p^{n-1}(pq)\,q^{n-1} = p^{n-1}q^{n-1}(pq + n - 1),$$

d'où par récurrence

$$p^n q^n = pq\,(pq + 1)\,(pq + 2)\ldots(pq + n - 1), \tag{3}$$

(ceci est le théorème XVI de [7]). On déduit aussitôt de là que

$$A^0 = k[pq].$$

3.3. Pour n entier $\geqq 0$, on a

$$A^n = p^n A^0 = p^n k[pq],$$
$$A^{-n} = A^0 q^n = k[pq]\,q^n.$$

Si f, $g \in k[X]$, il résulte de (1) et (2) que

$$p^n f(pq)\,p^{n'} g(pq) = p^{n+n'} f(pq - n')\,g(pq),$$
$$f(pq)\,q^n g(pq)\,q^{n'} = f(pq)\,g(pq - n)\,q^{n+n'}.$$

4. Commutant d'un élément.

4.1. Si A est une algèbre sur k, et si $x \in A$, on notera $C(x; A)$ ou simplement $C(x)$ le commutant de x dans A.

4.2. Théorème. — *Soit x un élément non scalaire de A_1. Le commutant de x dans A_1 est commutatif et est un module libre de type fini sur $k[x]$.*

Démonstration. — Celle de [1], théorème 1, s'applique mot pour mot (bien que l'algèbre considérée dans [1] soit légèrement différente de A_1).

4.3. Corollaire. — *Soit* B *une sous-algèbre de A_1. Les conditions suivantes sont équivalentes :*

(i) *B est une sous-algèbre commutative maximale de A_1;*
(ii) *il existe un élément non scalaire x de A_1 tel que $B = C(x)$;*
(iii) *$B \neq k$, et, pour tout élément non scalaire y de B, on a $B = C(y)$.*

Démonstration.

(i) $\Rightarrow$ (iii). Supposons B commutative maximale. Il est clair que $B \neq k$. On a évidemment $B \subset C(y)$, d'où $B = C(y)$ d'après la maximalité de B et le théorème 4.2.

(iii) $\Rightarrow$ (ii). Évident.

(ii) $\Rightarrow$ (i). Supposons qu'il existe un élément non scalaire x de A_1 tel que $B = C(x)$. Alors B est commutative (th. 4.2), et $x \in B$. Si $y \in A_1$ commute à B, y commute à x, donc $y \in B$. Donc B est une sous-algèbre commutative maximale de A_1.

4.4. Corollaire. — *Soient B une sous-algèbre de A_1 distincte de k, B' son commutant dans A_1.*

(i) *Si B est non commutative, $B' = k$.*

(ii) *Si B est commutative, B' est une sous-algèbre commutative maximale de A_1.*

Démonstration. — (i) résulte aussitôt du théorème 4.2.

Supposons B commutative. On a $B \subset B'$, donc B' contient le commutant B'' de B' dans A_1. Comme $B \neq k$, B' est commutative d'après le théorème 4.2, donc $B' \subset B''$ et finalement $B' = B''$. Donc B' est une sous-algèbre commutative maximale de A_1.

4.5. Corollaire. — *Si x et y sont des éléments non scalaires permutables de A_1, on a $C(x) = C(y)$.*

Démonstration. — Comme $y \in C(x)$, cela résulte du corollaire 4.3.

4.6. Corollaire. — *Soient C une sous-algèbre commutative maximale de A_1, y un élément de A_1, et $P \in k[X]$ un polynôme non scalaire. Si $P(y) \in C$, on a $y \in C$.*

Démonstration. — Si $y \in k$, c'est évident. Si $y \notin k$, on a $P(y) \notin k$ (prop. 2.5), donc $y \in C(P(y)) = C$ d'après le corollaire 4.3.

4.7. Corollaire. — *Dans A_1, l'intersection de deux sous-algèbres commutatives maximales distinctes est réduite à k.*

Démonstration. — Si deux sous-algèbres commutatives maximales B_1 et B_2 de A_1 ont en commun un élément non scalaire x, on a $B_1 = C(x) = B_2$ d'après le corollaire 4.3.

4.8. Corollaire. — *Soit N une algèbre de Lie nilpotente sur k, de défaut de commutativité égal à 1. Soient E son algèbre enveloppante, x un élément non central de E. Alors le commutant $C(x; E)$ est commutatif.*

Démonstration. — D'après ce qu'on a rappelé dans l'introduction, E se plonge dans une algèbre $A_1(F)$, où F désigne le corps des fractions du centre de E. Il suffit alors d'appliquer le théorème 4.2.

4.9. Il serait maintenant facile de démontrer pour E des propriétés analogues à celles de 4.3-4.7 pour A_1. D'autre part, soient L l'algèbre de Lie résoluble non commutative de dimension 2 sur k, et F son algèbre enveloppante. Alors F est isomorphe à la sous-algèbre de A_1 engendrée par p et pq, donc le théorème 4.2 et ses corollaires 4.3-4.7 restent valables en remplaçant A_1 par F.

5. Sous-algèbres commutatives.

5.1. Théorème. — *Soit B une sous-algèbre commutative de A_1, distincte de k. Alors B est intègre, de type fini sur k, de degré de transcendance* 1 *sur k. Pour toute sous-algèbre B_1 de B distincte de k, B est un module de type fini sur B_1.*

Démonstration. — Choisissons un élément non scalaire x de B_1. D'après 4.2, l'algèbre commutative $C(x)$ est de type fini sur k et est un module de type fini sur $k[x]$. Comme l'anneau $k[x]$ est noethérien, B, qui est contenu dans $C(x)$, est un module de type fini sur $k[x]$ (et *a fortiori* sur B_1). Il résulte de là que l'algèbre B est de type fini sur k. Tout élément de $C(x)$ est algébrique sur $k[x]$, donc B est de degré de transcendance 1 sur k.

5.2. La structure précise des sous-algèbres commutatives maximales de A_1 ne semble pas facile à préciser davantage. Nous pouvons seulement donner les propositions 5.2, 5.3 et 5.5 ci-dessous.

Proposition. — *Soit x un élément de A_1. Soient $\rho > 0$, $\sigma > 0$ et $f(X, Y)$ le polynôme (ρ, σ)-associé à x. On suppose qu'il n'existe aucun polynôme $f_1(X, Y)$ et aucun entier $n > 1$ tel que f soit proportionnel à f_1^n. Alors $C(x) = k[x]$.*

Démonstration. — Il existe des entiers $\rho' > 0$, $\sigma' > 0$ tels que f soit le polynôme (ρ', σ')-associé à x : c'est évident si ρ et σ sont linéairement dépendants sur $\mathbf{Q}$, et sinon, cela résulte facilement du lemme 1.3 (ii).

On supposera donc désormais que ρ et σ sont entiers. Soient $y \in C(x)$, et g le polynôme (ρ, σ)-associé à y. Montrons, par récurrence sur $v_{\rho,\sigma}(y)$, que $y \in k[x]$. C'est évident si $v_{\rho,\sigma}(y) = 0$. Supposons-le prouvé pour $v_{\rho,\sigma}(y) < w$, et envisageons le cas où $v_{\rho,\sigma}(y) = w > 0$. Posons $v = v_{\rho,\sigma}(x)$. On a $v > 0$ (sinon f serait une constante, et l'hypothèse faite sur f ne serait pas vérifiée). D'après le lemme 2.7, f^w est proportionnel à g^v. Soient v' et w' les quotient de v et w par leur p. g. c. d. Alors $f^{w'}$ est proportionnel à $g^{v'}$. En utilisant les décompositions de f et g en facteurs irréductibles, on en déduit l'existence d'un polynôme $h(X, Y)$ tel que f soit proportionnel à $h^{v'}$. D'après l'hypothèse faite sur f, on a $v' = 1$. Donc g est proportionnel à $f^{w'}$. Donc il existe $\lambda \in k$ tel que

$v_{\rho,\sigma}(y-\lambda x^{w'}) < v_{\rho,\sigma}(y)$. On a $y-\lambda x^{w'} \in C(x)$. D'après l'hypothèse de récurrence, $y-\lambda x^{w'} \in k[x]$, d'où $y \in k[x]$.

5.3. On a $C(p)=k[p]$, $C(q)=k[q]$, soit d'après la proposition 5.2, soit par un raisonnement direct immédiat. D'après le corollaire 4.5, on en déduit que $C(p^n)=k[p]$, $C(q^n)=k[q]$ pour tout entier $n>0$. Voici maintenant un commutant moins évident.

PROPOSITION. — *Soient i et j des entiers tels que $i \geq j > 0$. Soit d leur p. g. c. d. et posons $i=i'd$, $j=j'd$.*

(i) *Si $i=j$, on a $C(p^i q^j)=k[pq]$.*

(ii) *Si $i \neq j$ et $i' \neq j'+1$, on a $C(p^i q^j)=k[p^i q^j]$.*

(iii) *Si $i'=j'+1$, on a*

$$p^i q^j = (p(pq+d-1)(pq+2d-1)\dots(pq+j'd-1))^d,$$
$$C(p^i q^j) = k[p(pq+d-1)(pq+2d-1)\dots(pq+j'd-1)].$$

Démonstration. — On a $[pq, p]=-p$, $[pq, q]=q$, donc

$$[pq, p^l q^m] = (m-l)p^l q^m, \tag{4}$$

d'où

$$C(pq)=\sum_{l\geq 0} kp^l q^l = k[pq] \quad (cf.\ 3.2).$$

Compte tenu du corollaire 4.5, on en déduit que $C(p^l q^l)=k[pq]$ pour tout entier $l>0$.

Supposons désormais $i>j>0$. Puisque A_1 est graduée par les A^v et que $p^i q^j \in A^{i-j}$, $C(p^i q^j)$ est la somme de ses intersections avec les A^v. Soit y un élément non nul de $C(p^i q^j) \cap A^v$. Soient f et g les polynômes $(1, 1)$-associés à $p^i q^j$ et y. On a $f(X, Y)=X^i Y^j$. D'après le lemme 2.7, une puissance de g est proportionnelle à une puissance de $X^i Y^j$. Donc il existe des entiers m, n tels que $m>n>0$ et que $g(X, Y)$ soit proportionnel à $X^m Y^n$. Ceci prouve que $v>0$. Donc il existe un polynôme non nul $h \in k[X]$ tel que $y=p^v h(pq)$. D'après (3), on a

$$p^i q^j = p^{i-j} pq(pq+1)(pq+2)\dots(pq+j-1).$$

D'après 3.3, le fait que y commute avec $p^i q^j$ s'écrit donc

$$\begin{aligned}&(pq-v)(pq+1-v)\dots(pq+j-1-v)h(pq)\\&=h(pq-(i-j))pq(pq+1)\dots(pq+j-1)\end{aligned}$$

ou

$$\begin{aligned}&h(X)(X-v)(X-v+1)\dots(X-v+j-1)\\&=h(X-(i-j))X(X+1)\dots(X+j-1).\end{aligned}$$

Pour tout $\lambda \in k$, soit $\mu(\lambda)$ la multiplicité de λ comme zéro de $h(X)$. L'égalité précédente entraîne, en notant δ_λ la fonction caractéristique de $\{\lambda\}$ dans k,

$$(5) \qquad \begin{aligned} &\mu(\lambda) - \mu(\lambda - (i-j)) \\ &= (\delta_0 + \delta_{-1} + \ldots + \delta_{-(j-1)} - \delta_v - \delta_{v-1} - \ldots - \delta_{v-(j-1)})(\lambda) \end{aligned}$$

quel que soit λ dans k. Comme μ est nulle sauf pour un nombre fini de valeurs de λ, ceci prouve (en se plaçant dans une clôture algébrique de k) que h est déterminé à une constante multiplicative près, donc que $\dim_k(C(p^i q^j) \cap A^v) = 1$.

Pour tout $a \in \mathbf{Z}$, soit Γ_a la classe de congruence modulo $i-j$ de a. Alors

$$\sum_{\lambda \in \Gamma_a} \mu(\lambda) = \sum_{\lambda \in \Gamma_a} \mu(\lambda - (i-j)).$$

Donc (5) entraîne

$$(6) \qquad \begin{aligned} &\operatorname{Card}(\Gamma_a \cap \{0, -1, -2, \ldots, -(j-1)\}) \\ &= \operatorname{Card}(\Gamma_a \cap \{v, v-1, v-2, \ldots, v-(j-1)\}). \end{aligned}$$

Or il est clair que

$$(7) \qquad \begin{aligned} &\operatorname{Card}(\Gamma_a \cap \{0, -1, -2, \ldots, -(j-1)\}) \\ &> \operatorname{Card}(\Gamma_{a+1} \cap \{0, -1, -2, \ldots, -(j-1)\}) \\ &\Leftrightarrow \quad 0 \in \Gamma_a \quad \text{et} \quad -j \notin \Gamma_a, \end{aligned}$$

et

$$(8) \qquad \begin{aligned} &\operatorname{Card}(\Gamma_a \cap \{v, v-1, \ldots, v-(j-1)\}) \\ &> \operatorname{Card}(\Gamma_{a+1} \cap \{v, v-1, \ldots, v-(j-1)\}) \\ &\Leftrightarrow \quad v \in \Gamma_a \quad \text{et} \quad v-j \notin \Gamma_a. \end{aligned}$$

Supposons d'abord j non divisible par $i-j$. Alors

$$0 \in \Gamma_a \Rightarrow -j \notin \Gamma_a, \qquad v \in \Gamma_a \Rightarrow v-j \notin \Gamma_a,$$

donc (7) et (8) entraînent

$$\begin{aligned} &\operatorname{Card}(\Gamma_a \cap \{0, -1, -2, \ldots, -(j-1)\}) \\ &> \operatorname{Card}(\Gamma_{a+1} \cap \{0, -1, -2, \ldots, -(j-1)\}) \quad \Leftrightarrow \quad 0 \in \Gamma_a, \end{aligned}$$

et

$$\begin{aligned} &\operatorname{Card}(\Gamma_a \cap \{v, v-1, \ldots, v-(j-1)\}) \\ &> \operatorname{Card}(\Gamma_{a+1} \cap \{v, v-1, \ldots, v-(j-1)\}) \quad \Leftrightarrow \quad v \in \Gamma_a. \end{aligned}$$

D'après (6), on a donc

$$0 \in \Gamma_a \quad \Leftrightarrow \quad v \in \Gamma_a,$$

donc v est divisible par $i-j$. Comme $(p^i q^j)^{v/(i-j)} \in C(p^i q^j) \cap A^v$ et que $\dim(C(p^i q^j) \cap A^v) = 1$, on a $C(p^i q^j) \cap A^v = k(p^i q^j)^{v/(i-j)}$. Donc $C(p^i q^j) \subset k[p^i q^j]$ et finalement $C(p^i q^j) = k[p^i q^j]$.

Supposons maintenant j divisible par $i-j$. Alors $d = i - j$, donc $i' = j' + 1$. Par suite,

$$\begin{aligned}
p^i q^j &= p^d p^{dj'} q^{dj'} \\
&= p^d pq(pq+1)(pq+2)\dots(pq+dj'-1) \quad \text{d'après (3)} \\
&= p^d pq(pq+d)(pq+2d)\dots(pq+(j'-1)d) \\
&\quad .(pq+1)(pq+d+1)(pq+2d+1)\dots(pq+(j'-1)d+1) \\
&\quad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\
&\quad .(pq+d-1)(pq+2d-1)(pq+3d-1)\dots(pq+j'd-1) \\
&= (p(pq+d-1)(pq+2d-1)\dots(pq+j'd-1))^d \quad \text{d'après (1)}.
\end{aligned}$$

Posons $x = p(pq+d-1)(pq+2d-1)\dots(pq+j'd-1)$. Le polynôme $(1, 1)$-associé à x est $X^{j'+1} Y^{j'}$. D'après la proposition 5.2, on a $C(x) = k[x]$. D'autre part, $C(p^i q^j) = C(x^d) = C(x)$ d'après le corollaire 4.5.

5.4. Lemme. — *Soient u et v des éléments d'une algèbre associative sur k, et $a = u^3 + 3(uv + vu)$, $b = u^2 + 4v$. Soient $v' = [u, v]$, $v'' = [u, v']$. On suppose que*

$$v'' = -12v^2. \tag{9}$$

Alors on a

$$a^2 - b^3 = 2u[v, v'] + v'^2 + 8v^3. \tag{10}$$

Démonstration. — On a

$$\begin{aligned}
a^2 - b^3 &= u^6 + 3u^4 v + 3u^3 vu + 3uvu^3 \\
&\quad + 9uvuv + 9uv^2 u + 3vu^4 + 9vu^2 v + 9vuvu \\
&\quad -(u^6 + 4u^4 v + 4u^2 vu^2 + 16u^2 v^2 + 4vu^4 + 16vu^2 v + 16v^2 u^2 + 64v^3) \\
&= c + d,
\end{aligned}$$

avec

$$\begin{aligned}
c &= -u^4 v + 3u^3 vu + 3uvu^3 - vu^4 - 4u^2 vu^2, \\
d &= 9uvuv + 9uv^2 u - 7vu^2 v + 9vuvu - 16u^2 v^2 - 16v^2 u^2 - 64v^3.
\end{aligned}$$

Or

$$\begin{aligned}
u^3 vu &= u^4 v - u^3 v', \\
u^2 vu^2 &= u^3 vu - u^2 v' u = u^4 v - u^3 v' - u^2 v' u, \\
uvu^3 &= u^2 vu^2 - uv' u^2 = u^4 v - u^3 v' - u^2 v' u - uv' u^2, \\
vu^4 &= uvu^3 - v' u^3 = u^4 v - u^3 v' - u^2 v' u - uv' u^2 - v' u^3,
\end{aligned}$$

d'où

$$c = -u^3v' + 2u^2v'u - 2uv'u^2 + v'u^3.$$

Or

$$\begin{aligned} u^2v'u &= u^3v' - u^2v'', \\ uv'u^2 &= u^2v'u - uv''u = u^3v' - u^2v'' - uv''u, \\ v'u^3 &= uv'u^2 - v''u^2 = u^3v' - u^2v'' - uv''u - v''u^2, \end{aligned}$$

d'où

$$\begin{aligned} c &= -u^2v'' + uv''u - v''u^2 = -u[u, v''] - v''u^2 \\ &= 12u[u, v^2] + 12v^2u^2 = 12u(vv' + v'v) + 12v^2u^2. \end{aligned}$$

Alors

$$a^2 - b^3 = c + d = 12u(vv' + v'v) + e - 64v^3,$$

avec $e = 9uvuv + 9uv^2u - 7vu^2v + 9vuvu - 16u^2v^2 - 4v^2u^2$.

Or

$$\begin{aligned} vuvu &= v^2u^2 + vv'u, \\ uv^2u &= vuvu + v'vu = v^2u^2 + vv'u + v'vu, \\ vu^2v &= vuvu + vuv' = v^2u^2 + vv'u + vuv', \\ uvuv &= uv^2u + uvv' = v^2u^2 + vv'u + v'vu + uvv', \\ u^2v^2 &= uvuv + uv'v = v^2u^2 + vv'u + v'vu + uvv' + vu'v, \end{aligned}$$

d'où

$$\begin{aligned} e = {} & 4vv'u + 2v'vu - 7vuv' - 7uvv' - 16uv'v \\ = {} & 4uvv' - 4(v'^2 + vv'') + 2uv'v - 2(v'^2 + v''v) \\ & - 7uvv' + 7v'^2 - 7uvv' - 16uv'v \\ = {} & -10uvv' - 14uv'v + v'^2 - 4vv'' - 2v''v. \end{aligned}$$

Donc

$$\begin{aligned} a^2 - b^3 &= 2uvv' - 2uv'v + v'^2 - 4vv'' - 2v''v - 64v^3 \\ &= 2u[v, v'] + v'^2 + 48v^3 + 24v^3 - 64v^3 \\ &= 2u[v, v'] + v'^2 + 8v^3. \end{aligned}$$

5.5. Proposition. — *Il existe dans A_1 une sous-algèbre commutative maximale dont le corps des fractions n'est pas extension transcendante pure de k.*

Démonstration. — Soit $\alpha \in k$. Posons $u = p^3 + q^2 + \alpha$, $v = \frac{1}{2}p$. On a

$$[u, v] = \left[q^2, \frac{1}{2}p\right] = -q,$$

$$[u, [u, v]] = [p^3, -q] = -3p^2 = -12v^2.$$

Soient $x = u^2 + 4v$, $y = u^3 + 3(uv + vu)$. D'après le lemme 5.4, on a

$$y^2 - x^3 = 2(p^3 + q^2 + \alpha)\left[\frac{1}{2}p, -q\right] + q^2 + p^3 = -\alpha.$$

Donc y^2 commute à x, et par suite x et y sont permutables (cor. 4.5). Soit $D = C(x) = C(y)$, qui est une sous-algèbre commutative maximale de A_1 (cor. 4.3). Pour $\alpha \neq 0$, le corps des fractions de $k[x, y]$ n'est pas extension transcendante pure de k. D'après le théorème de Lüroth, le corps des fractions de D n'est pas extension transcendante pure de k. (Cet emploi du théorème de Lüroth m'a été suggéré par P. SAMUEL.)

5.6. Conservons les notations précédentes. On peut montrer, en utilisant le lemme 2.7, que $D = k[x, y]$. Pour $\alpha = 0$, on a donc un exemple de sous-algèbre commutative maximale de A_1 qui n'est pas isomorphe à $k[X]$, mais dont le corps des fractions est isomorphe à $k(X)$. Celle-ci n'est pas intégralement close.

6. Classification des éléments de A_1.

6.1. Soient A une algèbre associative sur k, et $x \in A$. Pour tout $y \in \bar{A}$, posons $V_y = \sum_{n \geq 0} k(\mathrm{ad}\, x)^n y$. On notera $F(x; A)$, ou $F(x)$, l'ensemble des $y \in A$ tels que $\dim V_y < +\infty$. On a $F(x; \bar{A}) = F(x; A) \otimes_k \bar{k}$.

Si $\lambda \in \bar{k}$, on notera $F(x, \lambda; \bar{A})$ ou $F(x, \lambda)$ l'ensemble des $y \in F(x; \bar{A})$ tels que toutes les valeurs propres de $(\mathrm{ad}_{\bar{A}}\, x) \mid V_y$ soient égales à λ, autrement dit l'ensemble des $y \in \bar{A}$ tels que $(\mathrm{ad}_{\bar{A}}\, x - \lambda)^n y$ soit nul pour n assez grand. D'après la théorie des endomorphismes dans les espaces vectoriels de dimension finie, on a

$$F(x; \bar{A}) = \bigoplus_{\lambda \in \bar{k}} F(x, \lambda; \bar{A}). \tag{11}$$

D'autre part, il est connu et facile à voir que

$$F(x, \lambda; \bar{A}) . F(x, \mu; \bar{A}) \subset F(x, \lambda + \mu; \bar{A}) \tag{12}$$

(parce que $\mathrm{ad}_{\bar{A}}\, x$ est une dérivation de $\bar{A}$). Donc $F(x; \bar{A})$ *est une sous-algèbre de* $\bar{A}$, *graduée par les* $F(x, \lambda; \bar{A})$, *et* $F(x; A)$ *est une sous-algèbre de* A.

Si $\lambda \in k$, on posera $F(x, \lambda; A) = F(x, \lambda; \bar{A}) \cap A$, de sorte que $F(x, \lambda; \bar{A}) = F(x, \lambda; A) \otimes_k \bar{k}$. La somme des $F(x, \lambda; A)$ pour $\lambda \in k$ est directe mais distincte de $F(x; A)$ en général.

6.2. L'ensemble $F(x, 0; A)$ sera noté $N(x; A)$ ou $N(x)$. C'est l'ensemble des $y \in A$ tels que $(\mathrm{ad}_{\bar{A}}\, x) \mid V_y$ soit nilpotent, ou encore l'ensemble des $y \in A$ tels que $(\mathrm{ad}_A x)^n y$ soit nul pour n assez grand; *c'est une sous-algèbre* de A. Pour $n = 0, 1, 2, \ldots$, on notera $N(x, n; A)$ ou $N(x, n)$, le noyau de $(\mathrm{ad}_A x)^{n+1}$. Ainsi, $N(x, 0) = C(x)$, et $N(x)$ est réunion de la suite croissante des $N(x, n)$. Si $b, b' \in A$, on a

$$(13) \qquad (\mathrm{ad}\, x)^{n+n'}(bb') = \sum_{m=0}^{n+n'} \binom{n+n'}{m} (\mathrm{ad}\, x)^m b (\mathrm{ad}\, x)^{n+n'-m} b'.$$

Il résulte de là que

$$N(x, n)\, N(x, n') \subset N(x, n+n').$$

Autrement dit, l'algèbre $N(x)$ est *filtrée* par les $N(x, n)$.

6.3. Si $\lambda \in \bar{k}$, on notera $D(x, \lambda; \bar{A})$ ou $D(x, \lambda)$ l'ensemble des $y \in \bar{A}$ tels que $(\mathrm{ad}_{\bar{A}} x)\, y = \lambda y$. On a $D(x, \lambda; \bar{A}) \subset F(x, \lambda; \bar{A})$, et

$$(14) \qquad F(x, \lambda; \bar{A}) \neq 0 \iff D(x, \lambda; \bar{A}) \neq 0.$$

On notera $D(x; \bar{A})$ la somme des $D(x, \lambda; \bar{A})$ pour $\lambda \in \bar{k}$, de sorte que

$$(15) \qquad D(x; \bar{A}) = \bigoplus_{\lambda \in \bar{k}} D(x, \lambda; \bar{A}).$$

On posera

$$D(x) = D(x; A) = D(x; \bar{A}) \cap A,$$

de sorte que $D(x; \bar{A}) = D(x; A) \otimes_k \bar{k}$. Il est immédiat que

$$(16) \qquad D(x, \lambda; \bar{A}).D(x, \mu; \bar{A}) \subset D(x, \lambda + \mu; \bar{A}).$$

Donc $D(x; \bar{A})$ *est une sous-algèbre de* $\bar{A}$, *graduée par les* $D(x, \lambda; \bar{A})$, et $D(x; A)$ *est une sous-algèbre de* A.

Si $\lambda \in k$, on posera $D(x, \lambda; A) = D(x, \lambda; \bar{A}) \cap A$, de sorte que

$$D(x, \lambda; \bar{A}) = D(x, \lambda; A) \otimes_k \bar{k}.$$

La somme des $D(x, \lambda; A)$, pour $\lambda \in k$, est directe, mais distincte de $D(x; A)$ en général. On a $D(x, 0; A) = C(x; A)$.

6.4. Lemme. — *Soient* $\lambda \in k$ *et* $z \in A$ *tels que* $(\mathrm{ad}\, x - \lambda)^2 z = 0$. *Alors*

$$(17) \quad (\mathrm{ad}\, x - n\lambda)^n z^n = n!\, ((\mathrm{ad}\, x - \lambda)\, z)^n \qquad \text{pour} \quad n = 1, 2, 3, \ldots$$

$$(18) \qquad (\mathrm{ad}\, x - n\lambda)^{n+1} z^n = 0.$$

Démonstration. — L'hypothèse $(\mathrm{ad}\, x - \lambda)^2 z = 0$ s'écrit

$$(\mathrm{ad}\, x - \lambda)\, z \in D(x, \lambda).$$

D'après (16), on a

$$(19) \qquad ((\mathrm{ad}\, x - \lambda)\, z)^n \in D(x, n\lambda) \qquad \text{pour} \quad n = 1, 2, 3, \ldots.$$

L'égalité (17) est claire pour $n=1$. Admettons-la pour n. Alors

$$\begin{aligned}(\mathrm{ad}\,x-(n+1)\lambda)^{n+1}z^{n+1} &= (\mathrm{ad}\,x-(n+1)\lambda)^{n+1}(z^n.z)\\ &= ((\mathrm{ad}\,x-n\lambda)^{n+1}z^n).z+(n+1)((\mathrm{ad}\,x-n\lambda)^n z^n).((\mathrm{ad}\,x-\lambda)z)\\ &\quad+\frac{1}{2}(n+1)n((\mathrm{ad}\,x-n\lambda)^{n-1}z^n).((\mathrm{ad}\,x-\lambda)^2 z)+\ldots\\ &= ((\mathrm{ad}\,x-n\lambda)^{n+1}z^n).z+(n+1)((\mathrm{ad}\,x-n\lambda)^n z^n).((\mathrm{ad}\,x-\lambda)z).\end{aligned}$$

D'après (19) et l'hypothèse de récurrence, on a

$$(\mathrm{ad}\,x-n\lambda)^{n+1}z^n=(\mathrm{ad}\,x-n\lambda)(n!((\mathrm{ad}\,x-\lambda)z)^n)=0,$$

donc

$$\begin{aligned}(\mathrm{ad}\,x-(n+1)\lambda)^{n+1}z^{n+1} &= (n+1)((\mathrm{ad}\,x-n\lambda)^n z^n).((\mathrm{ad}\,x-\lambda)z)\\ &= (n+1)n!((\mathrm{ad}\,x-\lambda)z)^n.((\mathrm{ad}\,x-\lambda)z)\\ &= (n+1)!((\mathrm{ad}\,x-\lambda)z)^{n+1},\end{aligned}$$

ce qui achève la démonstration de (17). La formule (18) résulte de (17) et (19).

6.5. Désormais, nous revenons à l'étude de A_1.

PROPOSITION. — *Soit λ un élément non nul de $\bar{k}$. Soit $x\in\bar{A}_1$. On a $D(x,\lambda)=F(x,\lambda)$.*

Démonstration. — On peut supposer $k=\bar{k}$. En remplaçant x par $\lambda^{-1}x$, on se ramène à prouver que $D(x,1)=F(x,1)$. Supposons $D(x,1)\neq F(x,1)$. Alors il existe des éléments non nuls y, z de A_1 tels que

$$\begin{aligned}(\mathrm{ad}\,x)\,y&=y,\\ (\mathrm{ad}\,x-1)\,z&\neq 0,\\ (\mathrm{ad}\,x-1)^2 z&=0.\end{aligned}$$

Supposons qu'on ait une relation de la forme

$$\sum_{i,j} d_{ij}z^i=0 \qquad (i,j \text{ entiers } \geq 0),$$

avec $d_{ij}\in D(x,j)$. Nous allons montrer que les d_{ij} sont tous nuls. Comme $d_{ij}z^i\in F(x,i+j)$ d'après (12), et que la somme des $F(x,\mu)$ est directe, on se ramène au cas d'une relation de la forme

$$d_i z^n+d_{i+1}z^{n-1}+d_{i+2}z^{n+2}+\ldots=0,$$

avec $d_j\in D(x,j)$, et il s'agit de montrer que les d_j sont nuls. Or

$$\begin{aligned}&(\mathrm{ad}\,x-(n+i))^n(d_{i+l}z^{n-l})\\ &=\sum_{r=0}^{n}\binom{n}{r}(\mathrm{ad}\,x-(i+l))^r d_{i+l}.(\mathrm{ad}\,x-(n-l))^{n-r}z^{n-l}.\end{aligned}$$

Comme $(\mathrm{ad}\,x-(i+l))^r d_{i+l}=0$ pour $r>0$, cela est égal à

$$d_{i+l}.(\mathrm{ad}\,x-(n-l))^n z^{n-l}$$

donc, d'après le lemme 6.4, est nul si $l>0$ et égal à $d_i n!\,((\mathrm{ad}\,x-1)\,z)^n$ si $l=0$. Par suite,

$$\begin{aligned} 0 &= (\mathrm{ad}\,x-(n+i))^n(d_i z^n + d_{i+1}z^{n-1} + d_{i+2}z^{n-2}+\ldots) \\ &= n!\,d_i((\mathrm{ad}\,x-1)\,z)^n. \end{aligned}$$

Puisque A_1 est intègre, on en conclut que $d_i=0$. On prouve ensuite de la même manière que $d_{i+1}=0$, $d_{i+2}=0$, ...

Montrons maintenant que les $x^r y^j z^i$ (r, i, j entiers ≥ 0) sont linéairement indépendants sur k. Considérons une relation

$$\sum_{r,i,j}\lambda_{rij}x^r y^j z^i = 0 \qquad \text{avec} \quad \lambda_{rij}\in k \text{ quels que soient } r,\ i,\ j.$$

Comme $x^r y^j \in D(x, j)$, on déduit de ce qui précède que

$$\sum_r \lambda_{rij}x^r y^j = 0 \quad \text{quels que soient } i \text{ et } j,$$

d'où

$$\sum_r \lambda_{rij}x^r = 0 \quad \text{quels que soient } i \text{ et } j,$$

donc $\lambda_{rij}=0$ quels que soient r, i, j (prop. 2.5).

Or, ce résultat contredit le fait que la dimension de Gel'fand-Kirillov de A_1 est égale à 2. [Les $x^r y^j z^i$, pour $r+j+i\leq N$, engendrent un espace vectoriel de dimension $\frac{1}{6}(N+3)(N+2)(N+1)$; or, si

$$m=\sup(v_{1,1}(x),\ v_{1,1}(y),\ v_{1,1}(z)),$$

ces $x^r y^j z^i$ sont combinaisons linéaires des $p^a q^b$ avec $a+b\leq Nm$, donc engendrent un espace vectoriel de dimension $\leq \frac{1}{2}(Nm+2)(Nm+1)$; il y a contradiction pour N assez grand.]

6.6. Corollaire. — *Pour tout $x\in A_1$, on a, ou bien $F(x)=D(x)$, ou bien $F(x)=N(x)$.*

Démonstration. — On peut supposer $k=\bar{k}$. D'après la proposition 6.5, on a

$$F(x)=\sum_{\lambda\in k}F(x,\lambda)=N(x)+\sum_{\lambda\in k,\,\lambda\neq 0}D(x,\lambda)=N(x)+D(x),$$

et d'autre part $N(x) \cap D(x) = C(x)$. Supposons $F(x) \neq N(x)$ et $F(x) \neq D(x)$. D'une part, il existe un λ non nul dans k et un y non nul dans $D(x, \lambda)$; d'autre part, il existe un $z \in A_1$ tel que $(\mathrm{ad}\, x)\, z \neq 0$, $(\mathrm{ad}\, x)^2 z = 0$. Alors

$$(\mathrm{ad}\, x - \lambda)(yz) = y((\mathrm{ad}\, x)\, z) \neq 0,$$
$$(\mathrm{ad}\, x - \lambda)^2 (yz) = y((\mathrm{ad}\, x)^2 z) = 0$$

donc $F(x, \lambda) \neq D(x, \lambda)$ contrairement à la proposition 6.5.

6.7. Corollaire. — *L'ensemble $A_1 - \{k\}$ est réunion disjointe des sous-ensembles suivants :*

(i) *l'ensemble Δ_1 des $x \in A_1 - \{k\}$ tels que $N(x) = A_1$, $D(x) = C(x)$;*

(ii) *l'ensemble Δ_2 des $x \in A_1 - \{k\}$ tels que $N(x) \neq A_1$, $N(x) \neq C(x)$, $D(x) = C(x)$;*

(iii) *l'ensemble Δ_3 des $x \in A_1 - \{k\}$ tels que $D(x) = A_1$, $N(x) = C(x)$;*

(iv) *l'ensemble Δ_4 des $x \in A_1 - \{k\}$ tels que $D(x) \neq A_1$, $D(x) \neq C(x)$, $N(x) = C(x)$;*

(v) *l'ensemble Δ_5 des $x \in A_1 - \{k\}$ tels que $D(x) = N(x) = C(x)$.*

Démonstration. — Il est clair que les Δ_i sont deux à deux disjoints. D'autre part, si $x \notin \Delta_5$, on a : ou bien $N(x) \neq C(x)$, ou bien $D(x) = C(x)$. Dans le premier cas (resp. le deuxième), on a $D(x) = C(x)$ [resp. $N(x) = C(x)$] d'après le corollaire 6.6, donc $x \in \Delta_1 \cup \Delta_2$ (resp. $x \in \Delta_3 \cup \Delta_4$).

6.8. On dira que les éléments de $\Delta_1 \cup \Delta_2$ (resp. de Δ_1) sont *de type nilpotent* (resp. *de type strictement nilpotent*), et que les éléments de $\Delta_3 \cup \Delta_4$ (resp. de Δ_3) sont *de type semi-simple* (resp. *de type strictement semi-simple*). On verra qu'aucun des ensembles Δ_i de 6.7 n'est vide.

7. Éléments x tels que $C(x) = F(x)$.

7.1. La proposition 7.4 fournira beaucoup d'exemples d'éléments x tels que $C(x) = N(x) = F(x)$. Elle jouera aussi un rôle essentiel dans la détermination des automorphismes de A_1.

7.2. Lemme. — *Soit $x \in A_1$. Considérons $F(x)$ comme un $C(x)$-module (à gauche par exemple), et supposons que ce module soit de type fini. Alors $F(x) = C(x)$.*

Démonstration. — Supposons $N(x) \neq C(x)$. Soit $(y_1, \ldots, y_r)$ un système générateur du $C(x)$-module $N(x)$. Il existe un entier $n > 0$ tel que

$$(\mathrm{ad}\, x)^n y_1 = \ldots = (\mathrm{ad}\, x)^n y_r = 0.$$

Alors $(\mathrm{ad}\, x)^n (N(x)) = 0$. Or, il existe un $y \in N(x)$ tel que

$$(\mathrm{ad}\, x) y \neq 0, \ (\mathrm{ad}\, x)^2 y = 0.$$

D'après le lemme 6.4, on a $(\mathrm{ad}\, x)^n y^n \neq 0$, d'où contradiction.

Supposons $D(x) \neq C(x)$. Comme $D(x, \lambda) \neq 0$ implique $D(x, n\lambda) \neq 0$ pour tout entier $n > 0$, $D(x)$ est une somme directe *infinie* de sous-$C(x)$-modules non nuls, d'où contradiction.

7.3. Lemme. — *Soient ρ, σ des entiers > 0. Soient $x \in A_1$, $y \in F(x)$, $v = v_{\rho,\sigma}(x)$, $w = v_{\rho,\sigma}(y)$, f et g les polynômes (ρ, σ)-associés à x et y. On suppose que $v > \rho + \sigma$ et que f n'est pas un monôme. Alors on est dans l'un des cas suivants :*

(*a*) *f^w est proportionnel à g^v;*

(*b*) *$\sigma > \rho$, σ est multiple de ρ, et $f(X, Y)$ est de la forme $\lambda X^\alpha (X^{\sigma/\rho} + \mu Y)^\beta$, où λ, $\mu \in k$ et où α, β sont des entiers ≥ 0;*

(*c*) *$\rho > \sigma$, ρ est multiple de σ, et $f(X, Y)$ est de la forme $\lambda Y^\alpha (Y^{\rho/\sigma} + \mu X)^\beta$, où λ, $\mu \in k$ et où α, β sont des entiers ≥ 0;*

(*d*) *$\rho = \sigma$, et $f(X, Y)$ est de la forme $\lambda(\mu X + \nu Y)^\alpha(\mu' X + \nu' Y)^\beta$, où λ, μ, ν, μ', $\nu' \in k$ et où α, β sont des entiers ≥ 0.*

Démonstration. — Posons $y_n = (\mathrm{ad}\, x)^n y$, pour $n = 0, 1, 2, \ldots$. On a $v_{\rho,\sigma}(y_0) = w$. Il est impossible qu'on ait $v_{\rho,\sigma}(y_n) = w + n(v - \rho - \sigma)$ pour tout n [car $v - \rho - \sigma > 0$ et $y \in F(x)$]. Il existe donc un $n \geq 0$ tel que

$$v_{\rho,\sigma}(y_m) = w + m(v - \rho - \sigma) \qquad \text{pour} \quad m \leq n,$$
$$v_{\rho,\sigma}(y_{n+1}) < w + (n+1)(v - \rho - \sigma).$$

Soit h le polynôme (ρ, σ)-associé à y_n. Posons $v_{\rho,\sigma}(y_n) = t$. D'après le lemme 2.7, f^t est proportionnel à h^v. Si $n = 0$, on a $y_n = y$, $h = g$, $t = w$, et nous sommes dans le cas (*a*). Nous supposerons donc désormais que $n > 0$. On peut donc considérer y_{n-1}. Soit l le polynôme (ρ, σ)-associé à y_{n-1}. On a $v_{\rho,\sigma}(y_n) - v_{\rho,\sigma}(y_{n-1}) = v - \rho - \sigma$, donc

$$v_{\rho,\sigma}(y_{n-1}) = t - v + \rho + \sigma.$$

Alors

$$\sigma Y h = \sigma Y \left(\frac{\partial f}{\partial X} \frac{\partial l}{\partial Y} - \frac{\partial f}{\partial Y} \frac{\partial l}{\partial X} \right) \quad \text{[lemme 2.7 (iii)]}$$
$$= f^{-t+v-\rho-\sigma+1} l^{v+1} \frac{\partial}{\partial X} (l^{-v} f^{t-v+\rho+\sigma}) \quad \text{[lemme 1.4 (i)]}$$

d'où, puisque f^t est proportionnel à h^v,

$$\frac{\partial}{\partial X}\left(\left(\frac{h}{fl}\right)^v f^{\rho+\sigma}\right) = \sigma Y \left(\frac{h}{fl}\right)^{v+1} f^{\rho+\sigma}. \tag{20}$$

En utilisant le lemme 1.4 (ii) au lieu du lemme 1.4 (i), il vient de même

$$\frac{\partial}{\partial Y}\left(\left(\frac{h}{fl}\right)^v f^{\rho+\sigma}\right) = -\rho X \left(\frac{h}{fl}\right)^{v+1} f^{\rho+\sigma}. \tag{21}$$

Considérons f, h, l comme des polynômes en X à coefficients dans $k(Y)$. Soit $\mu \in \overline{k(Y)}$. Si μ est zéro de $\frac{h}{fl}$ d'ordre $\nu > 0$ et zéro de f d'ordre $\nu' \geqq 0$, la relation (20) prouve que $v\nu + (\rho + \sigma)\nu' - 1 = (v + 1)\nu + (\rho + \sigma)\nu'$, ce qui est absurde. Donc $\frac{h}{fl}$ n'a pas de zéro dans $\overline{k(Y)}$. Ainsi, $\frac{fl}{h} \in k(Y)[X]$. En utilisant (21), on voit de même que $\frac{fl}{h} \in k(X)[Y]$. Donc il existe un polynôme non nul $m \in k[X, Y]$ tel que $fl = hm$. Comme f (resp. h, l) est (ρ, σ)-homogène de (ρ, σ)-degré v, (resp. t, $t - v + \rho + \sigma$), m est (ρ, σ)-homogène et

$$v_{\rho,\sigma}(m) = v + (t - v + \rho + \sigma) - t = \rho + \sigma.$$

Les relations (20) et (21) s'écrivent maintenant

$$\frac{\partial}{\partial X}\left(\frac{f^{\rho+\sigma}}{m^{\nu}}\right) = \sigma Y \frac{f^{\rho+\sigma}}{m^{\nu+1}}, \tag{22}$$

$$\frac{\partial}{\partial Y}\left(\frac{f^{\rho+\sigma}}{m^{\nu}}\right) = -\rho X \frac{f^{\rho+\sigma}}{m^{\nu+1}}. \tag{23}$$

Considérons f et m comme des éléments de $k(Y)[X]$ (resp. $k(X)[Y]$). D'après (22) [resp. (23)], tout zéro de f dans $\overline{k(Y)}$ [resp. $\overline{k(X)}$] est zéro de m dans $\overline{k(Y)}$ [resp. $\overline{k(X)}$].

Si m était un monôme, on en déduirait que f est un monôme, contrairement à l'hypothèse. Donc $E(m)$ (*cf.* 1.1) contient au moins deux éléments. Or, si $(i, j) \in E(m)$, on a $\rho i + \sigma j = \rho + \sigma$. Si $i > 0$ et $j > 0$, on a nécessairement $(i, j) = (1, 1)$. Comme $E(m)$ ne se réduit pas à $(1, 1)$ d'après ce qui précède, $E(m)$ contient ou bien un point de la forme $(i, 0)$, qui est nécessairement $\left(\frac{\rho + \sigma}{\rho}, 0\right)$, ou bien un point de la forme $(0, j)$, qui est nécessairement $\left(0, \frac{\rho + \sigma}{\sigma}\right)$. On est donc dans l'un des cas suivants :

Premier cas : $\rho < \sigma$, σ est multiple de ρ, $E(m) = \left\{(1, 1), \left(1 + \frac{\sigma}{\rho}, 0\right)\right\}$, et

$m(X, Y) = \mu X^{1+(\sigma/\rho)} + \nu XY$ avec $\mu, \nu \in k$, $\mu \neq 0$, $\nu \neq 0$.

Deuxième cas : $\rho > \sigma$, ρ est multiple de σ, $E(m) = \left\{(1, 1), \left(0, 1 + \frac{\rho}{\sigma}\right)\right\}$, et

$m(X, Y) = \mu Y^{1+(\rho/\sigma)} + \nu XY$ avec $\mu, \nu \in k$, $\mu \neq 0$, $\nu \neq 0$.

Troisième cas : $\rho = \sigma$, $E(m) \subset \{(2,0), (1, 1), (0, 2)\}$, et

$$m(X, Y) = \mu X^2 + \nu XY + \zeta Y^2$$

avec deux au moins des éléments μ, ν, ζ non nuls.

Plaçons-nous dans le premier cas. Alors $m \in k(X)[Y]$ a un seul zéro dans $\overline{k(X)}$. Donc $f \in k(X)[Y]$ a pour unique zéro dans $\overline{k(X)}$ ce zéro de m. Donc il existe un entier $\beta \geqq 0$ et un élément $\tau(X)$ de $k(X)$ tel que $f = \tau(X)(\nu Y + \mu X^{\sigma/\rho})^\beta$. Comme $\nu \neq 0$, on a $\tau(X) \in k[X]$. D'autre part, tout zéro de $f \in k(Y)[X]$ dans $\overline{k(Y)}$ est zéro de $m \in k(Y)[X]$. Ceci prouve que tout zéro de $\tau(X)$ est nul, donc que $\tau(X)$ est un monôme. Aux notations près, on est dans la situation (*b*) de l'énoncé.

On voit de même que, dans le deuxième cas, la situation (*c*) de l'énoncé est réalisée.

Plaçons-nous dans le troisième cas. Si $\zeta = 0$, on a $\mu \neq 0$, $\nu \neq 0$; on peut raisonner comme dans le premier cas, et l'on est dans la situation (*d*) de l'énoncé. De même si $\mu = 0$. Supposons $\mu \neq 0$ et $\zeta \neq 0$. Si $m(X, Y) = \mu(X + \eta Y)(X + \theta Y)$ avec $\eta, \theta \in k$, $f \in k(Y)[X]$ admet les seuls zéros $-\eta Y$, $-\theta Y$ dans $\overline{k(Y)}$, d'où

$$f = \tau(Y)(X + \eta Y)^\alpha (X + \theta Y)^\beta \qquad \text{avec} \quad \tau(Y) \in k(Y) \text{ et } \alpha, \beta \text{ entiers} \geqq 0;$$

évidemment $\tau(Y) \in k[Y]$; en échangeant les rôles de X et Y, on voit que $\tau(Y) \in k$, et l'on est dans la situation (*d*) de l'énoncé. Enfin, supposons

$$m(X, Y) = \mu(X + \eta Y)(X + \theta Y)$$

avec

$$\eta, \theta \in \bar{k}, \quad \eta, \theta \notin k, \quad \eta \text{ et } \theta \text{ conjugués sur } k.$$

On a $f = \tau(Y)(X + \eta Y)^\alpha (X + \theta Y)^\beta$, avec cette fois $\alpha = \beta$, et comme ci-dessus $\tau(Y) \in k$. Mais alors f est proportionnel à une puissance de m; comme

$$v_{\rho,\sigma}(f^{\rho+\sigma}) = (\rho + \sigma)v = v_{\rho,\sigma}(m^v),$$

on a $\dfrac{f^{\rho+\sigma}}{m^v} \in k$, ce qui est absurde d'après (22) et (23).

7.4. Proposition. — *Soient ρ, σ des entiers > 0, $x \in A_1$, $v = v_{\rho,\sigma}(x)$, et f le polynôme (ρ, σ)-associé à x. On suppose que :*

1° $v > \rho + \sigma$;

2° *f n'est pas un monôme;*

3° *on n'est pas dans l'un des cas (b), (c), (d) du lemme 7.3 (il en sera ainsi par exemple si aucun des nombres ρ, σ n'est multiple de l'autre).*

Alors $F(x) = C(x)$.

Démonstration. — Soit Λ l'ensemble des entiers λ tels qu'il existe un $y \in F_1(x)$ avec $v_{\rho,\sigma}(y) = \lambda$. On a $\Lambda + \Lambda \subset \Lambda$, et en particulier $\{0, v, 2v, \ldots\} \subset \Lambda$. Soit Λ' l'image canonique de Λ dans $\mathbf{Z}/v\mathbf{Z}$. Dans chaque élément de Λ', choisissons le plus petit élément, d'où des entiers $\lambda_0 = 0, \lambda_1, \lambda_2, \ldots, \lambda_r$. Les éléments de Λ sont les suivants :

$$\begin{array}{lllll} 0, & v, & 2v, & 3v, & \ldots; \\ \lambda_1, & \lambda_1 + v, & \lambda_1 + 2v, & \lambda_1 + 3v, & \ldots; \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \lambda_r, & \lambda_r + v, & \lambda_r + 2v, & \lambda_r + 3v, & \ldots. \end{array}$$

Soit y_i un élément de $F(x)$ tel que $v_{\rho,\sigma}(y_i) = \lambda_i$. Soit $y \in F(x)$. Montrons, par récurrence sur $v_{\rho,\sigma}(y)$, que $y \in k[x]y_0 + k[x]y_1 + \ldots + k[x]y_r$. C'est évident si $v_{\rho,\sigma}(y) = 0$. Supposons-le établi pour $v_{\rho,\sigma}(y) < n$, et envisageons le cas où $v_{\rho,\sigma}(y) = n > 0$. Il existe un $i = 0, 1, \ldots, r$ et un entier $s \geq 0$ tels que $v_{\rho,\sigma}(x^s y_i) = n$. Soient g, h les polynômes (ρ, σ)-associés à y, $x^s y_i$. D'après le lemme 7.3, g^v et h^v sont proportionnels à f^n, donc g et h sont proportionnels. Donc il existe $\lambda \in k$ tel que $v_{\rho,\sigma}(y - \lambda x^s y_i) < n$. On a $y - \lambda x^s y_i \in F(x)$, et il suffit d'appliquer l'hypothèse de récurrence à $y - \lambda x^s y_i$.

Ainsi, $F(x) = \sum_i k[x]y_i$, et il suffit d'appliquer le lemme 7.2.

7.5. Par exemple, soit $x = p^3 + q^2$. On a $v_{2,3}(x) = 6$ et le polynôme $(2, 3)$-associé à x est $X^3 + Y^2$. Alors $F(x) = C(x)$. Il est de même si x, non scalaire, appartient à la sous-algèbre commutative maximale D de la démonstration 5.5.

8. Automorphismes de A_1.

8.1. Pour $\lambda \in k$ et n entier ≥ 0, nous avons défini dans l'introduction des automorphismes $\Phi_{n,\lambda}$, $\Phi'_{n,\lambda}$ de A_1. Nous noterons provisoirement G le groupe d'automorphismes de A_1 engendré par les $\Phi_{n,\lambda}$ et les $\Phi'_{n,\lambda}$ (on verra que c'est le groupe de *tous* les automorphismes de A_1).

8.2. Soit V l'espace vectoriel $kp + kq$. Tout élément du groupe spécial linéaire $SL(V)$ de V se prolonge en un automorphisme de A_1. On obtient ainsi un groupe G' d'automorphismes de A_1. Il est connu et facile à voir que les applications $\Phi_{1,\lambda} \mid V$ et $\Phi'_{1,\lambda} \mid V$ engendrent le groupe $SL(V)$. Donc $G' \subset G$. En particulier, on notera Ψ l'élément de G' tel que $\Psi(p) = q$, $\Psi(q) = -p$.

8.3. Lemme. — *Si $x \in k[p]$, on a $N(x) = A_1$.*

Démonstration. — On a $p \in N(x)$, et $[x, q] \in k[p]$, donc $q \in N(x)$.

8.4. Lemme. — *Soit $x = \lambda p^2 + \mu q^2 + \nu$, avec $\lambda, \mu, \nu \in k$, $\lambda \neq 0$, $\mu \neq 0$. Alors $D(x) = A_1$.*

Démonstration. — On peut supposer $k = \bar{k}$. Alors il existe $\Phi \in G'$ tel que $\Phi(x) = \zeta pq + \theta$ avec $\zeta \in k$, $\theta \in k$. Il suffit alors d'utiliser l'égalité (4) de 5.3.

8.5. Lemme. — *Soit x un élément de A_1 de la forme*

$$\alpha_{00} + \alpha_{10} p + \alpha_{20} p^2 + \ldots + \alpha_{r0} p^r + \alpha_{01} q + \alpha_{11} pq$$

avec $\alpha_{01} \neq 0$ ou $\alpha_{11} \neq 0$. Il existe $\Phi \in G$ tel que Φ soit de la forme $\beta_{00} + \beta_{10} p + \beta_{01} q + \beta_{11} pq$.

Démonstration. — Le lemme est évident pour $r \leq 1$. Supposons-le démontré pour $r - 1$. Si $\alpha_{11} \neq 0$, on se ramène au cas où $\alpha_{11} = 1$. On a alors

$$\begin{aligned}\Phi_{r-1, -\alpha_{r0}}(x) &= \alpha_{00} + \alpha_{10} p + \ldots + \alpha_{r0} p^r + \alpha_{01}(q - \alpha_{r0} p^{r-1}) + p(q - \alpha_{r0} p^{r-1}) \\ &= \alpha_{00} + \alpha_{10} p + \ldots + \alpha_{r-2, 0} p^{r-2} + \alpha'_{r-1, 0} p^{r-1} + \alpha_{01} q + pq,\end{aligned}$$

et il suffit d'appliquer l'hypothèse de récurrence. Si $\alpha_{11} = 0$ et $\alpha_{01} \neq 0$, on se ramène au cas où $\alpha_{01} = 1$. On a alors

$$\begin{aligned}\Phi_{r, -\alpha_{r0}}(x) &= \alpha_{00} + \alpha_{10} p + \ldots + \alpha_{r0} p^r + q - \alpha_{r0} p^r \\ &= \alpha_{00} + \alpha_{10} p + \ldots + \alpha_{r-1, 0} p^{r-1} + q,\end{aligned}$$

et l'on applique l'hypothèse de récurrence.

8.6. Lemme. — *Soit x un élément de A_1 de la forme*

$$\alpha p^2 + 2\beta pq + \gamma q^2 + \delta p + \varepsilon q + \zeta \qquad (\alpha, \beta, \ldots, \zeta \in k).$$

(i) *Si $\beta^2 - \alpha\gamma = 0$, il existe $\Phi \in G$ tel que $\Phi(x) \in k[p]$.*

(ii) *Si $\beta^2 - \alpha\gamma \neq 0$, il existe $\Phi \in G$ et $\lambda, \mu, \nu \in k$ tels que $\lambda \neq 0$, $\mu \neq 0$, $\Phi(x) = \lambda p^2 + \mu q^2 + \nu$.*

Démonstration. — Si $\beta^2 - \alpha\gamma = 0$, il existe $\Phi_1 \in G'$ tel que

$$\Phi_1(x) = \alpha' p^2 + \delta' p + \varepsilon' q + \zeta'.$$

Si $\varepsilon' = 0$, le lemme est établi. Si $\varepsilon' \neq 0$, on se ramène au cas où $\varepsilon' = 1$; on a alors

$$\Phi_{2, -\alpha'}(\Phi_1(x)) = \alpha' p^2 + \delta' p + q - \alpha' p^2 + \zeta' = \delta' p + q + \zeta',$$

et il suffit d'utiliser un nouvel élément de G'.

Si $\beta^2 - \alpha\gamma \neq 0$, il existe $\Phi_1 \in G'$ tel que

$$\Phi_1(x) = \alpha' p^2 + \gamma' q^2 + \delta' p + \varepsilon' q + \zeta'$$

avec $\alpha' \neq 0$, $\gamma' \neq 0$. On a

$$\begin{aligned} y &= \Phi_{0,\,-\frac{1}{2}\varepsilon'\gamma'^{-1}}(\Phi_1(x)) \\ &= \alpha' p^2 + \delta' p + \zeta' + \gamma'\left(q - \frac{1}{2}\varepsilon'\gamma'^{-1}\right)^2 + \varepsilon'\left(q - \frac{1}{2}\varepsilon'\gamma'^{-1}\right) \\ &= \alpha' p^2 + \delta' p + \zeta' + \gamma' q^2 + \zeta_1. \end{aligned}$$

De même, il existe $\Phi_2 \in G'$ tel que $\Phi_2(y) = \alpha' p^2 + \gamma' q^2 + \zeta_2$.

8.7. Lemme. — *Soit* $x = \sum \alpha_{ij} p^i q^j \in A_1$. *Soit* r *le plus petit entier* ≥ 0 *tel que* $\alpha_{i0} = 0$ *pour* $i > r$. *Soit* s *le plus petit entier* ≥ 0 *tel que* $\alpha_{0j} = 0$ *pour* $j > s$. *On suppose qu'il existe des entiers* $i_1 \geq 0$, $j_1 \geq 0$ *tels que* $\alpha_{i_1 j_1} \neq 0$, $(i_1, j_1) \neq (1, 1)$, $si_1 + rj_1 > rs$. *Alors* $F(x) \neq A_1$.

Démonstration. — Si $i_1 = 0$, on a $rj_1 > rs$, d'où $j_1 > s$, contrairement à la définition de s. Donc $i_1 > 0$ et de même $j_1 > 0$.

Il existe des nombres $\rho > 0$, $\sigma > 0$, de rapport irrationnel, tels que

$$\sigma i_1 + \rho j_1 > \rho s, \qquad \sigma i_1 + \rho j_1 > r\sigma$$

(on prend ρ assez voisin de r et σ assez voisin de s). Puis il existe des entiers $i_2 \geq 0$, $j_2 \geq 0$ tels que $\alpha_{i_2 j_2} \neq 0$, $\sigma i_2 + \rho j_2 = v_{\sigma,\rho}(x)$. Alors

$$\sigma i_2 + \rho j_2 > \rho s, \qquad \sigma i_2 + \rho j_2 > r\sigma.$$

Ceci entraîne d'abord $i_2 > 0$, $j_2 > 0$. Si $i_2 = j_2 = 1$, on a

$$\sigma + \rho \leq \sigma i_1 + \rho j_1 \leq \sigma i_2 + \rho j_2 = \sigma + \rho,$$

d'où $i_1 = i_2$, $j_1 = j_2$, et $(i_1, j_1) = (1,1)$ contrairement à l'hypothèse. Donc $i_2 > 1$, ou $j_2 > 1$. D'après le lemme 1.3 (ii), le polynôme (σ, ρ)-associé à x est $\alpha_{i_2 j_2} X_{i_2} Y_{j_2}$.

Supposons $i_2 \leq j_2$. Pour $n = 0, 1, 2, \ldots$, posons $y_n = (\operatorname{ad} x)^n q$. Montrons par récurrence sur n que le polynôme (σ, ρ)-associé à y_n est

$$\beta_n X^{n(i_2-1)} Y^{1+n(j_2-1)}$$

avec $\beta_n \in k$, $\beta_n \neq 0$. C'est évident pour $n = 0$. Supposons-le établi pour n. On a

$$i_2(1 + n(j_2 - 1)) - j_2 n(i_2 - 1) = i_2 + nj_2 - ni_2 \geq i_2 > 0,$$

donc, compte tenu du lemme 2.7, le polynôme (σ, ρ)-associé à $y_{n+1} = [x, y_n]$ est

$$(i_2 + nj_2 - ni_2)\alpha_{i_2 j_2}\beta_n X^{i_2 + n(i_2-1)-1} Y^{j_2+1+n(j_2-1)-1}$$

d'où notre assertion pour $n + 1$. On a en outre

$$v_{\sigma,\rho}(y_n) = \sigma n(i_2 - 1) + \rho(1 + n(j_2 - 1)).$$

Comme $i_2 > 1$ ou $j_2 > 1$, on voit que $v_{\sigma,\rho}(y_n)$ tend vers $+\infty$ avec n. Donc $q \notin F(x)$ et $F(x) \neq A_1$.

Si $i_2 \geqq j_2$, on a $p \notin F(\Psi(x))$ d'après ce qui précède, donc $F(\Psi(x)) \neq A_1$ et $F(x) \neq A_1$.

8.8. Lemme. — *Soit $x \in A_1$, tel que $F(x) = A_1$. Il existe $\Phi \in G$ tel que $\Phi(x)$ possède l'une des propriétés suivantes : ou bien $\Phi(x) \in k[p]$, ou bien $\Phi(x)$ est de la forme $\lambda p^2 + \mu q^2 + \nu$, avec $\lambda, \mu, \nu \in k$, $\lambda \neq 0$, $\mu \neq 0$.*

Démonstration. — Introduisons les entiers r, s du lemme 8.7. Nous raisonnerons par récurrence sur $r+s$. Si $r \leqq 2$ et $s \leqq 2$, le lemme 8.7 prouve que $v_{1,1}(x) \leqq 2$, et l'on applique le lemme 8.6. Nous supposerons donc $r > 2$ ou $s > 2$ et le lemme établi pour $r+s < n$; nous envisageons désormais le cas où $r+s = n$.

Utilisant l'automorphisme Ψ de 8.2, on peut supposer que $r \geqq s$. Si $s \leqq 1$, x est, d'après le lemme 8.7, de la forme

$$\alpha_{00} + \alpha_{10} p + \alpha_{20} p^2 + \ldots + \alpha_{r0} p^r + \alpha_{01} q + \alpha_{11} pq,$$

et il suffit d'appliquer les lemmes 8.5 et 8.6. Supposons donc désormais $r \geqq s \geqq 2$ et $r > 2$, donc $r+s < rs$. Si $(i, j) \in E(x)$, le lemme 8.7 prouve que : ou bien $si + rj \leqq rs$, ou bien $i = j = 1$, et alors $si + rj = s + r < rs$. Donc $v_{s,r}(x) = rs$ et le polynôme (s, r)-associé à x est de la forme

$$(24) \quad f(X, Y) = \alpha_{r0} X^r + \ldots + \alpha_{0s} Y^s \qquad \text{avec} \quad \alpha_{r0} \neq 0, \qquad \alpha_{0s} \neq 0.$$

D'après la proposition 7.4, appliquée pour $\rho = s$, $\sigma = r$, on voit qu'on est dans l'un des cas (*b*), (*c*), (*d*) du lemme 7.3. Comme $r \geqq s$, on est dans le cas (*b*) ou le cas (*d*).

Supposons qu'on soit dans le cas (*b*). Alors r est multiple de s et, d'après (24), f est proportionnel à $(X^{r/s} + \mu Y)^s$ avec $\mu \in k$, $\mu \neq 0$. Donc, en multipliant x par un scalaire, on peut supposer

$$x = (p^{r/s} + \mu q)^s + \sum_{(i,j) \in E} \alpha_{ij} p^i q^j,$$

avec $si + rj < rs$ pour $(i, j) \in E$. Alors

$$y = \Phi_{r/s, -1/\mu}(x) = \mu^s q^s + \sum_{(i,j) \in E} \alpha_{ij} p^i (q - \mu^{-1} p^{r/s})^j.$$

On a

$$v_{s,r}(q - \mu^{-1} p^{r/s}) = r \qquad \text{et} \qquad v_{s,r}(p) = s,$$

donc

$$v_{s,r}\left(\sum_{(i,j) \in E} \alpha_{ij} p^i (q - \mu^{-1} p^{r/s})^j \right) < rs.$$

Si l'on note r_1 et s_1 les entiers analogues aux entiers r et s du lemme 8.7, mais relatifs à y, on voit que $s_1 = s$ et $r_1 < r$. D'après l'hypothèse de récurrence, il existe $\Phi \in G$ tel que $\Phi(y)$ possède l'une des deux propriétés du lemme. Comme $\Phi(y) = (\Phi \circ \Phi_{r/s, -1/\mu})(x)$, le lemme est démontré dans ce cas.

Supposons qu'on soit dans le cas (d) du lemme 7.3. Alors $r = s$ et f est proportionnel à $(X + \mu Y)^\alpha (X + \nu Y)^{r-\alpha}$ avec $\mu, \nu \in k$, α entier tel que $0 \leq \alpha \leq r$. En multipliant x par un scalaire, on peut supposer

$$x = (p + \mu q)^\alpha (p + \nu q)^{r-\alpha} + \sum_{(i,j) \in E} \alpha_{ij} p^i q^j,$$

avec $i + j < r$ pour $(i, j) \in E$. En échangeant au besoin les rôles de μ et ν, on peut supposer aussi $\alpha > 0$. Alors

$$y = \Phi_{1, -1/\mu}(x) = \mu^\alpha q^\alpha ((1 - \nu\mu^{-1}) p + \nu q)^{r-\alpha} + \sum_{(i,j) \in E} \alpha_{ij} p^i (q - \mu^{-1} p)^j.$$

Si l'on note r_1 et s_1 les entiers analogues aux entiers r et s du lemme 8.7, mais relatifs à y, on voit que $s_1 = s = r$ et $r_1 < r$. On termine comme dans le cas (b).

8.9. Lemme. — *Soit* $x \in A_1$.

(i) *Si* $N(x) = A_1$, *il existe* $\Phi \in G$ *tel que* $\Phi(x) \in k[p]$.

(ii) *Si en outre* $C(x) = k[x]$, *il existe* $\Phi \in G$ *tel que* $\Phi(x) = p$.

Démonstration. — (i) résulte des lemmes 8.4 et 8.8. Supposons $N(x) = A_1$, $C(x) = k[x]$, et prouvons (ii). Grâce à (i), on peut supposer $x \in k[p]$. Alors $p \in C(x) = k[x]$, donc $x \in k.1 + k.p$, et (ii) est alors évident.

8.10. Théorème. — *Le groupe des automorphismes de* A_1 *est engendré par les automorphismes* $\Phi_{n,\lambda}$ *et* $\Phi'_{n,\lambda}$ *de l'introduction.*

Démonstration. — Soit Φ un automorphisme de A_1 et prouvons que $\Phi \in G$. On a $N(\Phi(p)) = A_1$ (lemme 8.3), et $C(\Phi(p)) = k[\Phi(p)]$ (*cf.* 5.3). D'après le lemme 8.9, on se ramène au cas où $\Phi(p) = p$. Alors

$$[p, \Phi(q) - q] = \Phi([p, q]) - [p, q] = 1 - 1 = 0.$$

Donc $\Phi(q) \in q + k[p]$, et Φ est produit d'automorphismes $\Phi_{n,\lambda}$.

9. Éléments de type strictement nilpotent ou strictement semi-simple.

9.1. Théorème. — *Soit* $x \in A_1 - \{k\}$. *Les conditions suivantes sont équivalentes :*

(i) *x est de type strictement nilpotent;*

(ii) *il existe un automorphisme* Φ *de* A_1 *tel que* $\Phi(x) \in k[p]$.

Les conditions suivantes sont équivalentes :

(i') *x est de type strictement nilpotent et $C(x) = k[x]$;*

(ii') *il existe un automorphisme Φ de A_1 tel que $\Phi(x) = p$.*

Démonstration. — Cela résulte de 5.3 et des lemmes 8.3 et 8.9.

9.2. THÉORÈME. — *Soit $x \in A_1 - \{k\}$. Les conditions suivantes sont équivalentes :*

(i) *x est de type strictement semi-simple;*

(ii) *il existe un automorphisme Φ de A_1 tel que $\Phi(x)$ soit de la forme $\lambda p^2 + \mu q^2 + \nu$ avec $\lambda, \mu, \nu \in k$, $\lambda \neq 0$, $\mu \neq 0$.*

Démonstration. — Cela résulte des lemmes 8.3, 8.4 et 8.8.

9.3. COROLLAIRE. — *Si $x \in A_1 - \{k\}$ est de type strictement semi-simple, il existe $\rho \in k$ tel que l'ensemble des valeurs propres de* $\mathrm{ad}_{\overline{A}_1}$ *soit* $\mathbf{Z}\rho$.

Démonstration. — On peut supposer k algébriquement clos. D'après le thèorème 9.2, il existe un automorphisme Φ de A_1 tel que $\Phi(x)$ soit de la forme $\lambda pq + \mu$ avec $\lambda, \mu \in k$. Le corollaire résulte alors de l'égalité (4) de 5.3.

9.4. PROPOSITION. — *Soit x un élément de A_1 de type strictement nilpotent. Soit K_1 le corps des fractions de A_1. Alors $C(x; K_1)$ est le corps des fractions de $C(x; A_1)$, et $F(x; K_1) = N(x; K_1) = A_1 C(x; K_1)$.*

Démonstration. — Soit $z \in C(x; K_1)$. Soit I l'ensemble des $a \in A_1$ tels que $za \in A_1$ (l'idée d'utiliser I est inspirée de [12]). Alors I est un idéal à droite non nul de A_1. On a

$$a \in I \Rightarrow za \in A_1 \Rightarrow xza \in A_1 \Rightarrow zxa \in A_1 \Rightarrow xa \in I$$

donc $(\mathrm{ad}\, x)(I) \subset I$. Comme x est de type strictement nilpotent, il existe un u non nul dans I tel que $(\mathrm{ad} x)u = 0$, c'est-à-dire $u \in C(x; A_1)$. Soit $v = zu \in zI \subset A_1$. Comme z et u commutent à x, on a $v \in C(x; A_1)$. Puisque $z = vu^{-1}$, $C(x; K_1)$ est le corps des fractions de $C(x; A_1)$.

Il est clair que $A_1 C(x; K_1) \subset N(x; K_1) \subset F(x; K_1)$. Soit $z' \in F(x, K_1)$. Il existe un sous-k-espace vectoriel de dimension finie E de K_1 tel que $z' \in E$ et $(\mathrm{ad} x)E \subset E$. Soit J l'ensemble des $a \in A_1$ tels que $Ea \subset A_1$. Alors J est un idéal à droite de A_1, non nul parce que $\dim E < +\infty$. On a

$$a \in J \Rightarrow Ea \subset A_1 \Rightarrow Exa \subset xEa + Ea \subset A_1 \Rightarrow xa \in J,$$

donc $(\mathrm{ad} x)(J) \subset J$. Il existe un u' non nul dans $J \cap C(x; A_1)$. Soit $v' = z'u' \in EJ \subset A_1$. On a $z' = v'u'^{-1} \in A_1 C(x; K_1)$.

10. Éléments de type nilpotent ou semi-simple.

10.1. Il résulte de 7.5, 8.3, 8.4 que les ensembles Δ_1, Δ_3, Δ_5 du corollaire 6.7 sont non vides. Nous allons voir (10.9) que Δ_2 et Δ_4 sont non vides, et donner quelques renseignements, malheureusement très incomplets, sur les éléments de ces ensembles.

10.2. Si $x \in A_1$, rappelons que l'algèbre $N(x)$ est filtrée par les $N(x, n)$ (*cf.* 6.2).

Proposition. — *Soit* $x \in A_1 - \{k\}$.

(i) *L'algèbre graduée* $G = \bigoplus_{n \geq 0} N(x, n+1)/N(x, n)$ *associée à l'algèbre filtrée* $N(x)$ *est commutative et intègre.*

(ii) *Chaque* $N(x, n+1)/N(x, n)$, *considéré comme module sur* $N(x, 0) = C(x)$, *est un module de type fini.*

Démonstration. — Soient $b \in N(x, n)$, $b' \in N(x, n')$ tels que

$$b \notin N(x, n-1), \quad b' \notin N(x, n'-1).$$

D'après (13), on a

$$(\mathrm{ad}\, x)^{n+n'}(bb') = \binom{n+n'}{n}((\mathrm{ad}\, x)^n b)((\mathrm{ad}\, x)^{n'} b') \neq 0$$

donc G est intègre. D'autre part, $(\mathrm{ad}\, x)^n b$ et $(\mathrm{ad}\, x)^{n'} b'$ appartiennent à $C(x)$, donc sont permutables (th. 4.2). Comme

$$(\mathrm{ad}\, x)^{n+n'}(b' b) = \binom{n+n'}{n}((\mathrm{ad}\, x)^{n'} b')((\mathrm{ad}\, x)^n b),$$

on voit que $(\mathrm{ad}\, x)^{n+n'}[b, b'] = 0$, donc $[b, b'] \in N(x, n+n'-1)$. Cela prouve que G est commutative.

Pour $b \in N(x, n)$, posons $u(b) = (\mathrm{ad}\, x)^n b$. On a $(\mathrm{ad}\, x)(u(b)) = 0$, donc $u(b) \in C(x)$. Donc u est une application k-linéaire de $N(x)$ dans $C(x)$, de noyau $N(x, n-1)$. Si $b \in N(x, n)$ et $c \in C(x)$, on a

$$u(cb) = (\mathrm{ad}\, x)^n(cb) = c((\mathrm{ad}\, x)^n b) = cu(b),$$

donc u définit par passage au quotient un isomorphisme du $C(x)$-module $N(x, n)/N(x, n-1)$ sur un idéal de $C(x)$. Comme l'algèbre $C(x)$ est noethérienne (th. 5.1), le $C(x)$-module $N(x, n)/N(x, n-1)$ est de type fini.

10.3. Proposition. — *Soient x et y deux éléments non scalaires permutables de A_1. On a $N(x, n) = N(y, n)$ pour tout $n \geq 0$, donc $N(x) = N(y)$.*

Démonstration. — D'après le corollaire 4.5, on a Ker ad x = Ker ad y. Admettons que $\mathrm{Ker}(\mathrm{ad}\,x)^n = \mathrm{Ker}(\mathrm{ad}\,y)^n$. Alors, pour tout $b \in A_1$, on a

$$(\mathrm{ad}\,x)^{n+1} b = 0 \iff (\mathrm{ad}\,x)^n (\mathrm{ad}\,x)\, b = 0 \iff (\mathrm{ad}\,y)^n (\mathrm{ad}\,x)\, b = 0$$
$$\iff (\mathrm{ad}\,x)(\mathrm{ad}\,y)^n b = 0 \iff (\mathrm{ad}\,y)(\mathrm{ad}\,y)^n b = 0 \iff (\mathrm{ad}\,y)^{n+1} b = 0,$$

donc $\mathrm{Ker}(\mathrm{ad}\,x)^{n+1} = \mathrm{Ker}(\mathrm{ad}\,y)^{n+1}$. Ainsi, $\mathrm{Ker}(\mathrm{ad}\,x)^n = \mathrm{Ker}(\mathrm{ad}\,y)^n$ pour tout $n \geqq 0$.

10.4. La proposition 10.3 est l'analogue du corollaire 4.5. Mais l'analogue correspondant du corollaire 4.6 est inexact. Par exemple, $q^2 \in N(p^3 q)$ mais $q \notin N(p^3 q)$.

10.5. Corollaire. — *Soit B une sous-algèbre commutative maximale de A_1. Si $B \cap \Delta_1 \neq \emptyset$, on a $B - \{k\} \subset \Delta_1$. Si $B \cap \Delta_2 \neq \emptyset$, on a $B - \{k\} \subset \Delta_2$.*

Les assertions analogues pour Δ_3, Δ_4, Δ_5 sont fausses.

10.6. Proposition. — *Soit $x \in A_1$.*

(i) *Les valeurs propres de $\mathrm{ad}_{\bar{A}_1} x$ sont linéairement dépendantes sur* $\mathbf{Q}$.

(ii) *Chaque $D(x, \mu; \bar{A}_1)$, considéré comme module (à gauche par exemple) sur $C(x; \bar{A}_1)$, est un module de type fini.*

Démonstration. — On se ramène au cas où $\bar{k} = k$. Supposons que $\mathrm{ad}\,x$ admette deux valeurs propres λ et μ linéairement indépendantes sur $\mathbf{Q}$. Alors les $\lambda i + \mu j$ (i, j entiers $\geqq 0$) sont deux à deux distincts. Donc la somme des $D(x, \lambda i + \mu j)$ est directe. Soit y (resp. z) un élément non nul de $D(x, \lambda)$ [resp. $D(x, \mu)$]. Alors $k[x] y^i z^j \subset D(x, \lambda i + \mu j)$, donc les $x^r y^i z^j$ (r, i, j entiers $\geqq 0$) sont linéairement indépendants sur k. On en tire une contradiction comme à la fin de la démonstration 6.5.

Soit μ une valeur propre de $\mathrm{ad}\,x$, et prouvons (ii). Posons $v = v_{1,1}(x) \geqq 0$. Si $v_{1,1}(x) \leqq 2$, on se ramène, grâce au lemme 8.6, au cas où $x = pq$, et le résultat est alors évident (*cf.* 3.3). Supposons désormais $v_{1,1}(x) > 2$. Soit f le polynôme $(1, 1)$-associé à x. Soit Λ l'ensemble des entiers $\lambda \geqq 0$ tels qu'il existe un $y \in D(x, \mu)$ avec $v_{1,1}(y) = \lambda$. On a

$$\lambda \in \Lambda \Rightarrow \lambda + v \in \Lambda.$$

Dans chaque classe de congruence modulo v qui rencontre Λ, choisissons le plus petit élément appartenant à Λ. On obtient ainsi des entiers λ_1, $\lambda_2, \ldots, \lambda_r$. Les éléments de Λ sont les λ_i, $\lambda_i + v$, $\lambda_i + 2v, \ldots$, pour $i = 1, 2, \ldots, r$. Soit y_i un élément de $D(x, \mu)$ tel que $v_{1,1}(y_i) = \lambda_i$. Soit $y \in D(x, \mu)$. Montrons, par récurrence sur $v_{1,1}(y)$, que

$$y \in k[x] y_1 + \ldots + k[x] y_r.$$

C'est évident si $v_{1,1}(y) = 0$. Supposons-le établi quand $v_{1,1}(y) < n$, et envisageons le cas où $v_{1,1}(y) = n > 0$. Il existe un $i \in \{1, 2, \ldots, r\}$ et un entier $s \geq 0$ tels que $v_{1,1}(x^s y_i) = n$. Soient g, h les polynômes $(1, 1)$-associés à y, $x^s y_i$. On a $[x, y] = \mu y$, $[x, x^s y_i] = \mu x^s y_i$, et $v > 2$, donc (lemme 2.7) g^v et h^v sont proportionnels à f^n, de sorte que g et h sont proportionnels. Donc il existe $\zeta \in k$ tel que $v_{1,1}(y - \zeta x^s y_i) < n$. On a $y - \zeta x^s y_i \in D(x, \mu)$, et il suffit d'appliquer à $y - \zeta x^s y_i$ l'hypothèse de récurrence. Ainsi, $D(x, \mu)$ est un module à gauche de type fini sur $k[x]$ et *a fortiori* sur $C(x)$.

10.7. Corollaire. — *Soient $x \in A_1$ un élément de type semi-simple, et Λ l'ensemble des valeurs propres de* $\mathrm{ad}_{A_1} x$. *On est dans l'un des cas suivants :*

(*a*) $\Lambda \subset k$; *alors* $D(x, A_1) = \bigoplus_{\lambda \in k} D(x, \lambda; A_1)$;

(*b*) $\Lambda \cap k = \{0\}$; *alors $\lambda^2 \in k$ pour tout $\lambda \in \Lambda$; si λ_0 est un élément non nul de Λ, il existe un sous-groupe additif G de $\mathbf{Q}$ tel que $\Lambda = G\lambda_0$; on a $D(x, \lambda; A_1) = 0$ pour tout $\lambda \in \Lambda - \{0\}$.*

Démonstration. — Si $\Lambda \subset k$, on a évidemment $D(x; A_1) = \bigoplus_{\lambda \in k} D(x, \lambda; A_1)$. Nous supposerons désormais qu'il existe un $\lambda_0 \in \Lambda$ tel que $\lambda_0 \notin k$. D'après la proposition 10.6, on a $\Lambda \cap k = \{0\}$, et $\Lambda = G\lambda_0$, où G est un sous-ensemble de $\mathbf{Q}$ stable par addition. Soit Γ le groupe de Galois de k sur k. Si $g \in \Gamma$, on a $g(\lambda_0) \in \Lambda$, donc il existe $\alpha \in \mathbf{Q} - \{0\}$ tel que $g(\lambda) = \alpha\lambda$. Par suite, $g^n(\lambda_0) = \alpha^n \lambda_0$ pour $n = 0, 1, 2, \ldots$. Donc $\alpha = \pm 1$. Alors $g(\lambda_0^2) = \lambda_0^2$, d'où $\lambda_0^2 \in k$, et $\lambda^2 \in k$ pour tout $\lambda \in \Lambda$. Il existe $g_0 \in \Gamma$ tel que $g_0(\lambda_0) \neq \lambda_0$, d'où $g_0(\lambda_0) = -\lambda_0$. Si $\alpha \in G$, on a $\alpha\lambda_0 \in \Lambda$, d'où $-\alpha\lambda_0 = g_0(\alpha\lambda_0) \in \Lambda$, donc $-\alpha \in G$. Ainsi, G est un sous-groupe additif de $\mathbf{Q}$. Puisque $\Lambda \cap k = \{0\}$, il est clair que $D(x, \lambda; A_1) = 0$ pour tout $\lambda \in \Lambda - \{0\}$.

10.8. Proposition. — *Soient x, y des éléments non nuls de A_1 tels que $[x, y] = \lambda y$, avec $\lambda \in k$, $\lambda \neq 0$.*

(i) *$x + y$ est de type semi-simple;*

(ii) *y est de type nilpotent, et $x^i y^j \in N(y)$ quels que soient les entiers $i \geq 0$, $j \geq 0$;*

(iii) *si $C(x) = k[x]$, on a $\sum_{r=0}^{\infty} D(x, -\lambda r) \subset N(y)$.*

Démonstration. — On a $[x + y, y] = \lambda y$, donc $x + y$ est de type semi-simple. D'autre part, $(\mathrm{ad}\, y)\, x \neq 0$, $(\mathrm{ad}\, y)^2 x = 0$, donc y est de type nilpotent, et x, $y \in N(y)$, ce qui prouve (ii). Supposons $C(x) = k[x]$. On a $C(x) \subset N(y)$ d'après (ii). D'autre part, $(\operatorname{ad} y) D(x, -\lambda r) \subset D(x, -\lambda r + \lambda)$, d'où

$$(\operatorname{ad} y)^r D(x, -\lambda r) \subset D(x, 0) = C(x) \subset N(y)$$

pour tout entier $r \geqq 0$.

10.9. Par exemple, soient i et j des entiers $\geqq 0$ tels que $i \neq j$. On a $\left[\frac{1}{j-i} pq, p^i q^j\right] = p^i q^j$ d'après (4). Donc $\frac{1}{j-i} pq + p^i q^j$ est de type semi-simple, et $p^i q^j$ est de type nilpotent. Si de plus $i \neq 0$ et $j \neq 0$, on a $F(p^i q^j) \neq A_1$ et $F\left(\frac{1}{j-i} pq + p^i q^j\right) \neq A_1$ d'après la fin de la démonstration du lemme 8.7. Donc Δ_2 et Δ_4 sont non vides.

10.10. Soit $x \in A_1$. Alors $\operatorname{ad} x \mid N(x)$ est une dérivation localement nilpotente de $N(x)$; donc $u = \exp(\operatorname{ad} x \mid N(x))$ est un automorphisme de $N(x)$. Si $y \in N(x)$ est de type strictement nilpotent (resp. strictement semi-simple), $u(y)$ est donc de type nilpotent (resp. semi-simple), mais pas en général de type strictement nilpotent (resp. strictement semi-simple).

Par exemple, soit $x = p^{id} q^{(i-1)d}$ avec i, d entiers > 0. D'après la proposition 5.3, on a $x = x'^d$ avec x' homogène de degré 1. D'après les propositions 10.8 (où l'on remplace x par pq et y par x') et 5.3, tout élément de A_1 de degré $\leqq 0$ appartient à $N(x')$, donc à $N(x)$ (prop. 10.3). En particulier, $q \in N(x)$, donc $(\exp \operatorname{ad} x) q$ est défini et de type nilpotent.

10.11. Le calcul de l'élément $(\exp \operatorname{ad} x) q$ précédent nécessite quelque soin. Observons d'abord que, pour l et m entiers $\geqq 1$, on a

$$\begin{aligned}
[p^l q^m, p^{l-1} q^{m-1}] &= [p(p^{l-1} q^{m-1}) q, p^{l-1} q^{m-1}] \\
&= [p, p^{l-1} q^{m-1}] p^{l-1} q^m + p^l q^{m-1} [q, p^{l-1} q^{m-1}] \\
&= (m-1) p^{l-1} q^{m-2} p^{l-1} q^m - (l-1) p^l q^{m-1} p^{l-2} q^{m-1} \\
&= (m-1) p^{l-1} q^{m-2} [p^{l-1}, q] q^{m-1} + (m-1) p^{l-1} q^{m-1} p^{l-1} q^{m-1} \\
&\quad - (l-1) p^{l-1} [p, q^{m-1}] p^{l-2} q^{m-1} - (l-1) p^{l-1} q^{m-1} p^{l-1} q^{m-1} \\
&= (m-1)(l-1) p^{l-1} q^{m-2} p^{l-2} q^{m-1} \\
&\quad - (l-1)(m-1) p^{l-1} q^{m-2} p^{l-2} q^{m-1} \\
&\quad + (m-l) p^{l-1} q^{m-1} p^{l-1} q^{m-1},
\end{aligned}$$

d'où

$$[p^l q^m, p^{l-1} q^{m-1}] = (m-l)(p^{l-1} q^{m-1})^2 \tag{25}$$

et par suite, pour n entier $\geqq 0$,

$$[p^l q^m, (p^{l-1} q^{m-1})^n] = (m-l) n (p^{l-1} q^{m-1})^{n+1}. \tag{26}$$

Si l et r sont des entiers $\geqq 0$ tels que $l - r \geqq 1$, on a

$$[p^l q^{l-r}, q] = l(p^{l-1} q^{l-r-1}) q. \tag{27}$$

Supposons prouvé que

$$(28)\qquad (\operatorname{ad} p^l q^{l-r})^n q = l(l-r)\ldots(l-(n-1)\,r)\,(p^{l-1} q^{l-r-1})^n q.$$

On en déduit

$$(\operatorname{ad} p^l q^{l-r})^{n+1} q = l(l-r)\ldots(l-(n-1)r)\,[p^l q^{l-r},\ (p^{l-1} q^{l-r-1})^n q],$$

et cela est égal, d'après (26) et (27), à

$$\begin{aligned} &l(l-r)\ldots(l-(n-1)\,r)\,(-rn\,(p^{l-1} q^{l-r-1})^{n+1} q + (p^{l-1} q^{l-r-1})^n\, l(p^{l-1} q^{l-r-1})\, q) \\ &\quad = l(l-r)\ldots(l-(n-1)\,r)\,(l-nr)\,(p^{l-1} q^{l-r-1})^{n+1} q, \end{aligned}$$

donc la formule (28) est établie par récurrence. En particulier, pour i, d entiers tels que $i \geq 2$, $d \geq 1$, on a

$$(\operatorname{ad} p^{id} q^{(i-1)d})^n q = i\,(i-1)\ldots(i-n+1)\,(dp^{id-1} q^{(i-1)d-1})^n q,$$

et l'on vérifie de nouveau que $q \in N\,(p^{id} q^{(i-1)d})$. En outre, pour $\lambda \in k$,

$$\begin{aligned} \left(\exp \operatorname{ad} \frac{\lambda}{d} p^{id} q^{(i-1)d}\right) q = \Big(1 &+ \frac{i}{1!}\,\lambda\, p^{id-1} p^{(i-1)d-1} \\ &+ \frac{i(i-1)}{2!}\,(\lambda\, p^{id-1} q^{(i-1)d-1})^2 + \ldots\Big)\, q, \end{aligned}$$

d'où

$$(29)\qquad \left(\exp \operatorname{ad} \frac{\lambda}{d} p^{id} q^{(i-1)d}\right) q = (1 + \lambda\, p^{id-1} q^{(i-1)d-1})^i q.$$

Ainsi, l'élément $(1 + \lambda\, p^{id-1} q^{(i-1)d-1})^i q$ est de type nilpotent. Mais, si $\lambda \neq 0$, cet élément n'est pas de type strictement nilpotent (lemme 8.7).

10.12. L'élément $\left(\exp \operatorname{ad} \frac{1}{d}\, p^{id} q^{(i-1)d}\right) p$ n'est pas défini. Toutefois, un calcul analogue au précédent fournit pour cet « élément » le développement formel

$$p\left(1 + \frac{-i+1}{1!}\, p^{id-1} q^{(i-1)d-1} + \frac{(-i+1)(-i)}{2!}\,(p^{id-1} q^{(i-1)d-1})^2 + \ldots\right),$$

auquel il est raisonnable d'attribuer la valeur

$$(30)\qquad p\,(1 + p^{id-1} q^{(i-1)d-1})^{-i+1}$$

dans le corps des fractions D_1 de A_1. On observera que D_1 est aussi le corps des fractions de $N\,(p^{id} q^{(i-1)d})$, que l'automorphisme $\exp \operatorname{ad} \frac{1}{d}\, p^{id} q^{(i-1)d}$ de $N(p^{id} q^{(i-1)d})$ se prolonge en un automorphisme u de D_1 et que u transforme p en l'élément (30).

11. Problèmes.

11.1. Tout endomorphisme de A_1 est-il un automorphisme ? Autrement dit, si P, Q sont deux éléments de A_1 tels que $[P, Q] = 1$, engendrent-ils A_1 ? (A. A. Kirillov m'informe que l'école de Moscou a aussi considéré ce problème).

11.2. Peut-on classer les éléments de type semi-simple et les éléments de type nilpotent modulo les automorphismes de A_1, en analogie avec les théorèmes 9.1 et 9.2 ?

11.3. Si $x \in A_1$ est de type semi-simple, l'ensemble des valeurs propres de $\text{ad}_{\overline{A}_1} x$ est-il de la forme $\mathbf{Z}\rho$, où $\rho \in k$?

11.4. L'algèbre G de la proposition 10.2 est-elle de type fini ?

11.5. Soit x un élément de type nilpotent. Posons $I_n = (\text{ad}\, x)^n N(x, n)$; c'est un idéal de $C(x)$. A-t-on $I_{n+1} = I_1 . I_n$ pour n assez grand ?

11.6. Si $x \in \Delta_5$, a-t-on $k[x] - k \subset \Delta_5$?

BIBLIOGRAPHIE.

[1] Amitsur (S. A.). — Commutative linear differential operators, *Pacific J. of Math.*, t. 8, 1958, p. 1-10.

[2] Bernat (Pierre). — Sur le corps enveloppant d'une algèbre de Lie résoluble, *Bull. Soc. math. France, Mémoire* n° 7, 1966, 175 p.

[3] Dixmier (Jacques). — Sur les représentations unitaires des groupes de Lie nilpotents, II, *Bull. Soc. math. France*, t. 85, 1957, p. 325-388.

[4] Dixmier (Jacques). — Représentations irréductibles des algèbres de Lie nilpotentes, *Anais Acad. Bras. Cienc.*, t. 35, 1963, p. 491-519.

[5] Dixmier (Jacques). — Représentations irréductibles des algèbres de Lie résolubles, *J. Math. pures et appl.*, 9e série, t. 45, 1966, p. 1-66.

[6] Gel'fand (I. M.) et Kirillov (A. A.). — *Sur les corps liés aux algèbres enveloppantes des algèbres de Lie*, Paris, Presses universitaires de France, 1966 (*Institut des Hautes Études scientifiques, Publications mathématiques*, t. 31, p. 5-19).

[7] Littlewood (D. E.). — On the classification of algebras, *Proc. London math. Soc.*, t. 35, 1933, p. 200-240.

[8] Nouazé (Y.) et Gabriel (P.). — Idéaux premiers de l'algèbre enveloppante d'une algèbre de Lie nilpotente, *J. of Algebra*, t. 6, 1967, p. 77-99.

[9] Rentschler (R.) et Gabriel (P.). — Sur la dimension des anneaux et ensembles ordonnés, *C. R. Acad. Sc. Paris*, t. 265, 1967, série A, p. 712-715.

[10] Rinehart (George S.). — Note on the global dimension of a certain ring, *Proc. Amer. math. Soc.*, t. 13, 1962, p. 341-346.

[11] Segal (I. E.). — *Quantized differential forms* (à paraître).

[12] Solomon (L.) et Verma (D.-N.). — Sur le corps des quotients de l'algèbre enveloppante d'une algèbre de Lie, *C. R. Acad. Sc. Paris*, t. 264, 1967, série A, p. 985-986.

(Manuscrit reçu le 5 février 1968.)

Jacques Dixmier,
Professeur à la Faculté des Sciences de Paris,
64, rue Gay-Lussac, 75-Paris, 5e.