§ 15. Matrices inversibles et changements de bases

1. *Le groupe des automorphismes d'un module*

Rappelons (§ 12, n° 1) qu'on appelle *automorphisme* d'un module M tout homomorphisme bijectif de M dans M, i.e. tout isomorphisme de M sur M. Les automorphismes de M sont donc en particulier des permutations de l'ensemble M; et le Théorème 1 du § 12 montre que, si u et v sont des automorphismes de M, il en est de même de l'application $u \circ v^{-1}$; par suite, l'ensemble

$$\mathrm{GL}(\mathrm{M})$$

des automorphismes du module M est un sous-groupe du groupe $\mathfrak{S}(\mathrm{M})$ des permutations de l'ensemble M; on dit que GL(M) est le **groupe des automorphismes du module** M, ou encore le **groupe linéaire du module** M. Les groupes de la forme GL(M), et leurs sous-groupes, ont joué un rôle de premier plan dans le développement de la théorie générale des groupes.

On remarquera qu'on pourrait aussi définir le groupe GL(M) à partir de l'anneau Hom (M, M) des endomorphismes du module M; on a évidemment

$$\mathrm{GL}(\mathrm{M}) \subset \mathrm{Hom}\ (\mathrm{M}, \mathrm{M}),$$

et les éléments de GL(M) ne sont autres que les éléments inversibles de l'anneau Hom (M, M); si en effet un endomorphisme u est inversible dans l'anneau Hom (M, M), il existe un endomorphisme v tel que $u \circ v = v \circ u = j_{\mathrm{M}}$, et par suite u est bijectif, donc appartient à GL(M); et la réciproque est évidente. En conclusion, GL(M) *n'est autre que le groupe des éléments inversibles de l'anneau* Hom (M, M), au sens du § 8, *Remarque* 1.

2. *Les groupes* GL (n, K)

On dit qu'une matrice $\mathrm{U} \in \mathrm{M}_n(\mathrm{K})$ est **inversible** s'il existe une matrice $\mathrm{V} \in \mathrm{M}_n(\mathrm{K})$ telle que

$$\mathrm{UV} = \mathrm{VU} = 1_n.$$

autrement dit si U est un élément inversible de l'anneau $M_n(K)$; la matrice V est alors unique, se note U^{-1}, et s'appelle **l'inverse de** U. On note

$$GL(n, K)$$

l'ensemble des matrices carrées inversibles de degré n à coefficients dans K; muni de la loi de composition $(U, V) \mapsto UV$, cet ensemble est un groupe, appelé le **groupe linéaire à n variables sur l'anneau** K; ce n'est pas autre chose, par conséquent, que le groupe multiplicatif des éléments inversibles de l'anneau $M_n(K)$.

Soit M un module *libre de type fini*, et choisissons une base $a_1, \ldots, a_n$ de M; à chaque endomorphisme f de M on peut alors attacher sa matrice par rapport à la base en question (§ 12, n° 3); en la notant $A(f)$, on obtient une *bijection*

$$f \mapsto A(f)$$

de l'anneau Hom (M, M) sur l'anneau $M_n(K)$ des matrices carrées d'ordre n à coefficients dans K, et la façon même dont on a défini la somme et le produit de deux matrices montre qu'on a les relations

$$A(f+g) = A(f) + A(g), \qquad A(fg) = A(f)A(g), \qquad A(j_M) = 1_n,$$

autrement dit que l'application $f \to A(f)$ est un *isomorphisme* (§ 8, n° 6) de l'anneau Hom (M, M) sur l'anneau $M_n(K)$.

Comme un isomorphisme d'un anneau U sur un anneau V applique évidemment l'ensemble U^* des éléments inversibles de U sur l'ensemble V^* des éléments inversibles de V, on en conclut que, *pour qu'un endomorphisme f de* M *soit un automorphisme de* M *il faut et il suffit que sa matrice* $A(f)$ *soit un élément inversible de l'anneau* $M_n(K)$; autrement dit, les relations

$$f \in GL(M) \qquad \text{et} \qquad A(f) \in GL(n, K)$$

sont équivalentes.

Si l'on identifie $M_n(K)$ à l'anneau des endomorphismes du K-module à droite K^n comme on l'a dit au § 14, n° 3, on voit donc que $GL(n, K)$ *s'identifie au groupe des automorphismes de* K^n, autrement dit au groupe des applications

$$(\xi_1, \ldots, \xi_n) \mapsto (\eta_1, \ldots, \eta_n)$$

de K^n dans K^n qui sont d'une part *bijectives* et d'autre part *linéaires*, i.e. données par des formules du type

$$\eta_j = \alpha_{1j}\xi_1 + \cdots + \alpha_{nj}\xi_n \quad (1 \leqslant j \leqslant n).$$

3. *Exemples : les groupes* GL (1, K) *et* GL (2, K)

Pour $n = 1$, l'anneau $M_n(K)$ est identique à l'anneau K lui-même, et par suite que le groupe GL(1, K) se réduit au groupe multiplicatif K^* des éléments inversibles de K.

Pour étudier le groupe GL(2, K), nous supposerons K *commutatif*. Pour qu'une

matrice

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

admette une inverse

$$A^{-1} = \begin{pmatrix} x & z \\ y & t \end{pmatrix}$$

il faut qu'il existe $x, y, z, t \in K$ tels que

$$(1) \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x & z \\ y & t \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

i.e. tels que

$$(2) \qquad \begin{cases} ax + by = 1 \\ cx + dy = 0 \end{cases} \qquad \begin{cases} az + bt = 0 \\ cz + dt = 1. \end{cases}$$

Pour trouver des conditions nécessaires et suffisantes de résolubilité des équations (2) introduisons la notion de *déterminant* d'une matrice carrée d'ordre 2 à coefficients dans un anneau commutatif K : pour une matrice

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

on appelle ainsi le scalaire $ad - bc$ qu'on désigne par

$$\text{dét}(A) \qquad \text{ou} \qquad \begin{vmatrix} a & b \\ c & d \end{vmatrix}$$

Nous étendrons plus loin cette définition aux matrices carrées d'ordre n quelconque.

Pour le moment, il nous suffira de savoir qu'on a

$$\text{dét}(AB) = \text{dét}(A) \cdot \text{dét}(B)$$

quelles que soient $A, B \in M_2(K)$; cette relation est en effet équivalente à l'identité

$$(ad - bc)(xt - yz) = (ax + by)(cz + dt) - (az + bt)(cx + dy),$$

que le lecteur vérifiera sans mal en tenant compte de la commutativité de K.

Cela fait, et comme le déterminant de la matrice unité 1_2 est évidemment égal à 1, la relation

$$\text{dét}(A) \cdot \text{dét}(A^{-1}) = 1$$

montre que, pour que la matrice A soit inversible, il est nécessaire que son déterminant le soit. Inversement, supposons $ad - bc$ inversible; considérons dans le système (2) les deux relations en x et y; elles seront visiblement vérifiées si l'on prend

$$x = (ad - bc)^{-1}d, \qquad y = (ad - bc)^{-1}c,$$

et les relations en z et t le seront pour

$$z = -(ad - bc)^{-1}b, \qquad t = (ad - bc)^{-1}a;$$

on vérifie facilement que la matrice

$$\begin{pmatrix} x & z \\ y & t \end{pmatrix}$$

ainsi construire est inverse à droite *et* à gauche de A.

En conclusion, si K est un anneau commutatif, la matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *est inversible si et seulement si* $ad - bc$ *est inversible dans* K.

Si par exemple K est un *corps commutatif*, GL(2, K) est formé des matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ telles que

$$ad - bc \neq 0.$$

Par contre, le groupe GL(2, **Z**) est formé des matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ à coefficients entiers telles que

$$ad - bc = +1 \quad \text{ou} \quad -1.$$

Remarque 1. Soient L un anneau et K un sous-anneau de L; on peut évidemment considérer $M_n(K)$ comme un sous-anneau de $M_n(L)$. Cela dit, il peut arriver qu'une matrice

$$U \in M_n(K)$$

soit inversible dans l'anneau $M_n(L)$ sans l'être dans l'anneau $M_n(K)$: c'est ainsi que la matrice (2), ou la matrice $\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$, est inversible lorsqu'on la regarde comme matrice à coefficients dans le corps **Q**, mais ne l'est pas en tant que matrice à coefficients dans l'anneau **Z**. La notion de matrice inversible risque donc de prêter à confusion si l'on ne précise pas l'anneau de base choisi.

Cependant ce genre de difficulté ne se présente pas lorsque les anneaux de base considérés sont des *corps*; autrement dit, soient L un corps et K un sous-corps de L; alors si une matrice $U \in M_n(K)$ est inversible dans l'anneau $M_n(L)$, elle l'est déjà dans l'anneau $M_n(K)$. Voir une démonstration au § 20, *Exercice* 20; si L est commutatif, on peut aussi utiliser le Corollaire 1 du Théorème 18 du § 23.

4. *Changements de bases : matrices de passage*

Soit M un K-module à droite libre de type fini, et considérons deux bases $(a_1, \ldots a_n)$ et $(b_1, \ldots, b_n)$ de M ayant le même nombre n d'éléments [cette condition est d'ailleurs toujours réalisée si K est un corps (§ 19, Théorème 6), ou bien est commutatif (§ 23, Corollaire du Théorème 5)]. On se propose, pour chaque $x \in M$, de calculer les coordonnées de x par rapport à la seconde base en fonction de ses coordonnées par rapport à la première.

Considérons pour cela les homomorphismes

$$u, v : K^n \to M$$

donnés par

$$u(e_i) = a_i \qquad v(e_i) = b_i \qquad (1 \leqslant i \leqslant n) \tag{3}$$

où $e_1, \ldots, e_n$ est la base canonique de K^n. Pour que (a_i) et (b_i) soient des bases de M il faut et il suffit que u et v soient des isomorphismes (§ 12, Corollaire 1 du Théorème 3) et si l'on désigne par $\xi_1, \ldots, \xi_n$ les coordonnées de x par rapport à la base (a_i), par $\eta_1, \ldots, \eta_n$ ses coordonnées par rapport à la base (b_i), on a les relations

$$x = u(\xi_1, \ldots, \xi_n) = v(\eta_1, \ldots, \eta_n);$$

en introduisant l'*automorphisme* (§ 12, Théorème 1)

$$w = v^{-1} \circ u \tag{4}$$

de K^n, on a donc

$$(\eta_1, \ldots, \eta_n) = w(\xi_1, \ldots, \xi_n);$$

et en désignant par

$$(\alpha_{ij})_{1 \leqslant i, j \leqslant n}$$

la matrice de w par rapport à la base canonique de K^n, on obtient les formules

$$\eta_j = \alpha_{1j}\xi_1 + \cdots + \alpha_{nj}\xi_n \quad (1 \leqslant j \leqslant n) \tag{5}$$

qui résolvent le problème posé. On les appelle les **formules de changement de coordonnées,** et la matrice (α_{ij}) qui figure dans ces formules s'appelle la **matrice de passage de la base** $(a_i)_{1 \leqslant i \leqslant n}$ **à la base** $(b_i)_{1 \leqslant i \leqslant n}$; comme c'est la matrice d'un *automorphisme* de K^n, on a

$$(\alpha_{ij}) \in GL(n, K).$$

On observera que la relation (4) s'écrit aussi $u = v \circ w$, et implique donc

$$v = u \circ w^{-1}; \tag{6}$$

soit

$$(\beta_{ij}) = (\alpha_{ij})^{-1}$$

la matrice de w^{-1} (par rapport à la base canonique de K^n), matrice qui est nécessairement l'inverse de la matrice de passage (α_{ij}); on a les relations

$$w^{-1}(e_i) = e_1\beta_{i1} + \cdots + e_n\beta_{in},$$

et en tenant compte de (3) il vient

$$\begin{aligned} b_i = v(e_i) &= u[w^{-1}(e_i)] = u(e_1\beta_{i1} + \cdots + e_n\beta_{in}) \\ &= u(e_1)\beta_{i1} + \cdots + u(e_n)\beta_{in} \end{aligned}$$

i.e.

$$b_i = a_1\beta_{i1} + \cdots + a_n\beta_{in} \qquad (1 \leqslant i \leqslant n); \tag{7}$$

on aura soin d'observer que les matrices (α_{ij}) et (β_{ij}) figurant dans les relations (5) et (7) sont non pas identiques mais *inverses l'une de l'autre.*

On démontrerait par un calcul analogue les relations

$$a_i = b_1\alpha_{i1} + \cdots + b_n\alpha_{in}. \tag{7 bis}$$

Remarque 2. Le cas le plus simple est celui où $n = 1$; on a alors deux bases (a) et (b) comprenant chacune un vecteur, avec les relations

$$x = a\xi = b\eta;$$

posant

$$\eta = \alpha\xi$$

on doit avoir $a\xi = b\alpha\xi$ quel que soit ξ, donc $a = b\alpha$, i.e.

$$b = a\alpha^{-1}.$$

Autrement dit, si l'on remplace le vecteur de base a par le vecteur $a\alpha$, la coordonnée ξ de x est remplacée par $\alpha^{-1}\xi$, ce qui est conforme au bon sens puisque le produit $a\xi$ doit rester constant !

Les résultats précédents permettent, à partir d'une base de M, d'en construire toutes les autres :

THÉORÈME 1. *Soit $a_1, \ldots, a_n$ une base d'un* K*-module à droite* M. *Pour que les vecteurs*

$$b_i = a_1\beta_{i1} + \cdots + a_n\beta_{in} \quad (1 \leqslant i \leqslant n)$$

forment une base de M, *il faut et il suffit que la matrice $(\beta_{ij})_{1 \leqslant i,j \leqslant n}$ soit inversible dans l'anneau* $\mathrm{M}_n(\mathrm{K})$.

Considérons en effet les homomorphismes $u, v : \mathrm{K}^n \to \mathrm{M}$ donnés par les formules (3); on sait, puisque les a_i forment une base, que u est bijectif. Pour exprimer que les b_i forment une base, on doit exprimer que v est bijectif, ou, ce qui revient évidemment au même, que $u^{-1} \circ v$ est un *auto*morphisme de K^n; or on a

$$\begin{aligned} u^{-1} \circ v(e_i) &= u^{-1}(b_i) = u^{-1}(a_1\beta_{i1} + \cdots + a_n\beta_{in}) \\ &= u^{-1}(a_1)\beta_{i1} + \cdots + u^{-1}(a_n)\beta_{in} \\ &= e_1\beta_{i1} + \cdots + e_n\beta_{in}; \end{aligned}$$

il s'ensuit que (β_{ij}) est précisément la matrice de l'endomorphisme $u^{-1} \circ v$ de K^n; comme un endomorphisme de K^n est bijectif si et seulement si sa matrice est dans $\mathrm{GL}(n, \mathrm{K})$, le Théorème est démontré.

La condition du Théorème 1 peut encore s'obtenir en introduisant l'endomorphisme f de M tel que

$$f(a_i) = b_i \quad (1 \leqslant i \leqslant n)$$

(son existence résulte du § 12, Théorème 3); pour que les b_i forment une *base* de M, il faut et il suffit que f soit un *automorphisme* de M (§ 12, Corollaire 1 du Théorème 3); or, la matrice (β_{ij}) n'est autre que la matrice de f par rapport à la base (a_i) de M.

Ce résultat est d'ailleurs évident directement, car en introduisant à nouveau les homomorphismes u et v ci-dessus on a

$$f = v \circ u^{-1};$$

comme u est bijectif, dire que v est bijectif revient à dire que f l'est...

5. *Influence d'un changement de bases sur la matrice d'un homomorphisme*

Soient L et M deux K-modules à droite libres de type fini et $f : \mathrm{L} \to \mathrm{M}$ un homomorphisme. Soient

$$(a'_1, \ldots, a'_p) \qquad \text{et} \qquad (a''_1, \ldots, a''_p)$$

deux bases de L possédant le même nombre p d'éléments, et

$$(b'_1, \ldots, b'_q) \qquad \text{et} \qquad (b''_1, \ldots, b''_q)$$

deux bases de M ayant le même nombre q d'éléments. Soit A' la matrice de f par rapport aux bases (a'_i) et (b'_j), et soit A'' sa matrice par rapport aux bases (a''_i) et (b''_j); on se propose de *calculer* A'' *en fonction de* A', *de la matrice*

$$\mathrm{U} \in \mathrm{GL}(p, \mathrm{K})$$

qui fait passer de la base (a'_i) à la base (a''_i), et de la matrice

$$\mathrm{V} \in \mathrm{GL}(q, \mathrm{K})$$

qui fait passer de la base (b'_j) à la base (b''_j).

Pour cela considérons les homomorphismes $u'; u'' : \mathrm{K}^p \to \mathrm{L}$ qui appliquent la base canonique de K^p sur les bases (a'_i) et (a''_i) respectivement, et les homomorphismes $v', v'' : \mathrm{K}^q \to \mathrm{M}$ qui appliquent la base canonique de K^q sur les bases (b'_j) et (b''_j) de M respectivement. On a des relations $u' = u'' \circ u$, $v' = v'' \circ v$ où u (resp. v) est un automorphisme de K^p (resp. K^q) dont la matrice par rapport à la base canonique de K^p (resp. K^q) est précisément U (resp. V) en vertu du n° précédent. D'autre part, si l'on introduit les homomorphismes

$$f', f'' : \mathrm{K}^p \to \mathrm{K}^q$$

donnés par

$$f' = v'^{-1} \circ f \circ u', \qquad f'' = v''^{-1} \circ f \circ u''$$

alors les matrices A' et A'' définies plus haut ne sont autres que les matrices de f' et f'' par rapport aux bases canoniques de K^p et K^q en vertu du § 12, *Remarque* 2. Or en introduisant les applications u et v définies ci-dessus il vient

$$\begin{aligned} f' &= (v'' \circ v)^{-1} \circ f \circ (u'' \circ u) \\ &= v^{-1} \circ v''^{-1} \circ f \circ u'' \circ u = v^{-1} \circ f'' \circ u; \end{aligned}$$

comme la composition de deux homomorphismes se traduit par la multiplication de leurs matrices, on a donc, en prenant les matrices de u, v, f', f'' par rapport aux bases canoniques, la relation

$$\mathrm{A}' = \mathrm{V}^{-1}.\mathrm{A}''.\mathrm{U},$$

laquelle résoud le problème posé au début de ce n°. Ainsi :

THÉORÈME 2. *Soient* L *et* M *deux* K*-modules à droite libres de type fini, f un homomorphisme*

de L *dans* M, A′ *la matrice de f par rapport à une base* $(a'_i)_{1\leqslant i\leqslant p}$ *de* L *et à une base* $(b'_j)_{1\leqslant j\leqslant q}$ *de* M, *et* A″ *sa matrice par rapport à une base* $(a''_i)_{1\leqslant i\leqslant p}$ *de* L *et à une base* $(b''_j)_{1\leqslant j\leqslant q}$ *de* M. *Soient en enfin* U *la matrice de passage de la base* (a'_i) *à la base* (a''_i), *et* V *la matrice de passage de la base* (b'_j) *à la base* (b''_j). *On a alors la relation*

$$A' = V^{-1}A''U.$$

Lorsqu'en particulier L = M, on peut supposer dans ce qui précède que la base (b'_j) est identique à la base (a'_i), et la base (b''_j) identique à la base (a''_i), auquel cas on a évidemment U = V; donc :

COROLLAIRE. *Soient* L *un* K*-module à droite libre de type fini, f un endomorphisme de* L, *et*

$$(a'_i)_{1\leqslant i\leqslant p}, \qquad (a''_i)_{1\leqslant i\leqslant p}$$

deux bases de L *ayant le même nombre d'éléments. Soient* A′ *la matrice de f par rapport à la base* (a'_i) *et* A″ *sa matrice par rapport à la base* (a''_i). *On a alors la relation*

$$A'' = UA'U^{-1}$$

où U *est la matrice de passage de la base* (a'_i) *à la base* (a''_i).

Ce dernier résultat conduit à une notion importante : étant données des matrices

$$A', A'' \in M_p(K),$$

on dit que A′ et A″ sont **semblables** (sur l'anneau de base K) s'il existe une matrice

$$U \in GL(p, K)$$

telle que l'on ait la relation

$$A'' = UA'U^{-1}.$$

Remarque 3. Il existe toujours (Théorème 1) un changement de base admettant pour matrice de passage une matrice inversible arbitrairement choisie. On voit donc que le Théorème 2 admet une réciproque : si l'on se donne d'avance l'homomorphisme f, et les bases (a'_i) et (b'_j), donc la matrice A′, alors quelles que soient les matrices $U \in GL(p, K)$ et $V \in GL(q, K)$ il existe dans L et M des bases par rapport auxquelles f est représenté par la matrice

$$V^{-1}A'U.$$

On a un résultat analogue dans la situation décrite par le Corollaire.

Remarque 4. La démonstration que nous avons donnée du Théorème 2 évite tout calcul explicite, mais oblige par contre à passer par l'intermédiaire des modules « prototypes » K″ et K′, ce qui risque de gêner le lecteur débutant.

On peut encore démontrer le Théorème 2 comme suit. Soient U et V les matrices de passage, et posons

$$U^{-1} = (\omega_{ij})_{1\leqslant i,j\leqslant p}, \qquad V^{-1} = (\rho_{kh})_{1\leqslant k,h\leqslant q};$$

d'après le n° 4 on a alors les relations

$$a'_i = \sum_j a'_j\omega_{ij}; \qquad b'_k = \sum_h b'_h\rho_{kh}; \tag{8}$$

d'autre part, en posant

$$A' = (\alpha'_{jh})_{1\leqslant j\leqslant p,\ 1\leqslant h\leqslant q}$$
$$A'' = (\alpha''_{ik})_{1\leqslant i\leqslant p,\ 1\leqslant k\leqslant q}$$

il vient

$$f(a'_j) = \sum_h b'_h\alpha'_{jh}; \qquad f(a''_i) = \sum_k b''_k\alpha''_{ik}; \tag{9}$$

tenant compte de (8), la seconde relation (9) s'écrit

$$\sum_j f(a'_j)\omega_{ij} = \sum_k\sum_h b'_h\rho_{kh}\alpha''_{ik},$$

ou encore, d'après la première relation (9),

$$\sum_j\sum_h b'_h\alpha'_{jh}\omega_{ij} = \sum_k\sum_h b'_h\rho_{kh}\alpha''_{ik};$$

comme les vecteurs b'_h sont linéairement indépendants, leurs coefficients dans les deux membres doivent être égaux, ce qui conduit à la relation

$$\sum_j \alpha'_{jh}\omega_{ij} = \sum_k \rho_{kh}\alpha''_{ik},$$

valable quels que soient i et h. Or au premier membre figure le coefficient d'indices h et i de la matrice $A'U^{-1}$, et au second membre le coefficient d'indices h et i de la matrice $V^{-1}A''$; il vient donc $A'U^{-1} = V^{-1}A''$, d'où la relation cherchée $A'' = VA'U^{-1}$.

Les calculs de ce genre étaient autrefois fréquents en Algèbre linéaire et dans la théorie des « tenseurs », et impressionnaient grandement (et à juste titre) les nombreuses personnes qui croyaient qu'Einstein était seul à pouvoir comprendre ses propres travaux. Aujourd'hui, la plupart des mathématiciens préfèrent remplacer les déluges d'indices par des raisonnements géométriques ou, pour mieux dire, conceptuels, qui ont l'avantage d'être beaucoup plus simples. Néanmoins, la plupart des physiciens utilisent encore des méthodes analogues à celle qu'on a exposée dans cette *Remarque* (ce qui est d'autant plus étrange qu'un physicien, encore plus qu'un mathématicien, devrait s'intéresser aux objets « géométriques » ou « physiques » et non pas à leurs coordonnées, tout au moins aussi longtemps qu'il n'a pas en vue des calculs effectifs). Il est donc utile de se familiariser avec les calculs sur les indices et les Σ, même en sachant qu'ils sont théoriquement superflus.

§ 16. Transposée d'une application linéaire

1. *Dual d'un module*

Soit L un module *à droite* sur un anneau quelconque K. Rappelons (§ 12, n° 4, *Exemple* 3) qu'on appelle *forme linéaire sur* L tout homomorphisme de L dans le K-module à droite K, autrement dit toute application

$$f : \mathrm{L} \to \mathrm{K}$$

telle que l'on ait

$$f(x\alpha + y\beta) = f(x)\alpha + f(y)\beta \tag{1}$$

quels que soient $x, y \in \mathrm{L}$ et $\alpha, \beta \in \mathrm{K}$. En vertu du § 13, ces formes linéaires sur L sont les éléments du *groupe commutatif* Hom (L, K), la somme $f + g$ de deux formes linéaires sur L étant par définition la fonction $f(x) + g(x)$.

Nous allons voir (en utilisant le fait que K est non seulement un K-module à droite mais aussi un K-module à gauche) qu'en fait on peut regarder l'ensemble Hom (L, K) non seulement comme un groupe commutatif mais même comme un K-*module à gauche*. Soient pour cela une forme linéaire f sur L et un scalaire $\lambda \in \mathrm{K}$; considérons sur L la fonction g donnée par

$$g(x) = \lambda \cdot f(x);$$

en multipliant à gauche par λ la relation (1), et en tenant compte des règles de calcul (associativité, distributivité) dans un anneau, il vient

$$g(x\alpha + y\beta) = g(x)\alpha + g(y)\beta,$$

ce qui prouve que g est encore une forme linéaire sur L. On écrit naturellement

$$g = \lambda f,$$

et on a ainsi défini que l'ensemble Hom (L, K) une seconde opération, consistant à « multiplier » un élément de cet ensemble par un scalaire. Il resterait à voir que

l'ensemble Hom (L, K), muni de l'addition définie au § 13 et de la seconde opération que nous venons de définir, est effectivement un K-module à gauche; on laisse au lecteur le soin de le faire à titre d'exercice (on peut aussi utiliser le fait suivant : soit E l'ensemble de *toutes* les applications de L dans K, linéaires ou non; en regardant L comme un simple ensemble, et K comme un K-module à gauche, l'*Exemple* 4 du § 10 permet de considérer E comme un K-module à gauche; cela dit, pour faire de même avec Hom (L, K), il suffit de montrer que Hom (L, K) est un sous-module de E — ce qui était évidemment le but des considérations qui précèdent).

L'ensemble Hom (L, K), muni de la « structure » de K-module à gauche que nous venons de définir, s'appelle le **dual du K-module à droite** L; on le désigne généralement par la notation

$$\mathrm{L}^*,$$

plus commode que Hom (L, K).

Si l'on partait d'un K-module *à gauche* L, on définirait de même son dual; ce serait, cette fois, un K-module *à droite*.

Rappelons à ce sujet que les distinctions entre « droite » et « gauche » n'ont aucun intérêt si l'anneau de base K est commutatif, ce qui, dans la pratique, est presque toujours le cas.

Remarque 1. Soit f une forme linéaire sur un K-module à droite L; pour montrer que λf est encore linéaire, on peut aussi observer qu'elle est composée de f et de l'application $\xi \mapsto \lambda\xi$ de K dans K; il suffit donc de montrer que cette dernière application est un endomorphisme du K-module *à droite* K, autrement dit vérifie

$$\lambda(\xi + \eta) = \lambda\xi + \lambda\eta, \qquad \lambda(\xi\mu) = (\lambda\xi)\mu,$$

ce qui est clair.

Soit L un K-module à droite; puisqu'on a défini sur l'ensemble L^* des formes linéaires sur L une structure de K-module à gauche, on peut appliquer à L^* les définitions et théorèmes de la théorie des modules. En particulier, étant données des formes linéaires $f_1, \ldots, f_p$ sur L, on dira qu'une forme linéaire f sur L est *combinaison linéaire de* $f_1, \ldots, f_p$ s'il existe des scalaires $\lambda_1, \ldots, \lambda_p \in \mathrm{K}$ tels que l'on ait

$$f = \lambda_1 f_1 + \cdots + \lambda_p f_p,$$

relation qui, vu la définition des opérations sur les formes linéaires, signifie que

$$f(x) = \lambda_1 f_1(x) + \cdots + \lambda_p f_p(x) \quad \text{pour tout} \quad x \in \mathrm{L}.$$

De même, on appellera *relation linéaire entre* $f_1, \ldots, f_p$ tout système

$$(\lambda_1, \ldots, \lambda_p) \in \mathrm{K}^p$$

de scalaires tels que l'on ait

$$\lambda_1 f_1 + \cdots + \lambda_p f_p = 0$$

dans L*, i.e.

$$\lambda_1 . f_1(x) + \cdots + \lambda_\rho . f_\rho(x) = 0 \quad \text{pour tout} \quad x \in \mathrm{L},$$

etc, etc...

2. *Dual d'un module libre de type fini*

Dans la pratique élémentaire, le débutant n'aura pas besoin de résultat plus « profond » que le suivant :

THÉORÈME 1. *Soient* L *un* K*-module à droite libre de type fini et* $(a_1, \ldots, a_n)$ *une base de* L. *Considérons l'application* $\theta : \mathrm{L}^* \to \mathrm{K}^n$, *donnée par*

$$\theta(f) = (f(a_1), \ldots, f(a_n));$$

alors θ *est un isomorphisme de* K*-modules à gauche, et* L* *possède une base* $(u_1, \ldots, u_n)$ *telle que l'on ait*

$$u_i(a_j) = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j. \end{cases}$$

Soient $\alpha_1, \ldots, \alpha_n$ des éléments arbitraires de K; le Théorème 3 du § 12 montre qu'il existe *une et une seule* $f \in \mathrm{L}^*$ telle que l'on ait $f(a_i) = \alpha_i$ pour $1 \leqslant i \leqslant n$, i.e. telle que

$$\theta(f) = (\alpha_1, \ldots, \alpha_n);$$

l'application θ est donc *bijective*. Pour montrer que c'est un isomorphisme, il reste à faire voir qu'elle est *linéaire*; or on a, pour $f, g \in \mathrm{L}^*$ et en posant $f + g = h$,

$$\begin{aligned} \theta(f+g) &= (h(a_1), \ldots, h(a_n)) = (f(a_1) + g(a_1), \ldots, f(a_n) + g(a_n)) \\ &= (f(a_1), \ldots, f(a_n)) + (g(a_1), \ldots, g(a_n)) = \theta(f) + \theta(g); \end{aligned}$$

d'autre part, en remplaçant f par λf, on multiplie évidemment les coefficients $f(a_i)$ à gauche par λ, d'où l'identité

$$\theta(\lambda f) = \lambda . \theta(f),$$

de sorte que θ est bien linéaire.

Pour terminer la démonstration du Théorème, il reste à prouver l'existence d'une base $(u_i)_{1 \leqslant i \leqslant n}$ de L* possédant les propriétés indiquées; or les relations imposées aux u_i signifient que

$$\begin{aligned} \theta(u_1) &= (1, 0, 0, \ldots, 0) \\ \theta(u_2) &= (0, 1, 0, \ldots, 0) \\ &\cdots\cdots\cdots\cdots\cdots \\ \theta(u_n) &= (0, 0, \ldots, 0, 1), \end{aligned}$$

autrement dit que θ applique la base $(u_i)_{1 \leqslant i \leqslant n}$ de L* sur la base canonique de K^n; comme θ est un isomorphisme de modules, l'existence de la base (u_i) cherchée est claire : il suffit de prendre les images par l'application θ^{-1} des éléments de la base canonique de K^n, ce qui termine la démonstration.

On notera que les relations imposées aux u_i donnent, pour tout élément

$$x = a_1\xi_1 + \cdots + a_n\xi_n$$

de L, la relation

$$u_i(x) = u_i(a_1)\xi_1 + \cdots + u_i(a_n)\xi_n = \xi_i;$$

autrement dit, les u_i ne sont autres que les *fonctions coordonnées du module* L *par rapport à la base* $(a_i)_{1 \leqslant i \leqslant n}$ *de* L (§ 11, n° 4). Pour toute $f \in \mathrm{L}^*$, soient $\alpha_1, \ldots, \alpha_n$ les coordonnées de f par rapport à la base $(u_i)_{1 \leqslant i \leqslant n}$ de L*; la relation

$$f = \alpha_1 u_1 + \cdots + \alpha_n u_n$$

s'écrit alors

$$f(x) = \alpha_1\xi_1 + \cdots + \alpha_n\xi_n \quad \text{pour tout } x \in \mathrm{L},$$

et par suite il vient

$$\alpha_i = f(a_i);$$

autrement dit, *les coordonnées de* f *par rapport à la base* (u_i) *de* L* *ne sont autres que les coefficients de* f *par rapport à la base* (a_i) *de* L, définis au § 12, *Exemple* 3.

Le Théorème 1 montre qu'à toute base (a_i) de L, on peut associer une base (u_i) de L*; on dit que (u_i) est la **base duale de la base** (a_i) de L.

3. *Bidual d'un module*

Soit L un module *à droite* sur un anneau K; nous lui avons attaché un module *à gauche* L* sur K; celui-ci possède à son tour un dual, qu'on note

$$\mathrm{L}^{**} = (\mathrm{L}^*)^*,$$

et qu'on appelle le **bidual** de L; comme L, c'est un K-module *à droite*. On définirait de même le **tridual** $\mathrm{L}^{***} = (\mathrm{L}^{**})^*$, le **quadridual** $\mathrm{L}^{****} = (\mathrm{L}^{***})^*$, et ainsi de suite indéfiniment.

On peut, dans tous les cas, définir une **application canonique de** L **dans** L**, de la façon suivante. Soit x un élément « fixe » de L, et considérons l'application

$$u : \mathrm{L}^* \to \mathrm{K}$$

donnée par

$$u(f) = f(x) \qquad \text{pour tout} \quad f \in \mathrm{L}^*;$$

elle consiste donc à associer à chaque forme linéaire f sur L sa valeur au point x de L. L'application u est *linéaire*, i.e. vérifie

$$u(\alpha f + \beta g) = \alpha . u(f) + \beta . u(g)$$

quels que soient $f, g \in \mathrm{L}^*$ et les scalaires $\alpha, \beta \in \mathrm{K}$; posant

$$\alpha f + \beta g = h,$$

la relation en question s'écrit en effet

$$h(x) = \alpha f(x) + \beta g(x),$$

et sous cette forme elle se réduit purement et simplement à la *définition* même de l'élément $h = \alpha f + \beta g$ de L^*.

Ainsi, u est une forme linéaire sur L^*, autrement dit $u \in L^{**}$, et de cette façon nous avons bien attaché à chaque $x \in L$ un $u \in L^{**}$; d'où une application de L dans L^{**}, et c'est, par définition, l'application canonique de L dans son bidual.

Cette application est d'ailleurs *linéaire*; soient en effet $x, y \in L$, $\alpha, \beta \in K$ et posons $z = x\alpha + y\beta$; soient $u, v, w \in L^{**}$ les images de x, y, z par l'application canonique; tout revient à établir la relation

$$w = u\alpha + v\beta;$$

mais comme u, v, w sont des formes linéaires sur L^*, celle-ci signifie

$$w(f) = u(f)\alpha + v(f)\beta \qquad \text{pour tout} \quad f \in L^*;$$

or, par définition de l'application canonique de L dans L^{**}, on a

$$u(f) = f(x), \qquad v(f) = f(y), \qquad w(f) = f(z)$$

et par suite tout revient à montrer que $f(z) = f(x)\alpha + f(y)\beta$, ou, en remplaçant z par sa valeur, que

$$f(x\alpha + y\beta) = f(x)\alpha + f(y)\beta \qquad \text{pour toute} \quad f \in L^*;$$

or cette identité n'est autre que celle qui définit les formes linéaires sur L.

THÉORÈME 2. *Soit* L *un module libre de type fini; l'application canonique de* L *dans son bidual est un isomorphisme.*

Pout établir ce Théorème il nous reste à faire voir que l'application canonique

$$j : L \to L^{**}$$

est bijective si L est libre de type fini. Or soient $(a_i)_{1 \leqslant i \leqslant n}$ une base de L, $(f_i)_{1 \leqslant i \leqslant n}$ la base duale dans L^*, et posons

$$u_i = j(a_i) \in L^{**};$$

il suffit évidemment de montrer que les u_i forment une *base* de L^{**} : nous allons en fait montrer qu'ils forment la base de L^{**} duale de la base (f_i) du module L^*, autrement dit qu'on a les relations

$$u_i(f_j) = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j. \end{cases}$$

Or, par définition de l'homomorphisme canonique de L dans L^{**}, on a

$$u_i(f) = f(a_i) \quad \text{pour tout } f \in L^*,$$

et par suite $u_i(f_j) = f_j(a_i)$; mais comme les f_j forment la base duale de la base (a_i) de L, on a les relations

$$f_j(a_i) = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j, \end{cases}$$

ce qui fournit les relations cherchées et achève la démonstration.

COROLLAIRE 1. *Soient* L *un* K*-module à droite libre de type fini et* u *une forme linéaire sur le module dual* L^*. *Alors il existe un et un seul* $x \in L$ *tel que l'on ait*

$$u(f) = f(x) \quad \textit{pour tout } f \in L^*.$$

En effet, il existe un et seul $x \in L$ tel que $u = j(x)$, où j désigne l'isomorphisme canonique de L sur son bidual.

COROLLAIRE 2. *Soient* L *un* K*-module à droite libre de type fini et* $(f_1, \ldots, f_n)$ *une base du module dual* L^*. *Alors, quels que soient* $\beta_1, \ldots, \beta_n \in K$, *il existe un et un seul* $x \in L$ *tel que l'on ait*

$$f_i(x) = \beta_i \quad (1 \leqslant i \leqslant n).$$

En effet, puisque les f_i forment une base de L^* il existe une et une seule forme linéaire u sur L^* telle que $u(f_i) = \beta_i$ pour tout i (§ 12, Théorème 3), et comme $u(f) = f(x)$ pour un $x \in L$ entièrement déterminé par u, le Corollaire est démontré.

4. *Transposé d'un homomorphisme*

Soient L et M deux K-modules à droite et $f : L \to M$ un homomorphisme. Soit u une forme linéaire sur M; alors l'application composée $u \circ f$ est évidemment (§ 12, Théorème 1) une forme linéaire sur L. On peut donc définir une application

$$^t f : M^* \to L^*$$

en posant

$$^t f(u) = u \circ f \quad \text{pour tout } u \in M^*.$$

L'application $^t f$ s'appelle la **transposée de l'homomorphisme** f.

Cette application est, comme f, un *homomorphisme*. Soient en effet $u, v \in M^*$; on a

$$^t f(u + v) = (u + v) \circ f = u \circ f + v \circ f$$

en vertu du § 14, Théorème 1, et par suite

$$^t f(u + v) = {}^t f(u) + {}^t f(v);$$

de même, pour tout $\lambda \in K$ notons h_λ l'homothétie $\xi \to \lambda\xi$ dans K; on a alors, pour tout $u \in M^*$,

$$ {}^t f(\lambda u) = {}^t f(h_\lambda \circ u) = (h_\lambda \circ u) \circ f = h_\lambda \circ (u \circ f) = h_\lambda \circ {}^t f(u) = \lambda . {}^t f(u) $$

ce qui établit la linéarité de l'application transposée ${}^t f$.

Remarque 2. La démonstration que nous venons de donner risque de paraître inintelligible au lecteur débutant, à cause de son aspect purement mécanique. Bien entendu on conseille vivement au lecteur de s'exercer à la retraduire en langage clair (en ramenant tout à la *définition* de la structure de module du dual d'un module). Cependant, on doit aussi faire observer que lorsqu'on énonce un théorème (par exemple le Théorème 1 du § 14) c'est dans l'espoir de s'en servir à l'occasion ! Cette Remarque s'applique aussi à la démonstration du résultat suivant.

THÉORÈME 2. *L'opération consistant à passer d'un homomorphisme à son transposé possède les propriétés suivantes :*

a) Soient L, M *deux* K*-modules à droite et* $f, g : L \to M$ *deux homomorphismes; on a*

$$ {}^t(f + g) = {}^t f + {}^t g. $$

b) Soient L, M, N *trois* K*-modules à droite,* $f : L \to M$ *et* $g : M \to N$ *deux homomorphismes; on a*

$$ {}^t(g \circ f) = {}^t f \circ {}^t g. $$

c) Soit L *un* K*-module à droite; le transposé d'un automorphisme (resp. de l'automorphisme identique) de* L *est un automorphisme (resp. l'automorphisme identique) de* L^*.

Pour établir l'assertion *a*), posons $h = f + g$; pour $u \in M^*$ on a

$$ {}^t h(u) = u \circ h = u \circ (f + g) = u \circ f + u \circ g = {}^t f(u) + {}^t g(u), $$

ce qui prouve que ${}^t h = {}^t f + {}^t g$ comme annoncé.

Pour établir *b*), posons $h = g \circ f$; pour $u \in N^*$ on a

$$ {}^t h(u) = u \circ h = u \circ (g \circ f) = (u \circ g) \circ f = {}^t g(u) \circ f = {}^t f[{}^t g(u)], $$

d'où ${}^t h = {}^t f \circ {}^t g$, ce qui prouve *b*).

Pour établir *c*) montrons d'abord que si $f : L \to L$ est l'application identique il en est de même de son transposé; on a en effet, pour toute forme linéaire u sur L,

$$ {}^t f(u) = u \circ f = u $$

puisque f est l'identité, d'où notre assertion. Ceci dit supposons que f soit un automorphisme de L; il y a donc un homomorphisme g de L tel que

$$ f \circ g = g \circ f = j_L; $$

il s'ensuit que

$$ {}^t g \circ {}^t f = {}^t f \circ {}^t g = {}^t(j_L) = j_{L^*}, $$

et par suite ${}^t f$ est bien un automorphisme de L^*. On a du reste, comme le montre le calcul précédent, la relation

$$ {}^t(f^{-1}) = ({}^t f)^{-1} $$

pour tout automorphisme f de L.

Remarque 3. On aura soin de ne pas remplacer l'assertion *b*) du Théorème 3 par la formule « évidente », mais fausse (et même dépourvue de sens), que voici :

$$ {}^t(f \circ g) = {}^t f \circ {}^t g. $$

5. *Transposée d'une matrice*

Soit $f : L \to M$ un homomorphisme de K-modules à droite libres de type fini. Choisissons une base $(a_1, \ldots, a_p)$ de L et une base $(b_1, \ldots, b_q)$ de M; désignons par $(u_1, \ldots, u_p)$ la base de L^* duale de la base $(a_1, \ldots, a_p)$ de L, et par $(v_1, \ldots, v_q)$ la base de M^* duale de la base $(b_1, \ldots, b_q)$ de M. Par rapport aux bases (a_i) et (b_j), l'homomorphisme

$$ f : L \to M $$

est représenté par une matrice de la forme

$$ (\alpha_{ij})_{1 \leqslant i \leqslant p,\ 1 \leqslant j \leqslant q}; $$

et par rapport aux bases (v_j) et (u_i), l'homomorphisme transposé

$$ {}^t f : M^* \to L^* $$

est représenté par une matrice de la forme

$$ (\beta_{ji})_{1 \leqslant i \leqslant p,\ 1 \leqslant j \leqslant q}; $$

on se propose de calculer celle-ci en fonction de la matrice de f.

Par définition de la matrice de ${}^t f$, on a les relations

$$ {}^t f(v_j) = \beta_{j1} u_1 + \cdots + \beta_{jp} u_p \quad (1 \leqslant j \leqslant q) $$

i.e.

$$ v_j \circ f = \beta_{j1} u_1 + \cdots + \beta_{jp} u_p; $$

cela signifie que pour tout $x \in L$ on a

$$ (y) \qquad v_j[f(x)] = \beta_{j1} . u_1(x) + \cdots + \beta_{jp} . u_p(x); $$

or en posant

$$ x = a_1 \xi_1 + \cdots + a_p \xi_p, \quad f(x) = b_1 \eta_1 + \cdots + b_q \eta_q $$

on a, d'après le n° 2, les relations

$$ u_i(x) = \xi_i, \qquad v_j[f(x)] = \eta_j; $$

par suite la relation (2) équivaut à

$$\tau_{ij} = \beta_{j1}\xi_1 + \cdots + \beta_{jp}\xi_p,$$

et comme par définition de la matrice (α_{ij}) de f on a aussi les relations

$$\tau_{ij} = \alpha_{1j}\xi_1 + \cdots + \alpha_{pj}\xi_p,$$

on voit en comparant les deux résultats que

$$\beta_{ji} = \alpha_{ij} \qquad \text{pour} \quad 1 \leqslant i \leqslant p,\ 1 \leqslant j \leqslant q.$$

Ce résultat conduit à introduire la définition suivante. Étant donnée une matrice

$$A = \begin{pmatrix} \alpha_{11} & \cdots & \alpha_{p1} \\ \cdots\cdots & & \cdots\cdots \\ \alpha_{1q} & \cdots & \alpha_{pq} \end{pmatrix}$$

à coefficients dans un anneau K, on appelle **transposée de** A la matrice

$${}^tA = \begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1q} \\ \cdots\cdots & & \cdots\cdots \\ \alpha_{p1} & \cdots & \alpha_{pq} \end{pmatrix}$$

obtenue, comme on dit, en « permutant les lignes et les colonnes » de A.

¶ *Remarque* 4. Le passage de A à ${}^tA$ correspond évidemment à celui de f à ${}^tf$ dans ce qui précède. Or, si f est un homomorphisme de K-modules *à droite*, ${}^tf$ est au contraire un homomorphisme de K-modules *à gauche*, i.e. de modules à droite sur l'anneau K^o opposé à K (§ 10, n° 4). Comme le calcul des matrices est adapté, lorsque K est non commutatif, à la théorie des modules *à droite*, *on doit donc regarder la transposée* ${}^tA$ *d'une matrice* A *à coefficients dans un anneau* K *comme une matrice à coefficients dans l'anneau opposé* K^o. C'est ce qu'on fera, sans y référer à nouveau, dans ce qui suit.

Bien entendu, les considérations qui précèdent sont superflues si l'anneau K est commutatif.

THÉORÈME 4. *Soit* K *un anneau.*

a) Étant données deux matrices A *et* B *à coefficients dans* K *on a la relation*

$${}^t(A + B) = {}^tA + {}^tB$$

pourvu que la somme A + B *soit définie.*

b) Étant données deux matrices A *et* B *à coefficients dans* K, *on a la relation* (*)

$${}^t(AB) = {}^tB.{}^tA$$

pourvu que le produit AB *soit défini.*

(*) Conformément à la *Remarque* 4, le produit ${}^tB.{}^tA$ doit être calculé dans l'anneau K^o opposé à K (i.e. dans l'anneau K si K est commutatif).

c) Si A *est une matrice carrée à coefficients dans* K, *pour que* A *soit inversible il faut et il suffit que* ${}^tA$ *le soit.*

d) Pour toute matrice A *à coefficients dans* K *on a*

$${}^t({}^tA) = A.$$

Pour prouver *a*), posons

$$A = (\alpha_{ij}), \qquad B = (\beta_{ij});$$

alors $A + B = (\alpha_{ij} + \beta_{ji})$, et par suite

$${}^t(A + B) = (\alpha_{ji} + \beta_{ji}) = (\alpha_{ji}) + (\beta_{ji}) = {}^tA + {}^tB.$$

Pour établir maintenant l'assertion *b*), posons

$$A = (\alpha_{jk})_{1 \leqslant j \leqslant q,\ 1 \leqslant k \leqslant r},\ B = (\beta_{ij})_{1 \leqslant i \leqslant p,\ 1 \leqslant j \leqslant q};$$

la matrice

$$AB = (\gamma_{ik})_{1 \leqslant i \leqslant p,\ 1 \leqslant k \leqslant r}$$

est donnée par les relations

$$\gamma_{ik} = \sum_j \alpha_{jk}\beta_{ij} \tag{3}$$

(cf. § 14, n° 2), les produits $\alpha_{jk}\beta_{ij}$ étant bien entendu calculés dans l'anneau K donné. D'autre part on a

$${}^tA = (\alpha'_{kj})_{1 \leqslant k \leqslant r,\ 1 \leqslant j \leqslant q} \qquad \text{avec} \qquad \alpha'_{kj} = \alpha_{jk},$$
$${}^tB = (\beta'_{ji})_{1 \leqslant j \leqslant q,\ 1 \leqslant i \leqslant p} \qquad \text{avec} \qquad \beta'_{ji} = \beta_{ij};$$

posant

$${}^tB{}^tA = (\gamma'_{ji})_{1 \leqslant k \leqslant r,\ 1 \leqslant i \leqslant p},$$

on a

$$\gamma'_{ki} = \sum_j \beta'_{ji}\alpha'_{kj},$$

où le produit $\beta'_{ji}\alpha'_{kj}$ est calculé dans l'anneau opposé à K. En calculant dans K, et en tenant compte des relations $\beta'_{ji} = \beta_{ij}$, $\alpha'_{kj} = \alpha_{jk}$, il vient donc

$$\gamma'_{ki} = \sum_j \alpha'_{kj}\beta'_{ji} = \sum_j \alpha_{jk}\beta_{ij} = \gamma_{ik}$$

en vertu de (3); ce qui prouve la relation figurant dans l'énoncé *b*).

L'assertion *d*) est triviale.

Il reste à prouver l'assertion *c*). Soit $A \in M_n(K)$; supposons A inversible et soit B son inverse; des relations $AB = BA = 1_n$ résultent les relations ${}^tB{}^tA = {}^tA{}^tB = {}^t(1_n)$;

or il est clair que

$$^t(1_n) = 1_n;$$

donc ^tA est inversible, et de plus le calcul fait montre que

$$(^tA)^{-1} = ^t(A^{-1}).$$

Réciproquement, si ^tA est inversible, ce qu'on vient d'établir montre qu'il en est de même de la matrice $^t(^tA)$, i.e. de A elle-même. Le Théorème 4 est donc entièrement démontré.

Remarque 5. On pourrait évidemment déduire les assertions *a*) et *b*) du Théorème 4 des assertions analogues du Théorème 3; on laisse au lecteur le soin de le faire à titre d'exercice.

EXERCICES

Il est parfaitement utopique d'espérer apprendre des Mathématiques, si élémentaires ou si supérieures soient-elles, sans résoudre des Exercices.

Les Exercices qu'on trouvera dans ce livre sont de trois sortes. Certains sont des illustrations pratiques ou même numériques des théories exposées dans le texte; le lecteur débutant ne pourra pas acquérir la technique du calcul sans résoudre une partie appréciable des Exercices de ce genre. D'autres apportent au texte des compléments théoriques élémentaires; en les étudiant, le lecteur s'habituera à manipuler le langage et les modes de raisonnements utilisés dans le texte; ceux de ces Exercices qui ne sont pas *très* faciles sont précédés d'un signe ¶. Enfin, la dernière catégorie est constituée par des Exercices qui apportent au texte des compléments importants et difficiles; ils sont destinés uniquement aux étudiants déjà avancés qui s'intéressent vraiment aux Mathématiques; ces Exercices sont précédés de deux ou même trois signes ¶.

Nous ne saurions trop insister enfin sur le fait que résoudre un Exercice ne consiste pas seulement à se convaincre, à l'aide d'un « brouillon » fait à la hâte, du fait qu'on en a à peu près compris la solution; si cette méthode est admissible pour les Exercices de calcul numérique, il faut par contre s'efforcer de *rédiger intégralement* les Exercices plus théoriques, où l'on doit construire de véritables démonstrations. De cette façon, et uniquement de cette façon, l'étudiant parviendra à acquérir un langage clair et correct, et à utiliser les termes techniques dans leur sens propre, ce qui, en Mathématiques, est le signe le plus certain de la compréhension d'un sujet.

1. L'anneau de base étant **R**, trouver les inverses des matrices suivantes (*) :

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}; \quad \begin{pmatrix} 2 & 5 & 7 \\ 6 & 3 & 4 \\ 5 & -2 & -3 \end{pmatrix}; \quad \begin{pmatrix} 1 & 2 & -3 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}; \quad \begin{pmatrix} 2 & 2 & 3 \\ 1 & -1 & 0 \\ -1 & 2 & 1 \end{pmatrix}.$$

2. Calculer l'inverse de la matrice

$$\begin{pmatrix} 1 & a & a^2 & \dots & a^n \\ 0 & 1 & a & \dots & a^{n-1} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}.$$

3. Soit N une matrice carrée nilpotente (i.e. dont une puissance est nulle) à coefficients dans un anneau. Montrer que la matrice $1 - N$ est inversible, et que

$$(1 - N)^{-1} = 1 + N + N^2 + \cdots$$

Application : calculer l'inverse de la matrice

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

4. Calculer l'inverse de la matrice

$$\begin{pmatrix} 1 + a_1 & 1 & 1 & \dots & 1 \\ 1 & 1 + a_2 & 1 & \dots & 1 \\ \dots & \dots & \dots & \dots & \dots \\ 1 & 1 & 1 & \dots & 1 + a_n \end{pmatrix}$$

(*) Le lecteur plus avancé pourra aussi résoudre cet *Exercice* en utilisant les formules de Cramer.

¶ 5. Soit $\omega = \cos(2\pi/n) + i.\sin(2\pi/n)$. Montrer que l'inverse de la matrice

$$\begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & \dots & \omega^{2(n-1)} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \omega^{n-1} & \omega^{2(n-1)} & \dots & \omega^{(n-1)^2} \end{pmatrix}$$

s'obtient en remplaçant ω par ω^{-1} dans cette matrice, et en divisant par n la matrice ainsi obtenue.

6. Trouver une matrice carrée X d'ordre 3 telle que (*)

$$\begin{pmatrix} 2 & -3 & 1 \\ 4 & -5 & 2 \\ 5 & -7 & 3 \end{pmatrix} X \begin{pmatrix} 9 & 7 & 6 \\ 1 & 1 & 2 \\ 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 0 & -2 \\ 18 & 12 & 9 \\ 23 & 15 & 11 \end{pmatrix}.$$

7. Montrer que les vecteurs

$$(1, 2, 1), \quad (2, 3, 3), \quad (3, 7, 1)$$

forment une base de $\mathbf{R}^3$, ainsi que les vecteurs

$$(3, 1, 4), \quad (5, 2, 3), \quad (1, 1, -6),$$

et calculer la matrice de passage de la première base à la seconde.
Même problème, dans $\mathbf{R}^4$, pour les vecteurs

$$(1, 1, 1, 1), \quad (1, 2, 1, 1), \quad (1, 1, 2, 1), \quad (1, 3, 2, 3)$$

et

$$(1, 0, 3, 3), \quad (-2, -3, -5, -4), \quad (2, 2, 5, 4), \quad (-2, -3, -4, -4).$$

8. Les matrices

$$\begin{pmatrix} x+y & 4y \\ -y & x-y \end{pmatrix}$$

où x et y sont des nombres rationnels arbitraires, forment un sous-corps de l'anneau $M_2(\mathbf{Q})$.

9. Les matrices

$$\begin{pmatrix} x & y & z \\ 2z & x & y \\ 2y & 2z & x \end{pmatrix}$$

où x, y, z sont des nombres rationnels, forment un sous-corps de $M_3(\mathbf{Q})$.

¶ 10. Soient K un anneau commutatif, p et q deux éléments donnés de K. On considère l'anneau

$$L = K[\sqrt{p}]$$

et l'ensemble $M \subset M_2(L)$ des matrices de la forme

$$z = \begin{pmatrix} x & qy \\ \bar{y} & \bar{x} \end{pmatrix} \quad \text{avec } x, y \in L$$

(pour les notations, voir le § 9).

(*) Voir note page précédente.

a) Montrer que M est un sous-anneau de $M_2(L)$.

b) Pour toute matrice

$$z = \begin{pmatrix} x & qy \\ \bar{y} & \bar{x} \end{pmatrix} \tag{1}$$

de M on pose

$$z^* = \begin{pmatrix} \bar{x} & -qy \\ -\bar{y} & x \end{pmatrix};$$

montrer qu'on a $(z_1 z_2)^* = z_2^* z_1^*$ quels que soient $z_1, z_2 \in M$.

c) Pour la matrice (1), calculer le produit $z^* z$, et montrer que z est un élément inversible de l'anneau M si et seulement si

$$N(z) = \bar{x}x - q\bar{y}y$$

est un élément inversible de l'anneau L.

d) On suppose que K soit un corps commutatif et que p ne soit pas un carré dans K. Montrer que les assertions suivantes sont équivalentes : (*i*) l'anneau M est un corps (*ii*) il n'existe aucun couple d'éléments x, y de K tels que

$$q = x^2 - py^2.$$

e) On suppose $K = \mathbf{R}$. Montrer que M est un corps si et seulement si l'on a

$$p < 0, \qquad q < 0.$$

Montrer que le corps M ainsi obtenu est isomorphe à celui qu'on obtiendrait en prenant $p = q = -1$ (et qu'on appelle le **corps des quaternions**, premier exemple, historiquement, d'un corps non commutatif).

f) On suppose $K = \mathbf{Q}$ et p et q entiers. Montrer que, pour que M soit un corps, il faut et il suffit que l'équation

$$px^2 + qy^2 = z^2$$

ne possède aucune solution (x, y, z) *entière* autre que $(0, 0, 0)$. Montrer que cette condition est satisfaite dans les cas suivants par exemple :

$$p = 5, \quad q \equiv 2 \pmod 5; \qquad p = 5, \quad q \equiv 3 \pmod 5;$$
$$p = 11, \quad q \equiv 2, 6, 7, 8 \text{ ou } 10 \pmod{11}.$$

¶ 11. Montrer que les matrices de la forme

$$\begin{pmatrix} x & -y & -z & -t \\ y & x & -t & z \\ z & t & x & -y \\ t & -z & y & x \end{pmatrix},$$

où x, y, z, t sont des nombres réels arbitraires, forment un sous-corps de $M_4(\mathbf{R})$, et que ce sous-corps est isomorphe au corps des quaternions défini dans l'*Exercice* précédent. Montrer que, considéré comme espace vectoriel réel, ce corps admet une base formée de quatre éléments e, i, j, k vérifiant les formules suivantes :

$$e^2 = e, \quad i^2 = j^2 = k^2 = -e,$$
$$ei = ie = i, \quad ej = je = j, \quad ek = ke = k,$$
$$ij = -ji = k; \quad jk = -kj = i; \quad ki = -ik = j.$$

Obtiendrait-on encore un corps si l'on autorisait les variables x, y, z, t à prendre des valeurs complexes quelconques?

12. L'anneau de base étant C, calculer l'inverse de la matrice

$$\begin{pmatrix} 1 & 1+i & -i \\ 0 & i & 1-2i \\ 1 & 1 & i \end{pmatrix}.$$

13. On considère la matrice $U(t)$ de l'*Exercice* 11 des §§ 12, 13, 14. Calculer son inverse en effectuant le moins possible de calculs.

14. Soit K un anneau commutatif. Montrer que les matrices de la forme

$$\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}$$

$(x, y, z \in K)$ forment un sous-groupe de $GL(3, K)$. Déterminer le centre de ce sous-groupe.

¶ 15. Soient K un anneau commutatif et n un entier. Montrer que les matrices carrées d'ordre n, à coefficients dans K, et de la forme

$$\begin{pmatrix} 1 & * & * & \dots & * \\ 0 & 1 & * & \dots & * \\ 0 & 0 & 1 & \dots & * \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}$$

(où les signes * désignent des éléments arbitraires de K) forment un sous-groupe de $GL(n, K)$, dont on déterminera le centre.

16. Soit K un corps. On désigne par H le sous-groupe de $GL(n, K)$ formé des matrices diagonales de $GL(n, K)$. Trouver le normalisateur (§ 7, *Exercice* 13) de H dans $GL(n, K)$.

¶ 17. Pour que des éléments (a, b) et (c, d) de $\mathbf{Z}^2$ forment une base de $\mathbf{Z}^2$ il faut et il suffit que $ad - bc = +1$ ou -1.

18. Soient K un anneau commutatif et I un idéal de K. Soit H l'ensemble des matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, à coefficients dans K, qui vérifient

$$ad - bc = 1, \qquad a \equiv d \equiv 1 \pmod{I}, \qquad b \equiv c \equiv 0 \pmod{I}.$$

Montrer que H est un sous-groupe invariant de $GL(2, K)$.

¶¶ 19. Soit K un corps fini à q éléments. Calculer le nombre d'éléments du groupe $GL(n, K)$.

¶ 20. Pour tout entier $n \geqslant 1$, on note G_n l'ensemble des matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ avec

$$a, b, c, d \in \mathbf{Z}, \qquad ad - bc = n,$$

et on pose $G_1 = G$.

a) Montrer que G est un sous-groupe de $GL(2, \mathbf{Z})$. En est-il de même de G_n pour $n \geqslant 2$?

b) Montrer que si $X \in G_n$ on a $UXV \in G_n$ quelles que soient $U, V \in G$.

c) Montrer que, pour toute $X \in G_n$, il existe $U, V \in G$ telles que UXV soit diagonale.

¶ 17. Soit $u = (a, b)$ un élément du $\mathbf{Z}$-module $\mathbf{Z}^2$.

a) Montrer que s'il existe une base de $\mathbf{Z}^2$ qui contient u, alors il existe une forme linéaire sur le module considéré telle que $f(u) = 1$. En déduire qu'alors les entiers a et b sont premiers entre eux.

b) On suppose inversement a et b premiers entre eux. Montrer qu'il existe une forme linéaire f sur $\mathbf{Z}^2$ telle que $f(u) = 1$. Montrer qu'il existe un vecteur v tel que $\mathrm{Ker}(f)$ soit l'ensemble des multiples entiers de v. Prouver que les vecteurs u et v forment une base de $\mathbf{Z}^2$.

c) On prend $u = (6, 35)$; trouver un vecteur v tel que u et v forment une base de $\mathbf{Z}^2$.

18. Soient L et M deux modules à gauche sur un anneau quelconque K, et

$$f : M \to L$$

un homomorphisme *surjectif*. On suppose L libre de type fini. Montrer qu'il existe un homomorphisme

$$g : L \to M$$

tel que

$$f \circ g = id.$$

¶ 19. Soient L et M deux modules à gauche sur un anneau, L' et M' des sous-modules de L et M et u un homomorphisme de L dans M tel que $u(L') \subset M'$. On note p et q les applications canoniques de L sur L/L' et de M sur M/M' (§§ 10, 11, *Exercice* 10). Montrer qu'il existe un et un seul homomorphisme

$$\bar{u} : L/L' \to M/M'$$

tel que l'on ait

$$q \circ u = \bar{u} \circ p$$

(on dit que $\bar{u}$ est l'homomorphisme déduit de u par passage aux quotients). A quelles conditions $\bar{u}$ est-il injectif, ou surjectif, ou bijectif?

20. Soit k un corps commutatif. Dans le groupe $SL(2, k)$ des matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ à coefficients dans k et telles que $ad - bc = 1$, on considère les matrices

$$x_+(t) = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}, \qquad x_-(t) = \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}$$

où $t \in k$. Désignant par α l'un des deux symboles $+$ ou $-$, et par $-\alpha$ le symbole opposé, on définit pour $t \neq 0$ les matrices

$$w_\alpha(t) = x_\alpha(t) x_{-\alpha}(-t^{-1}) x_\alpha(t), \qquad h_\alpha(t) = w_\alpha(t) w_\alpha(1)^{-1}.$$

a) Calculer ces matrices, et montrer que les matrices $x_+(t)$ et $x_-(t)$ engendrent $SL(2, k)$.

b) Établir les relations suivantes :

(R 1)	$x_\alpha(t+u) = x_\alpha(t)\, x_\alpha(u)$	pour	$t, u \in k$;
(R 2)	$w_\alpha(t)\, x_\alpha(u)\, w_\alpha(t)^{-1} = x_{-\alpha}(-u/t^2)$	pour	$t, u \in k$, $t \neq 0$;
(R 3)	$h_\alpha(tu) = h_\alpha(t)\, h_\alpha(u)$	pour	$t, u \in k$, $t \neq 0$, $u \neq 0$.

c) Montrer que toute matrice $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, k)$ peut se mettre d'une façon et d'une seule soit sous la forme $g = h_+(t) x_-(u)$, soit sous la forme $g = h_+(t)\, x_+(u)\, w x_+(v)$, où l'on pose $w = w_+(1)$ (distinguer deux cas, suivant que $c = 0$ ou que $c \neq 0$).

d) On appelle *groupe dérivé* d'un groupe G le sous-groupe G' de G engendré par les « commu

tateurs » $(x, y) = xyx^{-1}y^{-1}$ de ses éléments. Montrer que $SL(2, k)$ est égal à son groupe dérivé pourvu que k contienne au moins 4 éléments.

¶ **21.** On considère dans $SL(2, k) = G$ le sous-groupe U formé des $x_+(t)$, et le sous-groupe H formé des $h_-(t)$; on a donc $G = HU \cup HUwU$ d'après la question *c*) de l'*exercice* précédent. On se propose de montrer que *si k possède au moins 4 éléments le groupe G contient un seul sous-groupe invariant M autre que $\{e\}$ et G, à savoir le sous-groupe Z formé des matrices 1 et -1* (qui se réduit d'ailleurs à l'élément neutre en caractéristique 2; noter que, dans tous les cas, ce sous-groupe est le centre de G, comme on le vérifiera facilement). On pose $B = HU$.

a) Montrer que $B \cap wBw^{-1} = H$, et en déduire que si $M \subset B$ alors on a $M \subset H$.

b) On suppose $M \subset H$. Supposons $h = h_+(t) \in M$. En calculant le commutateur de h et de $x_-(u)$ montrer que M contient $x_-(u - u/t^2)$, et en déduire que $M \subset Z$.

c) On suppose M non contenu dans B. Montrer, à l'aide de la question *c*) de l'*exercice* précédent, que $G = MB$, et en déduire (§ 7, exercice 16) que le groupe quotient G/M est isomorphe à $B/B \cap M$.

d) On suppose $\mathrm{Card}(k) \geqslant 4$, et donc $G = G'$ d'après l'*exercice* précédent. Montrer que le groupe G/M est égal à son groupe dérivé. Déduire de là et de la question précédente que $M = G$ si M n'est pas contenu dans B (remarquer que $B' \subset U$ et que $U' = \{e\}$, et observer que le seul sous-groupe invariant L de B tel que B/L soit son propre groupe dérivé est B lui-même).

¶ **22.** Dans un groupe G, on considère deux familles d'éléments que l'on notera $\hat{x}_+(t)$ et $\hat{x}_-(t)$ et qui dépendent d'un paramètre t qui varie dans un corps commutatif k donné. A partir des éléments $\hat{x}_\alpha(t)$ de G on définit des éléments $\hat{w}_\alpha(t)$ et $\hat{h}_\alpha(t)$ de G par les formules de l'*exercice* 20, i.e. en posant

$$\hat{w}_\alpha(t) = \hat{x}_\alpha(t)\hat{x}_{-\alpha}(-1/t)\hat{x}_\alpha(t), \qquad \hat{h}_\alpha(t) = \hat{w}_\alpha(t)\hat{w}_\alpha(1)^{-1},$$

et on suppose vérifiées les relations

$$\text{(R 1)} \quad \hat{x}_\alpha(t+u) = \hat{x}_\alpha(t)\hat{x}_\alpha(u), \qquad \text{(R 2)} \quad \hat{w}_\alpha(t)\hat{x}_\alpha(u)\hat{w}_\alpha(t)^{-1} = \hat{x}_{-\alpha}(-u/t^2)$$

de l'*exercice* 20.

a) Démontrer les formules suivantes :

$$\hat{w}_\alpha(t)\hat{w}_\alpha(u)\hat{w}_\alpha(t)^{-1} = \hat{w}_{-\alpha}(-u/t^2), \qquad \hat{w}_\alpha(t)\hat{h}_\alpha(u)\hat{w}_\alpha(t)^{-1} = \hat{h}_{-\alpha}(-u/t^2)\hat{h}_{-\alpha}(-1/t^2)^{-1},$$
$$\hat{w}_\alpha(t)\hat{x}_\alpha(u)\hat{w}_\alpha(t)^{-1} = \hat{x}_{-\alpha}(-u/t^2), \qquad \hat{h}_\alpha(t)\hat{x}_\alpha(u)\hat{h}_\alpha(t)^{-1} = \hat{x}_\alpha(t^2u),$$
$$\hat{h}_\alpha(t)\hat{w}_\alpha(u)\hat{h}_\alpha(t)^{-1} = \hat{w}_\alpha(t^2u), \qquad \hat{h}_\alpha(t)\hat{h}_\alpha(u)\hat{h}_\alpha(t)^{-1} = \hat{h}_\alpha(t^2u)\hat{h}_\alpha(t^2)^{-1},$$
$$\hat{w}_\alpha(-1/t) = \hat{w}_{-\alpha}(t), \qquad \hat{w}_\alpha(t)^{-1} = \hat{w}_\alpha(-t),$$
$$\hat{h}_\alpha(-1/t) = \hat{h}_{-\alpha}(t), \qquad \hat{h}_\alpha(t)\hat{h}_\alpha(-1/t) = \hat{h}_\alpha(-1),$$
$$\hat{w}_\alpha(1)\hat{h}_\alpha(t)\hat{w}_\alpha(1)^{-1} = \hat{h}_\alpha(1/t), \qquad \hat{w}_\alpha(1)^{-2} = \hat{h}_\alpha(-1).$$

b) Soient U le sous-groupe de G formé par les $\hat{x}_+(t)$, et H le sous-groupe engendré par les $\hat{h}_+(t)$. On pose $\hat{w} = \hat{w}_\alpha(1)$ et $N = H \cup \hat{w}H$. Montrer que N est un sous-groupe de G et que H est invariant dans N. Montrer que l'on a $\hat{w}U\hat{w} \subset UNU$ (ensemble des produits $u'nu''$ avec $u' \in U$, $u'' \in U$ et $n \in N$), et que l'ensemble $UH \cup UH\hat{w}U$ est le sous-groupe de G engendré par les $x_\alpha(t)$.

c) On reprend le groupe $SL(2, k)$ de l'*exercice* 20 et les éléments $x_\alpha(t)$, $w_\alpha(t)$ et $h_\alpha(t)$ de ce groupe. Montrer, en utilisant la question *c*) de l'*exercice* 20, qu'il existe une application π de $SL(2, k)$ dans G, et une seule, telle que

$$\pi(h_\alpha(t)x_\alpha(u)) = \hat{h}_\alpha(t)\hat{x}_\alpha(u), \qquad \pi(h_\alpha(t)x_\alpha(u)wx_\alpha(v)) = \hat{h}_\alpha(t)\hat{x}_\alpha(u)\hat{w}\hat{x}_\alpha(v).$$

Montrer que, pour que π soit un homomorphisme, il faut et il suffit que la relation

$$\text{(R 3)} \qquad \hat{h}_\alpha(tu) = \hat{h}_\alpha(t)\hat{h}_\alpha(u)$$

soit vérifiée. Autrement dit, *pour construire un homomorphisme de $SL(2, k)$ dans un groupe quelconque G, il suffit de se donner des éléments $\hat{x}_+(t)$ et $\hat{x}_-(t)$ de G vérifiant les relations* (R 1), (R 2) *et* (R 3) (« définition de $SL(2, k)$ par générateurs et relations »).

¶¶ **23.** On considère le groupe $G = GL(n, k)$ sur un corps commutatif k, le sous-groupe T de G formé des matrices diagonales, le sous-groupe B des matrices dont les termes situés en dessous de la diagonale sont tous nuls, et le sous-groupe U de B formé des matrices de B dont tous les termes diagonaux sont égaux à 1. Enfin on note N l'ensemble des $n \in G$ tels que $nTn^{-1} = T$ (normalisateur de T dans G). On identifie les éléments de G aux automorphismes de l'espace vectoriel k^n, dont la base canonique sera notée $e_1, \ldots, e_n$.

a) Montrer que $g \in N$ si et seulement s'il existe une permutation $w \in \mathfrak{S}_n$ et des scalaires $t_i \neq 0$ tels que l'on ait $g(e_i) = t_i e_{w(i)}$ pour $1 \leqslant i \leqslant n$. En déduire que le groupe quotient $N/T = W$ est isomorphe au groupe symétrique $\mathfrak{S}_n$. Pour $1 \leqslant i \leqslant n-1$, soit $\omega_i \in G$ la matrice qui permute les vecteurs de base e_i et e_{i+1} et laisse fixe e_j pour tout $j \neq i, i+1$. Montrer que N est engendré par T et les ω_i.

b) Pour $i \neq j$ et $t \in k$ on note $x_{ij}(t)$ l'élément de G défini par les formules suivantes :

$$x_{ij}(t)e_j = e_j - te_i, \qquad x_{ij}(t)e_k = e_k \quad \text{si} \quad k \neq j.$$

Quelle est la matrice de $x_{ij}(t)$? Montrer que l'on a $x_{ij}(t+u) = x_{ij}(t)x_{ij}(u)$ quels que soient $t, u \in k$, et que les $x_{ij}(t)$, pour i et j donnés et t variable, forment un sous-groupe U_{ij} de G. En posant d'une manière générale $(a, b) = aba^{-1}b^{-1}$ montrer qu'on a

$$(x_{ij}(t), x_{jk}(u)) = x_{ik}(tu) \quad \text{si } i, j, k \text{ sont deux à deux distincts.}$$
$$(x_{ij}(t), x_{kl}(u)) = 1 \quad \text{si } j \neq k \text{ et } i \neq l.$$

Montrer que U est engendré par les matrices $x_{i,i+1}(t)$ $(1 \leqslant i \leqslant n-1, t \in k)$. Calculer $nx_{ij}(t)n^{-1}$ pour $n \in N$.

c) Soit B' le sous-groupe de G formé des matrices dont les termes situés au-dessus de la diagonale sont tous nuls. Montrer qu'il existe un $n \in N$ tel que $B' = nBn^{-1}$, et que B' est engendré par T et les $x_{i-1,i}(t)$. Soit g un élément quelconque de G; montrer qu'il existe un $b \in B$ et un $b' \in B'$ tels qu'en posant $g = bb'g_1$ la matrice g_1 soit de la forme

$$g_1 = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & * & \cdots & * \\ \cdots & \cdots & \cdots & \cdots \\ 0 & * & \cdots & * \end{pmatrix}.$$

En déduire que G est engendré par B et B' ou, ce qui revient au même, par B et N (raisonner par récurrence sur n).

Montrer, en utilisant les formules de l'exercice 20, que le sous-groupe de G engendré par les $x_{i,i+1}(t)$ et les $x_{j+1,j}(t)$ est $SL(n, k)$, ensemble des $g \in GL(n, k)$ tels que $\det(g) = 1$ (cette question suppose le lecteur au courant de la théorie des déterminants, et ne sera pas utilisée par la suite).

d) On considère le sous-groupe $B_i = B \cap \omega_i^{-1}B\omega_i$. Montrer que B_i est invariant dans B, et que tout $b \in B$ s'écrit, de façon unique, comme produit d'un élément de $U_{i,i+1}$ et d'un élément de B_i. En déduire que la double classe $B\omega_iB$, ensemble des $b'\omega_ib''$ avec $b', b'' \in B$, est réunion des classes $Bwx_{i,i+1}(t)$, $t \in k$.

c) En posant $n \cdot {}^t U_{i,i+1} n^{-1} = U_{jk}$ montrer que l'ensemble $B\omega_i BnB$ (pour $n \in N$) est réunion des classes $B\omega_i n x_{jk}(t)B$, où t varie. En déduire que l'on a

$$B\omega_i BnB = B\omega_i nB \quad \text{si } j < k, \qquad \text{et} \qquad B\omega_i BnB = BnB \cup B\omega_i nB \quad \text{si } j > k$$

(on utilisera le fait, qu'il suffit de vérifier dans $GL(2, k)$, que $x_{i+1,i}(t) \in B\omega_i B$ si $t \neq 0$).

f) Soit G_0 la réunion des doubles classes BnB (lesquelles sont en nombre fini puisque N/T est fini). En utilisant le fait que N est engendré par T et les ω_i, montrer à l'aide de la question précédente que $nG_0 \subset G_0$ pour tout $n \in N$. Montrer que G_0 est un sous-groupe de G, et en déduire que

$$G = \bigcup BnB$$

(théorème de Bruhat pour le groupe linéaire).

¶ **24.** Soit k un corps fini à q éléments, et soit V un espace vectoriel de dimension finie n sur k; soit m un entier compris entre 0 et n.

a) Soit X_m l'ensemble des familles $(x_1, \ldots, x_m)$ d'éléments de V linéairement indépendants. Montrer que l'on a :

$$\mathrm{Card}(X_m) = (q^n - 1)(q^n - q) \cdots (q^n - q^{m-1}).$$

(Raisonner par récurrence sur m.)

b) Montrer que l'ordre du groupe GL(V) des automorphismes de V est donné par la formule :

$$\mathrm{Card}\ GL(V) = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1}) = q^{n^2} \prod_{i=1}^{i=n} \left(1 - \frac{1}{q^i}\right).$$

c) Soit $G_{n,m}$ l'ensemble des sous-espaces vectoriels de V de dimension m (« grassmannienne »). Montrer que l'on a :

$$\mathrm{Card}\ G_{n,m} = q^{m^2 - mn} \prod_{i=n-1}^{i=n} \left(1 - \frac{1}{q^i}\right).$$

25. Soit V un espace vectoriel de dimension 2 sur le corps à 2 éléments; soient x, y, z les trois éléments non nuls de V.

a) Montrer que l'on a $x + x = y + y = z + z = 0$ et $x + y = z$, $y + z = x$, $z + x = y$.

b) En déduire que le groupe GL(V) des automorphismes de V est isomorphe au groupe des permutations de x, y, z.

26. Soit V un espace vectoriel de dimension 2 sur le corps à 3 éléments.

a) Montrer que V contient 4 sous-espaces de dimension 1, soient D_1, D_2, D_3, D_4.

b) Tout élément du groupe d'automorphismes GL(V) de V permute les D_i entre eux. On déduit de là un homomorphisme

$$\varepsilon : GL(V) \to S_4,$$

où S_4 désigne le groupe des permutations de $\{1, 2, 3, 4\}$. Montrer que le noyau de ε est $\{\pm 1\}$; en déduire que ε est surjectif (comparer les ordres des deux groupes).

c) Soit (LSV) le sous-groupe de GL(V) formé des éléments de déterminant 1. Montrer que ε définit un isomorphisme de SL(V) sur le groupe alterné A_4, formé des permutations paires, de S_4. [Cette question suppose le lecteur au courant de la théorie des déterminants.]

1. On considère les trois formes linéaires

$$2x - y + 3z, \qquad 3x - 5y + z, \qquad 4x - 7y + z$$

sur $\mathbf{R}^3$, Forment-elles une base du dual de $\mathbf{R}^3$?

2. Montrer que les formes linéaires

$$x + 2y + z, \qquad 2x + 3y + 3z, \qquad 3x + 7y + z$$

forment une base du dual de $\mathbf{R}^3$, et trouver la base de $\mathbf{R}^3$ duale de celle-ci.

3. Soient K un anneau et $f_1, \ldots, f_n$ des formes linéaires sur le K-module à droite K^n. Pour que celles-ci forment une base du dual de K^n, il faut et il suffit qu'il existe des vecteurs $x_1, \ldots, x_n \in K^n$ tels que l'on ait

$$f_i(x_j) = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j. \end{cases}$$

4. Soient K un anneau commutatif et U une matrice carrée d'ordre n à coefficients dans K.

a) Montrer que les relations

$${}^t U . U = 1_n, \qquad U . {}^t U = 1_n$$

sont équivalentes.

b) Montrer que les matrices $U \in M_n(K)$ vérifiant les conditions précédentes forment un sous-groupe de $GL(n, K)$ (**groupe orthogonal à n variables** sur l'anneau K).

c) On dit qu'une matrice $S \in M_n(K)$ est **symétrique** si ${}^t S = S$. Soient X et Y deux matrices symétriques; pour que XY soit symétrique, il faut et il suffit que $XY = YX$.

d) Montrer (en prenant $K = \mathbf{Q}$ ou un surcorps quelconque de $\mathbf{Q}$) que la matrice

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

est à la fois orthogonale et symétrique.

e) Trouver toutes les matrices orthogonales d'ordre 3 à coefficients entiers rationnels.

5. Soit $M_n(K)$ l'anneau des matrices carrées d'ordre n sur un anneau quelconque K; on regarde $M_n(K)$ comme un K-module à droite. Montrer que, pour toute forme linéaire f sur $M_n(K)$, il existe une et une seule matrice $A \in M_n(K)$ telle que

$$f(X) = \mathrm{Tr}(AX) \quad \text{pour tout } X \in M_n(K)$$

(voir l'*Exercice* 8 du § 12 pour une définition du symbole Tr). Pour que l'on ait

$$f(XY) = f(YX)$$

quelles que soient $X, Y \in M_n(K)$, il faut et il suffit, lorsque l'anneau K est commutatif, que la matrice A soit proportionnelle à 1_n.