Polynomes et équations algébriques

Les méthodes développées dans les Chapitres précédents avaient principalement pour but l'étude des systèmes d'équations *linéaires*. Mais tout le monde sait qu'il est aussi important — et beaucoup plus difficile — d'étudier les systèmes d'équations *algébriques*, i.e. ceux dont les premiers membres sont des combinaisons linéaires de monômes en les inconnues considérées. L'étude générale de ses systèmes est l'un des objectifs fondamentaux de l'Algèbre, et conduit à la Géométrie Algébrique, actuellement l'une des branches les plus actives des Mathématiques.

Le but du présent Chapitre est d'introduire des notions très élémentaires et de toute façon indispensables dans toutes les Mathématiques, par exemple celles de relation algébrique, de polynôme, de fraction rationnelle, d'équation algébrique, etc...

Comme dans les §§ précédents, nous avons cherché à introduire ces notions avec le degré de généralité maximum, en sorte que, par exemple, nous définissons des polynômes à plusieurs variables à coefficients dans un anneau commutatif K arbitraire. Ici encore il ne s'agit pas d'une généralisation séduisante mais par ailleurs gratuite; la notion de polynôme à coefficients dans un anneau qui n'est pas un corps est indispensable si l'on veut pouvoir, dans la théorie des polynômes à n variables, raisonner par récurrence sur le nombre n (les polynômes à n variables sont des polynômes à une variable à coefficients dans l'anneau, *qui n'est pas un corps*, des polynômes à $n-1$ variables), et il y a naturellement d'autres raisons plus sérieuses de se placer à ce niveau de généralité — sans parler du fait que, comme toujours, on ne simplifierait pratiquement pas l'exposé en supposant que l'anneau de base est le corps des nombres réels par exemple. (On pourrait alors se dispenser de faire la distinction entre « polynômes » et « fonctions polynomiales », mais non de prouver qu'une fonction polynomiale qui est « identiquement nulle » a tous ses coefficients nuls.)

Notons que les §§ 26 à 33 peuvent être étudiés par le lecteur qui n'a lu que les §§ 0 à 12, à l'exception du n° 3 du § 26 qui de toute façon n'est pas pour les lecteurs débutants.

1. Monômes et polynômes en les éléments d'un anneau

Soit L un anneau commutatif. Étant donnés un sous-anneau K de L et une partie B de L, considérons les sous-anneaux de L qui contiennent à la fois K et B; l'intersection de ces sous-anneaux est encore un sous-anneau contenant K et B, et c'est évidemment le *plus petit* sous-anneau de L contenant à la fois K et B. On dit que c'est le **sous-anneau de L engendré par K et B**, et on le désigne par la notation

$$K[B].$$

Considérons par exemple le cas où B se compose de n éléments $x_1, \ldots, x_n$ — on utilise alors la notation

$$K[x_1, \ldots, x_n]$$

pour désigner le sous-anneau engendré par K et les x_i. Il est clair que ce sous-anneau contient tout **monôme** en $x_1, \ldots, x_n$, i.e. tout élément de L qui peut s'écrire

$$x_1^{r_1} \ldots x_n^{r_n}$$

avec des exposants entiers r_i positifs ou nuls. Il contient aussi le produit d'un tel monôme par un élément de K, donc toute somme d'un nombre fini de tels produits, autrement dit tout **polynôme en $x_1, \ldots, x_n$ à coefficients dans K**; on appelle ainsi tout $y \in L$ qui peut se mettre sous la forme

$$(1) \qquad y = \sum_{r_1, \ldots, r_n \geq 0} a_{r_1 \ldots r_n} x_1^{r_1} \ldots x_n^{r_n},$$

avec des coefficients $a_{r_1 \ldots r_n} \in K$ presque tous nuls (*). Un tel polynôme s'écrit encore, si l'on préfère, sous la forme

$$(1\ bis) \qquad y = a + \sum_{1 \leq i \leq n} a_i x_i + \sum_{1 \leq i,j \leq n} a_{ij} x_i x_j + \sum_{1 \leq i,j,k \leq n} a_{ijk} x_i x_j x_k + \cdots$$

(*) Cela signifie (§ 11, n° 5) que les systèmes $(r_1, \ldots, r_n)$ tels que l'on ait $a_{r_1 \ldots r_n} \neq 0$ sont en nombre fini. Cette condition est indispensable pour donner un sens au second membre de (1) en tant que somme d'éléments de L.

avec des « coefficients » a, a_i, a_{ij}, a_{ijk}, ... dans K et presque tous nuls; il suffit pour le voir de considérer dans (1) les termes pour lesquels $r_1 + \cdots + r_n = 0$, puis ceux pour lesquels $r_1 + \cdots + r_n = 1$, puis ceux pour lesquels $r_1 + \cdots + r_n = 2$, et ainsi de suite.

Non seulement l'anneau $K[x_1, \ldots, x_n]$ contient tous les polynômes (1), mais tous les éléments de cet anneau sont de tels polynômes — autrement dit $K[x_1, \ldots, x_n]$ *est exactement l'ensemble des* $y \in L$ *qui peuvent s'écrire sous la forme* (1). En effet, comme le produit de deux monômes en les x_i est encore un monôme en les x_i, il est immédiat de voir que l'ensemble L' des polynômes (1) est un sous-anneau de L contenant K et les x_i, donc contenant $K[x_1, \ldots, x_n]$; mais comme on a aussi, d'après ce qui précède, l'inclusion opposée, on voit finalement que $L' = K[x_1, \ldots, x_n]$ comme annoncé.

Le cas le plus simple est celui où $n = 1$, i.e. où B contient un seul élément x; les polynômes en x à coefficients dans K, qui constituent le sous-anneau $K[x]$ de L engendré par K et x, sont alors les $y \in L$ pour lesquels il existe un entier $p \geqslant 0$ et des $a_0, \ldots, a_p \in K$ tels que l'on ait

$$y = a_0 + a_1 x + \cdots + a_p x^p.$$

Remarque 1. Le lecteur débutant, en dépit des idées préconçues qu'il pourrait avoir sur les polynômes, fera bien d'observer qu'ici les lettres x ou $x_1, \ldots, x_n$ désignent des éléments *fixes* de l'anneau L, et non pas des « variables ».

Exemple 1. On a $\mathbf{C} = \mathbf{R}[i]$ puisque tout nombre complexe s'écrit sous la forme $a + bi$ avec $a, b \in \mathbf{R}$.

Exemple 2. Prenons $K = \mathbf{Q}$, $L = \mathbf{R}$ et considérons le sous-anneau $K[x]$ où

$$x = \sqrt[3]{2};$$

les puissances successives de x sont

$$1, x, x^2, 2, 2x, 2x^2, 4, 4x, 4x^2, 8, \ldots$$

et par suite le sous-anneau $\mathbf{Q}[x]$ de $\mathbf{R}$ est l'ensemble des nombres réels qui peuvent s'écrire sous la forme

$$a + bx + cx^2 \qquad \text{avec} \qquad a, b, c \in \mathbf{Q}.$$

Exemple 3. Soient K un anneau commutatif et L l'anneau des applications de K dans K (§ 8, *Exemple* 3); on regarde K comme un sous-anneau de L en associant à chaque élément a de K la fonction constante donnée par

$$f(t) = a \quad \text{pour tout } t \in K.$$

Désignons alors par x l'application identique de K dans K, donnée par

$$x(t) = t \quad \text{pour tout } t \in K.$$

Les éléments du sous-anneau $K[x]$ de L sont appelés les **fonctions polynomiales sur l'anneau** K. Ce sont évidemment les applications f de K dans K pour lesquelles il existe un entier $r \geqslant 0$ et des éléments $a_0, \ldots, a_r$ de K tels que l'on ait

$$f(t) = a + a_1 t + \cdots + a_r t^r \quad \text{pour tout } t \in K.$$

Cette notion sera généralisée au § 28.

2. *Relations algébriques*

Soient L un anneau commutatif, K un sous-anneau de L, et $x_1, \ldots, x_n$ des éléments de L en nombre fini. On appelle **relation algébrique entre** $x_1, \ldots, x_n$ **à coefficients dans** K toute relation linéaire à coefficients dans K entre les monômes en $x_1, \ldots, x_n$, autrement dit toute famille $(a_{r_1 \ldots r_n})_{r_1, \ldots, r_n \geqslant 0}$ d'éléments presque tous nuls de K tels que l'on ait

$$\sum_{r_1, \ldots, r_n \geqslant 0} a_{r_1 \ldots r_n} x_1^{r_1} \ldots x_n^{r_n} = 0. \tag{2}$$

Lorsque la relation (2) n'a lieu que si *tous* les coefficients $a_{r_1 \ldots r_n}$ sont nuls, on dit que $x_1, \ldots, x_n$ sont **algébriquement indépendants sur** K; dans le cas contraire, i.e. s'il existe au moins une relation (2) non triviale, on dit que $x_1, \ldots, x_n$ sont **algébriquement liés sur K.**

Prenons en particulier $n = 1$, i.e. un seul $x \in L$. Si x est algébriquement lié sur K, i.e. s'il existe une relation de la forme

$$a_0 + a_1 x + \cdots + a_p x^p = 0 \tag{3}$$

pour au moins un entier $p \geqslant 0$ et des coefficients $a_i \in K$ non tous nuls, on dit que x est **algébrique sur** K. Dans le cas contraire, on dit que x est **transcendant sur K.**

Exemple 4. Le nombre complexe i est algébrique sur $\mathbf{R}$ et même sur $\mathbf{Q}$ puisqu'il vérifie la relation

$$i^2 + 1 = 0.$$

Exemple 5. Prenons $K = \mathbf{Q}$, $L = \mathbf{C}$ et

$$x = \sqrt[3]{2 - \sqrt{3}};$$

alors x est algébrique sur $\mathbf{Q}$; on a en effet $x^3 = 2 - \sqrt{3}$ et par suite

$$(x^3 - 2)^2 = 3,$$

ce qui s'écrit encore

$$x^6 - 4x^3 + 1 = 0.$$

On appelle **nombres algébriques** (§ 11, *Exemple* 11) les éléments du corps $\mathbf{C}$ des nombres complexes qui sont algébriques sur le corps $\mathbf{Q}$ des nombres ration-

nels, i.e. les $z \in \mathbf{C}$ qui vérifient au moins une relation de la forme

$$a_r z^r + \cdots + a_1 z + a_0 = 0$$

où les a_i sont des nombres *rationnels* non tous nuls (on peut du reste les supposer *entiers* en chassant les dénominateurs).

Exemple 6. On appelle **nombre transcendant** tout nombre complexe qui n'est pas algébrique. Les premiers exemples de tels nombres ont été donnés par Liouville en 1844. En 1882, Lindemann a démontré que le nombre $\pi = 3{,}14159\ldots$ est transcendant, résultat qui implique l'impossibilité de résoudre par l'affirmative le problème dit de la « quadrature du cercle », contrairement à ce que la plupart des mathématiciens avaient conjecturé depuis l'Antiquité.

On peut également démontrer (Hermite, 1873) que le nombre $e = 2{,}71828\ldots$ utilisé en Analyse est transcendant.

Exemple 7. Soient L l'anneau de toutes les applications de $\mathbf{R}$ dans $\mathbf{R}$ et K le sous-anneau de L formé des fonctions polynomiales (*Exemple* 3), i.e. le sous-anneau de L engendré par les fonctions constantes et la fonction x donnée par $x(t) = t$ pour tout $t \in \mathbf{R}$. On dit qu'une fonction $f \in \mathrm{L}$ est **algébrique** si les éléments x et f de L sont liés algébriquement sur le sous-anneau $\mathbf{R}$ de L, autrement dit s'il existe des constantes a_{pq} presque toutes nulles telles que l'on ait

$$\sum_{p,\,q \geqslant 0} a_{pq} t^p f(t)^q = 0 \quad \text{pour tout } t \in \mathbf{R}. \tag{4}$$

Il est clair par exemple que la fonction f donnée par

$$f(t) = \sqrt[3]{t^2 - 1}$$

est algébrique. Une fonction qui n'est pas algébrique est dite **transcendante**; c'est par exemple le cas de la fonction $f(t) = \sin t$; supposons en effet que celle-ci vérifie la relation (4); posant

$$f_p(t) = \sum_{q \geqslant 0} a_{pq} . \sin^q t$$

la relation en question s'écrit

$$\sum_p f_p(t) . t^p = 0,$$

et vu la périodicité de la fonction sinus on aura aussi

$$\sum_p f_p(t) . (t + 2\pi n)^q = 0$$

pour tout entier n; pour $t \in \mathbf{R}$ donné, le polynôme $\sum f_p(t) . x^q$ s'annule donc pour une infinité de valeurs de x, ce qui entraîne, comme on le montrera plus loin (§ 32, n° 4), que ses coefficients $f_p(t)$ sont tous nuls. Ainsi la relation (4) implique

$$\sum_q a_{pq} . \sin^q t = 0$$

quels que soient $p \geqslant 0$ et $t \in \mathbf{R}$; mais alors, pour tout entier $p \geqslant 0$, le polynôme $\sum a_{pq} x^q$ s'annule pour une infinité de valeurs de x (à savoir dès qu'on peut écrire $x = \sin t$, i.e. pour tout x tel que $-1 \leqslant x \leqslant +1$), donc a tous ses coefficients nuls, et on voit en définitive que la relation (4) implique $a_{pq} = 0$ quels que soient p et q, ce qui montre comme annoncé que $\sin t$ est une fonction transcendante.

3. *Cas des corps commutatifs*

Démontrons d'abord le résultat suivant :

THÉORÈME 1. *Soient* L *un corps commutatif,* K *un sous-corps de* L, *et* x *un élément de* L. *Les propriétés suivantes sont équivalentes :*

a) x *est algébrique sur* K;

b) K$[x]$ *est de dimension finie en tant qu'espace vectoriel sur* K;

c) K$[x]$ *est un sous-corps de* L.

Supposons x algébrique sur K; on a alors une relation

$$c_0 + c_1 x + \cdots + c_p x^p = 0$$

avec des coefficients $c_i \in \mathrm{K}$ non tous nuls. On peut supposer $c_p \neq 0$, et comme K est un corps on déduit de la relation précédente une relation de la forme

$$x^p = a_0 + a_1 x + \cdots + a_{p-1} x^{p-1} \tag{5}$$

avec des coefficients

$$a_i = -c_i / c_p$$

dans K. On va en déduire plus généralement que, pour tout $n \geqslant 0$, le monôme x^n est une combinaison linéaire à coefficients dans K des éléments $1, x, \ldots, x^{p-1}$ de K$[x]$. C'est évident pour $n = 0$, ce qui permet de raisonner par récurrence sur n; supposant établie l'existence d'une relation de la forme

$$x^{n-1} = d_0 + d_1 x + \cdots + d_{p-1} x^{p-1}$$

à coefficients $d_i \in \mathrm{K}$, il vient, en tenant compte de (5),

$$x^n = x . x^{n-1} = d_0 x + \cdots + d_{p-2} x^{p-1} + d_{p-1} x^p = d_0 x + \cdots + d_{p-2} x^{p-1} + d_{p-1}(a_0 + a_1 x + \cdots + a_{p-1} x^{p-1}),$$

ce qui prouve évidemment notre assertion. On voit donc que, si x est algébrique, il existe un entier p tel que *toute* puissance de x soit combinaison linéaire, à coefficients dans K, des puissances

$$1, x, \ldots, x^{p-1};$$

il s'ensuit évidemment que ces p éléments engendrent K$[x]$ regardé comme espace vectoriel sur K, et ceci montre que l'assertion *a)* de l'énoncé implique l'assertion *b)*.

Montrons maintenant que *b)* implique *c)*. Posons K$[x]$ = F et, pour un $a \in \mathrm{F}$

non nul, considérons l'application

$$f : \mathrm{F} \to \mathrm{F}$$

donnée par

$$f(u) = au \quad \text{pour tout } u \in \mathrm{F};$$

regardant F comme un espace vectoriel sur K, il est clair que f est un endomorphisme de F. Le noyau de f est formé des $u \in \mathrm{F}$ tels que $au = 0$; comme F est un anneau d'intégrité (comme sous-anneau du *corps* L) et comme $a \neq 0$, on voit que Ker (f) se réduit à zéro, donc que f est *injective*. Si F est de dimension finie, on en déduit (§ 19, Corollaire 1 du Théorème 13) que f est *surjective*, et en particulier qu'il existe un $u \in \mathrm{F}$ tel que $au = 1$; ceci montre que tout élément non nul de l'anneau F est inversible dans F, donc que F est un sous-corps de L.

Il reste à établir que *c*) implique *a*). Or si K[x] est un sous-corps de L, l'inverse (dans L) de tout élément non nul de K[x] est dans K[x]; en particulier K[x] contient l'inverse de x; on a donc une relation de la forme

$$x^{-1} = a_0 + a_1 x + \cdots + a_r x^r$$

avec des coefficients $a_j \in \mathrm{K}$, et comme cette relation s'écrit aussi

$$a_r x^{r+1} + \cdots + a_0 x - 1 = 0,$$

on voit que x est algébrique sur K, ce qui achève la démonstration.

Exemple 8. Prenons $\mathrm{K} = \mathbf{Q}$ et $\mathrm{L} = \mathbf{C}$; soit x un nombre algébrique, i.e. un élément de $\mathbf{C}$ vérifiant une relation de la forme

$$a_n x^n + \cdots + a_1 x + a_0 = 0$$

à coefficients rationnels $a_0, \ldots, a_n$ non tous nuls (*Exemple* 5); alors l'ensemble des nombres complexes qui peuvent s'écrire sous la forme

$$c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$$

avec des coefficients rationnels $c_0, \ldots, c_{n-1}$, est un *sous-corps* de $\mathbf{C}$. On comparera ce résultat à l'*Exemple* 2 du § 8.

THÉORÈME 2. *Soient* L *un corps commutatif,* K *un sous-corps de* L, *et* $\overline{\mathrm{K}}$ *l'ensemble des éléments de* L *qui sont algébriques sur* K. *Alors* $\overline{\mathrm{K}}$ *est un sous-corps de* L.

Supposons x et y algébriques sur K. Il existe des entiers p et q tels que toute puissance de x (resp. y) soit combinaison linéaire, à coefficients dans K, des puissances

$$1, x, \ldots, x^{p-1} \quad (\text{resp. } 1, y, \ldots, y^{q-1});$$

il s'ensuit évidemment, par multiplication, que *tous* les monômes $x^r y^s$ sont des combinaisons linéaires, à coefficients dans K, des pq monômes

$$x^i y^j \quad (0 \leqslant i \leqslant p-1,\ 0 \leqslant j \leqslant q-1).$$

Donc le sous-anneau K[x, y] de L est de dimension finie sur K. Pour tout $z \in \mathrm{K}[x, y]$ le sous-anneau K[z] est contenu dans K[x, y], donc est *a fortiori* de dimension finie sur K; par suite, tout élément de K[x, y] est algébrique sur K; en particulier, $x - y$ et xy sont algébriques sur K, ce qui montre déjà que $\overline{\mathrm{K}}$ est un sous-anneau de L.

Pour achever la démonstration, il reste à prouver que si un $x \neq 0$ est algébrique sur K, il en est de même de x^{-1}; or si l'on a une relation

$$a_n x^n + \cdots + a_1 x + a_0 = 0$$

à coefficients dans K, il est clair que l'élément $x^{-1} = y$ vérifie

$$a_n + \cdots + a_1 y^{n-1} + a_0 y^n = 0,$$

ce qui achève la démonstration.

Exemple 9. L'ensemble des nombres algébriques est un sous-corps de $\mathbf{C}$.

Le lecteur désireux de s'informer sur ces questions, qui jouent un rôle essentiel en Algèbre « supérieure », trouvera de nombreux résultats complémentaires dans les exercices de ce § et des §§ suivants, ainsi que dans certains des ouvrages cités dans la Bibliographie (Van der Waerden, Samuel-Zariski, Lang).

§ 27. Anneaux de polynômes

Soient K un anneau commutatif et n un entier positif. On se propose dans ce § de construire un anneau commutatif L et n éléments $X_1, \ldots, X_n$ de L tels que les conditions suivantes soient remplies :

(AP 1) K *est un sous-anneau de* L;

(AP 2) *les éléments* $X_1, \ldots, X_n$ *sont algébriquement indépendants sur* K;

(AP 3) L *est engendré par* K *et* $X_1, \ldots, X_n$.

Avant d'étudier le cas général, nous résoudrons ce problème dans le cas particulier où $n = 1$: il s'agit alors de construire un sur-anneau commutatif L de K et un $X \in L$ transcendant sur K (§ 26, n° 2) tel que $L = K[X]$.

1. *Préliminaires sur le cas d'une variable*

Supposons construit un sur-anneau commutatif L de K et un $X \in L$ transcendant sur K, tel que $L = K[X]$. Tout $f \in L$ s'écrit alors *d'une façon et d'une seule*

$$f = a_0 + a_1X + \cdots + a_nX^n + \cdots \tag{1}$$

avec des $a_n \in K$ presque tous nuls; en effet, comme $L = K[X]$, les puissances

$$1, X, \ldots, X^n, \ldots$$

engendrent L regardé comme module sur K, et comme X est transcendant sur K ces puissances sont linéairement indépendantes sur K (autrement dit, forment une *base* de L sur K au sens du § 11, n° 5). Réciproquement, il est clair que toute suite $(a_n)_{n \geqslant 0}$ d'éléments presque tous nuls de K définit, par la formule (1), un élément de L.

Soient

$$f = a_0 + a_1X + \cdots, \qquad g = b_0 + b_1X + \cdots$$

deux éléments de L, et posons

$$f + g = c_0 + c_1X + \cdots$$
$$fg = d_0 + d_1X + \cdots;$$

il est clair qu'on a

$$c_n = a_n + b_n \tag{2}$$

pour tout $n \geqslant 0$. Pour calculer fg, on multiplie chaque terme a_pX^p de f par chaque terme b_qX^q de g, et on ajoute les résultats obtenus; pour obtenir ainsi un terme en X^n, il faut prendre $p + q = n$, et on obtient alors la contribution a_pb_q pour calculer le coefficient d_n; ainsi

$$d_n = \sum_{p+q=n} a_pb_q = a_nb_0 + a_{n-1}b_1 + \cdots + a_1b_{n-1} + a_0b_n. \tag{3}$$

L'intérêt des formules (2) et (3) est qu'elles permettent de calculer $f + g$ et fg sans faire intervenir X; elles vont nous servir de point de départ pour la construction effective de l'anneau K[X] cherché.

2. *Polynômes à une indéterminée*

A partir de K, nous allons maintenant construire effectivement un anneau L satisfaisant aux conditions imposées (ce dernier point sera établi au n° suivant; dans le présent n° on va simplement définir les éléments de L, et les opérations algébriques sur ces éléments).

Par définition, L sera l'ensemble des suites

$$f = (a_n)_{n \geqslant 0} = (a_0, a_1, \ldots)$$

d'éléments *presque tous nuls* de K; une telle suite sera appelée un **polynôme à une indéterminée à coefficients dans** K, et les éléments a_n seront appelés les **coefficients** du polynôme f.

Étant donné un polynôme $f = (a_n)_{n \geqslant 0}$ à coefficients dans K, on appelle **degré** de f le plus grand entier $d \geqslant 0$ tel que l'on ait $a_d \neq 0$; cette définition, toutefois, est en défaut dans le cas où l'on a $a_n = 0$ pour tout $n \geqslant 0$; dans ce cas, on appelle degré de f le symbole $-\infty$ [ce symbole ne désigne naturellement pas un entier ordinaire; c'est un nouvel objet mathématique que nous utiliserons en observant les deux conventions suivantes : on posera, par définition

$$-\infty + n = -\infty \quad \text{si} \quad n \in \mathbf{Z} \quad \text{ou si} \quad n = -\infty,$$

et, d'autre part, on conviendra que

$$-\infty \leqslant n \quad \text{si} \quad n \in \mathbf{Z} \quad \text{ou si} \quad n = -\infty;$$

toute autre opération faisant intervenir le symbole $-\infty$, par exemple l'expression

$$-\infty - (-\infty),$$

sera considérée comme dépourvue de sens].

Le degré d'un polynôme f se désigne par la notation

$$d^0(f).$$

Dans l'ensemble des polynômes à une indéterminée à coefficients dans K, on va définir une **addition** et une **multiplication** comme suit : étant donnés deux polynômes

$$f = (a_n)_{n\geqslant 0}, \qquad g = (b_n)_{n\geqslant 0},$$

les polynômes

$$f + g = (c_n)_{n\geqslant 0}, \qquad fg = (d_n)_{n\geqslant 0}$$

sont donnés par les relations

$$c_n = a_n + b_n \tag{2}$$

$$d_n = a_n b_0 + a_{n-1} b_1 + \cdots + a_1 b_{n-1} + a_0 b_n = \sum_{r+s=n} a_r b_s \tag{3}$$

du n° précédent. Pour justifier ces définitions, on doit montrer que les suites (c_n) et (d_n) définies par (2) et (3) sont encore des polynômes, i.e. qu'on a $c_n = d_n = 0$ lorsque l'entier n est suffisamment grand. Or soient p et q les degrés de f et g; si l'on a $n > \text{Max}\,(p, q)$, il vient $a_n = b_n = 0$, donc $c_n = 0$, ce qui montre bien que $f + g$ est un polynôme, et même que

$$d^\circ(f + g) \leqslant \text{Max}\,(d^\circ(f), d^\circ(g)); \tag{4}$$

supposons d'autre part $n > p + q$; alors, dans le terme général $a_r b_s$ de l'expression (3), on a soit $r > p$ (et donc $a_r = 0$), soit $s > q$ (et donc $b_s = 0$); donc tous les termes de (3) sont nuls; ce raisonnement montre non seulement que fg est aussi un polynôme, mais en outre que

$$d^\circ(fg) \leqslant d^\circ(f) + d^\circ(g). \tag{5}$$

Nous devons maintenant vérifier que l'ensemble L, muni des lois de composition qu'on vient de définir, est un *anneau commutatif*. Les calculs à effectuer pour ce faire sont en principe triviaux, et du même ordre que ceux du § 9, n° 3; nous laisserons donc au lecteur le soin de vérifier lui-même la plupart des axiomes, et nous bornerons ici à établir que la multiplication est associative.

Soient pour cela

$$f = (a_n)_{n\geqslant 0}, \qquad g = (b_n)_{n\geqslant 0}, \qquad h = (c_n)_{n\geqslant 0}$$

trois polynômes à coefficients dans K. Posons

$$fg = (u_n)_{n\geqslant 0}, \qquad gh = (v_n)_{n\geqslant 0}.$$

Le coefficient d'indice n de $(fg)h$ est alors égal à

$$u_n c_0 + \cdots + u_0 c_n \tag{6}$$

et celui de $f(gh)$ à

$$a_n v_0 + \cdots + a_0 v_n, \tag{7}$$

de sorte que tout revient à établir que les expressions (6) et (7) sont égales quel que soit n. Or u_p est la somme des produits $a_i b_j$ tels que $i + j = p$; par suite (6) est la somme des expressions

$$(a_i b_j) c_k \quad \text{telles que} \quad (i + j) + k = n;$$

d'autre part, v_q est la somme des produits $b_j c_k$ tels que $j + k = q$; donc (7) est la somme des expressions

$$a_i (b_j c_k) \quad \text{telles que} \quad i + (j + k) = n;$$

l'égalité de (6) et (7) résulte évidemment de ces considérations.

On vérifie d'autre part aisément que les éléments 0 et 1 de L sont donnés par les relations

$$0 = (0, 0, \ldots)$$
$$1 = (1, 0, 0, \ldots).$$

3. *La notation polynomiale*

Montrons maintenant qu'*on peut identifier* K *à un sous-anneau de* L. Pour cela, définissons une application

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

en posant

$$j(a) = (a, 0, 0, \ldots)$$

pour tout $a \in \mathrm{K}$. Évidemment j est injective; et on vérifie trivialement, à l'aide des formules (2) et (3), que

$$j(a + b) = j(a) + j(b), \qquad j(ab) = j(a)\, j(b),$$
$$j(0) = 0, \qquad j(1) = 1.$$

Il s'ensuit que j est un isomorphisme de K sur un sous-anneau de L et qu'il revient au même, pour effectuer des calculs algébriques sur des éléments de K, de remplacer ceux-ci par leurs images par j, et d'effectuer les calculs en question sur les éléments de L ainsi obtenus. Par suite, il est naturel de considérer comme *identiques* un élément a de K et l'élément correspondant de L; autrement dit, nous écrirons dorénavant

$$a = (a, 0, 0, \ldots) \quad \text{pour tout } a \in \mathrm{K}. \tag{8}$$

Les éléments de L ainsi obtenus sont évidemment les polynômes de degré 0 à coefficients dans K (à ceci près que l'élément de L qui correspond à l'élément 0 de K est de degré $-\infty$, et non pas 0). Ces éléments de L s'appellent souvent des **constantes**.

Remarque 1. La notion de « constante » qu'on vient de définir est relative à un anneau de base K : c'est un polynôme, nul ou de degré 0, à coefficients dans K, ou, si l'on veut, un élément de K (regardé comme polynôme à coefficients dans K). La terminologie utilisée ici recevra au § suivant son explication intuitive.

On notera que puisque K est un sous-anneau de L, on peut regarder L comme un module sur K, le produit d'un $a \in K$ et d'un $f \in L$ étant le produit de f et de l'élément (8) de L. En utilisant (3), on trouve facilement que

$$a.(b_0, b_1, \ldots) = (ab_0, ab_1, \ldots). \tag{9}$$

Construisons maintenant un élément de L transcendant sur K. Nous poserons

$$X = (0, 1, 0, 0, \ldots). \tag{10}$$

En utilisant la formule (3), on trouve facilement que

$$X^2 = (0, 0, 1, 0, 0, \ldots)$$
$$X^3 = (0, 0, 0, 1, 0, \ldots),$$

et ainsi de suite; d'où, en utilisant (9), et si $a_0, a_1, \ldots$ sont des éléments de K, les formules

$$a_0 = (a_0, 0, 0, 0, \ldots)$$
$$a_1X = (0, a_1, 0, 0, \ldots)$$
$$a_2X^2 = (0, 0, a_2, 0, 0, \ldots)$$
$$a_3X^3 = (0, 0, 0, a_3, 0, \ldots)$$

et ainsi de suite. Si les a_i sont presque tous nuls, on trouve donc

$$a_0 + a_1X + a_2X^2 + \cdots = (a_0, a_1, a_2, \ldots). \tag{11}$$

Ce résultat, compte tenu de la relation

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

montre que le premier membre de (11) ne peut être nul que si $a_0 = a_1 = a_2 = \cdots = 0$: par suite, X est transcendant sur K.

En outre, la relation (11) montre que *tout* élément de L est un polynôme en X à coefficients dans K (au sens du § 26, n° 1), autrement dit que

$$L = K[X].$$

Ceci montre que l'anneau L satisfait bien aux conditions énoncées au début de ce §.

Dans la pratique, on dit que L est **l'anneau des polynômes à une indéterminée à coefficients dans** K, et pour désigner un élément

$$f = (a_0, a_1, \ldots)$$

de L on utilise *exclusivement* l'écriture

$$f = a_0 + a_1X + a_2X^2 + \cdots, \tag{12}$$

justifiée par la relation (11). Autrement dit, à partir de maintenant, le lecteur peut négliger les considérations du n° précédent, qui ne servent qu'à *définir* les polynômes;

pour tout ce qui suit (et tout ce qu'on peut faire des polynômes en Mathématiques), il n'y a rien de plus à retenir que les conditions (AP 1), (AP 2) et (AP 3) énoncées plus haut — autrement dit : *un polynôme à une indéterminée à coefficients dans* K *est un objet qui peut s'écrire d'une façon et d'une seule sous la forme* (12), *avec des coefficients* $a_n \in K$ *presque tous nuls, et on calcule sur les polynômes en les considérant comme des éléments d'un anneau commutatif, i.e. en utilisant les règles de calcul « évidentes »*.

Remarque 2. Le lecteur se demandera peut-être pourquoi nous n'avons pas défini *a priori* un polynôme comme une expression de la forme (12) sur laquelle on effectue des calculs conformément aux règles « évidentes ». La raison en est qu'en procédant ainsi on n'aurait pas pu donner de signification mathématique précise à la lettre X figurant dans (12), en sorte que la « définition » des polynômes qu'on aurait obtenue ainsi n'en serait pas une en réalité.

Remarque 3. Contrairement à des traditions qui ont parfois encore cours, on aura soin de ne pas considérer la lettre X comme représentant un « élément variable » de K; la lettre X désigne le polynôme particulier (10), dont la définition comporte aussi peu d'arbitraire et d'indétermination que possible...

L'idée que X représente un élément variable de K provient de la confusion, qu'on effectue souvent, entre un polynôme à coefficients dans K et une fonction polynomiale (§ 26, *Exemple* 3) sur l'anneau K. Les relations entre ces deux notions seront discutées au § suivant.

Il va de soi par ailleurs qu'au lieu de désigner le polynôme (10) par X, on peut le désigner par toute autre lettre (en pratique on utilise fréquemment les lettres Y, Z, T, etc...), pourvu que la lettre choisie n'ait pas déjà été utilisée par ailleurs à d'autres fins.

4. *Polynômes à plusieurs indéterminées*

Nous allons maintenant construire, par récurrence sur l'entier n, une solution au problème posé au début du présent §.

Désignons par K' un anneau commutatif contenant K comme sous-anneau, et engendré par K et $n - 1$ éléments $X_1, \ldots, X_{n-1}$ algébriquement indépendants sur K. Désignons par L l'anneau des polynômes à une indéterminée à coefficients dans K', et par X_n l'indéterminée en question : on a donc

$$L = K'[X_n] = K[X_1, \ldots, X_{n-1}][X_n].$$

Nous allons montrer que L répond aux conditions (AP 1), (AP 2) et (AP 3).

Comme K est un sous-anneau de K', lui-même sous-anneau de L, la vérification de (AP 1) est triviale.

D'autre part, soit L' le sous-anneau de L engendré par K et $X_1, \ldots, X_n$; comme il contient K et $X_1, \ldots, X_{n-1}$, il contient K'; comme il contient K' et X_n, il est identique à L; par suite L est engendré par K et $X_1, \ldots, X_n$, ce qui est la condition (AP 3).

Considérons enfin une relation

$$\sum a_{r_1 \ldots r_n} X_1^{r_1} \ldots X_n^{r_n} = 0$$

où les éléments $a_{r_1 \dots r_n}$ de K sont presque tous nuls. Introduisons les éléments

$$f_s = \sum_{r_1, \dots, r_{n-1}} a_{r_1 \dots r_{n-1} s} X_1^{r_1} \dots X_{n-1}^{r_{n-1}}$$

de K′; la relation considérée s'écrit

$$\sum_s f_s X_n^s = 0,$$

et comme X_n est transcendant sur K′, il s'ensuit que $f_s = 0$ pour tout $s \geqslant 0$. Mais comme $X_1, \dots, X_{n-1}$ sont algébriquement indépendants sur K, ceci implique

$$a_{r_1 \dots r_{n-1} s} = 0$$

quels que soient $r_1, \dots, r_{n-1}$ et s, ce qui établit (AP 2).

L'anneau

$$L = K[X_1, \dots, X_{n-1}][X_n] = K[X_1, \dots, X_n]$$

que nous venons de définir s'appelle l'**anneau des polynômes à n indéterminées à coefficients dans** K, et ses éléments s'appellent les **polynômes à n indéterminées à coefficients dans** K. Un tel polynôme f s'écrit donc *d'une façon et d'une seule* sous la forme

$$f = \sum a_{r_1 \dots r_n} . X_1^{r_1} \dots X_n^{r_n}, \tag{13}$$

avec des **coefficients** $a_{r_1 \dots r_n} \in K$ presque tous nuls; et les calculs sur ces polynômes s'effectuent de façon « évidente », i.e. en les regardant comme des éléments d'un anneau commutatif, ce qu'ils sont en effet !

Si par exemple $n = 2$, auquel cas on désigne le plus souvent les indéterminées X_1 et X_2 par X et Y, un polynôme à deux indéterminées à coefficients dans K est une expression de la forme

$$f = \sum a_{rs} X^r Y^s$$

avec des coefficients $a_{rs} \in K$ presque tous nuls; la sommation est étendue à tous les couples (r, s) d'entiers naturels. En groupant les termes pour lesquels $r + s$ possède une valeur donnée, on voit qu'un tel polynôme peut encore s'écrire sous la forme

$$f = a_{00} + (a_{10}X + a_{01}Y) + (a_{20}X^2 + a_{11}XY + a_{02}Y^2) + (a_{30}X^3 + a_{21}X^2Y + a_{12}XY^2 + a_{03}Y^3) + \cdots,$$

avec bien entendu un nombre fini seulement de termes non nuls.

De même, si $n = 3$, on désigne les indéterminées par X, Y, Z et un polynôme à trois indéterminées à coefficients dans K est une expression

$$f = \sum_{i, j, k \geqslant 0} a_{ijk} X^i Y^j Z^k$$

avec des $a_{ijk} \in K$ presque tous nuls; un tel polynôme s'écrit aussi

$$f = a_{000} + (a_{100}X + a_{010}Y + a_{001}Z) + (a_{200}X^2 + a_{020}Y^2 + a_{002}Z^2 + a_{011}YZ + a_{101}ZX + a_{110}XY) + \cdots$$

Il va de soi qu'on n'est pas obligé, pour désigner les coefficients d'un polynôme, d'utiliser les notations ci-dessus : en Mathématiques, chacun est libre de choisir ses notations (pourvu qu'elles soient cohérentes); on peut par exemple, au lieu de distinguer les coefficients les uns des autres à l'aide d'indices multiples, utiliser pour les désigner des lettres différentes, et écrire par exemple un polynôme à deux indéterminées sous la forme

$$f = a + bX + cY + dX^2 + eXY + fY^2 + gX^3 + \cdots;$$

l'inconvénient de cette méthode est que l'alphabet latin n'offre qu'un nombre limité de possibilités. On espère en outre que le lecteur détectera la contradiction interne dans les notations que nous venons d'exhiber à l'instant...

5. *Degrés partiels et degré total*

Si, dans la formule (13), on groupe ensemble tous les termes pour lesquels l'exposant r_i a une valeur donnée, on voit que l'on peut regarder f comme un polynôme à une indéterminée X_i, à coefficients dans l'anneau

$$K_i = K[X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_n].$$

Considérant f comme élément de l'anneau de polynômes $K_i[X_i]$, on peut définir le degré de f; celui-ci s'appelle le **degré de f par rapport à X_i**. Il est donc défini comme suit : on écrit

$$f = \sum_{n \geqslant 0} u_n . X_i^n$$

où les u_n sont des polynômes en les indéterminées autres que X_i, à coefficients dans K; cela fait, le degré de f par rapport à X_i est le plus grand entier n tel que $u_n \neq 0$, ou bien le symbole $-\infty$ si $f = 0$.

On appelle d'autre part **degré total**, ou simplement **degré**, de f le plus grand entier d tel qu'il existe des entiers $r_1, \dots, r_n$ vérifiant

$$a_{r_1 \dots r_n} \neq 0, \qquad r_1 + \cdots + r_n = d.$$

On peut encore définir le degré total comme suit. Disons qu'un polynôme à coefficients dans K est **homogène de degré d** si chacun des monômes qu'il contient effectivement (i.e. avec un coefficient non nul) est de degré total d. En groupant ensemble, dans (13), les termes pour lesquels $r_1 + \cdots + r_n$ a une valeur donnée, on voit que *tout polynôme f à coefficients dans* K *s'écrit d'une façon et d'une seule sous la forme*

$$f = f_0 + f_1 + \cdots + f_p + \cdots$$

où f_r est homogène de degré r pour tout $r \geqslant 0$, et nul pour presque tout r. Ceci fait, le degré total de f est aussi le plus grand entier d tel que $f_d \neq 0$ (on convient toutefois d'attribuer au polynôme 0 le degré total $-\infty$).

Le degré total de f se désigne par la notation $d^\circ(f)$, comme dans le cas d'une seule indéterminée. On a aussi les inégalités

$$d^\circ(f+g) \leqslant \mathrm{Max}\,[d^\circ(f), d^\circ(g)] \tag{4}$$
$$d^\circ(fg) \leqslant d^\circ(f) + d^\circ(g). \tag{5}$$

En effet, soient p et q les degrés de f et g; on a donc

$$f = f_0 + \cdots + f_p, \qquad g = g_0 + \cdots + g_q$$

(on désigne d'une façon générale par u_r la somme des monômes de degré total r d'un polynôme u). En ajoutant terme à terme, on voit que $f+g$ ne fait pas intervenir de monômes de degré supérieur au plus grand des entiers p, q, d'où la première relation. D'autre part, fg est somme des produits $f_i g_j$; mais il est clair que $f_i g_j$ est homogène et de degré total $i+j$; par suite, les monômes qui interviennent effectivement dans le produit fg sont de degré total au plus égal à $p+q$, ce qui prouve la seconde inégalité.

6. *Polynômes à coefficients dans un anneau d'intégrité*

Nous allons établir le résultat suivant :

Théorème 1. *Soit* K *un anneau d'intégrité commutatif; alors, pour tout entier* n, *l'anneau* $K[X_1, \ldots, X_n]$ *est intègre. En outre, quels que soient* $f, g \in K[X_1, \ldots, X_n]$, *on a*

$$d^\circ(fg) = d^\circ(f) + d^\circ(g).$$

Pour montrer que $K[X_1, \ldots, X_n]$ est un anneau d'intégrité, on tient compte de la relation

$$K[X_1, \ldots, X_n] = K[X_1, \ldots, X_{n-1}][X_n];$$

celle-ci permet, en raisonnant par récurrence (*) sur n, de se ramener au cas où $n = 1$.

Soient alors

$$f = a_0 + \cdots + a_p X^p, \qquad a_p \neq 0$$
$$g = b_0 + \cdots + b_q X^q, \qquad b_q \neq 0$$

deux polynômes non nuls à une variable, à coefficients dans K. Il est clair que fg contient un seul terme de degré $p+q$, à savoir

$$a_p b_q X^{p+q};$$

(*) Il est fréquent de procéder ainsi dans la théorie des polynômes à plusieurs indéterminées — mais on ne peut le faire que si l'on admet des polynômes à coefficients dans un *anneau* quelconque, car, même si K est un corps, l'anneau $K[X_1, \ldots, X_{n-1}]$ *n'est pas* un corps.

comme K est intègre, on a $a_p b_q \neq 0$, et par suite $fg \neq 0$. Ceci établit la première assertion du Théorème.

Pour établir la seconde (dans le cas général de plusieurs variables) on écrit

$$f = f_0 + \cdots + f_p, \qquad f_p \neq 0$$
$$g = g_0 + \cdots + g_q, \qquad g_q \neq 0;$$

il est clair que la partie homogène de degré total $p+q$ de fg est $f_p g_q$; or comme on sait déjà que $K[X_1, \ldots, X_n]$ est un anneau d'intégrité, on a $f_p g_q \neq 0$; donc f est de degré total $p+q$, ce qui achève la démonstration.

Remarque 4. A vrai dire nous n'avons démontré la relation

$$d^\circ(fg) = d^\circ(f) + d^\circ(g)$$

que dans le cas où f et g sont non nuls. Si $f = 0$, cette relation s'écrit $-\infty = -\infty + d^\circ(g)$, et résulte des règles de calcul dont on a convenu de se servir au n° 2 en ce qui concerne le symbole $-\infty$.

Remarque 5. Il est clair que, si K n'est pas intègre, $K[X_1, \ldots, X_n]$ ne peut pas l'être non plus. En outre, dans ce cas, la relation

$$d^\circ(fg) = d^\circ(f) + d^\circ(g)$$

peut aussi être en défaut : choisir dans K deux éléments a, b non nuls tels que $ab = 0$, et prendre

$$f = aX, \qquad g = bX;$$

on a

$$d^\circ(fg) = -\infty, \qquad d^\circ(f) + d^\circ(g) = 2.$$

§ 28. Fonctions polynomiales

1. *Valeurs d'un polynôme*

Soient K un anneau commutatif et

$$f = \sum a_{r_1 \dots r_n} X_1^{r_1} \dots X_n^{r_n} \tag{1}$$

un polynôme à n indéterminées à coefficients dans K. Étant donné un sur-anneau commutatif L de K, on appelle **valeur** de f en un point

$$u = (u_1, \dots, u_n) \in L^n$$

l'élément

$$\sum a_{r_1 \dots r_n} u_1^{r_1} \dots u_n^{r_n} \tag{2}$$

de L obtenu en remplaçant les lettres $X_1, \dots, X_n$ dans l'expression (1) de f par les éléments $u_1, \dots, u_n$ de L. La valeur de f en u se désigne par l'une ou l'autre des notations

$$f(u), \qquad f(u_1, \dots, u_n).$$

On dit que u est un **zéro** ou, si $n = 1$, une **racine** de f si l'on a

$$f(u) = 0.$$

Étant donnés un anneau commutatif L et un sous-anneau K de L, on appelle **fonction polynomiale à coefficients dans** K **sur** L^n toute application $\varphi : L^n \to L$ telle qu'il existe un polynôme f à n indéterminées, à coefficients dans K, tel que l'on ait

$$\varphi(u) = f(u) \quad \text{pour tout } u \in L^n.$$

Plus généralement, on dit qu'une application $\varphi : L^n \to L^r$ est polynomiale à coefficients dans K si l'on a (§ 2, n° 9)

$$\varphi = (\varphi_1, \dots, \varphi_r)$$

où les φ_j sont des fonctions polynomiales à coefficients dans K sur L^n.

Exemple 1. Si l'on prend K = L et $n = 1$, on retrouve évidemment les fonctions du § 26, *Exemple* 3, i.e. les applications de K dans K qui sont de la forme

$$a_0 + a_1 t + \dots + a_n t^n$$

où $a_0, \dots, a_n$ sont des éléments « fixes » de K et où t désigne l'élément « variable » de K.

Exemple 2. K et n étant quelconques, prenons pour L un anneau de polynômes à coefficients dans K, autrement dit

$$L = K[Y_1, \dots, Y_p].$$

Pour tout polynôme

$$f \in K[X_1, \dots, X_n]$$

et quels que soient

$$u_1, \dots, u_n \in K[Y_1, \dots, Y_p],$$

on peut donc définir $f(u_1, \dots, u_n)$; pour des raisons évidentes, on dit que c'est le **polynôme en** $Y_1, \dots, Y_p$ **obtenu en substituant les polynômes** $u_1, \dots, u_n$ **aux indéterminées** $X_1, \dots, X_n$ **dans** f.

On notera que si l'on prend en particulier $L = K[X_1, \dots, X_n]$ et

$$u_1 = X_1, \dots, u_n = X_n,$$

le polynôme $f(u_1, \dots, u_n)$ ainsi obtenu est évidemment f lui-même, résultat que l'on exprime à l'aide de la relation

$$f = f(X_1, \dots, X_n);$$

dans la pratique, on utilise fréquemment la notation $f(X_1, \dots, X_n)$ au lieu de f.

L'emploi de cette notation (qui permet de mettre en évidence les notations utilisées pour désigner les indéterminées figurant dans f) ne devra pas faire oublier au lecteur que les lettres X_i *ne désignent pas* des éléments variables de K; voir la *Remarque* 3 du § précédent.

2. *Somme et produit de fonctions polynomiales*

Soient K un anneau commutatif, L un sur-anneau commutatif de K, et n un entier au moins égal à 1. Étant donnés des éléments $u_1, \dots, u_n$ de L, considérons l'application

$$v : K[X_1, \dots, X_n] \to L$$

donnée par

$$v(f) = f(u_1, \dots, u_n)$$

pour tout polynôme $f \in K[X_1, \dots, X_n]$. On a évidemment

$$v(f) = f \quad \text{si } f \in K \text{ (i.e. si } f \text{ est une « constante »)} \tag{3}$$

$$v(f) = u_i \quad \text{si } f = X_i \tag{4}$$

D'autre part, l'application v est un *homomorphisme d'anneaux*; autrement dit, et puisque (3) montre déjà que $v(1) = 1$, on a les relations

$$v(f+g) = v(f) + v(g) \tag{5}$$
$$v(fg) = v(f)v(g) \tag{6}$$

quels que soient f et g. En effet, en posant

$$f = \sum a_{r_1 \dots r_n} X_1^{r_1} \dots X_n^{r_n}, \qquad g = \sum b_{r_1 \dots r_n} X_1^{r_1} \dots X_n^{r_n},$$

on a

$$f + g = h = \sum c_{r_1 \dots r_n} X_1^{r_1} \dots X_n^{r_n}$$

avec

$$c_{r_1 \dots r_n} = a_{r_1 \dots r_n} + b_{r_1 \dots r_n},$$

et par suite

$$h(u_1, \dots, u_n) = \sum c_{r_1 \dots r_n} u_1^{r_1} \dots u_n^{r_n} = \sum a_{r_1 \dots r_n} u_1^{r_1} \dots u_n^{r_n} + \sum b_{r_1 \dots r_n} u_1^{r_1} \dots u_n^{r_n}$$
$$= f(u_1, \dots, u_n) + g(u_1, \dots, u_n),$$

ce qui est la relation (5). La relation (6) s'obtient par des calculs analogues, mais un peu plus compliqués.

Les propriétés (3), (4), (5) et (6) *caractérisent* du reste l'application v comme on le voit immédiatement, et il est par ailleurs clair que *l'image par v de l'anneau de polynômes* $K[X_1, \dots, X_n]$ *n'est autre que le sous-anneau* $K[u_1, \dots, u_n]$ *de* L *engendré par* K *et les éléments* $u_1, \dots, u_n$ *de* L.

Remarque 1. Le noyau de l'homomorphisme v est formé des polynômes f tels que l'on ait $f(u_1, \dots, u_n) = 0$, i.e. des familles $(a_{r_1 \dots r_n})$ d'éléments presque tous nuls de K tels que l'on ait

$$\sum a_{r_1 \dots r_n} u_1^{r_1} \dots u_n^{r_n} = 0;$$

autrement dit, *le noyau de v est formé des relations algébriques entre $u_1, \dots, u_n$ à coefficients dans* K, définies au § 26, n° 2. Dans la pratique, on ne fait aucune différence entre ces relations algébriques et les polynômes f à coefficients dans K tels que $f(u_1, \dots, u_n) = 0$.

Ce qui précède montre en passant que, si $u_1, \dots, u_n$ sont *algébriquement indépendants sur* K, le noyau de v est réduit à 0, en sorte qu'alors v est un *isomorphisme* de l'anneau $K[X_1, \dots, X_n]$ sur le sous-anneau $K[u_1, \dots, u_n]$ de L.

Les formules (5) et (6) peuvent encore s'interpréter comme suit. Pour chaque polynôme $f \in K[X_1, \dots, X_n]$, considérons l'application polynomiale correspondante

$$f^* : L^n \to L,$$

définie par

$$f^*(u_1, \dots, u_n) = f(u_1, \dots, u_n)$$

quels que soient les $u_i \in L$. Les relations (5) et (6) s'écrivent alors

$$(f+g)^* = f^* + g^*,$$
$$(fg)^* = f^* g^*,$$

et montrent que *la somme et le produit de deux fonctions polynomiales sur* L^n, *à coefficients dans* K, *sont encore des fonctions polynomiales à coefficients dans* K. La relation (4) montre évidemment que parmi ces fonctions polynomiales figurent les fonctions coordonnées par rapport à la base canonique de L^n, et (3) que parmi ces fonctions figurent les applications constantes de L^n dans K.

En fait, et si l'on désigne par M l'anneau de toutes les applications de L^n dans L, il est clair que *l'ensemble des applications polynomiales considérées n'est autre que le sous-anneau de* M *engendré d'une part par les fonctions coordonnées, d'autre part par les applications constantes de* L^n *dans* K (applications que l'on identifie généralement aux éléments de K eux-mêmes).

3. Cas d'un corps infini

Soient K un anneau commutatif, f et g deux polynômes à n indéterminées à coefficients dans K, et

$$f^*, g^* : K^n \to K$$

les fonctions polynomiales correspondantes sur K^n. Il se peut que les applications f^* et g^* coïncident bien que les polynômes f et g soient distincts (et c'est précisément la raison pour laquelle on ne peut généralement pas identifier un *polynôme* à coefficients dans K avec une *fonction polynomiale* sur K^n).

Exemple 3. Prenons $n = 1$ et pour K un corps fini à q éléments. Comme le groupe multiplicatif K^* est à $q - 1$ éléments, le Théorème 5 du § 7 montre que l'on a

$$x^{q-1} = 1 \quad \text{pour tout } x \in K^*$$

et par conséquent

$$x^q = x \quad \text{pour tout } x \in K;$$

les polynômes X et X^q, bien qu'évidemment distincts, définissent donc la même fonction polynomiale sur K.

Cette difficulté ne se présente cependant pas dans les cas classiques ($K = \mathbf{Q}$, $\mathbf{R}$ ou $\mathbf{C}$) en vertu du résultat suivant :

THÉORÈME 1. *Soient f et g deux polynômes à n indéterminées à coefficients dans un anneau d'intégrité infini* K. *Pour que l'on ait $f = g$ il faut et il suffit que l'on ait*

$$f(x) = g(x) \quad \textit{pour tout } x \in K^n.$$

En considérant le polynôme $f - g$, il revient évidemment au même de montrer que, pour tout polynôme $h \in K[X_1, \dots, X_n]$, la relation

$$h(x) = 0 \quad \text{pour tout } x \in K^n$$

implique $h = 0$. Nous allons l'établir en plusieurs étapes.

LEMME 1. *Soit f un polynôme à une indéterminée à coefficients dans un anneau commutatif* K,

Pour qu'un élément a de K *soit racine de f, il faut et il suffit qu'il existe un polynôme $g \in K[X]$ tel que*

$$f(X) = (X - a)g(X).$$

(Cette relation exprime que f est un multiple de $X - a$ dans l'anneau K[X].)

Soit en effet Y une indéterminée distincte de X, et substituons à X le polynôme $a + Y$; on obtient un polynôme $f(a + Y)$ en Y, qui peut donc s'écrire

$$f(a + Y) = u_0 + u_1 Y + \cdots + u_m Y^m$$

avec des $u_j \in K$. Substituant 0 à Y dans cette relation on trouve évidemment

$$f(a) = u_0$$

et par suite on peut écrire

$$f(a + Y) = f(a) + Y.h(Y)$$

pour un certain polynôme h en Y. Substituant $X - a$ à Y dans le résultat obtenu, et posant $h(X - a) = g(X)$, il vient

$$f(X) = f(a) + (X - a)g(X).$$

Ceci montre évidemment que $f(X) = (X - a)g(X)$ si a est racine de f; la réciproque est triviale.

LEMME 2. *Soit f un polynôme de degré $n \geqslant 0$ à une indéterminée, à coefficients dans un anneau commutatif* K. *Supposons* K *intègre; alors f possède au plus n racines dans* K.

Si f est de degré 0, alors f est une constante non nulle et ne possède aucune racine, en sorte que le lemme est vrai pour $n = 0$. On va maintenant considérer le cas général en raisonnant par récurrence sur le degré n de f.

Soit $a \in K$ une racine de f; on peut écrire $f(X) = (X - a)g(X)$, où g est de degré $n - 1$ puisque K est intègre (§ 27, Théorème 1); si b est une autre racine de f dans K, on doit avoir $0 = (b - a)g(b)$, et comme K est intègre on en conclut que les racines de f dans K autres que a sont celles de g; comme g est de degré $n - 1$, il a au plus $n - 1$ racines dans K d'après l'hypothèse de récurrence, et par suite f possède lui-même au plus n racines dans K, ce qui démontre le Lemme.

Le Lemme 2 prouve évidemment le Théorème 1 dans le cas des polynômes à une variable puisqu'il montre que, si l'anneau de base K est intègre, un polynôme $h \in K[X]$ ne peut avoir une infinité de racines dans K que s'il est nul.

Il reste à établir le Théorème 1 dans le cas d'un polynôme h à n variables, en raisonnant par récurrence sur n. On peut écrire

$$h(X_1, \ldots, X_n) = \sum h_r(X_1, \ldots, X_{n-1}) X_n^r$$

avec des polynômes $h_r \in K[X_1, \ldots, X_{n-1}]$. Supposons $h(x) = 0$ pour tout $x \in K^n$; il vient alors évidemment

$$\sum h_r(y) t^r = 0$$

pour tout $y \in K^{n-1}$ et tout $t \in K$. Pour $y \in K^{n-1}$ donné, on voit donc que le polynôme à une indéterminée

$$\sum h_r(y) T^r$$

est nul en tout point de K, et comme le Théorème 1 est déjà établi pour les polynômes à une indéterminée on en déduit donc que

$$h_r(y) = 0 \quad \text{pour tout } y \in K^{n-1}$$

et tout r; mais alors l'hypothèse de récurrence montre que $h_r = 0$ pour tout r, et on a bien finalement la relation $h = 0$, ce qui termine la démonstration.

On peut en fait améliorer le Théorème 1; cf. *Exercice* 1.

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. Montrer que les nombres complexes suivants sont algébriques et former pour chacun d'entre eux une équation algébrique à coefficients rationnels :

$$\sqrt{2}+\sqrt{3}; \qquad \sqrt[3]{2}+\sqrt{3}; \qquad \sqrt[4]{2}+\sqrt[3]{3}; \qquad \sqrt{2}+\sqrt{3}+\sqrt{5}.$$

2. Soient L un corps commutatif, K un sous-corps de L, et x un élément de L transcendant sur K. Trouver toutes les relations algébriques à coefficients dans K existant entre les éléments

$$x^2+1 \qquad \text{et} \qquad x^3$$

de L. Même question pour

$$x^3+x+1 \qquad \text{et} \qquad x^5.$$

¶ **3.** Soient A un anneau d'intégrité commutatif et K un sous-corps de A. On suppose A de dimension finie en tant qu'espace vectoriel sur K ; montrer que A est un corps.
Soient L un corps commutatif, K un sous-corps de L, et $x_1, \ldots, x_n$ des éléments de L algébriques sur K. Montrer que le sous-anneau $K[x_1, \ldots, x_n]$ de L est un corps.

¶ ¶ **4.** Soit K un corps commutatif. On appelle **extension** de K tout corps L admettant K pour sous-corps (par exemple, **C** est une extension de **R**, qui est une extension de **Q**). On peut alors regarder L comme un espace vectoriel sur K ; si L est de dimension finie sur K, i.e. s'il existe des éléments $a_1, \ldots, a_r \in L$ en nombre fini tels que tout élément de L puisse s'écrire sous la forme

$$x_1a_1 + \cdots + x_ra_r$$

avec des $x_i \in K$, on dit que L est une **extension de degré fini** de K ; la dimension de L comme espace vectoriel sur K s'appelle alors le **degré** de L sur K, et se note

$$[L : K];$$

et on appelle **base** de L sur K toute base de L considéré comme espace vectoriel sur K. Lorsque $K = \mathbf{Q}$, les extensions de degré fini de K sont, par définition, les **corps de nombres algébriques** [historiquement, on imposait aux corps de nombres algébriques d'être des extensions de degré fini de **Q** *contenues dans* **C**, mais il est facile de voir que toute extention de degré fini de **Q** peut se « plonger » dans **C**, de sorte que cette condition est superflue]. On désigne dans ce qui suit

par K un corps commutatif et par L une extention de degré fini n de K. Pour tout $a \in L$, on note u_a l'application de L dans L donnée par

$$u_a(x) = ax \quad \text{pour tout } x \in L.$$

a) Montrer que u_a est un endomorphisme de L considéré comme espace vectoriel sur K, et qu'on a les relations

$$u_a + u_b = u_{a+b}, \qquad u_a \circ u_b = u_{ab}$$

quels que soient $a, b \in L$. Quels sont les endomorphismes de L (regardé comme espace vectoriel sur K) qui commutent à tous les u_a?

b) Pour tout $a \in L$, on pose

$$\mathrm{Tr}_{L/K}(a) = \mathrm{Tr}(u_a), \qquad \mathrm{N}_{L/K}(a) = \det(u_a)$$

(on regarde u_a comme un endomorphisme d'un espace vectoriel de dimension finie sur K; le déterminant de u_a est défini au § 23, n° 5, et la trace au § 19, *Exercice* 22). On dit que $\mathrm{Tr}_{L/K}(a)$ est la **trace** et $\mathrm{N}_{L/K}(a)$ la **norme** de a (relativement au sous-corps K); ce sont donc des éléments de K. Montrer qu'on a

$$\mathrm{Tr}_{L/K}(a+b) = \mathrm{Tr}_{L/K}(a) + \mathrm{Tr}_{L/K}(b), \qquad \mathrm{N}_{L/K}(ab) = \mathrm{N}_{L/K}(a)\mathrm{N}_{L/K}(b)$$

quels que soient $a, b \in L$. Si L est de degré n sur K, on a de plus

$$\mathrm{Tr}_{L/K}(a) = na, \qquad \mathrm{N}_{L/K}(a) = a^n$$

pour tout $a \in K$.

c) Soit $(a_i)_{1 \leqslant i \leqslant n}$ une base de L regardé comme espace vectoriel sur K; tout $x \in L$ s'écrit donc d'une façon et d'une seule sous la forme

$$x = \xi_1 a_1 + \cdots + \xi_n a_n \qquad \text{avec} \qquad \xi_1, \ldots, \xi_n \in K.$$

On pose

$$xa_i = \sum_{1 \leqslant j \leqslant n} \lambda_{ij} a_j$$

où les λ_{ij} sont dans K. Calculer $\mathrm{Tr}_{L/K}(x)$ et $\mathrm{N}_{L/K}(x)$ en fonction des λ_{ij}.

d) On suppose K de caractéristique 0 (i.e. que si $x \in K$ et $r \in \mathbf{Z}$ vérifient $rx = 0$, on a soit $r = 0$ soit $x = 0$; cf. § 30, n° 6). Montrer que si un $a \in L$ vérifie

$$\mathrm{Tr}_{L/K}(ax) = 0 \quad \text{pour tout } x \in L$$

on a $a = 0$. En déduire que, si $(a_i)_{1 \leqslant i \leqslant n}$ est une base de L sur K, on a

$$\det(\mathrm{Tr}_{L/K}(a_i a_j)_{1 \leqslant i,j \leqslant n}) \neq 0.$$

e) Soit $(a_i)_{1 \leqslant i \leqslant n}$ une base de L sur K; on considère n éléments

$$b_i = \sum_{1 \leqslant j \leqslant n} \rho_{ij} a_j \quad (\rho_{ij} \in K, \quad 1 \leqslant i \leqslant n)$$

de L. Montrer que, en introduisant les matrices

$$A = (\mathrm{Tr}_{L/K}(a_i a_j))_{1 \leqslant i,j \leqslant n}$$
$$B = (\mathrm{Tr}_{L/K}(b_i b_j))_{1 \leqslant i,j \leqslant n},$$

on a

$$\det(B) = \det(A) \cdot \det(\rho_{ij})^2.$$

En déduire (si K est de caractéristique 0) le résultat suivant : pour que n éléments $x_1, \ldots, x_n$ de L forment une base de L sur K, il faut et il suffit que le déterminant de la matrice

$$(\mathrm{Tr}_{L/K}(x_i x_j))_{1 \leqslant i,j \leqslant n}$$

soit non nul. Ce déterminant s'appelle le **discriminant** des n éléments $x_1, \ldots, x_n$ de L et se note généralement

$$\mathrm{D}_{L/K}(x_1, \ldots, x_n).$$

f) K étant supposé de caractéristique 0, soit $(u_i)_{1 \leqslant i \leqslant n}$ une base de L sur K; montrer qu'il existe une autre base $(v_i)_{1 \leqslant i \leqslant n}$ de L sur K telle que l'on ait

$$\mathrm{Tr}_{L/K}(u_i v_j) = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j \end{cases}$$

(on montrera que les coordonnées des v_i par rapport à la base (u_i) sont données par un système de Cramer). On dit que les bases (u_i) et (v_i) sont **complémentaires**.

g) Les hypothèses et notations étant celles de la question (*f*), montrer que les coordonnées de tout $x \in L$ par rapport à la base (v_i) sont les éléments

$$\mathrm{Tr}_{L/K}(xu_i)$$

de K.

h) On ne suppose plus K de caractéristique 0. On dit que L est une extension **séparable** de K s'il existe un $x \in L$ vérifiant

$$\mathrm{Tr}_{L/K}(x) \neq 0.$$

Montrer que les résultats des questions *d*), *e*), *f*) et *g*) sont encore valables dans ce cas.

¶¶ 5. Soient L un corps commutatif et K un sous-corps de L; on suppose que L est extension de degré fini de K (*Exercice* 4), et on désigne par E un sous-corps de L contenant K.

a) Montrer que L est extension de degré fini de E, et que E est extension de degré fini de K.

b) Soit $(a_i)_{1 \leqslant i \leqslant r}$ une base de L sur E, et soit $(b_j)_{1 \leqslant j \leqslant s}$ une base de E sur K. Montrer que les rs éléments $a_i b_j$ forment une base de L sur K. En déduire que, si l'on note [L : K] le degré de L sur K (i.e. la dimension de L comme espace vectoriel sur K) on a la relation

$$[L : K] = [L : E]\ [E : K]$$

c) Montrer que, pour tout $x \in L$, on a

$$\mathrm{Tr}_{L/K}(x) = \mathrm{Tr}_{E/K}(\mathrm{Tr}_{L/E}(x))$$
$$\mathrm{N}_{L/K}(x) = \mathrm{N}_{E/K}(\mathrm{N}_{L/E}(x))$$

(voir l'*Exercice* 4 en ce qui concerne les notations utilisées).

d) Soient x un élément de L et

$$x^s - a_{s-1}x^{s-1} + \cdots + (-1)^s a_0 = 0$$

une équation algébrique à coefficients dans K vérifiée par x, et de degré s *minimum*. Montrer que les éléments

$$1, x, \ldots, x^{s-1}$$

forment une base du corps K[x] sur K. En utilisant la question *c*) de l'*Exercice* 4, et en posant K[x] = E, montrer qu'on a

$$\mathrm{Tr}_{E/K}(x) = a_{s-1}, \qquad \mathrm{N}_{E/K}(x) = a_0.$$

En conclure que

$$\mathrm{Tr}_{L/K}(x) = \frac{n}{s} a_{s-1}, \qquad \mathrm{N}_{L/K}(x) = (a_0)^{n/s}$$

où $n = [L : K]$.

§§ 27 et 28

1. Soit K un anneau d'intégrité infini. On dit qu'une partie A de K^n est un **ouvert de Zariski** dans K^n s'il existe des polynômes $f_1, \ldots, f_r \in K[X_1, \ldots, X_n]$, en nombre fini, tels que le complémentaire de l'ensemble A dans K^n soit l'ensemble des $x \in K^n$ qui vérifient les relations

$$f_1(x) = \cdots = f_r(x) = 0.$$

Ceci dit, soient f et g deux polynômes à n indéterminées, à coefficients dans K; on suppose qu'il existe dans K^n un ouvert de Zariski non vide A tel que l'on ait

$$f(x) = g(x) \quad \text{pour tout } x \in A;$$

montrer qu'alors $f = g$ **(principe de prolongement des identités algébriques)**

2. Montrer que si trois polynômes $f, g, h \in \mathbf{R}[X]$ vérifient l'une quelconque des trois relations suivantes, on a $f = g = h = 0$:

$$f(X)^2 - Xg(X)^2 = Xh(X)^2$$
$$f(X)^2 - Xg(X)^2 + h(X)^2 = 0$$
$$f(X)^2 + g(X)^2 + (X+2)h(X)^2 = 0.$$

Peut-on dans ce qui précède remplacer **R** par un corps commutatif quelconque?

3. Soient K un corps commutatif, f un polynôme à une indéterminée à coefficients dans K, et $a_1, \ldots, a_r$ des racines deux à deux distinctes de f dans K. Montrer, à l'aide du lemme 1 du § 28, qu'il existe un polynôme g à coefficients dans K tel que

$$f(X) = (X - a_1) \ldots (X - a_r) g(X).$$

Application : calculer (sans calculs !) le déterminant

$$\begin{vmatrix} 1 & 1 & 2 & 3 \\ 1 & 2 - x^2 & 2 & 3 \\ 2 & 3 & 1 & 5 \\ 2 & 3 & 1 & 9 - x^2 \end{vmatrix}$$

4. Même question pour le déterminant

$$\begin{vmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & 1 - x & 1 & \ldots & 1 \\ 1 & 1 & 2 - x & \ldots & 1 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & 1 & 1 & \ldots & n - x \end{vmatrix}$$

5. Soient $f_1, \ldots, f_n$ des polynômes à une variable à coefficients danx un anneau commutatif K, et de degrés $n - 2$ au plus. Montrer qu'on a

$$\begin{vmatrix} f_1(x_1) & f_1(x_2) & \ldots & f_1(x_n) \\ \ldots & \ldots & \ldots & \ldots \\ f_n(x_1) & f_n(x_2) & \ldots & f_n(x_n) \end{vmatrix} = 0$$

quels que soient les $x_i \in K$.

¶ **6.** Soient K un corps commutatif infini et $a_0, \ldots, a_n$ des éléments donnés, deux à deux distincts, de K. Montrer qu'il existe un et un seul polynome $f \in K[X]$ de degré n au plus vérifiant

$$f(a_i) = b_i \quad (0 \leqslant i \leqslant n),$$

où les b_i sont des éléments donnés de K, et que f est fourni par la **formule d'interpolation de Lagrange**

$$f(X) = \sum_{i=0}^{i=n} b_i \frac{(X - a_0) \ldots (X - a_{i-1})(X - a_{i+1}) \ldots (X - a_n)}{(a_i - a_0) \ldots (a_i - a_{i-1})(a_i - a_{i+1}) \ldots (a_i - a_n)}.$$

Exemple : trouver un polynôme f de degré 3 tel que

$$f(1) = 2, \quad f(2) = 1, \quad f(3) = 4, \quad f(4) = 3.$$

¶ **7.** On pose

$$z_k = \cos \frac{2k\pi}{n} + i \cdot \sin \frac{2k\pi}{n};$$

trouver un polynôme f de degré $n - 1$, à coefficients complexes, tel que l'on ait

$$f(z_k) = k + 1 \quad \text{pour } 0 \leqslant k \leqslant n - 1$$

Réponse :

$$f(X) = \frac{n+1}{2} - \frac{1}{2} \sum_{k=1}^{k=n-1} \left(1 - i \cdot \operatorname{cotg} \frac{k\pi}{n}\right) X^k.$$

8. Soit f une fonction définie sur l'ensemble **N** des entiers naturels, et à valeurs complexes. On définit une nouvelle fonction Δf par

$$\Delta f(n) = f(n+1) - f(n),$$

et on définit successivement

$$\Delta^2 f = \Delta(\Delta f), \qquad \Delta^3 f = \Delta(\Delta^2 f), \ldots$$

Enfin, on dit que f est *polynomiale de degré r* s'il existe des constantes $a_0, \ldots, a_r$ telles que

$$f(n) = a_r n^r + a_{r-1} n^{r-1} + \cdots + a_0 \quad \text{pour tout } n \in \mathbf{N},$$

avec de plus $a_r \neq 0$.

a) Montrer que si f est polynomiale de degré r on a

$$\Delta^{r+1} f = 0, \qquad \Delta^r f \neq 0.$$

b) Calculer Δf lorsque

$$f(n) = \frac{n(n-1) \ldots (n - r + 1)}{r!} = \binom{n}{r} \quad \text{pour tout } n \in \mathbf{N};$$

en déduire que, si f est une fonction polynomiale quelconque de degré r, on a

$$f(n) = c_0 + c_1\binom{n}{1} + \cdots + c_r\binom{n}{r} \quad \text{avec } c_k = \Delta^k f(0).$$

c) Montrer que si une fonction $f(n)$ vérifie

$$\Delta^{r+1} f = 0, \qquad \Delta^r f \neq 0,$$

alors f est polynomiale de degré r.

d) Soit g une fonction polynomiale de degré $r - 1$ sur $\mathbf{N}$. Montrer qu'il existe une et une seule fonction polynomiale f sur $\mathbf{N}$, de degré r, telle que

$$\Delta f = g, \qquad f(0) = 0.$$

En calculant f par la formule de la question *b*), en déduire une expression de la somme

$$g(0) + g(1) + \cdots + g(n).$$

Application : calculer les sommes

$$1^2 + 2^2 + \cdots + n^2; \qquad 1^3 + 2^3 + \cdots + n^3.$$

¶¶ **9.** (On rappelle que si A est un anneau commutatif, un idéal I de A est dit *premier* si $I \neq A$ et si, pour $x, y \in A$, la relation $xy \in I$ implique $x \in I$ ou $y \in I$; qu'un idéal I de A est dit *maximal* si $I \neq A$ et si les seuls idéaux de A contenant I sont I et A; et qu'enfin tout idéal de A, autre que A tout entier, est contenu dans au moins un idéal maximal). On se propose de prouver que, *si* K *est un anneau commutatif, l'intersection de tous les idéaux premiers de* K *est l'ensemble des éléments nilpotents de* K.

a) Montrer que, si un idéal I de K vérifie $I \neq K$, alors l'idéal I' de l'anneau de polynômes K[X] engendré par I vérifie $I' \neq K[X]$. En déduire que, pour tout idéal premier de K, il existe un idéal maximal de K[X] qui le contient.

b) On suppose que $u \in K$ appartient à tous les idéaux premiers de K. Montrer que le polynôme $1 - uX$ n'appartient à aucun idéal maximal de l'anneau K[X]; en déduire qu'il est inversible dans l'anneau K[X].

c) Montrer que le polynôme $1 - uX$ ($u \in K$) est inversible dans K[X] si et seulement si u est nilpotent; en déduire le théorème annoncé.

d) Soit I un idéal d'un anneau commutatif K, avec $I \neq K$. Montrer que l'intersection des idéaux premiers de K contenant I est formée des $x \in K$ tels que l'on ait

$$x^n \in I$$

pour au moins un entier n.

10. Soit K un corps commutatif. Pour que le sous-anneau $K[f]$ de K[X] engendré par un polynôme $f \in K[X]$ soit K[X] tout entier, il faut et il suffit que

$$f(X) = aX + b, \qquad a \neq 0.$$

¶ **11.** Soit K un anneau commutatif. On appelle **série formelle à une indéterminée** à coefficients dans K toute suite

$$f = (a_0, a_1, \ldots, a_n, \ldots)$$

d'éléments de K (on ne suppose pas les a_i presque tous nuls). On définit la somme et le produit de deux telles séries formelles à l'aide des formules (2) et (3) du § 27, n° 2, utilisées pour définir la somme et le produit de deux polynômes. Montrer qu'avec ces définitions on obtient un *anneau commutatif* contenant un sous-anneau isomorphe à K[X].

L'anneau ainsi obtenu se note habituellement K[[X]]; au lieu de la notation initiale $f = (a_0, a_1, \ldots, a_n, \ldots)$, on représente les séries formelles par l'écriture

$$(*) \qquad f = a_0 + a_1X + \cdots + a_nX^n + \cdots = \sum_{n=0}^{\infty} a_nX^n,$$

qui permet de retenir plus facilement les formules définissant les opérations fondamentales : pour multiplier deux séries formelles, on les multiplie « terme à terme » puis on groupe ensemble les termes de même degré dans le résultat obtenu. Bien entendu, la formule (*) n'a théoriquement aucun sens, puisqu'elle peut contenir une infinité de termes non nuls; on ne doit la considérer que comme une simple *notation* commode pour représenter la suite des $a_i \in K$.

Démontrer les résultats suivants :

a) Pour que l'anneau K[[X]] soit intègre, il faut et il suffit que K le soit.

b) Pour qu'un élément (*) de K[[X]] soit inversible dans K[[X]], il faut et il suffit que son « terme constant » a_0 soit inversible dans K (différence majeure avec les anneaux de polynômes...).

c) Calculer l'inverse de $1 - X$ dans K[[X]].

¶¶ **12.** Soient K un anneau commutatif et

$$p(X, Y) = p_0(X) + p_1(X)Y + \cdots + p_n(X)Y^n$$

un polynôme à deux variables à coefficients dans K. On suppose $p_0(0) = 0$ et $p_1(0)$ inversible dans K [i.e. $p(0, 0) = 0$ et $p'_Y(0, 0) \neq 0$ si K est un *corps*.]

Montrer qu'il existe une série formelle et une seule

$$y = a_1X + a_2X^2 + \cdots$$

à coefficients dans K, sans terme constant, qui vérifie la relation $p(X, y) = 0$.

[On pourra procéder comme suit : supposant trouvées des constantes $a_1, \ldots, a_r \in K$ telles que le polynôme

$$p(X, a_1X + a_2X^2 + \cdots + a_rX^r)$$

ne contienne aucun terme de degré $\leqslant r$, on montrera qu'il existe $a_{r+1} \in K$ tel que le polynôme

$$p(X, a_1X + a_2X^2 + \cdots + a_{r+1}X^{r+1})$$

ne contienne aucun terme de degré $\leqslant r + 1$.]

Calculer y si $K = \mathbf{C}$ et $f(X, Y) = (X - 1)^p - Y^q$ où p et q sont des entiers positifs. Voyez-vous un rapport entre la série formelle obtenue et le développement en série entière, établi en Analyse, de la fonction

$$(z - 1)^{p/q}?$$

¶ **13.** Soient p un nombre premier, f et g deux polynômes à coefficients entiers rationnels.

a) Montrer que si p divise tous les coefficients de fg, il divise tous les coefficients de f, ou bien tous les coefficients de g.

b) On dit qu'un polynôme à coefficients entiers rationnels est **primitif** si le *pgcd* de ses coefficients est égal à 1. Montrer que si f, g sont primitifs, il en est de même de leur produit.

c) Étant donné un polynôme h à coefficients entiers rationnels, on appelle **contenu** de h le *pgcd*, noté $c(h)$, de ses coefficients. Montrer qu'on a

$$c(fg) = c(f)\,c(g) \qquad \text{quels que soient} \qquad f, g \in \mathbf{Z}[X]$$

(lemme de Gauss).

¶ **14.** Soient K un anneau commutatif, $\mathfrak{p}$ un idéal premier de K, et f, g deux polynômes à coefficients dans K. On suppose que tous les coefficients de fg sont dans $\mathfrak{p}$. Montrer que $\mathfrak{p}$ contient alors tous les coefficients de f, ou tous ceux de g.

¶ **15.** Soit K un anneau d'intégrité commutatif.

a) Soient f et g deux polynômes non constants à une indéterminée, à coefficients dans l'anneau K. Dans l'anneau K[X, Y] des polynômes à deux indéterminées à coefficients dans K, on considère l'idéal I engendré par les polynômes $f(X)$ et $g(Y)$. Montrer qu'on a

$$I \neq K[X, Y]$$

(on supposera qu'on a une relation de la forme

$$u(X, Y)\,f(X) + v(X, Y)\,g(Y) = 1$$

et on examinera les termes homogènes de degré maximum du premier membre).

b) Soient $f_1, \ldots, f_n$ des polynômes à une indéterminée, à coefficients dans K. Montrer que l'idéal de l'anneau $K[X_1, \ldots, X_n]$ engendré par $f_1(X_1), \ldots, f_n(X_n)$ n'est pas l'anneau $K[X_1, \ldots, X_n]$ tout entier si les f_i ne sont pas constants.

c) Montrer que, pour tout entier k tel que $1 \leqslant k \leqslant n$, l'idéal de $K[X_1, \ldots, X_n]$ engendré par $X_1, \ldots, X_k$ est premier. Ces n idéaux sont-ils deux à deux distincts?

¶ **16.** Soit K un anneau commutatif. Montrer que les propriétés suivantes de K sont équivalentes : (*i*) K n'a pas d'élément nilpotent non nul (*ii*) tout élément inversible de l'anneau K[X] est constant (cf. *Exercice* 9 de ce §, et l'*Exercice* 1 du § 8; on pourra aussi examiner les rapports avec l'*Exercice* 11 de ce §).

17. Soient V et W deux espaces vectoriels de dimension finie sur un corps commutatif **K.** On dit qu'une application f de V dans W est **polynomiale** s'il existe une base de V et une base de W telles que les coordonnées du vecteur $y = f(x) \in W$ soient données, en fonction de celles du vecteur $x \in V$, par des formules de la forme

$$\eta_j = p_j(\xi_1, \ldots, \xi_m) \quad (1 \leqslant j \leqslant n)$$

où les p_j sont des polynômes à $m = \dim(V)$ indéterminées, à coefficients dans K. On dit en outre que f est **homogène de degré** r si les p_j sont homogènes de degré r.
Montrer que ces définitions sont indépendantes des bases choisies dans V et W (i.e. que si les conditions énoncées sont satisfaites pour un choix particulier de ces bases, elles le sont pour tout autre choix). Montrer que, si le corps K est fini, toute application de V dans W est polynomiale (ce qui ôte beaucoup de son intérêt à cette notion dans ce cas...). On suppose K infini dans ce qui suit.
On note S(V, W) l'ensemble des applications polynomiales de V dans W, et $S_r(V, W)$ l'ensemble de celles qui sont homogènes de degré r. On pose enfin

$$S(V) = S(V, K), \qquad S_r(V) = S_r(V, K);$$

les éléments de S(V) [resp. $S_r(V)$] sont appelés les **fonctions polynomiales** [resp. les **fonctions polynomiales homogènes de degré** r] sur V.
Montrer que toute $f \in S(V, W)$ s'écrit d'une façon et d'une seule sous la forme

$$f = f_0 + f_1 + \ldots$$

où f_r est polynomiale et homogène de degré r, avec $f_r = 0$ pour presque tout r.
Montrer que S(V) est un sous-anneau de l'anneau de toutes les applications de l'ensemble V dans le corps K, que S(V) contient les applications linéaires et les applications constantes (qu'on identifie habituellement aux éléments de K, de sorte que K s'identifie canoniquement à un sous-corps de l'anneau S(V)). Soient $f_1, \ldots, f_m$ les fonctions coordonnées de V par rapport à une base de V; montrer que

$$S(V) = K[f_1, \ldots, f_m]$$

et que les éléments $f_1, \ldots, f_m$ sont algébriquement indépendants sur K.
Montrer que S(V, W) est un sous-espace vectoriel de l'espace vectoriel de toutes les applications de l'ensemble V dans l'espace vectoriel W. Montrer que, si $f \in S(V)$ et si $g \in S(V, W)$, l'application $h = fg$ de V dans W définie par

$$h(x) = f(x)g(x) \quad \text{pour tout } x \in V$$

est encore polynomiale. En déduire qu'on peut regarder S(V, W) comme un module sur l'anneau S(V). Soient (a_i) une base de V, (b_j) une base de W, et notons f_{ij} l'application *linéaire* de V dans W qui vérifie

$$f_{ij}(a_k) = \begin{cases} b_j & \text{si } k = i \\ 0 & \text{si } k \neq i; \end{cases}$$

montrer que les f_{ij} forment une *base* du S(V)-module S(V, W).
Soient U, V, W trois espaces vectoriels de dimension finie sur K, et

$$f : U \to V, \qquad g : V \to W$$

deux applications polynomiales. Montrer que l'application composée $g \circ f$ est polynomiale. Si f et g sont homogènes de degrés r et s, alors $g \circ f$ est homogène de degré rs.

18. Soit K un corps commutatif infini. On considère l'application polynomiale f de K dans K^3 donnée par

$$f(t) = (t^2 + t + 1,\ t^3 + t + 1,\ t^4 + t + 1);$$

trouver toutes les fonctions polynomiales sur K^3 qui sont nulles en tout point de $f(K)$. Quel sont les points de K^3 où toutes ces fonctions sont nulles?
Même question pour l'application de K^* dans K^3 donnée par

$$f(t) = \left(\frac{t+1}{t},\ \frac{t^2+1}{t},\ \frac{t^3+1}{t}\right).$$

¶ **19.** Soient K un anneau commutatif et M un K-module; on se propose de « plonger » M dans un module sur l'anneau K[X] des polynômes à une indéterminée à coefficients dans K. Pour cela, on considère l'ensemble, noté M[X], dont les éléments sont les suites

$$(m_0,\ m_1,\ \ldots)$$

d'éléments presque tous nuls de M; on définit une addition dans M[X] par la formule

$$(m'_0, m'_1, \ldots) + (m''_0, m''_1, \ldots) = (m'_0 + m''_0, m'_1 + m''_1, \ldots);$$

enfin, on définit le produit d'un élément de M[X] par un élément de K[X] en posant

$$(a_0, a_1, a_2, \ldots).(m_0, m_1, m_2, \ldots) = (a_0m_0, a_0m_1 + a_1m_0, \ldots)$$

Montrer qu'avec ces définitions l'ensemble M[X] est effectivement un K[X]-module; on l'appelle le **module des polynômes à une indéterminée, à coefficients dans** M. On identifie chaque $m \in M$ à l'élément $(m, 0, \ldots)$ de M[X]; montrer qu'on a alors

$$(m_0, m_1, m_2, \ldots) = m_0 + m_1X + m_2X^2 + \cdots$$

dans le K[X]-module M[X] (NB — On écrit ici les scalaires, i.e. les éléments de K[X], à droite des éléments de M[X] pour se conformer à la tradition suivant laquelle, dans un polynôme, on écrit les coefficients à gauche des monômes).
Soient M et N deux K-modules et u un homomorphisme de M dans N; montrer qu'il existe un et un seul homomorphisme

$$\bar{u} : M[X] \to N[X]$$

de K[X]-modules qui coïncide avec u sur M.
On suppose M libre de type fini; montrer qu'alors M[X] est un K[X]-module libre de type fini, et que toute base de M sur K est aussi une base de M[X] sur K[X].
(Pour une application des constructions précédentes, voir § 35, *Exercice* 10)

¶ **20.** Soient K un anneau commutatif, E un K-module, et u un endomorphisme de E. Étant donné un polynôme

$$f(X) = a_0 + a_1X + \cdots + a_nX^n$$

à coefficients dans K, on pose

$$f(u) = a_0 . j_E + a_1u + \cdots + a_nu^n,$$

d'où un nouvel endomorphisme de E. Ceci fait, on considère l'application de l'ensemble produit K[X] × E dans l'ensemble E donnée par

$$(f, x) \mapsto f(u)(x);$$

montrer que l'ensemble E, muni de la loi de composition $(x, y) \mapsto x + y$ et de l'application qu'on vient de définir, est un *module sur l'anneau* K[X]; on le note E_u.
Réciproquement, soit M un K[X]-module; soit E le K-module déduit de M par restriction des scalaires (*) à l'anneau K; on considère l'homothétie de rapport X dans M comme une application u de E dans E. Montrer que u est un endomorphisme du K-module E, et que $M = E_u$. Autrement dit : *un module sur l'anneau* K[X] *s'identifie à un couple formé d'un module sur l'anneau* K *et d'un endomorphisme u de ce* K*-module.* (Ce résultat montre que l'étude des endomorphismes des K-modules revient à celle des K[X]-modules, ce qui sera confirmé dans les *Exercices* du § 35).
On se donne E et u comme ci-dessus; quels sont les sous-modules du K[X]-module E_u?
On considère deux K-modules E et F, un endomorphisme u de E, et un endomorphisme v de F. Quels sont les homomorphismes du K[X]-module E_u dans le K[X]-module F_v?

(*) Soient L un anneau, K un sous-anneau de L, et M un L-module à gauche. Le module déduit de M par restriction à K des scalaires s'obtient en considérant le groupe additif M et l'application $(a, m) \to am$ de K × M dans M qui coïncide, sur K × M, avec l'application de L × M dans M donnée dans la structure de L-module de M. Autrement dit, on garde les mêmes « vecteurs », l'addition reste la même, mais on ne regarde que les homothéties dont le rapport appartient à K. Par exemple, tout espace vectoriel *complexe* définit aussi un espace vectoriel *réel*.

¶ **21.** En imitant les constructions de l'*Exercice* précédent, montrer que, si K est un anneau commutatif, les modules sur l'anneau de polynômes K[X, Y] s'identifient aux triplets (E, u, v) formés d'un K-module E et de deux endomorphismes u et v de E tels que $u \circ v = v \circ u$. Généralisation à n indéterminées?

¶¶ **22.** Soient L un corps commutatif et K un sous-corps de L.
a) On considère un système d'équations linéaires

$$(*) \qquad \begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = b_m \end{cases}$$

à coefficients et seconds membres dans K, et un polynôme p à coefficients dans K et à n indéterminées. On suppose qu'il existe une solution

$$(x_1, \ldots, x_n) \in L^n$$

telle que $p(x_1, \ldots, x_n) \neq 0$; montrer que, si K est infini, il existe alors dans K^n une solution de (*) qui n'annule pas p (exemple **R** et **C**).
b) On considère deux matrices $A, B \in M_n(K)$. On suppose qu'il existe une matrice $V \in GL(n, L)$ telle que $B = VAV^{-1}$; montrer qu'alors il existe $U \in GL(n, K)$ telle que $B = UAU^{-1}$ (considérer l'équation $UA = BU$ avec la condition dét(U) $\neq 0$ et appliquer la question précédente). [NB — Ce résultat subsiste si K est un corps fini, mais la démonstration est nettement plus difficile; cf. § 35, *Exercice* 13].

¶ **23.** Soient K un anneau commutatif et I l'idéal de K[X] engendré par X^{n+1}. Décrire l'anneau quotient $L = K[X]/I$ (on montrera que L est engendré par K et un élément ε assujetti à vérifier la relation $\varepsilon^{n+1} = 0$).
Trouver ses éléments inversibles. [L'anneau L intervient, pour $K = C$, dans la théorie des développements limités d'ordre n].