§ 17. Sommes de sous-modules

I. Somme de deux sous-modules

Soient K un anneau, L un K-module à gauche, M et N deux sous-modules de L. On appelle **somme de** M et N le sous-module de L engendré par l'ensemble $M \cup N$, autrement dit le plus petit sous-module de L contenant à la fois M et N.

Il est facile de donner une construction explicite de ce sous-module; c'est *l'ensemble des* $z \in L$ *pour lesquels il existe un* $x \in M$ *et un* $y \in N$ *tels que*

$$z = x + y.$$

En effet, il est clair que tout sous-module de L contenant M et N contient tout vecteur z possédant la propriété en question. Il suffit donc de montrer que ces vecteurs forment un sous-module P contenant M et N. Or il est clair que P contient M et N (faire $x = 0$ ou bien $y = 0$ dans la relation $z = x + y$); d'autre part, si

$$\begin{aligned} z' &= x' + y' \qquad (x' \in M, y' \in N) \\ z'' &= x'' + y'' \qquad (x'' \in M, y'' \in N) \end{aligned}$$

sont deux éléments de P, alors quels que soient les scalaires λ et μ on a

$$\lambda z' + \mu z'' = x + y$$

avec

$$x = \lambda x' + \mu x'' \in M, \qquad y = \lambda y' + \mu y'' \in N,$$

ce qui montre bien que P est un sous-module.

Étant donné ce qu'on vient d'établir, on désigne la somme des sous-modules M et N par la notation (*)

$$M + N.$$

(*) Plus généralement, si G est un groupe multiplicatif (resp. additif) et si A et B sont des parties de G, on note AB (resp. A + B) l'ensemble des $z \in G$ pour lesquels il existe $x \in A$ et $y \in B$ tels que $z = xy$ (resp. $z = x + y$).

Exemple 1. Prenons $K = \mathbf{R}$ et pour L l'ensemble des vecteurs d'origine donnée O dans l'espace usuel; prenons pour M et N des droites passant par O; alors $M + N$ est le plan engendré par ces deux droites si elles sont distinctes, ou bien $M + N = M = N$ si elles sont confondues.

La définition et la construction précédentes se généralisent immédiatement à un nombre quelconque de sous-modules. Soit $M_1, \ldots, M_p$ une famille finie quelconque de sous-modules de L; désignons par P l'ensemble des $z \in L$ qui possèdent la propriété suivante : il existe $x_1 \in M_1, \ldots, x_p \in M_p$ tels que

$$z = x_1 + \cdots + x_p; \tag{1}$$

alors P est le plus petit sous-module de L contenant $M_1, \ldots, M_p$.

Il est d'abord clair que P contient M_i (faire $x_j = 0$ pour $j \neq i$ dans la relation précédente), et qu'un sous-module de L contenant les M_i contient nécessairement les vecteurs (1). Il reste donc à faire voir que P est un sous-module de L; mais si

$$z' = x'_1 + \cdots + x'_p, \qquad z'' = x''_1 + \cdots + x''_p$$

sont des éléments de P, on a quels que soient $\lambda', \lambda'' \in K$ la relation

$$\lambda' z' + \lambda'' z'' = x_1 + \cdots + x_p$$

avec

$$x_i = \lambda' x'_i + \lambda'' x''_i \in M_i \quad (1 \leqslant i \leqslant p),$$

ce qui établit le résultat cherché.

Ici encore, on dit que le sous-module P est la **somme des sous-modules** $M_1, \ldots, M_p$ et on le désigne par la notation

$$M_1 + \cdots + M_p.$$

2. *Produit direct de modules*

Dans ce qui précède, les modules $M_1, \ldots, M_p$ étaient des sous-modules d'un module donné L. On va maintenant partir de K-modules à gauche $M_1, \ldots, M_p$ et, sans les supposer contenus dans un même module, construire un module qui les contient tous à un isomorphisme près.

Considérons pour cela l'ensemble produit

$$L = M_1 \times \cdots \times M_p,$$

formé des familles

$$x = (x_1, \ldots, x_p) \qquad \text{avec} \qquad x_1 \in M_1, \ldots, x_p \in M_p.$$

Nous allons définir sur L une structure de K-module à gauche en posant

$$(x_1, \ldots, x_p) + (y_1, \ldots, y_p) = (x_1 + y_1, \ldots, x_p + y_p)$$
$$\lambda(x_1, \ldots, x_p) = (\lambda x_1, \ldots, \lambda x_p);$$

le fait qu'on obtienne une structure de module sur L de cette façon se vérifie immédiatement, et nous laisserons au lecteur le soin de le faire.

Lorsque $M_1 = \cdots = M_p = K$, on retrouve évidemment le module K^p.

Lorsque $K = \mathbf{Z}$, on retrouve la notion de produit direct de groupes commutatifs définie au § 7, n° 2.

Dans le cas général, on dit que $M_1 \times \cdots \times M_p$, muni de la structure de module qu'on vient de définir, est le **produit direct des modules** $M_1, \ldots, M_p$.

Il est clair que, pour $1 \leqslant i \leqslant p$, l'application

$$\mathrm{pr}_i : M_1 \times \cdots \times M_p \to M_i$$

donnée par $\mathrm{pr}_i(x_1, \ldots, x_p) = x_i$ est un homomorphisme de modules. Il en est de même de l'application

$$u_i : M_i \to M_1 \times \cdots \times M_p$$

donnée par

$$u_i(x) = (0, \ldots, 0, x, 0, \ldots, 0),$$

la lettre $x \in M_i$ étant précédée au second membre de $i - 1$ zéros.

En fait, il est clair que l'homomorphisme u_i est injectif; c'est donc un isomorphisme de M_i sur un sous-module de $M_1 \times \cdots \times M_p$. Dans la pratique, on identifie le plus souvent M_i à son image par u_i. La formule

$$(x_1, x_2, \ldots, x_p) = (x_1, 0, \ldots, 0) + (0, x_2, 0, \ldots, 0) + \cdots + (0, \ldots, 0, x_p)$$

montre alors que tout élément de $M_1 \times \cdots \times M_p$ est somme d'un élément de M_1, d'un élément de M_2, ..., d'un élément de M_p; autrement dit, $M_1 \times \cdots \times M_p$ est somme des sous-modules $M_1, \ldots, M_p$.

3. *Somme directe de sous-modules*

Reprenons comme au n° 1 des sous-modules $M_1, \ldots, M_p$ d'un K-module à gauche L. Considérons l'application

$$f : M_1 \times \cdots \times M_p \to L$$

donnée par

$$f(x_1, \ldots, x_p) = x_1 + \cdots + x_p;$$

c'est évidemment un homomorphisme de modules. De plus ,on a

$$\mathrm{Im}\,(f) = M_1 + \cdots + M_p$$

par définition même de la somme d'une famille de sous-modules.

On dit que les sous-modules $M_1, \ldots, M_p$ sont **linéairement indépendants** lorsque l'homomorphisme f est *injectif*, autrement dit lorsque tout $x \in M_1 + \cdots + M_p$ s'écrit *d'une seule façon* sous la forme $x = x_1 + \cdots + x_p$ avec $x_1 \in M_1, \ldots, x_p \in M_p$. Il revient au même de dire (§ 7, Théorème 8) que $\mathrm{Ker}\,(f)$ est réduit à 0, autrement dit

que les relations

$$x_1 + \cdots + x_p = 0, \qquad x_1 \in M_1, \ \ldots, \ x_p \in M_p$$

impliquent

$$x_1 = \cdots = x_p = 0.$$

THÉORÈME 1. *Pour que deux sous-modules* M *et* N *d'un module* L *soient linéairement indépendants il faut et il suffit que* $M \cap N = 0$.

Si $x \in M \cap N$, on a $x + (-x) = 0$ avec $x \in M$ et $-x \in N$, donc $x = 0$ si M et N sont linéairement indépendants. Inversement supposons $M \cap N = 0$; si $x \in M$ et $y \in N$ vérifient $x + y = 0$, on a $x = -y \in M \cap N$, donc $x = y = 0$, ce qui achève la démonstration.

Remarque 1. Considérons l'application $f : M \times N \to L$ donnée par

$$f(x, y) = x + y;$$

le raisonnement qui précède montre que son noyau est formé des couples $(x, -x)$ avec $x \in M \cap N$; il est clair que l'application $x \to (x, -x)$ est un *isomorphisme de* $M \cap N$ *sur* $\mathrm{Ker}(f)$. Cette Remarque est fort importante pour calculer la dimension d'une somme de sous-espaces vectoriels (cf. § 19, n° 7).

Lorsque des sous-modules $M_1, \ldots, M_p$ d'un module L sont linéairement indépendants, on dit que $M_1 + \cdots + M_p$ est la **somme directe** des sous-modules donnés, et on désigne cette somme directe par la notation

$$M_1 \oplus \cdots \oplus M_p;$$

l'emploi du signe $\oplus$ au lieu du signe $+$ habituel indique donc qu'on a affaire à une somme de sous-modules linéairement indépendants. Il est clair qu'alors l'application f définie plus haut est un *isomorphisme du module* $M_1 \times \cdots \times M_p$ *sur le module* $M_1 \oplus \cdots \oplus M_p$; cet isomorphisme sera qualifié de « canonique ».

Remarque 2. Le module produit $M_1 \times \cdots \times M_p$ est évidemment somme directe des sous-modules auxquels on a identifié $M_1, \ldots, M_p$ au n° précédent.

Remarque 3. Soient $a_1, \ldots, a_p$ des éléments d'un K-module à gauche L, et prenons pour $M_1, \ldots, M_p$ les sous-modules engendrés par $a_1, \ldots, a_p$ respectivement. Alors $M_1 + \cdots + M_p$ est le sous-module de L engendré par $a_1, \ldots, a_p$; les sous-modules $M_1, \ldots, M_p$ sont linéairement indépendants si et seulement si les vecteurs $a_1, \ldots, a_p$ le sont; et la relation

$$L = M_1 \oplus \cdots \oplus M_p$$

signifie que $a_1, \ldots, a_p$ forment une *base* de L. On laisse au lecteur le soin de vérifier lui-même ces assertions.

Soient L un K-module à gauche et M un sous-module de L; on dit que M est **facteur direct** dans L s'il existe un sous-module N de L tel que L soit somme *directe* de M et de N; on dit alors que N est un **supplémentaire de M dans L**. On verra au § 19 que si L est un espace vectoriel de dimension finie sur un corps, tout sous-espace de L admet un supplémentaire. Mais cette propriété ne s'étend pas aux anneaux quelconques.

Exemple 2. Prenons $K = L = \mathbf{Z}$ et $M = p\mathbf{Z}$ avec $p \neq 0$; soit $N = q\mathbf{Z}$ un sous-module non nul de L; on a alors $M \cap N \neq 0$, par exemple parce que $pq \in M \cap N$; par suite (Théorème 1) M n'admet pas de supplémentaire dans $\mathbf{Z}$ (sauf bien entendu si $M = L$ ou si $M = 0$).

4. *Sommes directes et projecteurs*

Soit L un K-module à gauche, et considérons une **décomposition de L en somme directe** i.e. une relation de la forme

$$L = M_1 \oplus \cdots \oplus M_p$$

où les M_i sont des sous-modules de L, linéairement indépendants. Tout $x \in L$ s'écrit donc d'une façon et d'une seule sous la forme

$$x = x_1 + \cdots + x_p \qquad \text{avec} \qquad x_i \in M_i \quad \text{pour} \quad 1 \leqslant i \leqslant p,$$

de sorte qu'on peut poser

$$x_i = v_i(x)$$

où v_i est une application de L dans L. D'ailleurs, si l'on introduit l'isomorphisme

$$f : M_1 \times \cdots \times M_p \to L$$

donné par

$$f(x_1, \ldots, x_p) = x_1 + \cdots + x_p,$$

et les injections canoniques

$$j_i : M_i \to L,$$

il est clair qu'on a

$$v_i = j_i \circ pr_i \circ f^{-1},$$

ce qui montre que v_i est linéaire (résultat que le lecteur démontrera aussi par un calcul direct).

L'endomorphisme v_i a évidemment pour image le sous-module M_i; pour tout $x \in L$, $v_i(x)$ est le seul et unique vecteur de M_i tel que $x - v_i(x)$ appartienne au sous-module engendré par $M_1, \ldots, M_{i-1}, M_{i+1}, \ldots, M_p$; on dit pour cette raison que $v_i(x)$ est la **projection de** x **sur** M_i.

Il est clair qu'on a $v_i(x) = x$ si et seulement si $x \in M_i$. Comme $v_i(x) \in M_i$ pour tout $x \in L$, il s'ensuit que $v_i(v_i(x)) = v_i(x)$ pour tout $x \in L$, ce qui veut dire que

$$v_i \circ v_i = v_i;$$

on dit qu'un endomorphisme v d'un module L est un **projecteur** s'il vérifie la condition

précédente, i.e. si

$$v \circ v = v.$$

D'autre part, il est aussi évident que $v_j(x) = 0$ pour $x \in M_i$, $i \neq j$; donc on a $v_j(v_i(x)) = 0$ pour tout $x \in L$ si $i \neq j$, autrement dit

$$v_j \circ v_i = 0 \quad \text{si} \quad i \neq j.$$

Enfin, pour tout $x \in L$ on a $x = x_1 + \cdots + x_p = v_1(x) + \cdots + v_p(x)$, ce qui prouve que

$$v_1 + \cdots + v_p = j_L,$$

application identique de L dans lui-même.

Ces propriétés admettent une réciproque :

THÉORÈME 2. *Soient $v_1, \ldots, v_p$ des endomorphismes d'un module* L *vérifiant les conditions suivantes :*

$$v_j \circ v_i = \begin{cases} v_i & \text{si} \quad i = j \\ 0 & \text{si} \quad i \neq j, \end{cases}$$
$$v_1 + \cdots + v_p = j_L.$$

Alors L *est somme directe des sous-modules* $M_i = v_i(L)$.

La relation

$$x = v_1(x) + \cdots + v_p(x)$$

montre déjà que L est somme des M_i. Considérons maintenant des $x_i \in M_i$ ($1 \leqslant i \leqslant p$) tels que

$$x_1 + \cdots + x_p = 0; \tag{2}$$

il existe des $y_i \in L$ tels que $x_i = v_i(y_i)$; on a donc

$$v_i(x_j) = v_i[v_j(y_j)] = \begin{cases} 0 & \text{si } i \neq j \\ v_i(y_i) = x_i & \text{si } i = j; \end{cases}$$

il s'ensuit qu'en appliquant v_i à la relation (2) il reste la relation $x_i = 0$, ce qui montre que les sous-modules M_i sont linéairement indépendants, et achève la démonstration.

COROLLAIRE. *Soit* M *un sous-module d'un module* L. *Les propriétés suivantes sont équivalentes :*

(FD 1) M *est facteur direct dans* L;

(FD 2) *il existe un endomorphisme v de* L *tel que*

$$v \circ v = v, \qquad v(L) = M;$$

(FD 3) *il existe un homomorphisme q de* L *dans* M *tel que $q(x) = x$ pour tout $x \in M$.*

Il est clair que (FD 1) implique (FD 2) : on écrit $L = M \oplus N$ et on prend pour $v(x)$ la projection de x sur M parallèlement à N.

(FD 2) implique (FD 3) : comme v applique L sur M, on peut définir un homomorphisme q du module L dans le module M en posant $q(x) = v(x)$ pour tout $x \in L$ (la seule différence entre v et q est que v est une application de L dans L, tandis que q est une application de L dans M); pour $x \in M$, il existe un $y \in L$ tel que $v(y) = x$, et on a alors $q(x) = v(x) = v(v(y)) = v(y) = x$.

Montrons enfin que (FD 3) implique (FD 1). Soit N le noyau de q. On a

$$M \cap N = 0,$$

car si $x \in M \cap N$ on a d'une part $q(x) = x$, d'autre part $q(x) = 0$, donc $x = 0$. Par ailleurs, pour tout $x \in L$, on a $q(q(x)) = q(x)$, donc $q(x - q(x)) = 0$, donc $x - q(x) \in N$; écrivant $x = q(x) + (x - q(x))$ on voit donc que $L = M + N$. Comme $M \cap N = 0$, ceci prouve (Théorème 1) que M est facteur direct dans L et achève la démonstration.

Espaces vectoriels de dimension finie

Le but des §§ 18 à 20 est d'étudier les espaces vectoriels de dimension finie sur un corps quelconque K, en particulier d'introduire la notion fondamentale de dimension, et d'établir les propriétés les plus importantes des systèmes d'équations linéaires sur un corps.

Bien que, dans la pratique élémentaire, et en Analyse, on ne s'intéresse qu'au cas du corps des nombres réels ou des nombres complexes, il ne servirait *à rien* de supposer $K = \mathbf{R}$ ou $K = \mathbf{C}$ dans ce Chapitre.

Les exposés classiques de l'Algèbre linéaire utilisent d'autre part la théorie des déterminants, mais il y a plus de cinquante ans qu'on sait s'en passer; l'exposé purement « géométrique » ainsi obtenu est non seulement plus simple, il est aussi plus général que ceux reposant sur la théorie des déterminants, car celle-ci suppose le corps ou l'anneau de base commutatif. En fait, la théorie des déterminants (qui sera exposée dans des §§ ultérieurs) a pour principal intérêt de fournir des critères *explicites* d'indépendance linéaire, et des formules *explicites* de résolution des systèmes d'équations linéaires; elle n'est d'aucune utilité pour établir les théorèmes *d'existence* des §§ 19 et 20.

L'un des résultats les plus importants de l'Algèbre linéaire est le Théorème 13 du § 19, qui, étant donné un homomorphisme f d'un espace vectoriel L de dimension finie dans un autre, établit une relation simple entre les dimensions de L, du noyau de f, et de l'image de f. Quand on analyse la démonstration classique de ce Théorème, on constate qu'on peut le formuler de telle sorte qu'il se généralise aux modules sur un anneau quelconque. Le résultat général permet alors de démontrer très simplement des énoncés qui sont le point de départ de la « grande » théorie des anneaux dits noethériens et des anneaux principaux. Ces résultats font l'objet du § 18; l'étude de ce § et des *Exercices* correspondants, quoique peu utile en principe pour comprendre la suite, donnera au lecteur un aperçu de l'une des théories les plus importantes de l'Algèbre actuelle.

1. *Homomorphismes dont le noyau et l'image sont de type fini* (*)

Les résultats de ce § reposent sur le théorème suivant :

THÉORÈME 1. *Soient* K *un anneau,* L *et* M *deux* K*-modules à gauche, et f un homomorphisme de* L *dans* M.

Si Ker (f) *et* Im (f) *sont des* K*-modules de type fini, il en est de même de* L.

Si Ker (f) *est isomorphe à* K^p, *et* Im (f) *isomorphe à* K^q, *alors* L *est isomorphe à* K^{p+q}.

Supposons Ker (f) engendré par des vecteurs $a_1, \ldots, a_p$, et Im (f) engendré par des vecteurs $b_1, \ldots, b_q$; choisissons dans L des vecteurs $a_{p+1}, \ldots, a_{p+q}$ tels que

$$b_1 = f(a_{p+1}), \ \ldots, \ b_q = f(a_{p+q});$$

pour démontrer le Théorème 1, il suffit d'établir d'une part que $a_1, \ldots a_{p+q}$ engendrent L dans tous les cas, d'autre part que ces $p + q$ vecteurs forment une *base* de L dans le cas où $a_1, \ldots, a_p$ forment une *base* de Ker (f) et $b_1, \ldots, b_q$ une *base* de Im (f).

Pour établir la première assertion considérons un vecteur $x \in$ L. Comme $f(x)$ appartient au sous-module de M engendré par $b_1, \ldots, b_q$, il existe des scalaires τ_{ij} $(1 \leqslant j \leqslant q)$ tels que

$$f(x) = \tau_{i1} b_1 + \cdots + \tau_{iq} b_q,$$

ce qui s'écrit encore

$$f(x) = \tau_{i1} f(a_{p+1}) + \cdots + \tau_{iq} f(a_{p+q}) = f(\tau_{i1} a_{p+1} + \cdots + \tau_{iq} a_{p+q});$$

on a donc

$$x = \tau_{i1} a_{p+1} + \cdots + \tau_{iq} a_{p+q} + y$$

(*) Le lecteur débutant pourra se borner à lire le n° 1 de ce §, les autres n'étant pas utilisés dans la suite. Néanmoins la lecture des n° 2 à 5 sera certainement un exercice très profitable même pour le débutant.

avec $y \in \mathrm{Ker}\ (f)$; mais alors il existe des scalaires $\xi_i (1 \leqslant i \leqslant p)$ tels que

$$y = \xi_1 a_1 + \cdots + \xi_p a_p,$$

et en portant ce résultat dans la relation précédente on voit que x est bien une combinaison linéaire des vecteurs $a_1, \ldots, a_{p+q}$.

Pour établir la seconde assertion, il suffit de montrer que si les vecteurs $a_i (1 \leqslant i \leqslant p)$ sont linéairement indépendants, ainsi que les vecteurs $b_j (1 \leqslant j \leqslant q)$, alors il en est de même de $a_1, \ldots, a_{p+q}$. Or considérons une relation de la forme

$$\lambda_1 a_1 + \cdots + \lambda_{p+q} a_{p+q} = 0;$$

appliquons f au premier membre; comme $a_1, \ldots, a_p \in \mathrm{Ker}\ (f)$, il vient

$$\lambda_{p+1} f(a_{p+1}) + \cdots + \lambda_{p+q} f(a_{p+q}) = 0;$$

or les vecteurs $f(a_{p+1}) = b_1, \ldots, f(a_{p+q}) = b_q$ sont par hypothèse linéairement indépendants; on voit donc que

$$\lambda_{p+1} = \cdots = \lambda_{p+q} = 0;$$

la relation initiale se réduit alors à $\lambda_1 a_1 + \cdots + \lambda_p a_p = 0$, et comme $a_1, \ldots, a_p$ sont linéairement indépendants il s'ensuit que

$$\lambda_1 = \cdots = \lambda_p = 0,$$

ce qui termine la démonstration.

Remarque 1. On verra plus loin (§ 19, Théorème 13) que lorsque K est un *corps*, de sorte qu'on peut parler de la « dimension » d'un espace vectoriel de dimension finie sur K, le Théorème 1 signifie que

$$\dim (\mathrm{L}) = \dim [\mathrm{Ker}\ (f)] + \dim [\mathrm{Im}\ (f)].$$

Il va de soi que, comme toujours, il ne servirait à rien de supposer que K est un corps dans la démonstration du Théorème 1, et la suite de ce § montrera que, si l'on veut exploiter toutes les conséquences de ce Théorème, il est au contraire tout à fait essentiel de l'énoncer en toute généralité.

2. *Modules de type fini sur un anneau noethérien*

Soit I un *idéal à gauche* d'un anneau K (autrement dit, un sous-module de K regardé comme K-module à gauche); rappelons (§ 11, *Exemple* 6) que I est dit *de type fini* s'il est de type fini comme K-module à gauche, autrement dit s'il existe un nombre fini d'éléments $x_1, \ldots, x_n$ de I tels que I soit l'ensemble des éléments de K qui peuvent se mettre sous la forme $u_1 x_1 + \cdots + u_n x_n$.

On dit qu'un anneau K est **noethérien à gauche** lorsque *tout* idéal à gauche de K est de type fini. On définirait de même les anneaux noethériens à droite en considérant les idéaux à droite. Lorsque K est commutatif (cas de beaucoup le plus important dans ce contexte), on dit simplement que K est **noethérien**.

Exemple 1. Un corps est un anneau noethérien (car ses seuls idéaux à gauche sont $\{0\}$ et K, qui sont évidemment de type fini). Un anneau principal (§ 8, *Exemple* 10) est aussi noethérien.

En dehors des anneaux principaux, les exemples les plus importants d'anneaux noethériens sont les anneaux de polynomes à n indéterminées à coefficients dans un corps (cf. § 32. Exercice 27); ces anneaux — qui ne sont pas principaux pour $n \geqslant 2$ — jouent un rôle fondamental dans l'étude des « variétés algébriques », i.e. des « courbes », « surfaces », etc... définies par des équations algébriques.

THÉORÈME 2. *Soit* K *un anneau. Les propriétés suivantes sont équivalentes :*

a) *L'anneau* K *est noethérien à gauche.*

b) *Tout sous-module de tout* K*-module à gauche de type fini est lui-même de type fini.*

Il est immédiat de voir que *b*) implique *a*) : en effet, le K-module à gauche K est de type fini, donc ses sous-modules (i.e. les idéaux à gauche de K) doivent être de type fini si *b*) est vérifiée.

Montrons maintenant que *a*) implique *b*). On va procéder en deux temps : tout d'abord montrer que, pour tout entier $n \geqslant 1$, tout sous-module de K^n est de type fini; puis en déduire *b*) en toute généralité.

Montrons donc que tout sous-module L de K^n est de type fini. Si $n = 1$, cette assertion n'est autre que l'hypothèse *a*); nous allons donc raisonner par récurrence sur n, en supposant la propriété à établir vraie pour $n - 1$. Pour cela, définissons une application $f : \mathrm{L} \to \mathrm{K}$ en posant $f(\xi_1, \ldots, \xi_n) = \xi_n$; c'est un homomorphisme de L dans K. Pour montrer que L est de type fini, il suffit (Théorème 1) d'établir que Im (f) et Ker (f) sont de type fini. Or Im (f) est un sous-module de K, donc est de type fini d'après l'hypothèse *a*). Quant à Ker (f), c'est un sous-module du sous-module de K^n défini par la relation $\xi_n = 0$; ce sous-module de K^n étant évidemment isomorphe à K^{n-1}, tous ses sous-modules, et en particulier Ker (f), sont de type fini d'après l'hypothèse de récurrence.

Nous avons donc démontré, à l'aide de *a*), que tout sous-module de K^n est de type fini. Prenons maintenant un K-module à gauche M et un sous-module M′ de M; on va montrer que, si M est de type fini, il en est de même de M′.

Puisque M est de type fini, il existe (§ 12, Corollaire 2 du Théorème 3) un entier n et un homomorphisme f de K^n *sur* M. Considérons $\mathrm{L} = f^{-1}(\mathrm{M}')$; comme f est surjectif, f induit un homomorphisme de L *sur* M′; d'autre part L est de type fini d'après ce qu'on a déjà établi; donc M′ lui-même est de type fini (de façon précise, si L est engendré par des vecteurs a_i, $1 \leqslant i \leqslant p$, il est clair que M′ est engendré par les vecteurs $f(a_i)$, $1 \leqslant i \leqslant p$). Ceci achève la démonstration.

3. *Sous-modules d'un module libre sur un anneau principal*

La méthode utilisée pour démontrer le Théorème 2 conduit aussi au résultat suivant :

THÉORÈME 3. *Soit* K *un anneau. Les propriétés suivantes sont équivalentes :*

a) Pour tout idéal à gauche non nul I *de* K, *il existe un* $a \in I$ *tel que l'application* $x \to xa$ *de* K *dans* I *soit bijective;*

b) Si un K*-module à gauche* M *admet une base composée de n vecteurs, et si* M′ *est un sous-module de* M, *il existe un entier* $p \leqslant n$ *tel que* M′ *admette une base composée de p vecteurs.*

Pour montrer que *b*) implique *a*), on prend M = K; alors M admet une base comprenant *un* vecteur; donc tout sous-module de M (i.e. tout idéal à gauche de K) doit admettre une *base* formée de *zéro* ou de *un* vecteur, ce qui est précisément la propriété *a*) de l'énoncé.

Montrons maintenant que *a*) implique *b*). Il est clair que *b*) est équivalent à l'assertion suivante :

b′) Pour tout entier $n \geqslant 1$ *et tout sous-module* L *de* K^n, *il existe un entier* $p \leqslant n$ *tel que* L *soit isomorphe à* K^p.

Pour $n = 1$, il est clair que *b′*) se réduit à l'hypothèse *a*); on va donc raisonner par récurrence sur n, en supposant *b′*) établi pour $n - 1$. Soit donc L un sous-module de K^n, et considérons, comme au n° précédent, l'homomorphisme $f : L \to K$ donné par $f(\xi_1, \ldots, \xi_n) = \xi_n$; l'image de f est un sous-module de K, donc est isomorphe à K^r pour un entier $r \leqslant 1$; le noyau de f est isomorphe à un sous-module de K^{n-1}, donc, d'après l'hypothèse de récurrence, est isomorphe à K^s pour un entier $s \leqslant n - 1$. Faisant usage du Théorème 1, on en déduit que L est isomorphe à K^{r+s}, et comme

$$r + s \leqslant 1 + (n - 1) = n,$$

la démonstration est achevée.

Remarque 2. L'hypothèse *a*) est vérifiée lorsque K est un *anneau principal* i.e. un anneau intègre, commutatif, dont tous les idéaux sont principaux. En effet, soit I un idéal de K; on a $I = Ka$ pour un $a \in K$; l'application

$$x \to xa$$

de K dans I est donc surjective; de plus, son noyau est formé des x tels que $xa = 0$; mais si I n'est pas nul (auquel cas on a évidemment $a \neq 0$), ceci implique $x = 0$ puisque l'anneau K est intègre; donc l'application considérée est injective, ce qui montre bien que l'hypothèse *a*) est vérifiée.

Il va de soi qu'elle est aussi vérifiée lorsque K est un corps (commutatif ou non), car alors le seul idéal à gauche non nul de K est K, et il suffit de prendre $a = 1$ dans l'énoncé de l'hypothèse *a*).

Ces deux cas sont, dans la pratique, les seuls où l'on fasse usage du Théorème 3.

On notera que, l'anneau Z étant principal, le Théorème 3 implique le résultat suivant :

COROLLAIRE DU THÉORÈME 3. *Tout sous-groupe de* Z^n *est isomorphe à* Z^p *pour un entier* $p \leqslant n$.

Bien entendu on a résultat analogue lorsqu'on remplace Z par un corps; mais dans ce cas, on trouvera des résultats plus précis au § suivant.

4. *Applications aux systèmes d'équations linéaires*

Soient K un anneau et f un homomorphisme du K-module à droite K^n dans le K-module à droite K^p. Soit $(\alpha_{ij})_{1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant p}$ la matrice de f (par rapport aux bases canoniques de K^n et K^p); si $x = (\xi_1, \ldots, \xi_n)$ est un vecteur de K^n, son image

$$y = f(x) = (\eta_1, \ldots, \eta_p)$$

est donc donnée par les relations

$$\begin{aligned} &\alpha_{11}\xi_1 + \cdots + \alpha_{n1}\xi_n = \eta_1 \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ &\alpha_{1p}\xi_1 + \cdots + \alpha_{np}\xi_n = \eta_p. \end{aligned}$$

Il s'ensuit que le noyau de f est le sous-module de K^n formé des vecteurs qui vérifient les relations

$$(1) \qquad \begin{cases} \alpha_{11}\xi_1 + \cdots + \alpha_{n1}\xi_n = 0 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ \alpha_{1p}\xi_1 + \cdots + \alpha_{np}\xi_n = 0. \end{cases}$$

On dit que (1) est un **système de p équations linéaires et homogènes à n inconnues à** coefficients dans K.

Soit L le sous-module de K^n formé par les solutions de (1). Nous allons interpréter en langage d'équations linéaires les propriétés suivantes de L : (i) L est de type fini. (ii) Il existe un entier $r \leqslant n$ tel que L soit isomorphe à K^r. La première est vraie pourvu que K soit noethérien à droite (Théorème 2), et la seconde l'est si K est un corps ou bien un anneau principal (Théorème 3).

Supposons L de type fini; alors il existe un nombre fini de vecteurs (*)

$$(2) \qquad \begin{cases} x^1 = (\xi_1^1, \ldots, \xi_n^1), \\ x^2 = (\xi_1^2, \ldots, \xi_n^2), \\ \cdots\cdots\cdots\cdots \\ x^r = (\xi_1^r, \ldots, \xi_n^r) \end{cases}$$

dans L tels que les éléments de L soient les vecteurs

$$x = (\xi_1, \ldots, \xi_n)$$

(*) Les indices supérieurs figurant dans les formules ci-dessous ne sont naturellement pas des exposants.

qui peuvent se mettre sous la forme

$$x = x^1\tau_1 + \cdots + x^r\tau_r \tag{3}$$

où $\tau_1, \ldots, \tau_r$ sont des scalaires arbitraires. Tenant compte de (2), la relation (3) équivaut évidemment au système de relations que voici :

$$\begin{cases} \xi_1 = \xi_1^1\tau_1 + \cdots + \xi_1^r\tau_1 \\ \cdots\cdots\cdots\cdots\cdots \\ \xi_n = \xi_n^1\tau_1 + \cdots + \xi_n^r\tau_r. \end{cases} \tag{4}$$

Ainsi, *lorsque l'anneau* K *est noethérien à droite, il existe des constantes* $\xi_i^j \in K$ *telles que les solutions du système* (1) *soient les familles de scalaires* $\xi_1, \ldots, \xi_n$ *qui peuvent s'écrire sous la forme* (4), *avec des scalaires arbitraires* $\tau_j \in K$. On exprime ce résultat en disant que les solutions du système (1) *dépendent d'un nombre fini de paramètres arbitraires* (à savoir les variables $\tau_1, \ldots, \tau_r$ figurant dans les formules (4)).

Lorsque K est un corps, ou un anneau principal, on peut même supposer que les vecteurs (2) forment une *base* de L; alors chaque $x \in L$ s'écrit d'une seule façon sous la forme (3). Autrement dit, *si* K *est un corps ou un anneau principal, il existe des constantes*

$$\xi_i^j \in K \quad (1 \leqslant i \leqslant n, \quad 1 \leqslant j \leqslant r \leqslant n)$$

telles que l'application

$$(\tau_1, \ldots, \tau_r) \mapsto (\xi_1, \ldots, \xi_n)$$

donnée par les formules (4) *soit une bijection de* K^n *sur l'ensemble des solutions de* (1).

Lorsque K est un corps, on donnera plus loin des résultats beaucoup plus complets et explicites.

5. *Autres caractérisations des anneaux noethériens*

Dans ce n° nous allons donner quelques propriétés caractéristiques des anneaux noethériens. Introduisons tout d'abord la terminologie suivante.

Soit (A_n) une suite de parties d'un ensemble X; on dit que c'est une **suite croissante** si l'on a

$$A_n \subset A_{n+1} \quad \text{pour tout } n,$$

et que c'est une **suite stationnaire** s'il existe un entier p tel que

$$A_n = A_{n+1} \quad \text{pour tout} \quad n \geqslant p,$$

de sorte qu'on a alors $A_p = A_{p+1} = A_{p+2} = \cdots$.

D'autre part, considérons un ensemble F de parties de X; on dit qu'un $A \in F$ est un **élément maximal** de F si les relations

$$A \subset B \quad \text{et} \quad B \in F \quad \text{impliquent} \quad A = B,$$

autrement dit si F ne contient aucun ensemble strictement plus grand que A (ce qui *ne veut pas dire* que tout $B \in F$ soit contenu dans A...).

THÉORÈME 4. *Soit* K *un anneau. Les propriétés suivantes sont équivalentes :*

(AN 1) K *est noethérien à gauche* (i.e. tout idéal à gauche de K est de type fini);

(AN 2) *toute suite croissante d'idéaux à gauche de* K *est stationnaire;*

(AN 3) *tout ensemble non vide d'idéaux à gauche de* K *possède au moins un élément maximal.*

Montrons que (AN 1) implique (AN 2). Soit (I_n) une suite croissante d'idéaux à gauche de K; la réunion I des I_n est encore un idéal à gauche (§ 10, Théorème 1). Comme K est noethérien à gauche, I est engendré par des éléments $x_1, \ldots, x_r$ en nombre fini; et, par définition d'une réunion, il existe des entiers $p_1, \ldots, p_r$ tels que l'on ait $x_1 \in I_{p_1}, \ldots, x_r \in I_{p_r}$. Posons $p = \text{Max}(p_1, \ldots, p_r)$; alors I_p contient $x_1, \ldots, x_r$ puisqu'il contient $I_{p_1}, \ldots, I_{p_r}$; donc I_p contient l'idéal engendré par $x_1, \ldots, x_r$, autrement dit I; pour $n \geqslant p$ on a alors $I_p \subset I_n \subset I \subset I_p$ donc $I_p = I_n$, ce qui établit (AN 2).

Montrons maintenant que (AN 2) implique (AN 3). Soit F un ensemble non vide d'idéaux à gauche de K. Si F n'admettait aucun élément maximal, alors pour tout $I \in F$ on pourrait trouver un $J \in F$ contenant strictement I. Choisissant un $I_1 \in F$, il existerait un $I_2 \in F$ contenant *strictement* I_1, puis un $I_3 \in F$ contenant *strictement* I_2, et ainsi de suite; de cette façon il est clair qu'on obtiendrait une suite strictement croissante d'idéaux à gauche de K, contrairement à (AN 2).

Il reste à montrer que (AN 3) implique (AN 1). Soit I un idéal à gauche de K; soit F l'ensemble des idéaux à gauche de K qui sont *de type fini et contenus dans* I. L'ensemble F est non vide (il contient par exemple l'idéal 0 de K). D'après (AN 3), l'ensemble F admet donc un élément maximal J. Soit $(x_1, \ldots, x_n)$ un système de générateurs de J. Pour tout $x \in I$, l'idéal à gauche engendré par $x_1, \ldots, x_n$ et x est de type fini et contenu dans I — donc appartient à F — et contient J; comme J est un élément maximal de F, cet idéal ne peut être que J lui-même; on a donc $x \in J$ pour tout $x \in I$, d'où $I = J$, ce qui prouve que I est de type fini et achève la démonstration du Théorème.

Remarque 3. On dit qu'un idéal à gauche (resp. à droite, bilatère) I d'un anneau K est **maximal** si $I \neq K$ et si les seuls idéaux à gauche (resp. à droite, bilatères) de K contenant I sont I et K. On peut démontrer, à l'aide de raisonnements assez compliqués de théorie des ensembles, que si K est un anneau, *tout idéal à gauche (resp. à droite, bilatère)* I *de* K, *distinct de* K, *est contenu dans au moins un idéal à gauche (resp. à droite, bilatère) maximal de* K (Théorème de Krull).

Ce résultat, qui joue maintenant un rôle fondamental en Algèbre, peut se démontrer élémentairement si l'anneau K est noethérien : il suffit pour cela d'appliquer l'assertion (AN 3) du Théorème 4 à l'ensemble des idéaux à gauche (resp. à droite, bilatères) J de K tels que

$$I \subset J, \qquad J \neq K.$$

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. Soient K un anneau, L un K-module et

$$L = M_1 \oplus \cdots \oplus M_n$$

une décomposition de L en somme directe de sous-modules.

a) Pour tout endomorphisme u de L, montrer qu'il existe un et un seul système d'homomorphismes

$$u_{ij} : M_i \to M_j \quad (1 \leqslant i, j \leqslant n)$$

tels que l'on ait

$$u(x) = u_{ij}(x) + \cdots + u_{nj}(x) \quad \text{pour tout } x \in M_j$$

et tout j tel que $1 \leqslant j \leqslant n$. Montrer inversement qu'étant donnés de tels homomorphismes u_{ij}, il existe un et un seul endomorphisme u de L vérifiant les conditions précédentes.

b) A tout endomorphisme u de L on associe la « matrice »

$$\begin{pmatrix} u_{11} & \cdots & u_{n1} \\ \cdots & \cdots & \cdots \\ u_{1n} & \cdots & u_{nn} \end{pmatrix}$$

formée avec les homomorphismes définis dans la question *a*). Étant donnés deux endomorphismes u et v de L, comment calcule-t-on la « matrice » de $v \circ u$ en fonction de celles de u et v?

2. Soient r un entier $\geqslant 1$ donné et $r_1, \ldots, r_n$ des entiers $\geqslant 1$ tels que

$$r = r_1 + \cdots + r_n.$$

Étant donnée une matrice carrée

$$U = \begin{pmatrix} a_{11} & \cdots & a_{1r} \\ \cdots & \cdots & \cdots \\ a_{1r} & \cdots & a_{rr} \end{pmatrix}$$

à coefficients dans un anneau quelconque K, on désigne par U_{ij} $(1 \leqslant i, j \leqslant n)$ la matrice (à r_i colonnes et r_j lignes) formée avec ceux des termes a_{pq} de la matrice U pour lesquels on a à la fois

$$\begin{aligned} r_1 + \cdots + r_{i-1} < p \leqslant r_1 + \cdots + r_i \\ r_1 + \cdots + r_{j-1} < q \leqslant r_1 + \cdots + r_j, \end{aligned}$$

ce qui permet, avec des conventions évidentes, d'écrire U sous la form

$$U = \begin{pmatrix} U_{11} & \dots & U_{n1} \\ \dots & \dots & \dots \\ U_{1n} & \dots & U_{nn} \end{pmatrix}.$$

Soit V une autre matrice carrée d'ordre n à coefficients dans K, et soit $W = VU$ la matrice produit. Montrer que les « blocs » W_{ij} qui composent W sont donnés par la formule

$$W_{ij} = V_{1j}U_{i1} + \dots + V_{nj}U_{in}$$

analogue à la règle de calcul usuelle des matrices (**formule de multiplication par blocs** des matrices). Peut-on étendre ce résultat à des produits de matrices rectangulaires?

3. Montrer qu'avec les notations de l'Exercice précédent, la transposée d'une matrice U est donnée par

$$^tU = \begin{pmatrix} ^tU_{11} & \dots & ^tU_{1n} \\ \dots & \dots & \dots \\ ^tU_{n1} & \dots & ^tU_{nn} \end{pmatrix}.$$

4. Soit K un corps commutatif. On considère la matrice carrée

$$J = \begin{pmatrix} 0 & -1_n \\ 1_n & 0 \end{pmatrix}$$

(où 0 est la matrice nulle à n lignes et n colonnes), et on cherche les matrices carrées

$$U = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

d'ordre $2n$, à coefficients dans K, telles que

$$^tU.J.U = J$$

(où A, B, C, D sont des matrices carrées d'ordre n à coefficients dans K). Écrire les relations que doivent vérifier A, B, C, D. Trouver les matrices U pour lesquelles $C = 0$.

5. Soit $S = {}^tS$ une matrice symétrique carrée d'ordre n à coefficients dans un corps commutatif K On pose

$$J = \begin{pmatrix} 0 & 0 & 1_p \\ 0 & S & 0 \\ 1_p & 0 & 0 \end{pmatrix}$$

(de sorte que J est une matrice carrée d'ordre $n + 2p$). A quelles conditions la matrice

$$M = \begin{pmatrix} U & X & Z \\ 0 & V & Y \\ 0 & 0 & W \end{pmatrix}$$

(où la décomposition en blocs de M est de même nature que celle de J) vérifie-t-elle la relation

$$^tM.J.M = J?$$

6. Soient K un anneau et $r_1, \dots, r_n$ des entiers $\geqslant 1$. On pose $r = r_1 + \dots + r_n$, et on considère les matrices

$$U = \begin{pmatrix} U_{11} & \dots & U_{n1} \\ \dots & \dots & \dots \\ U_{1n} & \dots & U_{nn} \end{pmatrix}$$

(avec U_{ij} à r_i colonnes et r_j lignes) qui vérifient les conditions suivantes : on a

$$U_{ij} = 0 \quad \text{pour } i < j,$$

et de plus les matrices U_{ii} sont inversibles. Montrer que les matrices U forment un sous-groupe du groupe linéaire $GL(r, K)$. Même question pour les matrices telles que

$$U_{ij} = 0 \text{ si } i < j, \qquad U_{ii} = 1.$$

Montrer que le second sous-groupe est invariant dans le premier, et formé de matrices unipotentes.

7. Soit $L = M_1 \oplus \dots \oplus M_p$ une décomposition en somme directe de sous-modules d'un module à gauche L sur un anneau K. Dans le module à droite L^*, dual de L, on considère pour chaque i tel que $1 \leqslant i \leqslant p$ l'ensemble M_i' des formes linéaires f sur L telles que

$$f(M_j) = 0 \quad \text{pour tout } j \neq i.$$

Montrer que les M_i' sont des sous-modules de L^* et que $L^* = M_1' \oplus \dots \oplus M_p'$.

8. Soient M un module à gauche sur un anneau K et M' un sous-module M. On suppose que le module quotient M/M' (§§ 10, 11, *Exercice* 10) est libre de type fini. Montrer qu'alors M' est facteur direct dans M (considérer le sous-module de M engendré par des éléments dont les images dans M/M' forment une base de M/M'). Pour une application importante de ce résultat, voir § 29, *Exercice* 11, *g*).

9. Soient M un module à gauche sur un anneau K et a un élément de M tel que $\lambda a = 0$ implique $\lambda = 0$; pour que le sous-module Ka engendré par a soit facteur direct dans M, il faut et il suffit qu'il existe sur M une forme linéaire f telle que $f(a) = 1$; on a alors

$$M = Ka \oplus \mathrm{Ker}(f).$$

¶ **1.** Montrer que tout sous-groupe *de type fini* du groupe additif $\mathbf{Q}^n$ possède une *base* d'au plus n éléments (imiter la démonstration du Théorème 1).

¶ **2.** Pour qu'il existe une base de $\mathbf{Z}^n$ contenant un élément donné $(a_1, \ldots, a_n)$ de $\mathbf{Z}^n$, il faut et il suffit que les entiers a_i soient premiers entre eux (choisir des $u_i \in \mathbf{Z}$ tels que $\sum u_i a_i = 1$ et considérer le sous-groupe de $\mathbf{Z}^n$ défini par l'équation $\sum u_i x_i = 0$).
Plus généralement, soit K un anneau; pour qu'il existe une base de K^n contenant un $a \in K^n$ donné, il est nécessaire qu'il existe une forme linéaire f sur K^n telle que $f(a) = 1$, et cette condition est suffisante si K est principal (cf. § 17, *Exercice* 9).

¶ **3.** Pour qu'il existe une matrice $U \in GL(n, \mathbf{Z})$ ayant une première ligne donnée

$$a_{11} \quad a_{21} \quad \ldots \quad a_{n1},$$

il faut et il suffit que les entiers $a_{11}, a_{21}, \ldots, a_{n1}$ soient premiers entre eux.

¶ **4.** Soient L et M deux modules de type fini sur un anneau commutatif noethérien K. Montrer que le K-module $\mathrm{Hom}_K(L, M)$ est de type fini (construire un homomorphisme injectif de ce module dans une puissance convenable de M).

¶ **5.** Soit M un module de type fini sur un anneau noethérien K. Montrer que toute suite croissante de sous-modules de M est stationnaire, et que tout ensemble de sous-modules de M possède au moins un élément maximal.

¶¶ **6.** Soit $\mathfrak{a}$ un idéal d'un anneau commutatif noethérien K. Montrer qu'il existe une suite finie d'idéaux premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ (pas nécessairement deux à deux distincts) de K telle que l'on ait

$$\mathfrak{p}_1 \ldots \mathfrak{p}_n \subset \mathfrak{a}$$

(raisonner par l'absurde, considérer un élément maximal de l'ensemble des idéaux ne possédant pas cette propriété, et lui appliquer l'*Exercice* 11 du § 8).

¶¶ **7.** Soient K un corps commutatif et A un sous-anneau de K admettant K pour corps des fractions (i.e. tel que tout $x \in K$ soit quotient de deux éléments de A). On utilise dans ce qui suit les définitions et résultats de l'*Exercice* 14 des §§ 10, 11.

a) Si A est un anneau de Dedekind, A est noethérien.

b) On suppose A noethérien, et que tout idéal *maximal* de l'anneau A est inversible; montrer que tout idéal de A est produit d'un nombre fini d'idéaux maximaux (méthode analogue à celle de l'*Exercice* précédent). En déduire que A est un anneau de Dedekind.

c) Soit A un anneau de Dedekind. Montrer que tout idéal fractionnaire de A s'écrit sous la forme d'un produit fini de puissances (positives ou négatives) d'idéaux premiers de A, et que cette décomposition est unique à l'ordre près des facteurs.

d) Soit $\mathfrak{p}$ un idéal premier de l'anneau de Dedekind A. Pour tout $x \in K$ non nul, on désigne par $v_{\mathfrak{p}}(x)$ l'exposant (qui peut être nul) de $\mathfrak{p}$ dans la décomposition de l'idéal fractionnaire Ax de A en produit de facteurs premiers; et on définit $v_{\mathfrak{p}}(0) = +\infty$. Montrer que la fonction $v_{\mathfrak{p}}$ est une valuation discrète (§ 8, *Exercice* 6) du corps K.

¶ **8.** Soient K un anneau commutatif noethérien, M un K-module de type fini, et u l'homothétie de rapport $a \in K$ dans M, donnée par

$$u(x) = ax \quad \text{pour tout } x \in M.$$

a) Montrer qu'il existe un entier $p \geqslant 0$ tel que l'on ait $\mathrm{Ker}(u^n) = \mathrm{Ker}(u^{n+1})$ pour tout $n \geqslant p$ (utiliser l'*Exercice* 5).

b) Montrer qu'on a $\mathrm{Im}(u^n) \cap \mathrm{Ker}(u) = \{0\}$ pour tout $n \geqslant p$.

c) On dit que le module M est **primaire** si, dans M, toute homothétie est soit injective soit nilpotente. Montrer qu'il en est ainsi lorsque le module M possède la propriété suivante : l'intersection de deux sous-modules non nuls de M n'est jamais nulle.

d) Soit $\mathfrak{q}$ un idéal de l'anneau K. Pour que $\mathfrak{q}$ soit primaire (§ 8, *Exercice* 13) il faut et il suffit que le quotient $K/\mathfrak{q}$, regardé comme K-module, soit primaire.

e) Un idéal $\mathfrak{q}$ d'un anneau K est dit **irréductible** si $\mathfrak{q} \neq K$ et si, quels que soient les idéaux $\mathfrak{a}$ et $\mathfrak{b}$ de K, la relation

$$\mathfrak{a} \cap \mathfrak{b} = \mathfrak{q} \text{ implique } \mathfrak{a} = \mathfrak{q} \text{ ou } \mathfrak{b} = \mathfrak{q}.$$

Montrer que tout idéal irréductible d'un anneau noethérien est primaire.

NB. — La réciproque est fausse.

¶¶ **9.** Soit K un anneau commutatif noethérien.

a) Montrer que tout idéal $\mathfrak{a} \neq K$ est intersection finie d'idéaux irréductibles (méthode de l'*Exercice* 6).

b) En déduire que *tout idéal d'un anneau commutatif noethérien est intersection finie d'idéaux primaires* (Emmy Noether).

¶¶ **10.** Soit M un module de type fini sur un anneau commutatif noethérien K. On dit qu'un idéal premier $\mathfrak{p}$ de K est **associé à** M s'il existe un $x \in M$ tel que $\mathfrak{p}$ soit l'annulateur de x dans M (i.e. tel que la relation $a \in \mathfrak{p}$ soit équivalente à la relation $ax = 0$).

a) Si $M \neq \{0\}$, il existe au moins un idéal premier associé à M (considérer les annulateurs des éléments non nuls de M et en prendre un maximal).

b) Il existe une suite croissante

$$0 = M_0 \subset M_1 \subset \cdots \subset M_r = M$$

de sous-modules de M et des idéaux premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ de K tels que M_i/M_{i-1} soit isomorphe au module quotient $K/\mathfrak{p}_i$ pour tout i tel que $1 \leqslant i \leqslant r$ [observer que si l'annulateur d'un élément x d'un module est un idéal $\mathfrak{a}$ de K, alors le sous-module Kx engendré par x est isomorphe à $K/\mathfrak{a}$].

c) Avec les notations de la question précédente, tout idéal premier associé à M est l'un des $\mathfrak{p}_i$.

d) Soit $u(x) = ax (a \in K)$ une homothétie dans M. Pour que u soit injective, il faut et il suffit que a n'appartienne à aucun des idéaux premiers associés à M. Pour que u soit nilpotente, il faut et il suffit que a appartienne à tous les idéaux premiers associés à M.

e) On prend dans ce qui précède $M = K$ et on note $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ les idéaux premiers associés à M. Montrer que

$$\mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_r$$

est l'ensemble des diviseurs de zéro dans K, et que

$$\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r$$

est l'ensemble des éléments nilpotents de K.
Montrer que tout idéal premier de K contient l'un des $\mathfrak{p}_i$. En déduire que, dans un anneau noethérien, l'intersection de tous les idéaux premiers est l'ensemble des éléments nilpotents (ce résultat s'étend en fait à tous les anneaux commutatifs : §§ 27, 28, *Exercice* 9).

¶¶ **11.** Soit $\mathfrak{a}$ un idéal d'un anneau commutatif noethérien K; on suppose $\mathfrak{a} \neq K$. On appelle **idéal premier minimal de** $\mathfrak{a}$ tout idéal premier $\mathfrak{p}$ de K qui contient $\mathfrak{a}$, et qui ne contient aucun idéal premier contenant $\mathfrak{a}$ autre que lui-même.
Montrer que les idéaux premiers minimaux de $\mathfrak{a}$ sont en nombre fini, et que leur intersection est le radical (§ 8, *Exercice* 12) de $\mathfrak{a}$ (appliquer à $K/\mathfrak{a}$ la question *e*) de l'*Exercice* précédent).
(Les anneaux noethériens ont été inventés vers 1920 par Emmy Noether et ont été l'un des principaux points de départ de l'Algèbre « abstraite » moderne. Leur théorie, aujourd'hui extraordinairement développée, est à la base de la Géométrie Algébrique; mais on les utilise aussi ailleurs, en particulier dans la théorie des fonctions analytiques de plusieurs variables complexes; en fait, l'invention de ces anneaux est certainement l'une des découvertes mathématiques les plus utiles des temps modernes. Avant l'introduction des anneaux noethériens, on se bornait à en démontrer certaines propriétés sur les anneaux de polynômes — ce qui conduisait fréquemment à des démonstrations beaucoup plus compliquées que celles qu'on connaît aujourd'hui puisqu'on n'avait pas encore isolé l'idée fondamentale qui permet de les simplifier, à savoir les Théorèmes 3 et 4 de ce §.)

¶