§ 31. Anneaux principaux

Rappelons (§ 8, *Exemple* 10) qu'on appelle *anneau principal* tout anneau d'intégrité commutatif dont tous les idéaux sont principaux. Nous verrons au § suivant que, si K est un *corps*, l'anneau K[X] des polynômes à *une* variable à coefficients dans K est principal. Dans ce §, on va établir un certain nombre de propriétés arithmétiques des anneaux principaux; ces propriétés généralisent celles des nombres entiers, et seront appliquées aux polynômes au § suivant. *Dans tout ce § on désigne par* K *un anneau principal.*

1. *Plus grand commun diviseur*

Soient K un anneau principal et $x_1, \ldots, x_n$ des éléments de K; soit

$$\mathrm{I} = (x_1, \ldots, x_n)$$

l'idéal (*) de K engendré par $x_1, \ldots, x_n$. Comme K est principal, cet idéal est engendré par un élément d, unique à ceci près qu'on peut le remplacer par ud, où u est un élément inversible (une « unité ») quelconque de l'anneau K (**).

On appelle **plus grand commun diviseur** (p.g.c.d.) de $x_1, \ldots, x_n$ tout élément d de K tel que

$$(x_1, \ldots, x_n) = (d); \tag{1}$$

comme le premier membre est l'ensemble des $y \in \mathrm{K}$ tels qu'il existe $u_1, \ldots, u_n \in \mathrm{K}$ vérifiant

$$y = u_1x_1 + \cdots + u_nx_n, \tag{2}$$

(*) On espère que le lecteur débutant ne confondra pas $(x_1, \ldots, x_n)$ avec l'élément de K^n qu'on désigne par la même notation ! La notation utilisée ici pour désigner l'idéal engendré par $x_1, \ldots, x_n$ est traditionnelle en Arithmétique.

(**) Supposons en effet $(d) = (d')$; il existe $u, v \in \mathrm{K}$ tels que $d' = ud$, $d = vd'$, d'où $vud = d$; si $d \neq 0$ on en déduit (puisque K est intègre) que $vu = 1$, en sorte que u est inversible.

on voit que d est encore caractérisé (à une « unité » près) par le fait que l'ensemble des éléments de la forme (2) est identique à l'ensemble des multiples de d dans K. En particulier, comme $d \in (d)$, on voit qu'*il existe* $u_1, \ldots, u_n \in K$ *tels que*

$$d = u_1x_1 + \cdots + u_nx_n, \tag{3}$$

résultat connu sous le nom de *théorème de Bezout.*

La terminologie utilisée pour désigner d est justifiée par le résultat suivant : *pour qu'un élément de* K *divise simultanément* $x_1, \ldots, x_n$, *il faut et il suffit qu'il divise d.*

La relation (1) montre en effet que l'idéal (d) contient les x_i, qui sont donc des multiples de d; il est par suite clair que tout diviseur de d divise les x_i.

Soit inversement $m \in K$ un diviseur de $x_1, \ldots, x_n$; écrivons

$$x_i = my_i \quad (1 \leqslant i \leqslant n)$$

et portons dans (3); il vient

$$d = m(u_1y_1 + \cdots + u_ny_n),$$

ce qui prouve que m divise d, et achève la démonstration.

Exemple 1. Prenons pour K l'anneau **Z**, qui est effectivement principal (§ 10, *Exemple* 9). Étant donnés des entiers $x_1, \ldots, x_n$, il existe alors un moyen « naturel » ou « canonique » de choisir un générateur de l'idéal $(x_1, \ldots, x_n)$, c'est de prendre *le* générateur *positif* de cet idéal. On peut alors parler *du* pgcd de $x_1, \ldots, x_n$, comme on le fait classiquement. Les diviseurs communs à $x_1, \ldots, x_n$ étant aussi les diviseurs de ce pgcd, il est alors clair que celui-ci (choisi positif) est le plus grand de tous les diviseurs communs à $x_1, \ldots, x_n$. On retrouve donc bien la notion classique, complétée par le théorème de Bezout qu'on ne démontre pas dans l'enseignement élémentaire de l'Arithmétique. Voir l'*Exemple* 8 du § 7.

2. *Éléments premiers entre eux*

On dit que les éléments $x_1, \ldots, x_n$ de K sont **premiers entre eux** s'ils admettent 1 pour p.g.c.d.

THÉORÈME 1. *Soient* $x_1, \ldots, x_n$ *des éléments d'un anneau principal* K. *Les propriétés suivantes sont équivalentes:*

a) $x_1, \ldots, x_n$ *sont premiers entre eux;*

b) *les seuls diviseurs communs à* $x_1, \ldots, x_n$ *sont les éléments inversibles de* K;

c) *il existe des éléments* $u_1, \ldots, u_n$ *de* K *tels que*

$$u_1x_1 + \cdots + u_nx_n = 1;$$

d) *pour tout* $y \in K$, *il existe des éléments* $u_1, \ldots, u_n$ *de* K *tels que*

$$y = u_1x_1 + \cdots + u_nx_n.$$

a) signifie que

$$(x_1, \ldots, x_n) = (1) = K,$$

d'où l'équivalence de *a*) et *d*). Si les x_i sont premiers entre eux, leurs diviseurs communs sont les diviseurs de 1, i.e. les éléments inversibles de K; inversement, si tout diviseur commun aux x_i est inversible, alors le (ou, plus correctement, un) p.g.c.d. des x_i est inversible, et comme les multiples d'un élément inversible constituent l'anneau K tout entier on a donc $(x_1, \ldots, x_n) = K$, de sorte que les propriétés *a*) et *b*) sont équivalentes. Enfin, *a*) implique *c*) en vertu du théorème de Bezout; et *c*) implique *d*), car *c*) signifie que l'idéal $(x_1, \ldots, x_n)$ contient 1, et est donc K tout entier. Ceci achève la démonstration.

La propriété *c*) du Théorème 1 est fort utile pour démontrer certaines propriétés « classiques » mais peu évidentes à première vue. Par exemple :

THÉORÈME 2. *Soient* x, y *des éléments non nuls de* K *et d un diviseur du produit* xy; *si d est premier à* x, *alors d divise* y.

Comme d et x sont premiers entre eux, il existe $u, v \in K$ tels que

$$ud + vx = 1;$$

multipliant le résultat par y il vient

$$y = yud + vxy;$$

comme d divise xy et yud, il divise évidemment le second membre, donc divise aussi y, d'où le Théorème.

3. *Plus petit commun multiple*

Soient $x_1, \ldots, x_n$ des éléments non nuls de K. Les multiples de x_i sont les éléments de l'idéal (x_i); par suite, les multiples communs aux x_i sont les éléments de l'idéal $(x_1) \cap \cdots \cap (x_n)$. Celui-ci étant principal, on peut poser la définition suivante : on appelle **plus petit commun multiple** (p.p.c.m.) de $x_1, \ldots, x_n$ tout élément m de K tel que

$$(x_1) \cap \cdots \cap (x_n) = (m). \tag{4}$$

L'élément m est unique à une unité près (autrement dit, les p.p.c.m. des x_i sont obtenus en multipliant m par un élément inversible quelconque de K), et la relation (4) montre que *les multiples communs aux* x_i *ne sont autres que les multiples de m.*

THÉORÈME 3. *Soient* x *et* y *des éléments non nuls de* K. *On a alors*

$$xy = md$$

où m est un p.p.c.m. *et où d est un* p.g.c.d. *de* x *et* y.

Remarque 1. Comme on a le droit de remplacer d par ud et m par vm où u, v sont des éléments inversibles arbitraires de K, il est clair que la relation

$$xy = md$$

ne peut être valable que si m et d sont convenablement choisis; c'est sous cette forme qu'on doit interpréter l'énoncé.

Pour démontrer le Théorème 3, posons

$$x = x'd, \qquad y = y'd,$$

et soit m' un p.p.c.m. de x' et y'; pour qu'un élément z de K soit multiple de x et de y il faut et il suffit, évidemment, que l'on puisse écrire

$$z = z'd$$

où z' est multiple commun à x' et y', autrement dit est multiple de m'. Ainsi, les multiples communs à x et y sont les multiples de $m'd$, qui est donc un p.p.c.m. de x et y. La relation à établir s'écrit donc $xy = m'd.d$ ou, en simplifiant par d^2,

$$x'y' = m'.$$

Le Théorème 3 sera donc une conséquence des deux lemmes que voici :

LEMME 1. *Soient x, y deux éléments non nuls de* K *et d un* p.g.c.d. *de x et y; posons $x = x'd$, $y = y'd$: alors x' et y' sont premiers entre eux.*

En effet il existe u, $v \in$ K tels que $ux + vy = d$, ce qui, en simplifiant par d, s'écrit $ux' + vy' = 1$, et prouve le lemme vu le Théorème 1.

LEMME 2. *Si x et y sont premiers entre eux, xy est un* p.p.c.m. *de x et y* (ou encore : les multiples communs à x et y sont les multiples de xy).

Soit m un multiple commun à x et y; posons $m = xz$; l'élément y divise donc xz; comme il est premier à x, il divise z (Théorème 2), d'où le Lemme.

Le Théorème 3 est maintenant démontré.

Le lemme 2 peut se généraliser comme suit :

THÉORÈME 4. *Soient $x_1, \ldots, x_n$ des éléments non nuls de* K *deux à deux premiers entre eux; alors $x_1 \ldots x_n$ est un* p.p.c.m. *de $x_1, \ldots, x_n$.*

Pour $n = 2$, c'est le Lemme 2. On va donc montrer que si le Théorème est vrai pour un produit de $n - 1$ facteurs, il est vrai pour un produit de n facteurs.

Montrons d'abord par récurrence sur n que x_n *est premier au produit* $x_1 \ldots x_{n-1}$. Si $n = 2$, c'est l'hypothèse que les x_i sont deux à deux premiers entre eux. Supposons alors prouvé que x_n est premier à $x_1 \ldots x_{n-2}$, et doit d un diviseur commun à x_n et $x_1 \ldots x_{n-1}$; comme d divise x_n, qui est premier à x_{n-1}, il est clair que d est premier à x_{n-1}; comme d divise $x_n \ldots x_{n-2}x_{n-1}$, on voit donc que d divise $x_1 \ldots x_{n-2}$ (Théorème 2); mais comme x_n et $x_1 \ldots x_{n-2}$ sont premiers entre eux d'après l'hypothèse de récurrence, on voit que d est inversible, d'où notre assertion.

Nous pouvons maintenant démontrer le Théorème 4 par récurrence sur n. Soit m un multiple commun aux x_i; le théorème étant supposé établi pour un produit de $n - 1$ facteurs, on voit que m est un multiple de $x_1 \ldots x_{n-1}$, et aussi de x_n; ces deux éléments de K étant, comme on vient de le voir, premiers entre eux, m est donc, d'après le Lemme 2, un multiple de leur produit, ce qui achève la démonstration.

4. *Existence de diviseurs premiers*

On dit qu'un élément p de K est **premier** ou **irréductible** ou **extrémal** (*) s'il n'est pas inversible et si ses seuls diviseurs sont ceux qui sont évidents *a priori*, à savoir les éléments inversibles de K, et les éléments pu où u est inversible.

Lorsque K = **Z** on retrouve évidemment la notion classique de nombre premier; or on sait que, dans ce cas, tout $x \in$ K peut s'écrire sous forme d'un produit de nombres premiers; nous allons montrer que ce résultat s'étend aux anneaux principaux :

THÉORÈME 5. *Soit* K *un anneau principal; tout élément non nul de* K *est produit d'un élément inversible et d'éléments extrémaux de* K.

Ou encore : *tout $x \in$ K qui n'est ni nul ni inversible est un produit d'éléments extrémaux de* K (un élément inversible ne peut évidemment pas se décomposer en produits d'éléments extrémaux, car les diviseurs d'un élément inversible sont inversibles, et ne peuvent donc jamais être extrémaux).

Pour démontrer le Théorème 5, observons d'abord qu'un anneau principal est *a fortiori* noetherien : tous ses idéaux sont évidemment de type fini. Par conséquent (§ 18, Théorème 4 ou Remarque 2 ci-dessous) on a le résultat suivant :

LEMME 3. *Soit* X *un ensemble non vide d'idéaux d'un anneau principal* K; *alors* X *possède au moins un élément maximal,* i.e. il existe un I $\in$ X qui n'est contenu dans aucun autre J $\in$ X.

Ceci étant rappelé, on va démontrer le Théorème 5 en raisonnant par l'absurde. Soit X l'ensemble des idéaux I = (x) de K pour lesquels x est un élément non nul de K qui *ne peut pas* s'écrire comme produit d'un élément inversible et d'éléments extrémaux de K : pour établir le Théorème, tout revient à montrer que l'ensemble X est *vide*. S'il ne l'était pas, il contiendrait au moins un élément maximal, soit (a). L'élément a ne pouvant pas se décomposer en produit d'un élément inversible et d'éléments extrémaux ne serait ni inversible, ni extrémal. Par suite on pourait écrire $a = bc$ où ni b ni c ne seraient inversibles; il est clair qu'alors les idéaux (b) et (c) contiendraient *strictement* (a); comme (a) n'est strictement contenu dans aucun idéal appartenant à l'ensemble X, on voit donc que ni (b) ni (c) n'appartiendrait à X; donc le Théorème 5 serait vrai pour b et pour c; mais alors il serait évidemment vrai pour leur produit a, contrairement à l'hypothèse que $(a) \in$ X, ce qui termine la démonstration.

(*) La première terminologie s'emploie plutôt pour l'anneau **Z** et les anneaux analogues, la seconde pour les anneaux de polynômes, et la troisième pour les anneaux principaux généraux.

Remarque 2. On peut naturellement se passer du Lemme 3 lorsque $K = \mathbf{Z}$ (à vrai dire, les démonstrations élémentaires dans ce cas ne réfèrent pas explicitement au Lemme 3, mais en font néanmoins usage implicitement; la démonstration classique consisterait à introduire le *plus petit* entier $a > 0$ *non* décomposable en facteurs premiers, s'il en existe, puis à observer que a ne peut être premier, donc qu'on peut écrire $a = bc$ avec $0 < b < a$ et $0 < c < a$, auquel cas b et c sont décomposables en facteurs premiers et a aussi par conséquent; il est clair que la démonstration générale est directement calquée sur ce raisonnement traditionnel). On verra au § suivant qu'on peut aussi se passer du Lemme 3 (ou, si l'on préfère, le démontrer trivialement) lorsque $K = L[X]$ où L est un corps.

Rappelons au lecteur que, de toute façon, la démonstration du Lemme 3 est fort simple, et s'obtient comme suit. Si le Lemme 3 était faux, on pourrait, en partant d'un $I_1 \in X$ quelconque, construire un $I_2 \in X$ contenant *strictement* I_1, puis un $I_3 \in X$ contenant *strictement* I_2, et ainsi de suite indéfiniment; pour tirer de là une contradiction tout revient à montrer que *toute suite croissante*

$$I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots;$$

d'idéaux de K *est stationnaire*, autrement dit qu'il existe un entier r tel que

$$I_n = I_r \quad \text{pour tout} \quad n \geqslant r.$$

Or soit I la réunion des I_n, qui est un idéal; comme K est principal, on a $I = (x)$ pour un $x \in K$; comme x appartient à la réunion des I_n, on a $x \in I_r$ pour au moins un indice r; mais alors il est clair que I_r contient les multiples de x, donc que $I_r \supset I$, et pour $n \geqslant r$ il vient alors

$$I_r \subset I_n \subset I \subset I_r,$$

d'où $I_n = I_r$, ce qui prouve le Lemme 3.

5. *Propriétés des éléments extrémaux*

Le résultat suivant contient plusieurs caractérisations utiles des éléments extrémaux (y compris leur définition, qu'on a inclus dans ce résultat pour obtenir un énoncé aussi complet que possible) :

THÉORÈME 6. *Soit p un élément non nul et non inversible d'un anneau principal* K; *les propriétés suivantes sont équivalentes :*

a) p est extrémal;

b) tout diviseur de p est soit inversible, soit de la forme pu où u est inversible;

c) l'idéal $I = (p)$ est maximal (autrement dit on a $I \neq K$ et les seuls idéaux de K contenant I sont I et K);

d) si p divise un produit d'éléments de K, *p divise l'un au moins des facteurs de ce produit.*

L'équivalence des assertions *a*) et *b*) n'est autre que la définition des éléments extrémaux. Pour montrer l'équivalence de *b*) et *c*), considérons un idéal J contenant I; comme K est principal on a $J = (x)$ pour un $x \in K$, et dire que J contient I signifie que x divise p; de plus, la relation $J = K$ signifie que x est inversible, et la relation $J = I$ que $x = pu$ avec u inversible : l'équivalence de *b*) et *c*) résulte aussitôt de ces remarques.

Montrons enfin que la propriété *d*) caractérise aussi les éléments extrémaux. Supposons p extrémal, et soient $x_1, \ldots, x_n$ des éléments non nuls de K tels que p divise le produit $x_1 \ldots x_n$; pour montrer que p divise l'un au moins des x_i on écrit

$$x_1 \ldots x_n = (x_1 \ldots x_{n-1})x_n,$$

et un raisonnement par récurrence montre évidemment qu'il suffit d'examiner le cas où $n = 2$, autrement dit de prouver que *si p divise xy, alors p divise soit x soit y.* En vertu du Théorème 2, tout revient à prouver que, *quel que soit $x \neq 0$, ou bien p divise x ou bien p et x sont premiers entre eux*; or considérons l'idéal (p, x) engendré par p et x; il contient évidemment l'idéal (p); d'après l'assertion *c*) du Théorème 6, qui est déjà établie, deux cas seulement sont donc possibles : ou bien

$$(p, x) = K,$$

et alors p et x sont premiers entre eux, ou bien

$$(p, x) = (p),$$

auquel cas x appartient à (p), donc est multiple de p.

Nous avons démontré que tout élément extrémal vérifie *d*). Inversement considérons un élément non nul et non inversible vérifiant *d*), et montrons qu'il est extrémal. En vertu du Théorème 5, l'élément p considéré peut s'écrire

$$p = p_1 \ldots p_n$$

où les p_i sont extrémaux; d'après *d*), p divise l'un au moins des p_i; mais comme p_i est extrémal, et p non inversible, il s'ensuit que $p = up_i$ avec u inversible, et par suite p est extrémal, ce qui termine la démonstration du Théorème.

COROLLAIRE. *Soient $x, y_1, \ldots, y_n$ des éléments non nuls d'un anneau principal* K, *et supposons x et y_i premiers entre eux quel que soit i. Alors x est premier au produit $y_1 \ldots y_n$.*

Supposons en effet qu'il existe un diviseur commun non inversible d à x et $y_1 \ldots y_n$; comme d n'est pas inversible, il est produit d'éléments extrémaux, donc multiple d'au moins un élément extrémal; par suite il existe un élément extrémal p qui divise à la fois x et $y_1 \ldots y_n$; d'après le Théorème 6, *d*), il existe un i tel que p divise y_i, ce qui contredit l'hypothèse que x et y_i sont premiers entre eux, et démontre le Corollaire.

Il va de soi qu'en supposant $K = \mathbf{Z}$ on ne parviendrait pas à simplifier si peu que ce soit les démonstrations précédentes.

6. *Unicité de la décomposition en facteurs premiers*

On dit que deux éléments extrémaux p' et p'' de K sont **associés** s'il existe un élément inversible u de K tel que $p'' = up'$; cela signifie évidemment que les idéaux (p') et (p'') sont égaux. Lorsque $K = \mathbf{Z}$, cela veut dire que $p'' = \pm p'$.

THÉORÈME 7. *Soit x un élément non nul et non inversible d'un anneau principal* K. *Soient*

$$x = p'_1 \dots p'_m = p''_1 \dots p''_n$$

deux décompositions de x en produit d'éléments extrémaux de K. *On a alors $m = n$ et il existe une permutation σ des indices* 1, ..., n *telle que p'_i et $p''_{\sigma(i)}$ soient associés pour tout i tel que* $1 \leqslant i \leqslant n$.

Autrement dit, une décomposition étant donnée, on obtient *toutes* les autres en effectuant sur celle-ci les opérations « triviales » que voici : (1) modification de l'ordre des termes (2) multiplication de chaque facteur extrémal par un élément inversible de K (ces éléments étant choisis de telle sorte que leur produit soit égal à 1, de façon à ne pas modifier le produit des éléments extrémaux considérés). Lorsque $K = \mathbf{Z}$, on convient souvent de se borner à des nombres premiers *positifs*, ce qui élimine la possibilité (2) puisque, dans ce cas, le seul nombre premier associé à p est $-p$.

Pour établir le Théorème 7, considérons la relation

$$p'_1 \dots p'_m = p''_1 \dots p''_n; \tag{5}$$

p'_1 divise le produit $p''_1 \dots p''_n$ et est extrémal; il divise donc l'un des p''_j; en permutant l'ordre des facteurs du second produit, on peut donc supposer que p'_1 divise p''_1; mais comme p''_1 est premier, il s'ensuit que

$$p''_1 = u_1 p'_1$$

avec u_1 inversible; simplifiant la relation (5) par p'_1, il reste alors

$$p'_2 \dots p'_m = u_1 p''_2 \dots p''_n;$$

en raisonnant comme ci-dessus, on en déduit que p'_2 est associé à l'un des p''_j $(2 \leqslant j \leqslant n)$ et en poursuivant ainsi le raisonnement, il est clair qu'on parvient au Théorème 7 (le lecteur désireux de terminer correctement la démonstration devra raisonner par récurrence sur l'entier m).

Dans la pratique, on écrit souvent de la façon suivante les décompositions en facteurs extrémaux. On choisit une fois pour toutes un ensemble P d'éléments extrémaux de K possédant la propriété suivante : pour tout élément extrémal p de K, il existe *un et un seul* $p' \in P$ qui soit associé à p (pour construire un tel ensemble P, il suffit, en vertu du Théorème 6, *c*), de considérer l'ensemble des idéaux maximaux de K, et de choisir une fois pour toutes un générateur de chacun de ces idéaux; si $K = \mathbf{Z}$ on choisit, pour chaque idéal maximal I, *le* nombre premier *positif* qui engendre I). Soit alors

$$x = p'_1 \dots p'_n$$

une décomposition d'un $x \in K$ non inversible en produit d'éléments extrémaux; pour chaque i on peut écrire $p'_i = u_i p_i$ avec $p_i \in P$ et u_i inversible; d'où évidemment

$$x = u p_1 \dots p_n \quad \text{avec } u \text{ inversible, } p_1, \dots, p_n \in P; \tag{6}$$

la décomposition (6) est alors unique à l'ordre près des facteurs (car deux éléments de P ne peuvent être associés sans être égaux).

Il peut naturellement arriver que, dans la décomposition (6), un élément de P soit répété plusieurs fois; en bloquant ensemble les facteurs égaux, on trouve donc aussi une décomposition de la forme

$$x = u p_1^{n_1} \dots p_r^{n_r} \tag{7}$$

où $p_1, \dots, p_r$ sont des éléments de P deux à deux distincts, et les n_i des exposants positifs. Pour écrire sous une forme plus frappante ce résultat, considérons, pour chaque $p \in P$, le nombre (éventuellement nul) de facteurs de la décomposition (6) qui sont égaux à p, et notons-le

$$v_p(x);$$

il est clair qu'on a

$$v_p(x) = 0 \quad \text{pour presque tout } p \in P, \tag{8}$$

autrement dit qu'on n'a $v_p(x) \geqslant 1$ que pour un nombre fini d'éléments de P. Ceci dit, la décomposition (7), obtenue en groupant ensemble les facteurs égaux dans la décomposition (6), s'écrit encore sous la forme

$$x = u \cdot \prod_{p \in P} p^{v_p(x)}; \tag{9}$$

le produit figurant au second membre comporte en apparence une infinité de facteurs; mais d'après (8) on a

$$p^{v_p(x)} = 1 \quad \text{pour presque tout } p \in P,$$

de sorte que le produit en question ne comporte qu'un nombre fini de termes autres que 1.

7. *Calcul du pgcd et du ppcm à l'aide de la décomposition en facteurs premiers*

La décomposition (9) permet d'exprimer très simplement les propriétés de divisibilité dans l'anneau K. Tout repose sur le résultat suivant :

LEMME 4. *Soient x et y deux éléments non nuls de* K; *pour que x divise y il faut et il suffit que l'on ait*

$$v_p(x) \leqslant v_p(y)$$

pour tout $p \in P$.

La condition est suffisante car, si elle est remplie, on a

$$x = u' \prod p^{v_p(x)}$$
$$y = u'' \prod p^{v_p(x)+v_p}$$

avec des entiers

$$n_p = v_p(y) - v_p(x)$$

tous positifs et presque tous nuls, d'où résulte que $y = xz$ avec

$$z = u'^{-1}u'' \prod p^{n_p}.$$

Inversement, supposons $y = xz$; alors, en utilisant les décompositions en facteurs premiers de x et z, il vient

$$y = u.\prod p^{v_p(x)+v_p(z)},$$

avec un $u \in K$ inversible, et comme la décomposition de y en produit d'éléments de P est unique on voit que $v_p(y) = v_p(x) + v_p(z)$, donc que $v_p(y) \geqslant v_p(x)$ pour tout $p \in P$, ce qui termine la démonstration du Lemme 4.

Étant donnés deux éléments non nuls x et y de K, il est facile, à l'aide du lemme 4, de construire leur pgcd et leur ppcm. Soit en effet d un pgcd de x et y; on doit exprimer que les diviseurs de x et y sont les diviseurs de d; or les diviseurs de x et y sont, d'après le lemme 4, les $z \in K$ vérifiant

$$v_p(z) \leqslant v_p(x) \qquad \text{et} \qquad v_p(z) \leqslant v_p(y),$$

autrement dit

$$v_p(z) \leqslant \mathrm{Min}[v_p(x),\ v_p(y)] \tag{10}$$

pour tout $p \in P$; et les diviseurs de d sont les $z \in K$ qui vérifient

$$v_p(z) \leqslant v_p(d) \tag{11}$$

pour tout $p \in P$. Pour que d soit un pgcd, il est donc nécessaire et suffisant que les conditions (10) et (11) soient équivalentes, autrement dit que

$$v_p(d) = \mathrm{Min}\,[v_p(x), v_p(y)] \quad \text{pour tout } p \in P, \tag{12}$$

et on retrouve ainsi la règle classique : l'exposant de p dans la décomposition de d est égal à celui des exposants de p dans x et y qui est le plus petit.

Un raisonnement analogue montrerait qu'un ppcm m de x et y est donné par

$$v_p(m) = \mathrm{Max}[v_p(x), v_p(y)] \quad \text{pour tout } y \in P. \tag{13}$$

Autrement dit, les règles connues dans le cas de l'anneau **Z** s'étendent à tous les anneaux principaux — et s'établissent à l'aide des mêmes raisonnements que dans le cas classique.

Remarque 3. Il va de soi qu'un produit de la forme

$$\prod_{p \in P} p^{n_p}$$

n'a de sens dans K que si les exposants n_p sont des entiers *tous* positifs et *presque*

tous nuls. Si l'on voulait utiliser les relations (12) et (13) pour définir le pgcd et le ppcm de x et y, il faudrait vérifier que les seconds membres de ces relations vérifient les conditions en question. On l'établit comme suit. Soit X (resp. Y) l'ensemble des $p \in P$ tels que $v_p(x) \neq 0$ (resp. $v_p(y) \neq 0$) — autrement dit, l'ensemble des $p \in P$ qui divisent x (resp. y); X et Y sont des ensembles finis, donc aussi $Z = X \cup Y$; pour $p \notin Z$, on a $v_p(x) = v_p(y) = 0$, donc

$$\mathrm{Max}\,[v_p(x), v_p(y)] = \mathrm{Min}\,[v_p(x), v_p(y)] = 0,$$

ce qui est le résultat cherché.

8. *Décomposition en éléments simples des fractions sur un anneau principal*

Soient K un anneau principal et F le corps des fractions de K, défini au § 29. Soit

$$x = a/b, \qquad a,\ b \in K, \qquad b \neq 0$$

un élément de F; conservant les notations du n° précédent, on peut écrire

$$a = u \prod_{p \in P} p^{v_p(a)}, \qquad b = v \prod_{p \in P} p^{v_p(b)},$$

d'où

$$x = w.\prod_{p \in P} p^{v_p(x)} \tag{14}$$

avec un élément inversible w de K, et des entiers

$$v_p(x) = v_p(a) - v_p(b)$$

qui sont encore presque tous nuls, mais peuvent être de signe quelconque. On vérifie facilement — le lecteur l'établira à titre d'exercice — que la décomposition (14) de x est unique.

Nous allons maintenant établir, pour les éléments de F, une décomposition d'une toute autre nature; le résultat qui suit est utile en Analyse (calcul des primitives des fractions rationnelles à coefficients réels ou complexes), et à peu près complètement dépourvu d'intérêt par ailleurs.

THÉORÈME 8. *Soit*

$$x = \frac{a}{p_1^{r_1} \cdots p_n^{r_n}}$$

un élément de F; *on suppose* $a \in K$, *les* r_i *positifs, et les* $p_i \in K$ *extrémaux et deux à deux non associés. Alors il existe des éléments* $a_1, \ldots, a_n$ *de* K *tels que*

$$x = \frac{a_1}{p_1^{r_1}} + \cdots + \frac{a_n}{p_n^{r_n}}.$$

Autrement dit, tout élément de F est somme de fractions de la forme a/p^n avec $a \in K$, p extrémal et $n \geqslant 0$.

Exemple 2. Prenons $K = \mathbf{Z}$ et

$$x = 5/18 = 5/2.3^2;$$

on a alors

$$x = 1/2 - 2/9,$$

ce qui est le Théorème 8 dans ce cas.

Le Théorème sera visiblement une conséquence des deux lemmes que voici :

LEMME 5. *Supposons*

$$x = a/b_1 \dots b_n$$

où les éléments b_i de K sont deux à deux premiers entre eux. Alors il existe des $a_i \in K$ tels que

$$x = a_1/b_1 + \dots + a_n/b_n.$$

LEMME 6. *Soient $p_1, \dots, p_n$ des éléments extrémaux deux à deux non associés de K. Alors, quels que soient les entiers positifs $r_1, \dots, r_n$, les éléments*

$$b_1 = p_1^{r_1}, \dots, b_n = p_n^{r_n}$$

sont deux à deux premiers entre eux.

Démontrons d'abord le lemme 6; soit d un diviseur commun à b_i et b_j $(i \neq j)$; si d n'est pas inversible, il admet un diviseur premier p, qui divise donc b_i et b_j; mais si p divise

$$p_i^{r_i} = p_i p_i \dots p_i,$$

il divise p_i et est donc associé à p_i; si donc b_i et b_j n'étaient pas premiers entre eux, il existerait un élément extrémal p de K associé à la fois à p_i et p_j, contrairement à l'hypothèse que p_j et p_i sont non associés pour $i \neq j$; d'où le lemme 6.

Démontrons maintenant le lemme 5, tout d'abord pour $n = 2$. Comme b_1 et b_2 sont premiers entre eux, il existe $u_1, u_2 \in K$ tels que

$$u_1 b_1 + u_2 b_2 = 1;$$

on a alors

$$\frac{a}{b_1 b_2} = \frac{a(u_1 b_1 + u_2 b_2)}{b_1 b_2} = \frac{a u_2}{b_1} + \frac{a u_1}{b_2}$$

ce qui établit le lemme 5 dans ce cas. Pour l'établir dans le cas général, on va raisonner par récurrence sur n; puisque (Corollaire du Théorème 6) b_n est premier à $b_1 \dots b_{n-1}$ et puisque le lemme est déjà établi pour un produit de deux facteurs, on peut écrire

$$x = \frac{a'}{b_1 \dots b_{n-1}} + \frac{a_n}{b_n};$$

il suffit alors d'appliquer l'hypothèse de récurrence à la première fraction du second membre pour obtenir la décomposition cherchée de x.

§ 32. Division des polynômes

1. Division des polynômes à une variable

Soit

$$f(X) = a_0 + a_1 X + \dots + a_n X^n + \dots$$

un polynôme à une indéterminée, à coefficients dans un anneau commutatif K; on appelle **coefficient dominant** de f le coefficient du terme de plus haut degré de f (ce qui suppose $f \neq 0$); si f est de degré n, le coefficient dominant de f est donc le coefficient de X^n. On dit que f est **unitaire** si son coefficient dominant est un élément *inversible* de K; si K est un corps, tout polynôme $f \neq 0$ est donc unitaire.

Le résultat suivant est analogue à celui qui est à la base de la théorie de la division (avec reste) des entiers rationnels :

THÉORÈME 1. *Soient* K *un anneau commutatif et g un polynôme unitaire à une indéterminée à coefficients dans* K. *Pour tout polynôme $f \in K[X]$, il existe des polynômes $q, r \in K[X]$ vérifiant les relations*

$$(1) \qquad f = gq + r, \qquad d^o(r) < d^o(g) \quad ;$$

et les polynômes q et r sont uniques.

Soit

$$g(X) = b_0 + b_1 X + \dots + b_n X^n$$

avec b_n inversible; en multipliant les deux membres de (1) par la constante $b_n^{-1} \in K$, on se ramène évidemment au cas où g est de la forme

$$(2) \qquad g(X) = X^n + b_{n-1} X^{n-1} + \dots + b_0,$$

ce que nous supposerons dans ce qui suit.

Considérons alors (pour f donné et q variable) tous les polynômes de la forme $f - gq$; leurs degrés sont des entiers positifs ou le symbole $-\infty$ (ce qui se produit si f est multiple de g — dans ce cas le Théorème 1 est bien entendu trivial!); par conséquent, il est possible de choisir q de telle sorte que le degré de $f - gq$ soit mini-

mum; on a alors

$$d^\circ(f - gq) \leqslant d^\circ(f - gq') \tag{3}$$

pour *tout* polynôme $q' \in K[X]$. Posant

$$f = gq + r, \tag{4}$$

tout revient à faire voir que

$$d^\circ(r) < d^\circ(g). \tag{5}$$

Or supposons qu'il n'en soit pas ainsi, et posons

$$r(X) = c_{n+k}X^{n+k} + c_{n+k-1}X^{n+k-1} + \cdots$$

avec $c_{n+k} \neq 0$ et $k \geqslant 1$ puisqu'on suppose la relation (5) fausse; il est clair que r et le polynôme

$$c_{n+k}X^k g(X)$$

ont le même coefficient dominant c_{n+k}; par suite on peut écrire

$$r(X) = c_{n+k}X^k g(X) + r'(X) \quad \text{avec } d^\circ(r') < d^\circ(r); \tag{6}$$

(4) s'écrit alors

$$f(X) = [q(X) + c_{n+k}X^k]g(X) + r'(X),$$

et en posant

$$q'(X) = q(X) + c_{n+k}X^k$$

il vient donc

$$f = gq' + r' \qquad \text{avec} \qquad d^\circ(r') < d^\circ(r);$$

cette dernière inégalité s'écrit encore $d^\circ(f - gq') < d^\circ(f - gq)$, et contredit (3), ce qui établit (5).

Nous avons donc démontré qu'il existe *au moins* un couple de polynômes q, r vérifiant (1); il reste à montrer qu'il en existe *au plus* un. Or considérons deux relations de la forme

$$f = gq_1 + r_1 = gq_2 + r_2$$

avec

$$d^\circ(r_1) < d^\circ(g), \qquad d^\circ(r_2) < d^\circ(g); \tag{7}$$

on en tire

$$g(q_1 - q_2) = r_2 - r_1; \tag{8}$$

tout revient évidemment à montrer que $q_1 = q_2$; or, d'après (7), on a $d^\circ(r_2 - r_1) < d^\circ(g)$; la relation $q_2 - q_1 = 0$ sera donc une conséquence du résultat suivant :

LEMME 1. *Soient g un polynôme unitaire et q un polynôme non nul; on a*

$$d^\circ(gq) = d^\circ(g) + d^\circ(q) \geqslant d^\circ(g).$$

Posant

$$g(X) = b_nX^n + \cdots + b_0, \qquad q(X) = c_mX^m + \cdots + c_0$$

avec b_n inversible et c_m non nul, on voit que le coefficient de X^{m+n} dans gq est égal à b_nc_m; comme b_n est *inversible*, ce produit ne peut être nul que si $c_m = 0$, ce qui n'est pas le cas; d'où le lemme.

Le Théorème 1 est donc démontré.

Dans les hypothèses du Théorème 1 (si K est un *corps*, le Théorème 1 s'applique pour peu que $g \neq 0$), on dit que q est le **quotient** et r le **reste** de la **division de f par g**. La démonstration du Théorème 1 conduit à une méthode pratique pour les calculer. En effet, posons

$$f(X) = a_mX^m + \cdots + a_0, \qquad g(X) = b_nX^n + \cdots + b_0$$

avec a_m non nul et b_n inversible; si $m < n$, la division s'effectue trivialement : on prend $q = 0$, $r = f$; si au contraire $m \geqslant n$, on a visiblement

$$f(X) = a_mb_n^{-1}X^{m-n}g(X) + f_1(X) = c_kX^k g(X) + f_1(X) \tag{9}$$

avec

$$d^\circ(f_1) \leqslant d^\circ(f) - 1;$$

si f_1 est de degré inférieur à g, on a terminé et de façon précise on a

$$q(X) = a_mb_n^{-1}X^{m-n}, \qquad r(X) = f_1(X)$$

dans ce cas; si au contraire $d^\circ(f_1) \geqslant d^\circ(g)$, on effectue sur f_1 la même opération que sur f, en écrivant

$$f_1(X) = c_hX^h g(X) + f_2(X) \tag{10}$$

avec

$$d^\circ(f_2) < d^\circ(f_1);$$

en combinant (9) et (10); il vient

$$f(X) = (c_kX^k + c_hX^h)g(X) + f_2(X), \qquad d^\circ(f_2) \leqslant d^\circ(f) - 2;$$

si le degré de f_2 est inférieur à celui de g, le problème est résolu; sinon, on écrit

$$f_2(X) = c_lX^l g(X) + f_3(X)$$

avec

$$d^\circ(f_3) < d^\circ(f_2),$$

d'où

$$f(X) = (c_kX^k + c_hX^h + c_lX^l)g(X) + f_3(X), \quad d^\circ(f_3) \leqslant d^\circ(f) - 3;$$

il est clair qu'en procédant ainsi on parvient à former le quotient et le reste de la division de f par g.

Exemple 1. Prenons $f(X) = X^6 - X^4 - X^2 + 1$, $g(X) = X^3 - 1$; on dispose alors les opérations comme suit :

$$\begin{array}{l|l} X^6 - X^4 \quad - X^2 \quad + 1 & X^3 - 1 \\ \cline{2-2} - X^4 + X^3 - X^2 \quad + 1 & X^3 - X + 1 \\ \quad X^3 - X^2 - X + 1 & \\ \quad - X^2 - X + 2 & \end{array}$$

ici le quotient est $X^3 - X + 1$, et le reste $-X^2 - X + 2$. La méthode adoptée pour les calculs est la même que pour les divisions de nombres entiers.

2. *Idéaux d'un anneau de polynômes à une indéterminée*

L'une des conséquences les plus importantes du Théorème 1 est le résultat que voici :

Théorème 2. *Soit* K *un* corps *commutatif; l'anneau* K[X] *des polynômes à une indéterminée à coefficients dans* K *est principal.*

L'anneau K[X] est commutatif et intègre (§ 27, Théorème 1). Soit I un idéal de K[X]; pour montrer qu'il est principal, on peut supposer qu'il ne se réduit pas à 0. Parmi les éléments *non nuls* de I, choisissons un polynôme f *de degré minimum* : il est clair qu'alors les relations

$$(11) \qquad r \in I \quad \text{et} \quad d^0(r) < d^0(f) \quad \text{impliquent } r = 0.$$

Cela dit, soit g un élément de I; comme K est un corps et f non nul, le Théorème 1 montre que

$$g = fq + r \quad \text{avec } d^0(r) < d^0(f);$$

comme I contient f et g, il contient aussi $g - fq$, donc r; par suite on peut faire usage de (11), et on voit que $r = 0$. Ainsi tout élément de I est multiple de f, et tout multiple de f est évidemment dans I; l'idéal I est donc engendré par f, ce qui achève la démonstration.

Le lecteur devra rapprocher la démonstration précédente du § 7, *Exemple* 8, les méthodes utilisées dans ces deux cas étant analogues.

Soit $I = (f)$ un idéal de l'anneau K[X]; le polynôme f est unique à ceci près qu'on peut le multiplier par un élément inversible de K[X]; notons à ce sujet le résultat suivant :

Lemme 2. *Soit* K *un anneau d'intégrité commutatif; les éléments inversibles de* K[X] *sont ceux de* K.

Évidemment, tout élément inversible de K est inversible dans K[X]. Soit réciproquement

$$f(X) = a_n X^n + \cdots + a_0, \quad a_n \neq 0$$

un élément inversible de K, et

$$g(X) = b_m X^m + \cdots + b_0, \quad b_m \neq 0,$$

son inverse; on a donc, en effectuant le produit de f par g,

$$1 = a_n b_m X^{m+n} + \cdots,$$

les termes non écrits étant de degrés inférieurs à $m + n$; comme K est un anneau d'intégrité on a $a_n b_m \neq 0$; donc $m + n = 0$, et f se réduit à l'élément a_n de K, qui est inversible dans K vu la relation $a_n b_m = 1$; ceci achève la démonstration.

On aurait pu aussi (§ 27, Théorème 1) écrire directement que

$$d^0(f) + d^0(g) = d^0(fg) = 0,$$

ce qui exige que f et g se réduisent à des éléments de K.

Le lemme 2 montre que, si f est un générateur d'un idéal I de K[X] (on suppose à nouveau que K soit un corps), les autres générateurs de I s'obtiennent en multipliant f par une constante (i.e. un élément de K) non nulle. En particulier, en multipliant f par l'inverse de son coefficient dominant, *on peut s'arranger pour que le coefficient dominant de* f *soit égal à* 1, *et alors* f *est le seul générateur de* I *possédant cette propriété.* On voit qu'ici comme dans le cas de l'anneau **Z**, il existe un moyen « canonique » de choisir un générateur pour chaque idéal non nul de l'anneau considéré.

Le Théorème 2 est très important et très utile pour résoudre des problèmes relativement élémentaires; mais dès qu'on aborde la « Géométrie Algébrique » (voir la *Remarque* 3 plus loin) on a besoin de résultats beaucoup plus généraux que le Théorème 2; dans cet ordre d'idées, l'énoncé fondamental est le suivant : *soit* K *un anneau commutatif noethérien* (i.e. dont tous les idéaux sont de type fini); *alors l'anneau* K[X] *est encore noethérien.* On trouvera dans l'*Exercice* 27 de ce § une démonstration simple de ce résultat. En raisonnant par récurrence sur n, on en déduit plus généralement que *l'anneau* $K[X_1, \ldots, X_n]$ *est noethérien si* K *est noethérien*; en particulier, *si* K *est un corps, l'anneau* $K[X_1, \ldots, X_n]$ *est noethérien quel que soit* n. Ces résultats, dus à Hilbert, expliquent pourquoi les calculs concernant des polynômes à coefficients dans un corps peuvent toujours s'effectuer « en un nombre fini de pas »; mais leur importance réelle dépasse de loin cette remarque d'ordre plus ou moins métaphysique.

3. *Pgcd et ppcm de plusieurs polynômes; polynômes irréductibles*

Le Théorème 2 permet d'appliquer les résultats du § précédent à l'anneau K[X] lorsque K est un *corps*.

Soient en particulier $f_1, \ldots, f_n$ des polynômes non nuls à une indéterminée à coefficients dans K; alors ces polynômes admettent un **plus grand commun diviseur** d; et on a le résultat suivant :

Théorème 3. *Soient* $d, f_1, \ldots, f_n$ *des polynômes non nuls à une indéterminée à coefficients dans un corps commutatif* K. *Les propriétés suivantes sont équivalentes :*

a) *d est un* p.g.c.d. *de* $f_1, \ldots, f_n$;

b) *les diviseurs communs à* $f_1, \ldots, f_n$ *sont les diviseurs de d;*

c) *pour qu'un polynôme puisse s'écrire sous la forme*

$$u_1(X)f_1(X) + \cdots + u_n(X)f_n(X)$$

avec des $u_i \in K[X]$, *il faut et il suffit qu'il soit multiple de d;*

d) $d(X)$ *peut se mettre sous la forme*

$$u_1(X)f_1(X) + \cdots + u_n(X)f_n(X)$$

et est de degré minimum dans l'ensemble des polynômes non nuls possédant cette propriété.

L'équivalence de *a*) et *b*) est claire; *c*) signifie que *d* engendre l'idéal engendré par $f_1, \ldots, f_n$, ce qui est précisément la définition du p.g.c.d. donnée au § précédent; enfin, *d*) s'obtient en observant — voir la démonstration du théorème 2 — que les générateurs d'un idéal sont les éléments de degré minimum parmi les éléments non nuls de cet idéal. D'où le Théorème 3.

Corollaire. *Soient* $f_1, \ldots, f_n$ *des polynômes non nuls à une indéterminée à coefficients dans un corps* K. *Les propriétés suivantes sont équivalentes :*

a) *les seuls diviseurs communs à* $f_1, \ldots, f_n$ *sont les éléments non nuls de* K;

b) *il existe des polynômes* $u_i \in K[X]$ *tels que*

$$u_1(X)f_1(X) + \cdots + u_n(X)f_n(X) = 1.$$

Ce Corollaire est d'ailleurs un cas particulier du Théorème 1 du § 31. Lorsqu'il est vérifié, on dit bien entendu que les polynômes f_i sont **premiers entre eux.**

Il va de soi qu'on peut aussi définir un **plus petit commun multiple** de $f_1, \ldots, f_n$; c'est un multiple commun m des f_i possédant la propriété que les autres multiples communs aux f_i sont les multiples de m; ou encore, c'est un multiple commun aux f_i non nul et *de degré minimum.*

Les Théorèmes 2, 3, 4 du § 31 s'appliquent mot pour mot à l'anneau K[X], et il est parfaitement inutile de les énoncer ici à nouveau.

Les éléments extrémaux de l'anneau K[X] s'appellent généralement les **polynômes irréductibles** à une indéterminée à coefficients dans le corps K. *Tout polynôme* $f \in K[X]$ *peut se mettre, et essentiellement d'une seule façon, sous forme d'un produit de polynômes irréductibles* : cela résulte des Théorèmes 5 et 7 du § précédent.

Remarque 1. En multipliant un polynôme irréductible par l'inverse de son coefficient dominant (ce qui le remplace par un polynôme associé, au sens du § 31, n° 6), on voit que pour effectuer la décomposition d'un polynôme f en facteurs irréductibles on peut se borner à choisir des polynômes irréductibles dont le coefficient dominant est égal à 1; en vertu du Lemme 1, deux tels polynômes ne peuvent être associés que s'ils sont égaux; autrement dit, si l'on veut appliquer à K[X] la décomposition (9) du § 31, n° 6, il s'impose de prendre pour P l'ensemble des polynômes irréductibles dont le coefficient dominant est égal à 1.

Remarque 2. Soient p_1 et p_2 des polynômes à une indéterminée à coefficients dans le corps K. Pour calculer leur p.g.c.d., on peut procéder par divisions successives : supposant $d^0(p_1) > d^0(p_2)$, on écrit

$$p_1 = p_2v_2 + p_3 \quad \text{avec} \quad d^0(p_3) < d^0(p_2)$$
$$p_2 = p_3v_3 + p_4 \quad \text{avec} \quad d^0(p_4) < d^0(p_3)$$

et ainsi de suite; comme les degrés des p_i vont en diminuant, on aboutit finalement à une relation de la forme

$$p_{n-1} = p_nv_n.$$

Il est clair que le pgcd de p_1 et p_2 est aussi celui de p_2 et p_3, donc aussi celui de p_3 et p_4, etc..., donc aussi celui de p_{n-1} et p_n — autrement dit c'est p_n, i.e. le dernier reste *non nul* dans les divisions successives.

Cette méthode permet aussi d'expliciter le théorème de Bezout, i.e. de construire deux polynômes u_1 et u_2 tels que $u_1p_1 + u_2p_2 = p_n$; on a en effet

$$\begin{aligned} p_n &= p_{n-2} - p_{n-1}v_{n-1} = (p_{n-4} - p_{n-3}v_{n-3}) - (p_{n-3} - p_{n-2}v_{n-2})v_{n-1} \\ &= p_{n-4} - p_{n-3}(v_{n-3} + v_{n-1}) + p_{n-2}v_{n-2}v_{n-1} \\ &= p_{n-6} - p_{n-5}v_{n-5} - (p_{n-5} - p_{n-4}v_{n-4})\ (v_{n-3} + v_{n-1}) \\ &\qquad + (p_{n-4} - p_{n-3}v_{n-3})v_{n-2}v_{n-1} \end{aligned}$$

et en « remontant » ainsi les calculs on parvient évidemment à une relation de la forme cherchée. Voir *Exercice* 3.

4. *Application aux fractions rationnelles*

Soient K un corps commutatif et

$$f(X) = \frac{p(X)}{q(X)}$$

une fraction rationnelle à une indéterminée à coefficients dans K. Écrivons

$$q(X) = q_1(X)^{r_1} \ldots q_n(X)^{r_n}$$

où les q_i sont des polynômes irréductibles deux à deux non proportionnels. Le Théorème 8 du § 31 montre alors qu'il existe des polynômes $p_i(X)$ $(1 \leqslant i \leqslant n)$ tels que l'on ait

$$(11) \qquad f(X) = \frac{p_1(X)}{q_1(X)^{r_1}} + \cdots + \frac{p_n(X)}{q_n(X)^{r_n}}.$$

Or on a le lemme suivant (*) :

Lemme 3. *Soient p et q des polynômes à une indéterminée à coefficients dans un anneau commutatif* K. *Supposons q unitaire; il existe alors des polynômes* h_i $(i \geqslant 0)$ *presque tous nuls tels que l'on ait*

$$p = h_0 + h_1q + h_2q^2 + \cdots, \qquad d^0(h_i) < d^0(q) \text{ pour tout } i.$$

(*) On notera l'analogie existant entre ce Lemme et les raisonnements classiques conduisant, pour tout entier $q \neq 0$, à la « numération de base q ».

On écrit pour cela, à l'aide du Théorème 1, que

$$p = h_0 + p_1 q \quad \text{avec } d^0(h_0) < d^0(q),$$

puis que

$$p_1 = h_1 + p_2 q \quad \text{avec } d^0(h_1) < d^0(q),$$

et ainsi de suite; les degrés des polynômes p_i décroissent strictement, de sorte que l'on a $p_i = 0$ pour i suffisamment grand, et en portant chacune des relations obtenues dans la précédente on obtient évidemment le Lemme.

Le Lemme 3 montre que, pour tout entier $r > 0$, on peut écrire

$$\frac{p}{q^r} = \frac{h_0}{q^r} + \frac{h_1}{q^{r-1}} + \cdots + \frac{h_r}{q} + p_0$$

où $h_0, \ldots, h_r$ et p_0 sont des polynômes, avec

$$d^0(h_i) < d^0(q) \quad \text{pour } 0 \leqslant i \leqslant r.$$

Appliquant ce résultat à chacune des fractions qui figurent dans le second membre de (11), et en groupant ensemble les termes p_0 obtenus pour chacune de ces fractions, on obtient donc une relation de la forme

$$f(X) = g(X) + \sum_{i=1}^{i=n} \sum_{0 \leqslant r \leqslant r_i} \frac{h_{ir}(X)}{q_i(X)^r} \tag{12}$$

où g et les h_{ir} sont des polynômes, avec

$$d^0(h_{ir}) < d^0(q_i) \tag{13}$$

quels que soient i et r.

La formule (12) s'appelle la **décomposition en éléments simples sur le corps** K de la fraction rationnelle donnée f. On verra plus loin que, si $K = \mathbf{C}$, les h_{ir} sont nécessairement des constantes, et que si $K = \mathbf{R}$ ce sont des polynômes de degré 1 au plus.

Exemple 2. Prenons

$$f(X) = \frac{1}{X^2(X-1)^3};$$

les polynômes X et X — 1, étant de degré 1, sont irréductibles. On a

$$(X-1)^3 = X^3 - 3X^2 + 3X - 1 = X^2(X-3) + 3X - 1$$

puis

$$X^2 = (3X-1)\frac{X}{3} + \frac{X}{3},$$

puis

$$3X - 1 = \frac{X}{3} \cdot 9 - 1;$$

il vient donc

$$1 = \frac{X}{3} \cdot 9 - (3X-1) = 9X^2 - (3X+1)(3X-1)$$
$$= 9X^2 - (3X+1)((X-1)^3 - X^2(X-3))$$

de sorte que le théorème de Bezout pour X^2 et $(X-1)^3$ s'écrit

$$1 = (3X^2 - 8X + 6)X^2 - (3X+1)(X-1)^3.$$

On a donc

$$f(X) = \frac{(3X^2 - 8X + 6)X^2 - (3X+1)(X-1)^3}{X^2(X-1)^3}$$
$$= \frac{3X^2 - 8X + 6}{(X-1)^3} - \frac{3X+1}{X^2};$$

or

$$3X^2 - 8X + 6 = (X-1)(3X-5) + 1 = (X-1)[3(X-1) - 2] + 1$$
$$= 3(X-1)^2 - 2(X-1) + 1;$$

il vient donc

$$f(X) = \frac{3}{X-1} - \frac{2}{(X-1)^2} + \frac{1}{(X-1)^3} - \frac{1}{X^2} - \frac{3}{X}.$$

ce qui est la décomposition cherchée de f en éléments simples.

§ 33. Racines d'une équation algébrique

1. *Nombre maximum de racines*

Nous avons déjà démontré (§ 28, Lemme 2) qu'un polynôme de degré n à une indéterminée, à coefficients dans un anneau d'intégrité commutatif K, possède au plus n racines dans K. On peut, comme le montrera le Corollaire du Théorème ci-dessous, améliorer ce résultat.

THÉORÈME 1. *Soit f un polynôme de degré n à une indéterminée à coefficients dans un corps commutatif* K. *Soient $a_1, \ldots, a_p$ les racines de f dans* K, *et $r_1, \ldots, r_p$ leurs ordres de multiplicité. On a alors*

$$f(X) = (X - a_1)^{r_1} \ldots (X - a_p)^{r_p} g(X) \tag{1}$$

où g est un polynôme qui n'a aucune racine dans K.

Par définition de l'ordre de multiplicité d'une racine, f est divisible par chacun des polynômes

$$(X - a_1)^{r_1}, \ldots, (X - a_p)^{r_p}. \tag{2}$$

D'autre part, *tout polynôme de la forme $X - a$ est irréductible* car si

$$X - a = p(X)q(X)$$

on a $1 = d^0(p) + d^0(q)$, de sorte que l'un des polynômes p, q est de degré 0, i.e. est un élément inversible de l'anneau K[X]. Enfin, il est clair que les polynômes $X - a$ et $X - b$ sont non associés (i.e. non proportionnels) pour $a \neq b$.

Il résulte de là que les polynômes (2) sont deux à deux premiers entre eux (§ 31, Lemme 6), et par suite (§ 31, Théorème 4) que leur produit divise f; d'où l'existence d'une relation (1).

La relation (1) montre de plus que toute racine a de g dans K, étant racine de f dans K, est l'un des éléments $a_1, \ldots, a_p$; mais si a_1 par exemple était racine de g, le polynôme $g(X)$ serait divisible par $X - a_1$, et $f(X)$ serait par suite divisible par $(X - a_1)^{r_1+1}$, contrairement à la définition d'un ordre de multiplicité. Donc g n'a aucune racine dans K, ce qui achève la démonstration.

COROLLAIRE. *Avec les notations du Théorème* 1, *on a*

$$r_1 + \cdots + r_p \leqslant n = d^0(f).$$

C'est évident car

$$d^0(f) = r_1 + \cdots + r_p + d^0(g). \tag{3}$$

Le Corollaire exprime que *le nombre des racines de f dans* K *est au plus n même si l'on convient de compter une racine multiple d'ordre r comme l'équivalent de r racines simples.*

Supposons par exemple f de degré 3; alors les seules possibilités en ce qui concerne le nombre de racines de f dans K sont les suivantes : *a*) f n'a que des racines simples, il y en a alors au plus trois; *b*) f possède des racines doubles; alors f admet soit une seule racine dans K, laquelle est racine double, soit une racine double et une racine simple; *c*) f admet une racine triple; celle-ci est alors unique, et f n'admet aucune autre racine. En fait, ces possibilités ne se présentent pas toutes, en vertu du fait que si f admet deux racines simples distinctes, ou bien une racine double, alors f admet nécessairement une autre racine dans K; en effet, si l'on a

$$f(X) = (X - a)\,(X - b)g(X),$$

le polynôme g est nécessairement de degré 1, donc proportionnel à $X - c$ pour un $c \in$ K convenable, et c est racine de f.

Autrement dit, pour un polynôme du troisième degré, les éventualités suivantes peuvent se produire :

aucune racine
une racine simple
trois racines simples
une racine simple et une racine double
une racine triple.

Il est facile de donner des exemples de chacun de ces cas; pour le premier on prend (*)

$$K = \mathbf{Q} \qquad \text{et} \qquad f(X) = X^3 - 2;$$

pour les autres, il suffit de prendre $K = \mathbf{R}$ et les polynômes

$$(X - 1)\,(X^2 + 1), \quad (X - 1)\,(X - 2)\,(X - 3), \quad (X - 1)\,(X - 2)^2, \quad (X - 1)^3.$$

(*) Il n'est pas possible, pour donner un exemple du premier cas, de prendre $K = \mathbf{R}$, car on démontre en Analyse que tout polynôme de degré *impair* à coefficients réels possède au moins une racine réelle (rappelons la démonstration brièvement : on montre d'abord que, pour les valeurs très grandes de la variable, un polynôme est un « infiniment grand » équivalent à son terme de plus haut degré, donc du même signe que celui-ci; on en déduit qu'un polynôme de degré impair ne peut pas, sur $\mathbf{R}$, garder un signe constant; le théorème des valeurs intermédiaires pour les fonctions continues montre alors qu'un tel polynôme s'annule nécessairement quelque part).

Les résultats de ce genre, bien qu'ils concernent des polynômes, appartiennent en réalité à l'Analyse. C'est pourquoi nous ne les exposons pas dans ce volume.

Revenons au cas général, le corps K et le polynôme f étant quelconques. Il peut arriver que, dans la décomposition du Théorème 1, le polynôme g soit constant, i.e. de degré 0, autrement dit qu'on ait

$$f(X) = c(X - a_1)^{r_1} \dots (X - a_p)^{r_p}$$

où c est nécessairement le coefficient dominant de f; ou, ce qui revient au même, que f puisse s'écrire comme produit de polynômes du premier degré à coefficients dans K. Lorsqu'il en est ainsi on dit que f **a toutes ses racines dans** K; la raison de cette terminologie est que, si L est un surcorps de K, alors les racines de f dans L, i.e. les $x \in$ L tels que

$$c(x - a_1)^{r_1} \dots (x - a_p)^{r_p} = 0,$$

sont $a_1, \dots, a_p$, autrement dit les racines de f dans K. On verra plus loin par contre que si f n'a pas toutes ses racines dans K, il existe un surcorps L de K (par exemple un corps algébriquement clos contenant K — voir le n° 2) et des racines de f dans L qui ne sont pas des éléments de K.

Pour que f ait toutes ses racines dans K, il est évidemment nécessaire et suffisant que les ordres de multiplicité $r_1, \dots, r_p$ des racines de f dans K vérifient la relation

$$r_1 + \dots + r_p = d^0(f),$$

autrement dit que le nombre de racines de f dans K (chaque racine multiple d'ordre r étant considérée comme l'équivalent de r racines simples) soit *égal* au degré de f.

Notons enfin que *si f a toutes ses racines dans* K *il en est de même de tout diviseur g de f;* en effet, g est produit de polynômes irréductibles, lesquels, divisant g, divisent aussi f; mais comme f est produit de polynômes du premier degré, qui sont évidemment irréductibles, les seuls facteurs irréductibles de f sont ces facteurs du premier degré, et par suite les diviseurs irréductibles de g sont eux aussi de degré 1; par conséquent, g est produit de facteurs du premier degré, ce qui établit notre assertion. (On pourrait aussi appliquer à f et g le Lemme 4 du n° 7 du § 31, lequel montre comment trouver tous les diviseurs de f à partir de la décomposition de f en facteurs irréductibles.)

2. *Corps algébriquement clos*

Soient K un *corps commutatif* et f un polynôme à une indéterminée, à coefficients dans K, et de degré $n \geqslant 1$. D'après le n° précédent, f possède *au plus* n racines dans K; mais nous n'avons encore énoncé aucun théorème affirmant l'*existence* de racines de f dans K (et pour cause, le polynôme $X^2 + 1$ n'ayant pas de racines dans le corps **R**).

On dit qu'un corps commutatif K est **algébriquement clos** si *tout* polynôme à une indéterminée, à coefficients dans K, et non constant, possède au moins une racine dans K. En ce qui concerne l'existence de tels corps, les deux résultats fondamentaux sont les suivants :

THÉORÈME 2 (d'Alembert-Gauss). *Le corps des nombres complexes est algébriquement clos.*

THÉORÈME 3 (Steinitz). *Tout corps commutatif peut être plongé dans un corps algébriquement clos.*

Le Théorème 2 signifie que **toute équation algébrique**

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

à coefficients complexes, de degré $n \geqslant 1$, possède au moins une racine complexe — résultat d'autant plus extraordinaire que les nombres complexes ont été inventés pour attribuer des racines aux équations du *second degré* seulement. Quant au théorème de Steinitz, il signifie que, pour tout corps commutatif K, on peut construire un corps algébriquement clos L qui contient un sous-corps isomorphe à K; si K = **R** on peut par exemple prendre L = **C** (dans le cas général, la construction de L à partir de K est beaucoup plus compliquée que celle de **C** à partir de **R**, mais peut néanmoins s'effectuer à l'aide de méthodes analogues).

On ne peut démontrer le Théorème 2 sans recourir, d'une façon ou d'une autre, à des considérations qui relèvent de l'Analyse, et non de l'Algèbre. Voir une démonstration simple dans l'*Exercice* 25 de ce §. Quant au Théorème 3, sa démonstration dépasserait de beaucoup le cadre du présent ouvrage; cf. *Exercice* 20.

On peut se demander si l'existence de racines pour toutes les équations algébriques à *une* inconnue entraîne une propriété analogue pour les systèmes d'équations algébriques à *plusieurs* inconnues; la réponse à cette question est l'un des plus célèbres théorèmes que l'on doive à Hilbert :

THÉORÈME 4 (Nullstellensatz de Hilbert). *Soient* K *un corps commutatif algébriquement clos et* I *un idéal de l'anneau* $K[X_1, \dots, X_n]$. *Les propriétés suivantes sont équivalentes :*

a) il existe au moins un point $x \in K^n$ tel que l'on ait

$$f(x) = 0 \quad \textit{pour tout} \quad f \in I; \tag{4}$$

b) on a $I \neq K[X_1, \dots, X_n]$.

Il est trivial de démontrer que *a)* implique *b)*, attendu que le polynôme 1 ne saurait s'annuler en un point de K^n; mais la démonstration du fait que *b)* implique *a)* est trop compliquée pour être exposée ici; voir l'*Exercice* 33 de ce §.

Pour comprendre l'énoncé du Théorème 4, donnons-nous des polynômes

$$f_1, \dots, f_p \in K[X_1, \dots, X_n]$$

et cherchons à résoudre, dans K^n, le **système d'équations algébriques**

$$f_1(x) = \dots = f_p(x) = 0; \tag{5}$$

soit I l'idéal de $K[X_1, \dots, X_n]$ engendré par $f_1, \dots, f_p$, i.e. l'ensemble des polynômes de la forme

$$f = u_1 f_1 + \dots + u_p f_p;$$

il est *évident* que les solutions de (5) sont les mêmes que les solutions de (4); donc, dire que (5) possède au moins une solution signifie que I n'est pas l'anneau des

polynômes tout entier, ou, ce qui revient au même, que

$$1 \notin I.$$

En d'autres termes :

COROLLAIRE DU THÉORÈME 4. *Étant donnés un corps commutatif algébriquement clos* K *et des polynômes*

$$f_1, \ldots, f_p \in K[X_1, \ldots, X_n],$$

les propriétés suivantes sont équivalentes :

a) le système d'équations algébriques

$$f_1(x) = \cdots = f_p(x) = 0$$

n'a aucune solution $x \in K^n$;

b) il existe des polynômes

$$u_1, \ldots, u_p \in K[X_1, \ldots, X_n]$$

tels que l'on ait

$$u_1 f_1 + \cdots + u_p f_p = 1.$$

Remarque 1. Soit K un corps algébriquement clos; une partie de K^n est appelée une **variété algébrique affine** si c'est l'ensemble des solutions d'un système d'équations algébriques $f_1(x) = \ldots = f_p(x) = 0$. L'étude de ces variétés algébriques affines (et d'objets analogues) est le but de la Géométrie Algébrique. Une variété algébrique définie par une seule équation $f(x) = 0$, où f est un polynôme non nul, s'appelle une **hypersurface** (ou une **surface** lorsque $n = 3$, ou une **courbe plane** lorsque $n = 2$). Le Corollaire du Théorème 4 est donc une condition nécessaire et suffisante pour qu'une intersection d'hypersurfaces algébriques soit vide.

3. Nombre de racines d'une équation à coefficients dans un corps algébriquement clos

Sur un corps algébriquement clos, on peut améliorer grandement le Théorème 1 :

THÉORÈME 5. *Soit f un polynôme à une indéterminée, à coefficients dans un corps algébriquement clos* K, *et de degré* $n \geqslant 1$. *Soient* $a_1, \ldots, a_p$ *les diverses racines de f dans* K, *et* $r_1, \ldots, r_p$ *leurs ordres de multiplicité. On a alors*

$$f(X) = c(X - a_1)^{r_1}(X - a_2)^{r_2} \ldots (X - a_p)^{r_p} \tag{6}$$

où c est le coefficient dominant de f. En outre on a

$$r_1 + \cdots + r_p = n. \tag{7}$$

Il suffit d'appliquer le Théorème 1; comme le polynôme g ne s'annule jamais dans K, il est constant par définition d'un corps algébriquement clos, d'où la première assertion de l'énoncé. La seconde s'obtient en calculant le degré du second membre de la relation (6).

La relation (7) s'exprime généralement de la façon suivante : *dans un corps algébriquement clos, une équation algébrique de degré* $n \geqslant 1$ *possède exactement n racines* pourvu que l'on considère une racine multiple d'ordre r comme l'équivalent de r racines distinctes.

Exemple 1. Considérons l'équation

$$x^n = 1 \tag{8}$$

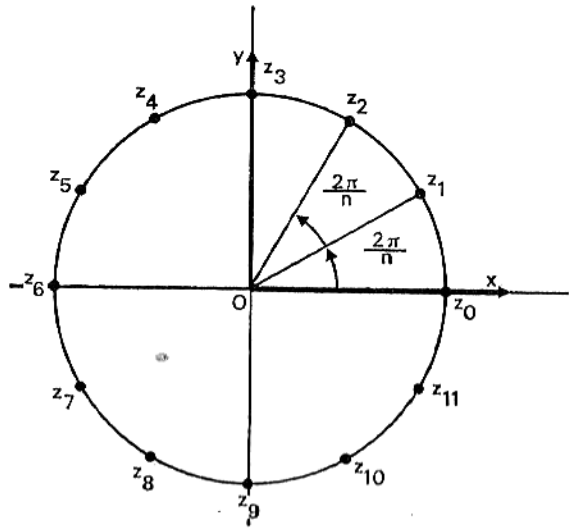
dans un corps commutatif K (ses racines sont les **racines n^e de l'unité** dans K); posant

$$f(X) = X^n - 1, \qquad \text{d'où} \qquad f'(X) = nX^{n-1},$$

on voit que, *si n n'est pas multiple de la caractéristique p de* K, la seule racine de f' est 0, qui n'est évidemment pas racine n^e de l'unité; donc (§ 30, Théorème 6) *les racines de f sont toutes simples* dans cette hypothèse, et si K est de plus algébriquement clos il s'ensuit qu'il existe dans K exactement n racines *distinctes* de l'équation considérée; c'est le cas dans C.

Lorsque K = C, les racines n^e de l'unité sont données par la formule

$$z_k = \cos(2k\pi/n) + i.\sin(2k\pi/n) \quad (0 \leqslant k \leqslant n-1),$$



autrement dit sont représentées, dans le plan complexe, par les sommets d'un polygone régulier de n côtés incrit dans le cercle unité (cf. la figure ci-contre). En effet, la formule de Moivre (§ 9, n° 6) montre que

$$z_k^n = \cos(2k\pi n/n) + i.\sin(2k\pi n/n) = 1,$$

de sorte que la formule ci-dessus représente n racines, deux à deux distinctes, de l'équation (8); celle-ci étant de degré n ne saurait en posséder d'autres.

Supposant toujours K = C, considérons plus généralement l'équation

$$z^n = a$$

où a est un nombre complexe non nul donné (**ses racines s'appellent les racines n^e de a**). Écrivant

$$z = \rho(\cos\theta + i.\sin\theta), \qquad a = r(\cos\varphi + i.\sin\varphi)$$

avec r et ρ réels positifs, θ et φ réels, tout revient à écrire que

$$\rho^n[\cos(n\theta) + i.\sin(n\theta)] = r(\cos\varphi + i.\sin\varphi);$$

le premier membre a pour valeur absolue ρ^n et pour argument $n\theta$ (à un multiple près de 2π : un argument est un nombre réel défini modulo 2π), le second pour valeur absolue r et pour argument φ; l'équation $x^n = a$ équivaut donc aux conditions

$$\rho^n = r, \qquad n\theta \equiv \varphi \pmod{2\pi};$$

il s'ensuit qu'elle a pour racines les nombres complexes

$$z_k = \sqrt[n]{r}\left[\cos\frac{\varphi + 2k\pi}{n} + i.\sin\frac{\varphi + 2k\pi}{n}\right]$$

comme on a évidemment $z_k = z_{k+n}$, il suffit du reste de donner n valeurs consécutives à l'entier k pour obtenir toutes les racines (en nombre n et deux à deux distinctes) de l'équation considérée.

Remarque 2. Le Théorème 5 peut évidemment être en défaut si le corps K n'est pas algébriquement clos; mais dans ce cas il redevient vrai si l'on considère les racines de f dans un corps *algébriquement clos* contenant K_1 corps dont l'existence résulte du Théorème de Steinitz. Par exemple, soit f un polynôme de degré n à coefficients réels; il est en général faux que f possède n racines réelles; mais il est toujours vrai que f possède n racines *réelles ou complexes* (le nombre de racines de f étant bien entendu calculé en tenant compte des ordres de multiplicité). Par exemple, le polynôme $X^2 + 1$ possède deux racines réelles ou complexes, à savoir i et $-i$. De même, l'équation

$$x^n = 1,$$

qui ne possède dans **R** qu'une racine (si n est impair) ou deux racines (si n est pair), en possède n dans **C**.

4. *Polynômes irréductibles à coefficients dans un corps algébriquement clos*

Soit $f(X)$ un polynôme à une indéterminée à coefficients dans un corps algébriquement clos K; alors *pour que f soit irréductible il faut et il suffit que f soit de degré* 1, i.e. de la forme

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

La condition est évidemment suffisante (même si K n'est pas algébriquement clos) puisqu'alors les seuls diviseurs de f sont de degré 0 (i.e. constants) ou 1 (i.e. proportionnels à f). Inversement, supposons f irréductible; f n'est pas inversible dans l'anneau K[X], donc est de degré $n \geqslant 1$ (§ 32, Lemme 2); comme K est algébriquement clos, f possède au moins une racine $a \in K$; mais alors f est multiple de $X - a$, donc proportionnel à $X - a$ puisqu'irréductible, et notre assertion est démontrée.

Lorsqu'on effectue, en utilisant la formule (9) du § 31, fin du n° 6, la décomposition d'un polynôme $f \in K[X]$ en facteurs irréductibles, on peut donc prendre pour P l'ensemble des polynômes de la forme

$$X - a, \qquad a \in K;$$

la formule (9) du § 31 se réduit alors évidemment à la formule (6) du Théorème 5.

Celle-ci constituant la décomposition de f en facteurs irréductibles dans l'anneau principal K[X], on peut l'utiliser par exemple pour former le pgcd de deux polynômes f et g; désignons les racines distinctes de f par

$$a_1, \ldots, a_m, b_1, \ldots, b_n$$

et celles de g par

$$a_1, \ldots, a_m, c_1, \ldots, c_p,$$

en mettant en évidence les racines $a_1, \ldots, a_m$ communes à f et g, s'il y en a; écrivant

$$f(X) = u(X - a_1)^{r'_1} \ldots (X - a_m)^{r'_m}(X - b_1)^{s_1} \ldots (X - b_n)^{s_n}$$
$$g(X) = v(X - a_1)^{r''_1} \ldots (X - a_m)^{r''_m}(X - c_1)^{t_1} \ldots (X - c_p)^{t_p},$$

où u et v sont des constantes, il est clair que d'après le § 31, n° 7, un pgcd de f et g sera donné par la formule

$$d(X) = (X - a_1)^{r_1} \ldots (X - a_m)^{r_m} \qquad \text{où} \qquad r_i = \operatorname{Min}(r'_i, r''_i).$$

Autrement dit, *les racines du* pgcd *sont les racines communes à f et g, et si une racine commune est d'ordre r' pour f et r'' pour g, elle est d'ordre* Min (r', r'') *pour le pgcd de f et g.*

En particulier, *pour que f et g soient premiers entre eux il faut et il suffit qu'ils n'admettent aucune racine commune*, résultat qui n'est autre que le Corollaire du Théorème 4 dans le cas particulier où $n = 1$.

Le Théorème 5 permet également d'améliorer, dans le cas d'un corps algébriquement clos, la décomposition d'une fraction rationnelle en éléments simples du § 32, n° 4. En effet, dans ce cas les polynômes irréductibles q_i du cas général sont donnés par

$$q_i(X) = X - a_i$$

et sont de degré 1; les polynômes h_{ir} figurant dans la formule (12) du § 32 sont donc de degré 0 au plus, autrement dit ce sont des *constantes*, et on voit en définitive que, sur un corps algébriquement clos, toute fraction rationnelle peut se mettre sous la forme

$$f(X) = g(X) + \sum_{i=1}^{i=n} \sum_{0 \leqslant r \leqslant r_i} \frac{c_{ir}}{(X - a_i)^r} \tag{9}$$

où les c_{ir} sont des éléments de K, les a_i les diverses racines du dénominateur de f, les r_i les multiplicités de ces racines, et g un polynôme (qui est du reste, comme on le vérifie facilement, le quotient du numérateur de f par son dénominateur).

5. *Polynômes irréductibles à coefficients réels*

Les résultats du n° 4 s'appliquent au corps **C** des nombres complexes, mais non au corps **R** des nombres réels puisque celui-ci n'est pas algébriquement clos. On peut toutefois, dans ce cas, obtenir encore des résultats complets :

THÉORÈME 6. *Les éléments irréductibles de l'anneau* $\mathbf{R}[X]$ *des polynômes à une indéterminée à coefficients réels sont d'une part les polynômes*

$$aX + b \quad avec \quad a \neq 0,$$

d'autre part les polynômes

$$aX^2 + bX + c \quad avec \quad b^2 - 4ac < 0.$$

Il est clair que, pour tout corps commutatif K, les polynômes de degré 1 sont des éléments irréductibles de K[X]. Il en est de même des polynômes de degré 2 *qui n'ont aucune racine dans* K, car un diviseur non trivial d'un tel polynôme f est nécessairement de degré 1, donc de la forme $aX + b$, et si f est divisible par $aX + b$ alors $-b/a$ est une racine de f dans K.

Il reste à faire voir que, pour $K = \mathbf{R}$, il n'existe pas d'autres polynômes irréductibles que ceux qu'on vient d'énumérer.

Soit f un élément irréductible (donc de degré 1 au moins) de $\mathbf{R}[X]$. Si f admet dans **R** une racine a, alors f est divisible par $X - a$, donc proportionnel à $X - a$ et par suite f est de degré 1, la réciproque étant claire.

Supposons maintenant que f ne possède aucune racine dans **R**. Comme **C** est algébriquement clos, le polynôme

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

considéré admet au moins une racine complexe

$$w = u + iv \quad (u,\ v \in \mathbf{R});$$

mais il admet alors aussi pour racine le nombre

$$\overline{w} = u - iv$$

conjugué de w, car, les coefficients a_i étant réels, on a

$$f(w) = a_0 + a_1w + \cdots + a_n\overline{w}^n = \overline{a_0} + \overline{a_1w} + \cdots + \overline{a_nw^n} = \overline{f(w)},$$

d'où notre assertion. Par conséquent, dans l'anneau $\mathbf{C}[X]$, le polynôme f est divisible par $X - w$ et $X - \overline{w}$; comme ces polynômes sont premiers entre eux puisque $w \neq \overline{w}$, on voit que dans $\mathbf{C}[X]$ il est même divisible par

$$(X - w)(X - \overline{w}) = (X - u - iv)(X - u + iv) = (X - u)^2 + v^2,$$

polynôme du second degré à coefficients *réels* et sans racine réelle. Pour en déduire

que le polynôme irréductible f est du second degré, il suffit de montrer que f est divisible par $(X - u)^2 + v^2$ non seulement dans $\mathbf{C}[X]$, mais aussi dans $\mathbf{R}[X]$.

Or considérons d'une manière générale un corps K, un surcorps L de K, et deux polynômes f et g à coefficients dans K. Soient q et r le quotient et le reste de la division de f par g dans K[X]; ce sont des polynômes à coefficients dans K vérifiant

$$f = gq + r, \qquad d^\circ(r) < d^\circ(g);$$

évidemment ces relations subsistent si l'on regarde f, g, q, r comme des polynômes à coefficients dans L; par suite, *le quotient et le reste de la division de* f *par* g *dans l'anneau* K[X] *sont les mêmes que dans l'anneau* L[X].

Si en particulier g divise f dans L[X], on voit que g divise aussi f dans K[X], et ceci achève la démonstration du Théorème.

Il résulte du Théorème 6 et du § 31, Théorème 5, que tout polynôme f à coefficients *réels* peut s'écrire sous la forme

$$f(X) = u.(X - a_1)^{r_1} \ldots (X - a_p)^{r_p}(X^2 + b_1X + c_1)^{s_1} \ldots (X^2 + b_qX + c_q)^{s_q}$$

où u est le coefficient dominant de f, où les a_i sont les diverses racines de f dans **R**, et les r_i leurs ordres de multiplicités, et où les polynômes $X^2 + b_jX + c_j$ sont sans racine réelle, i.e. vérifient $b_j^2 - 4c_j < 0$.

On peut obtenir encore comme suit cette décomposition. Étant donné que la conjuguée d'une racine complexe de f est encore une racine de f comme il résulte de la relation

$$f(\overline{w}) = \overline{f(w)}$$

établie plus haut, le polynôme f possède un nombre *pair* de racines non réelles, soit $2q$; désignant par

$$w_j = u_j + iv_j \quad (1 \leqslant j \leqslant q)$$

celles dont la partie imaginaire est positive, on voit que les autres sont les nombres

$$\overline{w}_j = u_j - iv_j$$

conjugués des précédents. Si l'on se place dans l'anneau $\mathbf{C}[X]$, on a donc une formule $f(X) = u.(X - a_1)^{r_1} \ldots (X - a_p)^{r_p}(X - w_1)^{s_1} \ldots (X - w_q)^{s_q}(X - \overline{w}_1)^{s'_1} \ldots (X - \overline{w}_q)^{s'_q}$; en fait, les ordres de multiplicité s_j et s'_j de deux racines imaginaires conjuguées sont les mêmes comme il résulte du § 30, Théorème 7, et en groupant les termes correspondants dans le décomposition on trouve un facteur

$$[(X - w_j)(X - \overline{w}_j)]^{s_j} = [(X - u_j)^2 + v_j^2]^{s_j},$$

d'où la décomposition en facteurs irréductibles dans l'anneau $\mathbf{R}[X]$.

Comme au n° précédent, ces résultats permettent d'améliorer la décomposition d'une fraction rationnelle en éléments simples donnée au § 32, n° 4. En effet, les polynômes q_i du cas général sont ici de deux espèces : ceux de la forme

$$q_i(X) = X - a_{ij}$$

qui correspondent aux racines réelles du dénominateur (les numérateurs h_{ir} des éléments simples sont alors de degré < 1, autrement dit sont des *constantes*); et ceux de la forme

$$q_j(X) = X^2 + b_jX + c_j \quad \text{avec} \quad b_j^2 - 4c_j < 0,$$

qui correspondent aux couples de racines imaginaires conjuguées (les polynômes h_{jr} sont alors de degré < 2, i.e. de la forme $u_{jr}X + v_{jr}$ avec des constantes u_{jr}, v_{jr}). Par suite, la formule (12) du § 32 s'écrit, dans le cas du corps des nombres réels, sous la forme

$$f(X) = g(X) + \sum_{i=1}^{i=m} \sum_{0 \leqslant r \leqslant r_i} \frac{c_{ir}}{(X - a_i)^r} + \sum_{j=1}^{j=s} \sum_{0 \leqslant r \leqslant s_j} \frac{u_{jr}X + v_{jr}}{(X^2 + b_jX + c_j)^r};$$

cette formule joue un grand rôle dans le calcul des primitives des fractions rationnelles, comme le lecteur s'en persuadera aisément en consultant la liste des questions posées, depuis plus de 150 ans, aux épreuves orales du concours d'entrée à l'École Polytechnique.

6. *Relations entre les coefficients et les racines d'une équation*

Soit

$$f(X) = u_nX^n + u_{n-1}X^{n-1} + \cdots + u_0 \tag{10}$$

un polynôme de degré $n \geqslant 1$ à coefficients dans un corps commutatif K, et supposons que f possède n racines (compte tenu des ordres de multiplicité de ces racines), ce qui sera par exemple toujours le cas si K est algébriquement clos. Désignons ces racines par

$$a_1, \ \ldots, \ a_n$$

en écrivant r fois chaque racine multiple d'ordre r. On a alors, d'après le Théorème 1, la relation

$$f(X) = u_n(X - a_1)(X - a_2) \ldots (X - a_n). \tag{11}$$

Posons

$$(X - a_1)(X - a_2) \ldots (X - a_n) = X^n + v_{n-1}X^{n-1} + \cdots + v_0; \tag{12}$$

en utilisant la formule

$$\prod_{i \in I} (x_i + y_i) = \sum_{V \subset I} x_V y_{I-V}$$

du § 8, n° 5, on trouve évidemment

$$v_{n-k} = (-1)^k \sum a_{i_1}a_{i_2} \ldots a_{i_k},$$

la somme du second membre étant étendue à toutes les *parties* $\{i_1, \ldots, i_k\}$ de l'ensemble $\{1, \ldots, n\}$; comme

$$u_{n-k} = u_nv_{n-k}$$

en vertu de (11) et (12), on obtient en définitive les relations

$$\sum a_{i_1}a_{i_2} \ldots a_{i_k} = (-1)^k u_{n-k}/u_n; \tag{13}$$

on les appelle les **relations entre les coefficients et les racines** de l'équation $f(x) = 0$; les premiers membres des relations (13) s'appellent les **fonctions symétriques élémentaires** des racines de l'équation $f(x) = 0$. Voir l'*Exercice* 13 de ce §.

Exemple 2. Si u et v sont les racines (distinctes ou non) d'une équation du second degré

$$ax^2 + bx + c = 0,$$

on a

$$u + v = -b/a, \qquad uv = c/a.$$

Exemple 3. Si u, v et w sont les trois racines (distinctes ou non) d'une équation

$$ax^3 + bx^2 + cx + d = 0,$$

on a

$$u + v + w = -b/a, \qquad vw + wu + uv = c/a, \qquad uvw = -d/a.$$

On observera que, pour $k = 1$, la relation (13) s'écrit

$$a_1 + \cdots + a_n = -u_{n-1}/u_n, \tag{14}$$

et que pour $k = n$ elle s'écrit

$$a_1 \ldots a_n = (-1)^n u_0/u_n. \tag{15}$$

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.

§ 31

1. Soient $x_1, \ldots, x_n$ des éléments non nuls d'un anneau principal K et d un de leurs pgcd; on choisit $u_1, \ldots, u_n \in K$ tels que $u_1x_1 + \cdots + u_nx_n = d$. Montrer que $u_1, \ldots, u_n$ sont premiers entre eux.

¶ **2.** Soient M un module libre de type fini sur un anneau principal K et a un élément non nul de M. Montrer que les cinq propriétés suivantes sont équivalentes : a fait partie d'une base de M; il existe une forme linéaire f sur M telle que $f(a) = 1$; les coordonnées de a par rapport à *une* base de M sont premières entre elles; les coordonnées de a par rapport à *toute* base de M sont premières entre elles; si $a = ux$ pour un $u \in K$ et un $x \neq 0$ dans M, alors u est inversible; si $ux = va$ avec $u, v \in K$ et $x \in M$ non nul alors v est multiple de u. (On utilisera l'*Exercice* 2 du § 18 et l'*Exercice* 11, *h*), du § 29). Un vecteur $a \in M$ satisfaisant aux conditions précédentes est dit **primitif.**

3. Soit M un module libre de type fini sur un anneau principal K. Montrer que tout $x \in M$ est multiple d'au moins un vecteur primitif de M. Faire le calcul en prenant $K = \mathbf{Z}$, $M = \mathbf{Z}^4$ et $x = (126, 210, 168, 504)$.

4. Soient $a_1, \ldots, a_n$ des éléments d'un anneau principal K; pour qu'il existe une matrice

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

dont la première ligne (resp. colonne) soit précisément $a_1, \ldots, a_n$, il faut et il suffit que $a_1, \ldots, a_n$ soient premiers entre eux. On peut alors choisir U de telle sorte que dét(U) = 1, i.e. supposer

$$U \in SL(n, K).$$

5. Construire une matrice $U \in SL(3, \mathbf{Z})$ dont la première colonne soit 2, 3, 4.

6. Construire une matrice $U \in SL(3, \mathbf{Z})$ dont la seconde colonne soit 2, 3, 4.

¶ **7.** Soit M un module libre de type fini sur un anneau principal K.

a) Montrer que, si a est un élément non nul de M, le pgcd des coordonnées de a par rapport à une base de M est indépendant du choix de celle-ci. Quelle est l'interprétation « géométrique » de ce résultat (cf. *Exercice* 3)?

b) Soit M' un sous-module non nul de M. On choisit une base de M et on considère l'idéal de K engendré par toutes les coordonnées de tous les éléments de M'. Montrer que cet idéal est indépendant du choix de la base. Montrer qu'il est engendré par les coordonnées d'un ensemble quelconque de générateurs de M'. [Cet idéal, ou l'un quelconque de ses générateurs, est appelé le *premier facteur invariant* de M' dans M; voir l'*Exercice* suivant.]

¶¶ **8.** Soient M un module libre de type fini sur un anneau principal K et M' un sous-module non nul de M; on note n et r les rangs (nombres d'éléments d'une base) de M et M'. On se propose de démontrer le résultat que voici : *il existe une base* $a_1, \ldots, a_n$ *de* M *et des éléments* $d_1, \ldots, d_r$ *de* K *tels que les vecteurs* $d_1a_1, \ldots, d_ra_r$ *forment une base de* M' *et que* d_i *divise* d_{i+1} *pour* $1 \leqslant i \leqslant r - 1$.

a) Montrer que, pour toute forme linéaire f sur M, l'ensemble $f(M') \subset K$ est un idéal de K.

b) Montrer qu'il existe une forme linéaire f_1 sur M telle que, pour toute forme linéaire f sur M, la relation

$$f_1(M') \subset f(M') \quad \text{implique} f_1(M') = f(M').$$

Montrer qu'on a alors

$$f_1(M) = K.$$

c) On choisit f_1 satisfaisant à *b*); on pose

$$f_1(M') = (d_1)$$

et on choisit un vecteur $u_1 \in M'$ tel que

$$f_1(u_1) = d_1.$$

Montrer qu'on a

$$f(u_1) \in (d_1)$$

pour toute forme linéaire f sur M (en posant $f(u_1) = d$, montrer qu'il existe une combinaison linéaire g de f et f_1 telle que $g(u_1)$ soit un pgcd de d et d_1).

d) Déduire de (*c*) qu'on a

$$u_1 = d_1e_1$$

pour un vecteur $e_1 \in M$, tel que $f_1(e_1) = 1$.

e) Montrer que M est somme directe du sous-module engendré par e_1 et de $\mathrm{Ker}(f_1)$; et que M' est somme directe du sous-module engendré par u_1 et de $M' \cap \mathrm{Ker}(f_1)$. Montrer que $f(M') \subset f_1(M')$ pour toute f.

f) Achever la démonstration par récurrence sur n.

¶¶ **9.** Soit A une matrice à n lignes et p colonnes à coefficients dans un anneau principal K. Montrer à l'aide de l'*Exercice* 8 qu'il existe des matrices

$$U \in GL(n, K) \quad \text{et} \quad V \in GL(p, K)$$

telles que l'on ait

$$UAV = \begin{pmatrix} d_1 & 0 & \ldots & 0 & 0 & \ldots & 0 \\ 0 & d_2 & \ddots & 0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & d_r & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 0 & 0 & \ldots & 0 \end{pmatrix}$$

où $d_1, \ldots, d_r$ sont des éléments non nuls de K tels que chacun divise le suivant. Les éléments

$d_1, \ldots, d_r$ sont appelés les **facteurs invariants** de la matrice A; on verra (*Exercice* 11) que les idéaux $(d_1), \ldots, (d_r)$ sont entièrement déterminés par A.

¶¶ **10.** Montrer que *tout groupe commutatif de type fini est isomorphe au produit direct d'un groupe* $\mathbf{Z}^q$ *et de groupes cycliques finis* $\mathbf{Z}/d_1\mathbf{Z}, \ldots, \mathbf{Z}/d_r\mathbf{Z}$ *où chaque* d_i *divise* d_{i+1}. (Observer qu'un K-module de type fini, où K est un anneau arbitraire, est isomorphe à un quotient M/M' où M est libre de type fini — et appliquer *l'Exercice* 8). Comment ce résultat se généralise-t-il à un anneau principal quelconque?

¶¶ **11.** On reprend les hypothèses et notations de l'*Exercice* 8, dont on utilise les résultats.

a) Soient $j_1, \ldots, j_h$ des entiers tels que

$$1 \leqslant j_1 < j_2 < \ldots < j_h \leqslant r;$$

montrer que $d_1 \ldots d_h$ divise $d_{j_1} \ldots d_{j_h}$.

b) Soit h tel que $1 \leqslant h \leqslant r$; montrer que, si f est une forme h-linéaire alternée sur M, le produit $d_1 \ldots d_h$ divise $f(x_1, \ldots, x_h)$ quels que soient $x_1, \ldots, x_h \in M'$; montrer qu'on peut en outre choisir f et $x_1, \ldots, x_h \in M'$ de telle sorte que

$$d_1 \ldots d_h = f(x_1, \ldots, x_h);$$

en déduire que $d_1 \ldots d_h$ est un pgcd des éléments de K de la forme $f(x_1, \ldots, x_h)$ et en conclure que *les idéaux* (d_i) *sont entièrement déterminés par le module* M *et le sous-module* M' (i.e. ne dépendent pas du choix des bases construites dans l'*Exercice* 8).

c) Soient $(a_i)_{1 \leqslant i \leqslant n}$ une base quelconque de M et $(b_j)_{1 \leqslant j \leqslant p}$ un système quelconque de générateurs de M'; on note A la matrice (à n lignes et p colonnes) formée avec les coordonnées des b_j par rapport à la base (a_i) de M.
Montrer que, pour $1 \leqslant h \leqslant r$, *l'élément* $d_1 \ldots d_h$ *est un pgcd des mineurs d'ordre* h *de la matrice* A.

d) En déduire que les facteurs $d_1, \ldots, d_r$ de *l'Exercice* 9 se calculent de même.

e) Soient A et B deux matrices à n lignes et p colonnes à coefficients dans un anneau principal K. Pour que A et B soient **équivalentes** (i.e. pour qu'il existe des matrices U et V *inversibles* telles que $B = UAV$) il faut et il suffit que A et B aient le même rang et les mêmes facteurs invariants.

(NB. — On exprime souvent ce résultat en introduisant, au lieu des facteurs invariants de A, ses **diviseurs élémentaires**

$$e_1 = d_1, e_2 = d_2/d_1, \ldots, e_r = d_r/d_{r-1})$$

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

$$a_j = (\alpha_{1j}, \ldots, \alpha_{nj}) \quad (1 \leqslant j \leqslant p)$$

des éléments de K^n. Pour qu'ils fassent partie d'une base de K^n, il faut et il suffit que les mineurs d'ordre p de la matrice

$$\begin{pmatrix} \alpha_{11} & \ldots & \alpha_{1p} \\ \ldots\ldots\ldots\ldots \\ \alpha_{n1} & \ldots & \alpha_{np} \end{pmatrix}$$

formée avec les composantes des vecteurs donnés soient *premiers entre eux* (et en particulier non tous nuls).

¶¶ **13.** Soient K un anneau principal et n et p deux entiers tels que $1 \leqslant p \leqslant n$. Soit A une matrice à n lignes et p colonnes à coefficients dans K. Pour qu'on puisse compléter A en une matrice carrée d'ordre n et *inversible* sur l'anneau K, il faut et il suffit que le pgcd des mineurs d'ordre p de A soit égal à 1.

14. Trouver toutes les matrices à coefficients entiers rationnels, de la forme

$$\begin{pmatrix} 1 & 4 & * \\ 2 & 5 & * \\ 1 & 6 & * \end{pmatrix},$$

et de déterminant 1.

¶ **15.** Soit A une matrice à coefficients dans un anneau commutatif K; on appelle **opération élémentaire** sur A une opération consistant soit à permuter deux lignes (resp. colonnes) de A, soit à ajouter à une ligne (resp. colonne) une combinaison linéaire des autres lignes (resp. colonnes), soit à multiplier une ligne (resp. colonne) par un élément inversible de K.

a) Montrer que toute matrice déduite de A par une succession d'opérations élémentaires est équivalente à A (i.e. de la forme UAV avec U, V inversibles sur K).

b) On suppose $K = \mathbf{Z}$, et $A \neq 0$. Soit d_1 le plus petit entier strictement positif possédant la propriété suivante : il existe une matrice qui se déduit de A par une succession d'opérations élémentaires, et dont d_1 est un coefficient. Montrer qu'il existe alors une matrice de la forme

$$\begin{pmatrix} d_1 & 0 \\ 0 & A_1 \end{pmatrix}$$

(où A_1 possède une ligne et une colonne de moins que A) qui se déduit de A par une succession d'opérations élémentaires, et de plus que tous les coefficients de A_1 sont multiples de d_1.

c) Déduire de là, pour $K = \mathbf{Z}$, une nouvelle démonstration du résultat de l'*Exercice* 9 (donc aussi de l'*Exercice* 8), et une méthode pratique pour réduire une matrice à coefficient dans $\mathbf{Z}$ à la forme canonique de l'*Exercice* 9.

d) Appliquer cette méthode aux matrices suivantes :

$$\begin{pmatrix} 0 & 2 & 4 & -1 \\ 6 & 12 & 14 & 5 \\ 0 & 4 & 14 & -1 \\ 10 & 6 & -4 & 11 \end{pmatrix}, \quad \begin{pmatrix} 0 & 6 & -9 & -3 \\ 12 & 24 & 9 & 9 \\ 30 & 42 & 45 & 27 \\ 66 & 78 & 81 & 63 \end{pmatrix},$$

$$\begin{pmatrix} 17 & -28 & 45 & 11 & 39 \\ 24 & -37 & 61 & 13 & 50 \\ 25 & -7 & 32 & -18 & -11 \\ 31 & 12 & 19 & -43 & -55 \\ 42 & 13 & 29 & -55 & -68 \end{pmatrix}.$$

16. Soit A une matrice à coefficients dans un anneau commutatif K quelconque, et soit B une matrice équivalente à A (i.e. de la forme UAV avec U et V inversibles sur l'anneau K). Montrer que, pour tout entier p inférieur au nombre de lignes et au nombre de colonnes de A, l'idéal de K engendré par les mineurs d'ordre p de A est égal à celui qui est engendré par les mineurs d'ordre p de B.

¶ **17.** Soit A une matrice carrée d'ordre n à coefficients dans un anneau principal K. Montrer qu'il existe une matrice $U \in GL(n, K)$ telle que UA soit triangulaire (utiliser les *Exercices* 1 et 4 et raisonner par récurrence sur n). Interprétation géométrique?

¶¶ **18.** On considère un système d'équations linéaires

$$\begin{cases} a_{11}x_1 + \cdots + a_{1p}x_p = b_1 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ a_{n1}x_1 + \cdots + a_{np}x_p = b_n \end{cases}$$

à coefficients, seconds membres et inconnues dans un anneau principal K. Montrer que, pour que ce système possède au moins une solution, il faut et il suffit d'une part que les deux matrices

$$\mathrm{A} = \begin{pmatrix} a_{11} & \cdots & a_{1p} \\ \cdots\cdots & & \cdots\cdots \\ a_{n1} & \cdots & a_{np} \end{pmatrix}, \qquad \mathrm{B} = \begin{pmatrix} a_{11} & \cdots & a_{1p} & b_1 \\ \cdots\cdots & & \cdots\cdots & \cdots\cdots \\ a_{n1} & \cdots & a_{np} & b_n \end{pmatrix}$$

aient le même rang r, d'autre part qu'un pgcd des mineurs d'ordre r de A soit égal à un pgcd des mineurs d'ordre r de B.

¶¶ **19.** Soient K un anneau principal, f une forme p-linéaire sur le module K^n et soit d un pgcd des coefficients de f par rapport à la base canonique; montrer qu'il existe $x_1, \ldots, x_p \in \mathrm{K}^n$ tels que

$$f(x_1, \ldots, x_p) = d.$$

20. Démontrer que tout nombre rationnel peut s'écrire, d'une façon et d'une seule, sous la forme d'une somme finie de fractions de la forme

$$a/p^n$$

avec p premier, $n \geqslant 1$, et $1 \leqslant a \leqslant p - 1$.
Effectuer cette décomposition pour les nombres

$$\frac{1887}{5400}, \qquad \frac{122}{1323}.$$

¶¶ **21.** Soit K un anneau d'intégrité commutatif. On dit qu'un $p \in \mathrm{K}$ est **irréductible** s'il n'est pas inversible et s'il n'a pas d'autres diviseurs dans K que ceux qui sont évidents (à savoir les éléments inversibles de K, et les up où $u \in \mathrm{K}$ est inversible).
On dit que K est **factoriel** s'il possède les deux propriétés suivantes :

(UFD 1) : Tout élément non inversible de K est produit d'un nombre fini d'éléments irréductibles.

(UFD 2) : Si $p_1 \ldots p_r = q_1 \ldots q_s$ où les p_i et les q_j sont des éléments irréductibles de K, alors on a $r = s$, et on peut changer l'ordre des q_j de telle sorte que l'on ait

$$\mathrm{K}p_i = \mathrm{K}q_i \quad \text{pour} \quad 1 \leqslant i \leqslant r$$

(ou, ce qui revient au même, $q_i = u_i p_i$ avec u_i inversible).
Ces propriétés expriment que *tout élément de* K *s'écrit, d'une façon essentiellement unique, sous la forme d'un produit d'éléments irréductibles de* K.

a) Montrer que tout anneau principal est factoriel (la réciproque est fausse; cf. § 32, *Exercice* 31).

b) Montrer que, dans la définition d'un anneau factoriel, on peut remplacer la condition (UFD 2) par

(UFD 3) : Si un élément irréductible p de K divise un produit xy, il divise l'un au moins des facteurs de ce produit.

c) Montrer qu'on peut aussi remplacer (UFD 2) par

(UFD 4) Pour tout élément irréductible p de K, l'idéal $\mathrm{K}p$ est premier.

d) Soit K un anneau factoriel. Montrer que, quels que soient $x, y \in \mathrm{K}$ il existe un $d \in \mathrm{K}$ tel que les diviseurs communs à x et y soient exactement les diviseurs de d (on dit que d est un **pgcd de** x **et** y), et que d est unique modulo la possibilité de le multiplier par un élément inversible de K.

e) Soient K un anneau factoriel, L son corps des fractions, et $\mathfrak{p}$ l'idéal premier de K engendré par un élément irréductible p de K. Montrer que l'anneau local $\mathrm{K}_{\mathfrak{p}}$ [§ 8, *Exercice* 7, (*g*)] est l'anneau d'une valuation discrète (§ 8, *Exercice* 6) de L.

f) Si un anneau d'intégrité commutatif est à la fois factoriel et de Dedekind, il est principal.

g) Soit K un anneau d'intégrité commutatif noethérien. Montrer que tout élément non inversible de K est produit d'éléments irréductibles — autrement dit que K vérifie (UFD 1). [Mais un anneau noethérien n'est pas nécessairement factoriel, i.e. la décomposition en éléments irréductibles peut ne pas être unique : prendre un anneau de Dedekind non principal; ce dernier phénomène se produit notamment pour l'anneau des entiers d'un corps de nombres algébriques, et a longtemps bloqué les progrès dans l'étude de ces anneaux — jusqu'à Dedekind, qui reconnut le premier que la notion importante, dans ce cas, était celle d'*idéal* premier et non d'*élément* irréductible, contrairement à ce qu'indiquait une analogie trompeuse avec les entiers rationnels.]

§ 32

1. Trouver le quotient et le reste de la division de

$$2X^4 - 3X^3 + 4X^2 - 5X + 6 \quad \text{par} \quad X^2 - 3X + 1$$
$$4X^3 + X^2 \quad \text{par} \quad X + 1 + i$$
$$X^4 - 2X^3 + 4X^2 - 6X + 8 \quad \text{par} \quad X - 1.$$

2. Calculer le pgcd des polynômes suivants :

a) $X^6 - 7X^4 + 8X^3 - 7X + 7$ et $3X^5 - 7X^3 + 3X^2 - 7$;

b) $X^5 + X^4 - X^3 - 3X^2 - 3X - 1$ et $X^4 - 2X^3 - X^2 - 2X - 1$;

c) $X^6 + X^5 - X^4 - 2X^3 - X^2 + X + 1$, $X^5 + X^3 - X^2 - 1$ et $X^4 - 2X^3 - X + 2$.

3. Pour chacun des couples de polynômes p, q indiqués ci-dessous, trouver des polynômes u et v tels que $up + vq$ soit un pgcd de p et q :

a) $X^5 + 3X^4 + X^3 + X^2 + 3X + 1$ et $X^4 + 2X^3 + X + 2$;

b) $3X^5 + 5X^4 - 16X^3 - 6X^2 - 5X - 6$ et $3X^4 - 4X^3 - X^2 - X - 6$;

c) $X^5 + 5X^4 + 9X^3 + 7X^2 + 5X + 3$ et $X^4 + 2X^3 + 2X^2 + X + 1$;

d) X^4 et $(1 - X)^4$

4. Trouver un polynôme de degré aussi petit que possible dont le reste de la division par $X^4 - 2X^3 - 2X^2 + 10X - 7$ soit égal à $X^2 + X + 1$, et dont le reste de la division par $X^4 - 2X^3 - 3X^2 + 13X - 10$ soit égal à $2X^2 - 3$.

¶ **5.** Montrer que le pgcd des polynômes

$$X^m - 1 \quad \text{et} \quad X^n - 1$$

est $X^d - 1$, où d est le pgcd des entiers m et n.

6. Soient p et q deux polynômes à une indéterminée. Si le polynôme $p(X^3) + Xq(X^3)$ est divisible par $X^2 + X + 1$, alors $p(1) = q(1) = 0$.

7. Soit

$$f(X) = \frac{p(X)}{q(X)}$$

une fraction rationnelle à une variable à coefficients dans un corps K, et soit a une racine *simple* de son dénominateur q, de sorte que la contribution du pôle a dans la décomposition de f en éléments simples est

$$\frac{A}{X - a}$$

pour un certain $A \in K$. Montrer qu'on a

$$A = \frac{p(a)}{q'(a)}$$

[Écrire

$$\frac{p(X)}{q(X)} = \frac{A}{X - a} + \frac{r(X)}{s(X)}$$

avec $r(a) \neq 0$, $s(a) \neq 0$, réduire au même dénominateur, dériver, et faire $X = a$ dans le résultat obtenu. Le processus de « passage à la limite » qu'on utilise en général dans les cours d'Analyse pour démontrer ce résultat ne s'étend pas à un corps quelconque].

8. Décomposer en éléments simples (sur **C**, puis sur **R**) les fractions rationnelles suivantes :

$$\frac{X^2 + 1}{X(X^2 - 1)}, \quad \frac{2}{(X - 1)(X - 2)(X - 3)}, \quad \frac{X^5 - X^3 - X^2}{X^2 - 1}, \quad \frac{4X^3}{(X^2 + 1)^2},$$
$$\frac{X^6 - X^2 + 1}{(X - 1)^3}, \quad \frac{3X^2 + 3}{X^3 - 3X - 2}, \quad \frac{X^5}{(X^4 - 1)^2}.$$

Le lecteur qui estimerait ces exemples insuffisants pourra facilement en construire autant qu'il en désire : la méthode consiste à choisir au hasard deux polynômes (en s'arrangeant tout de même pour que les racines du dénominateur soient évidentes, ou en tous cas calculables, si l'on désire avoir des résultats explicites).

¶ **9.** Soient L un corps commutatif, K un sous-corps de L, et x un élément de L algébrique sur K. Soit I l'ensemble des polynômes $f \in K[X]$ tels que $f(x) = 0$; montrer que c'est un idéal de K[X]. En déduire qu'il existe un et un seul polynôme

$$(*) \qquad f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$$

à coefficients dans K qui vérifie $f(x) = 0$ et tel que tout polynôme $g \in K[X]$ vérifiant $g(x) = 0$ soit un multiple de f. Montrer que

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

est l'équation (à coefficients dans K) de plus petit degré possible vérifiée par x. On dit que $(*)$ est le **polynôme minimal** et $(**)$ l'**équation minimale** de x sur K; son degré n s'appelle le **degré de x sur K**. Montrer que, considéré comme espace vectoriel sur K, le sous-corps $K[x]$ est de dimension n et admet pour base les éléments

$$1, x, \ldots, x^{n-1}.$$

Autrement dit, on a

$$[K[x] : K] = n$$

avec les notations du § 26, *Exercice* 5.

On prend $L = \mathbf{C}$, $K = \mathbf{Q}$ dans ce qui précède. Trouver les équations minimales des éléments suivants de L :

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

10. Soit K un corps commutatif.

a) Soient L un sur-corps de K et x un élément de L algébrique sur K. Montrer que le polynôme minimal de x sur K est irréductible (sur K).

b) Soit f un polynôme irréductible à une variable à coefficients dans K, et de coefficient dominant égal à 1. Soit x une racine de f dans une extension de K. Montrer que f est le polynôme minimal de x sur K.

c) Le polynôme f étant comme dans la question précédente, soient x et y deux racines de f dans un sur-corps L de K. Montrer qu'il existe un et un seul isomorphisme j du corps $K(x)$ sur le corps $K(y)$ vérifiant

$$j(x) = y, \qquad j(a) = a \text{ pour tout } a \in K.$$

d) On suppose de plus que K est le corps des fractions d'un anneau A. Avec les notations de la question *c*), montrer que si x est entier sur A (§ 26, *Exercice* 6) il en est de même de y.

e) Soient A un anneau d'intégrité commutatif, K son corps des fractions et L un sur-corps de K. Soit $x \in L$ entier sur A; montrer que les coefficients du polynôme minimal f de x sur K sont entiers sur A (plonger L dans un corps algébriquement clos, observer que toutes les racines de f sont des entiers sur A et appliquer le § 33, n° 6). En déduire que f est à coefficients dans A si A est intégralement clos (i.e. si tout élément de K entier sur A est dans A).

f) On suppose dans ce qui précède que L est une extension algébrique de degré fini de K (§ 26, *Exercice* 4). Montrer que, si $x \in L$ est entier sur A, et si A est intégralement clos, on a

$$\mathrm{Tr}_{L/K}(x) \in A, \qquad \mathrm{N}_{L/K}(x) \in A$$

(utiliser l'*Exercice* 5 du § 26).

11. Soient L un corps commutatif, K un sous-corps de L, et x un élément de L algébrique sur K. On dit que x est **séparable** sur K s'il est racine *simple* de son polynôme minimal f sur K.

a) Pour que x soit séparable sur K, il faut et il suffit que x soit racine simple d'au moins une équation algébrique à coefficients dans K.

b) On a $f' = 0$ si x n'est pas séparable sur K, et réciproquement.

c) Si K est de caractéristique 0, tout x algébrique sur K est séparable sur K, et toutes les racines de tout polynôme irréductible à coefficients dans K sont simples.

d) Si K est de caractéristique $p \neq 0$, pour tout $x \in L$ algébrique sur K il existe un entier $n \geqslant 0$ tel que

$$x^{p^n}$$

soit séparable sur K.

e) Soit L une extension algébrique de degré fini de K (§ 26, *Exercice* 4). Pour que L soit séparable sur K (§ 26, *Exercice* 4, (*h*)) il faut et il suffit que tout $x \in L$ soit séparable sur K.

12. Si un polynôme $f \in \mathbf{Z}[X]$ non constant n'est pas irréductible dans l'anneau $\mathbf{Q}[X]$, alors on peut le décomposer de façon non triviale en produit de polynômes à coefficients *entiers* rationnels (utiliser le lemme de Gauss, § 27, *Exercice* 13).

13. Parmi les polynômes

$$X^3 + X + 1, \qquad X^4 + X + 1, \qquad X^4 + X^3 + 1, \qquad X^3 + 7X + 7, \qquad X^6 + 3X + 2,$$

quels sont ceux qui sont irréductibles sur $\mathbf{Q}$?

14. Soit $f(X) = a_0 + a_1X + \cdots + a_nX^n$ un polynôme à coefficients dans $\mathbf{Z}$. On suppose qu'un certain nombre premier p divise $a_0, \ldots, a_{n-1}$, ne divise pas a_n, et de plus que a_0 n'est pas divisible par p^2. Montrer que f est irréductible sur $\mathbf{Q}$ (**critère d'irréductibilité d'Eisenstein**; utiliser l'*Exercice* 12).

15. (Diviseurs élémentaires d'une matrice à coefficients polynomiaux). Soient k un corps commutatif et $K = k[X]$ l'anneau des polynômes à une indéterminée à coefficients dans k.

a) Montrer que $GL(n, K)$ est l'ensemble des matrices $U \in M_n(K)$ dont le déterminant est un élément non nul du corps k (le déterminant d'une telle matrice est donc « constant »).

b) On utilise dans ce qui suit, pour les matrices à coefficients dans K, la notion d'opération élémentaire du § 31, *Exercice* 15. Soit A une matrice rectangulaire non nulle à coefficients dans K et soit $a_{ij}(X)$ le coefficient situé à l'intersection de la i^e colonne et de la j^e ligne de A. Montrer qu'on peut, à l'aide d'un nombre fini d'opérations élémentaires, remplacer les coefficients situés sur la i^e colonne ou la j^e ligne de A par les restes de leur division par $a_{ij}(X)$.

c) Soit $d_1(X)$ un polynôme non nul, de coefficient dominant égal à 1, et de plus petit degré possible parmi tous les coefficients non nuls de toutes les matrices déduites de A par une succession d'opérations élémentaires. Montrer qu'on peut déduire de A, par une succession d'opérations élémentaires, une matrice de la forme

$$\begin{pmatrix} d_1 & 0 \\ 0 & A_1 \end{pmatrix}$$

où A_1 a une ligne et une colonne de moins que A, et pour coefficients des polynômes tous divisibles par d_1. Montrer que d_1 est un pgcd des coefficients non nuls de A (et est par suite entièrement déterminé par la connaissance de A).

d) Montrer qu'on peut déduire de A, par une succession d'opérations élémentaires, une matrice de la forme

$$\begin{pmatrix} d_1(X) & 0 & \ldots & 0 & 0 & \ldots & 0 \\ 0 & d_2(X) & \ldots & 0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & d_r(X) & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 0 & 0 & \ldots & 0 \end{pmatrix}$$

où les d_i sont des polynômes non nuls tels que chacun divise le suivant. Montrer, à l'aide de l'*Exercice* 16 du § 31, que pour tout entier i inférieur au nombre de lignes et au nombre de colonnes de A, le polynôme $d_1(X) \ldots d_i(X)$ (où l'on pose $d_i = 0$ pour $i \geqslant r + 1$) est un pgcd des mineurs d'ordre i de A. En déduire que l'entier r est égal au rang de A, et que pour $1 \leqslant i \leqslant r$ les polynômes $d_i(X)$ sont entièrement déterminés par A si on impose à leurs coefficients dominants d'être égaux à 1.

e) On appelle $d_1, \ldots, d_r$ les **facteurs invariants** de la matrice A, et **diviseurs élémentaires** de A les quotients $d_i(X)/d_{i+1}(X)$. Enfin, on dit que deux matrices A et B à coefficients dans $K = k[X]$, et ayant toutes deux p lignes et q colonnes, sont **équivalentes** s'il existe des matrices

$$U \in GL(p, K) \qquad \text{et} \qquad V \in GL(q, K)$$

telles que $B = UAV$. Montrer que, pour que A et B soient équivalentes, il faut et il suffit que A et B aient même rang et mêmes facteurs invariants, et qu'on peut alors passer de A à B par une succession d'opérations élémentaires.

f) Soient M un K-module isomorphe à K^p et M' un sous-module de M. Montrer qu'il existe une base $(a_1, \ldots, a_p)$ de M, et des polynômes $d_1, \ldots, d_p \in K$ tels que d_i divise d_{i+1} et que M'

soit engendré par $d_1a_1, \ldots, d_pa_p$ (on n'interdit pas à certains des d_i d'être nuls). [Appliquer la question *d*) à la matrice, par rapport à une base de M, d'un endomorphisme de M ayant M′ pour image].

¶ *g*) Soit E un K-module de type fini (mais non nécessairement libre). Montrer que E est isomorphe au produit direct d'un module de la forme K^s et de modules de la forme $K/d_1K, \ldots, K/d_rK$ où $d_1, \ldots, d_r$ sont des polynômes non nuls tels que d_i divise d_{i+1} pour $1 \leqslant i \leqslant r-1$. [Choisir un homomorphisme f de K^p *sur* E et appliquer la question précédente à Ker (f)]. Montrer que les entiers r et s, et les polynômes d_i (dont on supposera qu'ils ont 1 pour coefficient dominant), sont entièrement déterminés par E et les conditions qu'on leur a imposées. [On dit que $d_1, \ldots, d_r$ sont les **facteurs invariants** du K-module E; l'entier s est le rang de E au sens du § 29, *Exercice* 11, *e*)]. Montrer que deux K-modules de type fini sont isomorphes si et seulement si leurs rangs et leurs facteurs invariants sont égaux.

¶ *h*) Déduire les résultats précédents du § 31, *Exercices* 8, 9, 10 et 11 et du fait que l'anneau K est principal.

[Les résultats de cet *Exercice*, qui constituent l'analogue pour les anneaux de polynômes à une variable sur un corps de la théorie des diviseurs élémentaires des matrices à coefficients dans **Z** (§ 31, *Exercice* 17), ont des applications importantes, notamment à la théorie des systèmes d'équations différentielles linéaires d'ordre quelconque à coefficients constants; on trouvera d'excellents exposés de ces résultats dans certains des ouvrages cités dans la Bibliographie (notamment dans Albert, Gelfand, Schreier-Sperner); mais la véritable explication de ces résultats est évidemment la théorie des modules de type fini sur un anneau principal.]

Dans les *Exercices* **16** à **21** qui suivent (*), on demande de réduire la matrice donnée à la forme canonique de l'*Exercice* 15, *d*), et d'en calculer les diviseurs élémentaires (le corps de base est **C**).

16. $\begin{pmatrix} X & 1 \\ 0 & X \end{pmatrix}$

17. $\begin{pmatrix} X^2-1 & X+1 \\ X+1 & X^2+2X+1 \end{pmatrix}$

18. $\begin{pmatrix} 1-X & X^2 & X \\ X & X & -X \\ 1+X^2 & X^2 & -X^2 \end{pmatrix}$

19. $\begin{pmatrix} X & 1 & 0 & 0 \\ 0 & X & 1 & 0 \\ 0 & 0 & X & 1 \\ 0 & 0 & 0 & X \end{pmatrix}$

20. $\begin{pmatrix} X & -1 & 0 & 0 & 0 \\ 0 & X & -1 & 0 & 0 \\ 0 & 0 & X & -1 & 0 \\ 0 & 0 & 0 & X & -1 \\ 1 & 2 & 3 & 4 & 5+X \end{pmatrix}$

21. $\begin{pmatrix} X & 1 & 1 & \ldots & 1 \\ 0 & X & 1 & \ldots & 1 \\ 0 & 0 & X & \ldots & 1 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & X \end{pmatrix}$ (*n* lignes et colonnes)

Dans les *Exercices* **22** et **23** qui suivent, on demande de trouver des matrices U et V à coefficients polynomiaux, de déterminant constant non nul, telles que, A désignant la matrice donnée, UAV soit mise sous la forme canonique de l'*Exercice* 15.

22. $\begin{pmatrix} X^4+4X^3+4X^2+X+2, & X^3+4X^2+4X \\ X^4+5X^3+8X^2+5X+2, & X^3+5X^2+8X+4 \end{pmatrix}$

23. $\begin{pmatrix} X^4+3X^3-5X^2+X+1, & 2X^4+3X^3-5X^2+X-1, & 2X^4+2X^3-4X^2 \\ X^4-X^3+1, & 2X^4-X^3-X^2, & 2X^4-2X^3 \\ X^4+2X^3-4X^2+X+1, & 2X^4+2X^3-4X^2+X-1, & 2X^4+X^3-3X^2 \end{pmatrix}$

(*) Les *Exercices* **16** à **26** sont extraits du recueil de Proskurjakov, où le lecteur trouvera de nombreux autres énoncés semblables.

24. Vérifier que les deux matrices suivantes, à coefficients dans **C**[X], sont équivalentes:

$$\begin{pmatrix} X^3+6X^2+6X+5, & X^3+4X^2+4X+3 \\ X^3+3X^2+3X+2, & X^3+2X^2+2X+1 \\ 2X^3+3X^2+3X+1, & 2X^3+2X^2+2X \end{pmatrix} = A$$

$$\begin{pmatrix} X^3+X^2+X, & 2X^3+X^2+X-1 \\ 3X^3+2X^2+2X-1, & 6X^3+2X^2+2X-4 \\ X^3-X^2-X-2, & 2X^3-X^2-X-3 \end{pmatrix} = B$$

(on calculera des matrices U, V telles que $B = UAV$).

25. Calculer les facteurs invariants de la matrice

$$\begin{pmatrix} X^3+X^2-X+3, & X^3-X^2+X, & 2X^3+X^2-X+4, & X^3+X^2-X+2 \\ X^3+3X^2-3X+6, & X^3-3X^2+3X-2, & 2X^3+3X^2-3X+7, & X^3+3X^2-3X+4 \\ X^3+2X^2-2X+4, & X^3-2X^2+2X-1, & 2X^3+2X^2-2X+5, & X^3+2X^2-2X+3 \\ 2X^3+X^2-X+5, & 2X^3-X^2+X+1, & 4X^3+X^2-X+7, & 2X^3+X^2-X+3 \end{pmatrix}$$

26. Calculer les diviseurs élémentaires de la matrice

$$\begin{pmatrix} X^4+1, & X^7-X^4+X^3-1, & X^4-4X^3+4X-5 \\ 2X^4+3, & 2X^7-2X^4+4X^3-2, & 3X^4-10X^3+X^2+10X-14 \\ X^4+2, & X^7-X^4+2X^3-2, & 2X^4-6X^3+X^2+6X-9 \end{pmatrix}$$

en prenant pour anneau de base soit **Q**[X], soit **R**[X], soit **C**[X].

¶ **27.** On se propose de démontrer que *si* K *est un anneau commutatif noethérien, l'anneau de polynômes* K[X] *est noethérien.* On désigne par I un idéal de K[X].

a) Pour tout entier $n \geqslant 0$, soit $J_n \subset K$ l'ensemble formé de 0 et des $a \in K$ vérifiant la condition suivante : il existe un polynôme $f \in I$, de degré n, dont le coefficient dominant est égal à a. Montrer que les J_n forment une suite croissante d'idéaux de K. En conclure qu'on a

$$J_r = J_{r+1} = \cdots$$

pour un certain entier r.

b) Pour tout entier i tel que $0 \leqslant i \leqslant r$, on choisit dans I des polynômes f_{ij} $(1 \leqslant j \leqslant n_i)$ en nombre fini, de degré i, dont les coefficients dominants a_{ij} engendrent l'idéal J_i. Montrer que, pour tout $f \in I$, il existe des polynômes $q_{ij} \in K[X]$ tels que l'on ait

$$f = \sum_{\substack{1 \leqslant j \leqslant n_i \\ 0 \leqslant i \leqslant r}} q_{ij} f_{ij} + g \qquad \text{avec} \qquad d^o(g) < d^o(f).$$

c) En déduire, par récurrence sur le degré de f, que les $n_0 + \cdots + n_r$ polynômes f_{ij} engendrent l'idéal I.

d) Déduire du résultat précédent que si un anneau commutatif L contient un sous-anneau noethérien K et des éléments $x_1, \ldots, x_n$ en nombre fini tels que $L = K[x_1, \ldots, x_n]$, alors L est noethérien. (Observer que L est un quotient d'un anneau de polynômes à coefficients dans K).

¶ **28.** Soit K un corps commutatif infini. On rappelle qu'une partie V de K^n est appelée une *variété algébrique* s'il existe un nombre *fini* de polynômes $p_1, \ldots, p_r \in K[X_1, \ldots, X_n]$ tels que V soit l'ensemble des $x \in K^n$ où l'on a $p_1(x) = \cdots = p_r(x) = 0$; et qu'une partie A de K^n est appelée un *ouvert de Zariski* si l'ensemble complémentaire $K^n - A$ est une variété algébrique

(§§ 27, 28, *Exercice* 1). En utilisant le fait que l'anneau $K[X_1, \ldots, X_n]$ est noethérien, démontrer les propriétés suivantes :

a) L'intersection d'une famille (finie ou infinie) de variétés algébriques dans K^n est une variété algébrique dans K^n. Toute réunion (finie ou non) d'ouverts de Zariski est un ouvert de Zariski.

b) Toute suite décroissante de variétés algébriques dans K^n est stationnaire. Toute suite croissante d'ouverts de Zariski est stationnaire.
Montrer en outre qu'on a

c) La réunion d'une famille *finie* de variétés algébriques dans K^n est encore une variété algébrique dans K^n. L'intersection d'une famille *finie* d'ouverts de Zariski est encore un ouvert de Zariski.

d) L'intersection de deux ouverts de Zariski non vides est non vide. Si U et V sont deux variétés algébriques dans K^n, telles que $U \neq K^n$ et $V \neq K^n$, alors on a $U \cup V \neq K^n$.
(On aura intérêt, pour chaque variété algébrique V dans K^n, à introduire l'idéal $I(V) \subset K[X_1, \ldots, X_n]$ formé des polynômes qui sont nuls en tout $x \in V$, et à interpréter en termes d'idéaux les opérations qu'on demande d'effectuer sur les variétés algébriques).

¶¶ **29.** Soit K un anneau commutatif noethérien. Montrer que l'anneau de séries formelle K[[X]] (§§ 27, 28, *Exercice* 11) est noethérien. (Étant donné un idéal I de K[[X]], considérer pour tout $n \geqslant 0$ l'idéal J_n de K formé des coefficients du terme en X^n dans les $f \in I$ qui ne comportent aucun terme de degré $\leqslant n-1$).

¶¶ **30.** Soient V un espace vectoriel de dimension finie sur un corps commutatif K de caractéristique 0, et G un groupe fini, d'ordre r, d'automorphismes de V. On désigne par A l'anneau des fonctions polynomiales sur V (§§ 27, 28, *Exercice* 17; ou bien § 28, n° 2 dans le cas où $V = K^n$, auquel on peut évidemment se ramener).
Étant donnés un $s \in G$ et une fonction polynomiale f sur V, on définit une nouvelle application f_s de V dans K par

$$f_s(x) = f(s^{-1}(x)) \quad \text{pour tout } x \in V.$$

On dit que f est un **invariant** du groupe G si $f_s = f$ pour tout $s \in G$. On note $I \subset A$ l'ensemble de ces invariants, qui est un sous-anneau de A.

a) Montrer qu'on a $f_s \in A$ pour toute $f \in A$ et tout $s \in G$, et que I est un sous-anneau de A.

b) Pour toute fonction polynomiale $f \in A$, on définit la fonction polynomiale

$$f^\natural = \frac{1}{r} \sum_{s \in G} f_s;$$

montrer que $f^\natural$ est un invariant de G. Montrer qu'on a les relations

$$(f+g)^\natural = f^\natural + g^\natural \quad \text{quels que soient } f, g \in A$$
$$f^\natural = f \quad \text{si et seulement si } f \in I$$
$$(fg)^\natural = f^\natural g \quad \text{quels que soient } f \in A \text{ et } g \in I.$$

c) Montrer que si f est un invariant de G, il en est de même de toutes les composantes homogènes de f (*Exercice* 17, §§ 27, 28).

d) Soit J l'idéal de l'anneau A engendré par I. En tenant compte de la question *c*) et du fait que A est noethérien (*Exercices* 14 et 15), montrer qu'il existe dans I des polynômes homogènes

$$f_1, \ldots, f_p$$

le nombre fini qui engendrent J. On pose dans ce qui suit $q_i = d^0(f_i)$.

e) Pour tout $f \in I$ homogène de degré q, montrer qu'il existe des $u_i \in A$ homogènes de degrés $q - q_i$ (on prendra $u_i = 0$ si $q - q_i < 0$) tels que $f = \sum f_i u_i$. Montrer qu'on peut même prendre les u_i dans I (Ecrire que $f = f^\natural$).

f) En raisonnant par récurrence sur le degré de f, déduire de là que *tout* $f \in I$ *est un polynôme en les* f_i, *à coefficients dans* K, autrement dit que les invariants du groupe G forment un anneau engendré sur K par un nombre *fini* d'éléments (*théorème des invariants* de Hilbert).

¶¶ **31.** (La résolution de cet *Exercice* suppose acquis les résultats de l'*Exercice* 21 du § 31). On se propose de démontrer que *si* A *est un anneau factoriel, l'anneau* A[X] *est factoriel.*

a) Étant donnés des polynômes $f, g \in A[X]$, soit p un élément irréductible de A qui divise tous les coefficients de fg; montrer que p divise tous les coefficients de f, ou bien tous ceux de g. (Raisonner comme dans l'*Exercice* 13 du § 27).

b) On dit qu'un polynôme $f \in A[X]$ est **primitif** si le pgcd de ses coefficients est 1. Montrer que si f et g sont primitifs, il en est de même de fg.

c) Pour tout $f \in A[X]$ non nul, on note $c(f)$ un pgcd de ses coefficients. Montrer que

$$c(fg) = c(f)c(g)$$

(lemme de Gauss pour les anneaux factoriels).

d) Soit K le corps des fractions de A. Montrer que si un $f \in A[X]$ n'est pas irréductible dans K[X], il n'est pas non plus irréductible dans A[X].

e) Déduire de là et de la question *a*) que les éléments irréductibles de l'anneau A[X] sont les éléments irréductibles de l'anneau factoriel A, et les polynômes non constants qui sont primitifs, et irréductibles dans l'anneau K[X].

f) Déduire de là et des résultats du § 32, n° 3 (qu'on appliquera à K[X]) que tout élément de A[X] s'écrit, d'une façon essentiellement unique, sous la forme d'un produit d'éléments irréductibles de A[X], et par suite que A[X] est factoriel comme annoncé.

g) Montrer que, si A est un anneau factoriel (par exemple si A est un corps, ou bien si $A = \mathbf{Z}$), l'anneau $A[X_1, \ldots, X_n]$ est factoriel.
En particulier, *tout polynôme* (à n variables) *à coefficients dans un corps* K *se décompose, d'une façon essentiellement unique, en un produit de polynômes irréductibles* à coefficients dans K (un polynôme f à coefficients dans K étant dit **irréductible** s'il est non constant, et si chacun de ses diviseurs est constant, ou est proportionnel à f).

h) Montrer que l'anneau $\mathbf{Z}[X]$ (qui est factoriel d'après ce qui précède) *n'est pas* principal (examiner l'idéal engendré par 2 et X). Même question pour K[X, Y] où K est un corps.

i) Montrer que, pour tout corps commutatif K, le polynôme $Y^2 - X^3$ est irréductible dans l'anneau K[X, Y]. (On écrira K[X, Y] = A[Y] où A = K[X] et on appliquera la question *d*) ci-dessus).

j) Montrer que toute fraction rationnelle f à n variables, à coefficients dans un corps K, peut se mettre sous la forme $f = p/q$ où p et q sont des polynômes à n variables, à coefficients dans K, et premiers entre eux (i.e. n'ayant aucun diviseur commun en dehors des constantes); et que, de plus, p et q sont uniques à des facteurs constants près. Montrer que les points d'indétermination de f sont les éléments de K^n où p et q s'annulent simultanément, et que les pôles de f sont les $x \in K^n$ où l'on a $p(x) \neq 0$ et $q(x) = 0$.

k) Soient p et q deux polynômes non constants à $n \geqslant 2$ indéterminées et à coefficients dans un corps commutatif K. On suppose p et q premiers entre eux; s'ensuit-il qu'il existe des polynômes u et v à n indéterminées, à coefficients dans K, tels que

$$up + vq = 1 \text{ ?}$$

[L'interprétation géométrique du fait que l'anneau $\mathbf{C}[X_1, \ldots, X_n]$, par exemple, est factoriel est la suivante. Soit $f \in \mathbf{C}[X_1, \ldots, X_n]$ non constant et soit V l'hypersurface de $\mathbf{C}^n$ définie

par l'équation $f(x) = 0$. Soit

$$f(X) = \prod_{i=1}^{i=s} p_i(X)^{r_i}$$

la décomposition de f en produit de facteurs irréductibles, et soit V_i l'hypersurface $p_i(x) = 0$. Alors V_i est irréductible (i.e. ne peut pas se représenter de façon non triviale comme réunion de deux autres variétés algébriques), on a

$$V = V_1 \cup \ldots \cup V_s,$$

et cette décomposition de V en hypersurfaces irréductibles est unique à l'ordre près.
On peut encore se placer au point de vue suivant. Soit V une variété algébrique dans $\mathbf{C}^n$ et soit $\mathfrak{a}$ l'idéal de $\mathbf{C}[X_1, \ldots, X_n]$ formé des polynômes f tels que $f(x) = 0$ pour tout $x \in V$. Comme $\mathbf{C}[X_1, \ldots, X_n]$ est noethérien, l'*Exercice* 9, *b*), du § 18 montre que $\mathfrak{a}$ est intersection finie d'idéaux primaires de $\mathbf{C}[X_1, \ldots, X_n]$ (et même d'idéaux *premiers* : appliquer l'*Exercice* 11 du § 18 en remarquant que l'idéal $\mathfrak{a}$ est identique à son radical, attendu que la relation

$$f(x)^q = 0 \text{ sur } V \quad \text{implique} \quad f(x) = 0 \text{ sur } V$$

pour des raisons triviales) ; écrivons donc

$$\mathfrak{a} = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_s$$

où les $\mathfrak{p}_i$ sont les idéaux premiers minimaux de $\mathfrak{a}$, et soit V_i la variété algébrique de $\mathbf{C}^n$ formée des x tels que

$$f(x) = 0 \quad \text{pour tout } f \in \mathfrak{p}_i$$

(V_i est définie par un nombre fini d'équations si l'on veut : prendre des générateurs de $\mathfrak{p}_i$). Comme $\mathfrak{p}_i$ est premier, chaque V_i est irréductible, et l'on a

$$V = V_1 \cup \ldots \cup V_s;$$

on dit que les V_i sont les **composantes irréductibles** de V. Ceci dit, le fait que l'anneau $\mathbf{C}[X_1, \ldots, X_n]$ soit factoriel montre que si V est une hypersurface (i.e. peut être définie par une seule équation) il en est de même de ses composantes irréductibles; ou encore : si une variété *irréductible* W est contenue dans une hypersurface V, il existe une *hypersurface* irréductible W′ telle que $W \subset W' \subset V$, résultat « évident » géométriquement...
Comme autre exemple important d'anneau factoriel, citons (Weierstrass) l'anneau des séries entières *convergentes* (i.e. à domaine de convergence non réduit à 0) à n variables complexes; cet anneau intervient dans l'étude « locale » des « variétés analytiques » dans $\mathbf{C}^n$ (parties de $\mathbf{C}^n$ définies par des équations dont les premiers membres sont des fonctions holomorphes). Cet anneau est aussi noethérien].

¶¶ **32.** Étendre le critère d'irréductibilité d'Eisenstein (*Exercice* 11) aux anneaux factoriels.

§ 33

¶ **1.** Soit G_n l'ensemble des nombres complexes z tels que $z^n = 1$.

a) Montrer que G_n est un sous-groupe d'ordre n du groupe multiplicatif $\mathbf{C}^*$ des nombres complexes non nuls.

b) Soit

$$z = \cos(2k\pi/n) + i.\sin(2k\pi/n)$$

un élément de G_n; pour que z soit un générateur du groupe G_n (i.e. pour que toute racine n^e de l'unité soit une puissance de z) il faut et il suffit que k soit premier à n (on dit alors que z est une **racine primitive** n^e de l'unité).

c) Sans supposer k et n premiers entre eux, montrer que l'**ordre** de z dans le groupe G_n (i.e. le plus petit entier $d \geqslant 1$ tel que $z^d = 1$) est n/pgcd (k, n), et qu'alors z est racine primitive d^e de l'unité.

d) Soit $\varphi(n)$ le nombre des racines primitives n^e de l'unité. Montrer que $\varphi(n)$ est le nombre d'entiers k tels que $1 \leqslant k \leqslant n$ qui sont premiers à n, et que c'est aussi le nombre des éléments inversibles de l'anneau $\mathbf{Z}/n\mathbf{Z}$. Montrer que

$$n = \sum_{d|n} \varphi(d),$$

la somme étant étendue à tous les diviseurs d et n (la notation $d|n$ signifie que d divise n). Montrer que

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \ldots \left(1 - \frac{1}{p_r}\right)$$

où $p_1, \ldots, p_r$ sont les divers diviseurs premiers de n.

e) Classer d'après leur ordre les racines n^e de l'unité pour $n = 2, 3, 4, 6, 8, 12, 16, 20, 24$. Calculer les parties réelles et imaginaires de toutes les racines 24^e de l'unité.

¶ **2.** Soient K un corps commutatif et n un entier tel que l'équation $x^n = 1$ possède n racines dans K. Montrer que le sous-groupe d'ordre n du groupe multiplicatif K* formé par les racines de cette équation est *cyclique* (utiliser l'*Exercice* 20 du § 7).
En déduire que si K est un corps fini à q éléments le groupe multiplicatif K* est cyclique (considérer l'équation

$$x^{q-1} = 1$$

dans K).
En particulier, pour tout nombre premier p, le groupe multiplicatif $(\mathbf{Z}/p\mathbf{Z})^*$ est cyclique.

¶ **3.** Soit K un corps commutatif fini à q éléments. Soient $a_1, \ldots, a_{q-1}$ les éléments non nuls de K. Montrer que si X désigne une indéterminée sur K on a

$$(X - a_1)\ldots(X - a_{q-1}) = X^{q-1} - 1$$

(utiliser le Théorème 1 du § 33). En déduire que

$$a_1 \ldots a_{q-1} = -1$$

(on utilisera, pour déterminer le signe, le fait que q est une puissance de la caractéristique p de K : § 30, *Exercice* 8).
En prenant $K = \mathbf{Z}/p\mathbf{Z}$, déduire de là le théorème de Wilson, à savoir que

$$(p-1)! \equiv -1 \pmod{p}$$

pour tout nombre premier p.

¶ **4.** Soient p un nombre premier et r un entier ; on dit qu'un entier n premier à p est une **puissance r^e modulo p** (si $r = 2$, on dit un **reste quadratique** modulo p) s'il existe des entiers x tels que l'on ait

$$x^r \equiv n \pmod{p}.$$

En utilisant le fait que le groupe multiplicatif $(\mathbf{Z}/p\mathbf{Z})^*$ est cyclique (*Exercice* 2) montrer que tout n premier à p est une puissance r^e modulo p si r est premier à $p-1$. Si r divise $p-1$ (exemple : $r = 2$ et p impair, cas le plus important), pour qu'un entier n premier à p soit puissance r^e modulo p il faut et il suffit que

$$n^{\frac{p-1}{r}} \equiv 1 \pmod{p}.$$

Les classes modulo p des puissances r^e mod p sont alors en nombre égal à $\frac{p-1}{r}$ (par exemple si p est impair il y a $\frac{p-1}{2}$ restes quadratiques modulo p).
On prend $p = 31$. Pour chaque diviseur r de $p - 1 = 30$, trouver les puissances r^e modulo p.

¶ **5.** (Cet Exercice repose sur l'*Exercice* 1). Pour tout entier $n \geqslant 1$, on appelle **polynôme cyclotomique** d'indice n le polynôme

$$\Phi_n(X) = (X - \xi_1) \ldots (X - \xi_h)$$

dont les racines sont les $h = \varphi(n)$ racines *primitives* n^e de l'unité dans le corps $\mathbf{C}$; ce polynôme est, en apparence, à coefficients dans $\mathbf{C}$, mais on va montrer qu'en fait il est à coefficients *entiers rationnels*. On convient de poser $\Phi_1(X) = X - 1$.
a) Montrer que

$$\Phi_p(X) = 1 + X + X^2 + \cdots + X^{p-1}$$

si p est premier.
b) Vérifier que

$$\Phi_{12}(X) = X^4 - X^2 + 1.$$

c) Montrer que, pour tout entier $n \geqslant 1$, on a

$$X^n - 1 = \prod_{d|n} \Phi_d(X)$$

où le produit figurant au second membre est étendu à tous les diviseurs d de n (y compris 1 et n). (Utiliser la décomposition du polynôme $X^n - 1$ en produit de facteurs du premier degré).
d) En utilisant la relation

$$\Phi_n(X) = \frac{X^n - 1}{\prod_{\substack{d|n \\ d \neq n}} \Phi_d(X)}$$

et en raisonnant par récurrence sur n, montrer que Φ_n est à coefficients entiers rationnels.
(Ces résultats s'étendent à tout corps algébriquement clos K, pourvu qu'on se limite aux entiers n qui ne sont pas divisibles par la caractéristique p de K, restriction qui n'en est d'ailleurs pas une en vertu du § 30, *Exercice* 14).

¶¶ **6.** Montrer qu'il existe, sur l'ensemble des entiers $n \geqslant 1$, une et une seule fonction μ (**fonction de Möbius**) à valeurs entières, vérifiant la relation

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n > 1 \end{cases}$$

(la somme est étendue aux diviseurs d de n tels que $1 \leqslant d \leqslant n$).
Montrer qu'on a

$$\mu(1) = 1$$
$$\mu(p) = -1 \quad \text{si } p \text{ est premier}$$
$$\mu(p^r) = 0 \quad \text{si } p \text{ est premier et si } r \geqslant 2.$$

Montrer qu'on a

$$(*) \qquad \mu(mn) = \mu(m)\,\mu(n) \quad \text{si } m \text{ et } n \text{ sont premiers entre eux}$$

(on observera que tout diviseur de mn, lorsque m et n sont premiers entre eux, s'écrit d'une façon et d'une seule comme produit d'un diviseur de m et d'un diviseur de n ; on raisonnera alors par récurrence en supposant (*) déjà établi pour les couples m', n' tels que $m'n' < mn$).
Déduire des résultats précédents que l'on a

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1 \\ (-1)^r & \text{si } n \text{ est produit de } r \text{ facteurs premiers distincts} \\ 0 & \text{si } n \text{ est divisible par le carré d'un nombre premier.} \end{cases}$$

Calculer $\mu(n)$ pour $1 \leqslant n \leqslant 100$.

¶¶ **7.** Soit f une fonction sur l'ensemble des entiers $n \geqslant 1$, et à valeurs dans un groupe additif A. On définit une nouvelle fonction g en posant

$$g(n) = \sum_{d|n} f(d)$$

où la somme est étendue aux diviseurs d de n tels que $1 \leqslant d \leqslant n$. Montrer qu'on a inversement

$$f(n) = \sum_{d|n} g(d)\,\mu\left(\frac{n}{d}\right)$$

où μ est la fonction de Möbius de l'*Exercice* précédent. (On utilisera exclusivement la propriété ayant servi à définir μ).

Comment modifier les formules précédentes si A est un groupe commutatif écrit multiplicativement?

¶¶ 8. (Cet Exercice repose sur les *Exercices* 5, 6 et 7). Montrer que les polynômes cyclotomiques sont donnés par la relation

$$\Phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu\left(\frac{n}{d}\right)}.$$

Calculer les polynômes Φ_n pour $n = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 15$, et montrer que

$$\begin{aligned}\Phi_{105}(X) = {} & X^{48} + X^{47} + X^{46} - X^{43} - X^{42} - 2X^{41} - X^{40} - X^{39} + X^{36} + X^{35} + X^{34} + X^{33} \\ & + X^{32} + X^{31} - X^{28} - X^{26} - X^{24} - X^{22} - X^{20} + X^{17} + X^{16} + X^{15} + X^{14} + X^{13} \\ & + X^{12} - X^9 - X^8 - 2X^7 - X^6 - X^5 + X^2 + X + 1,\end{aligned}$$

en supposant que Faddeev et Sominskii aient raison, ce que l'auteur n'a pas vérifié...

9. Décomposer en éléments simples complexes la fraction rationnelle

$$\frac{f(X)}{X^n - 1}$$

où f est un polynôme quelconque à coefficients complexes.

¶ 10. Soient $z_1, \ldots, z_n$ les racines n^e de l'unité dans $\mathbf{C}$. Montrer qu'on a

$$z_1^h + \ldots + z_n^h = \begin{cases} n & \text{si } h \equiv 0 \pmod{n} \\ 0 & \text{si } h \not\equiv 0 \pmod{n} \end{cases}$$

(multiplier le premier membre par z_1^h).

11. On désigne par $z_1, \ldots, z_n$ les racines n^e de l'unité dans $\mathbf{C}$. Démontrer les relations suivantes :

$$\prod_{k=1}^{k=n} (a + bz_k) = a^n + (-1)^{n-1} b^n$$

$$\prod_{k=1}^{k=n} (z_k^2 - 2z_k \cos\theta + 1) = 2(1 - \cos n\theta)$$

$$\prod_{k=1}^{k=n} \frac{(t + z_k)^n - 1}{t} = \prod_{k=1}^{k=n-1} [t^n - (z_k - 1)^n].$$

12. Soient u, v, w les trois racines (distinctes ou non) d'une équation

$$ax^3 + bx^2 + cx + d = 0$$

de degré 3 à coefficients complexes. En utilisant les résultats du § 33, n° 6, *Exemple 4*, calculer à l'aide de a, b, c, d les expressions

$$u^3 + v^3 + w^3, \qquad u^5 + v^5 + w^5,$$

¶ 13. Soient $X_1, \ldots, X_n$ des indéterminées sur un anneau commutatif K. On appelle **fonctions symétriques élémentaires** de $X_1, \ldots, X_n$ les polynômes

$$\begin{aligned} s_1 &= X_1 + X_2 + \cdots + X_n = \Sigma X_i \\ s_2 &= X_1X_2 + \cdots + X_{n-1}X_n = \sum_{1 \leqslant i < j \leqslant n} X_iX_j \\ s_3 &= X_1X_2X_3 + \cdots = \sum_{1 \leqslant i < j < k \leqslant n} X_iX_jX_k \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ s_n &= X_1X_2 \ldots X_n \end{aligned}$$

(ces expressions interviennent, cf. n° 6 du § 33, dans le calcul des coefficients d'une équation algébrique en fonction de ses racines). D'autre part, on dit qu'un polynôme $f \in K[X_1, \ldots, X_n]$ est **symétrique** si l'on a

$$f(X_{s(1)}, \ldots, X_{s(n)}) = f(X_1, \ldots, X_n)$$

pour toute permutation s des entiers $1, \ldots, n$.

a) Démontrer que *tout polynôme symétrique* $f(X_1, \ldots, X_n)$ *est un polynôme en* $s_1, \ldots, s_n$ *à coefficients dans* K. [On pourra procéder par récurrence sur l'entier $n + d^o(f)$. Observer d'abord que $f(X_1, \ldots, X_{n-1}, 0)$ est symétrique en $X_1, \ldots, X_{n-1}$, donc est un polynôme en les fonctions symétriques élémentaires de $X_1, \ldots, X_{n-1}$, lesquelles s'obtiennent en remplaçant X_n par 0 dans les fonctions symétriques élémentaires de $X_1, \ldots, X_n$. En déduire qu'il existe un polynôme $p(s_1, \ldots, s_{n-1})$, de degré au plus égal au degré de f, tel que le polynôme

$$g(X_1, \ldots, X_n) = f(X_1, \ldots, X_n) - p(s_1, \ldots, s_{n-1})$$

s'annule pour $X_n = 0$; en déduire, compte-tenu de la symétrie de g, que

$$g(X_1, \ldots, X_n) = X_1 \ldots X_n h(X_1, \ldots, X_n)$$

avec h symétrique et $d^o(h) < d^o(f)$].

b) Démontrer que si un polynôme $p \in K[X_1, \ldots, X_n]$ vérifie $p(s_1, \ldots, s_n) = 0$, alors $p = 0$ (raisonner par récurence sur n; prendre p de plus petit degré possible par rapport à s_n et faire $X_n = 0$ dans le résultat).

c) En conclure que *l'expression d'un polynôme symétrique* f *à l'aide de* $s_1, \ldots, s_n$ *est unique.*

d) On suppose f homogène de degré total k en $X_1, \ldots, X_n$, et on pose

$$f(X_1, \ldots, X_n) = p(s_1, \ldots, s_n);$$

montrer que les seuls monômes

$$s_1^{r_1} \ldots s_n^{r_n}$$

figurant effectivement dans p sont ceux pour lesquels on a

$$r_1 + 2r_2 + \cdots + nr_n = k.$$

e) Calculer à l'aide des fonctions symétriques élémentaires les polynômes suivants :

$$X_1^2X_2 + X_1X_2^2 + X_1^2X_3 + X_1X_3^2 + X_2^2X_3 + X_2X_3^2 \quad (n = 3)$$

$$(2X_1 - X_2 - X_3)(2X_2 - X_1 - X_3)(2X_3 - X_1 - X_2) \quad (n = 3)$$

$$(X_1X_2 + X_3X_4)(X_1X_3 + X_2X_4)(X_1X_4 + X_2X_3) \quad (n = 4)$$

$$\sum_{i \neq j} X_i^2X_j; \qquad \sum_{i \neq j \neq k} X_i^2X_jX_k; \qquad \sum_{i \neq j \neq k} X_iX_jX_k; \qquad \sum_{s \in \mathfrak{S}_n} (a_1X_{s(1)} + a_2X_{s(2)} + \cdots + a_nX_{s(n)})^3;$$

$$\sum_{\substack{i \geqslant k \\ j \neq k \\ i, j \neq k}} (X_i + X_k - X_j)^3 \quad (n \text{ quelconque}).$$

¶ **14.** Les notations étant celles de l'*Exercice* précédent, on considère les **sommes de Newton**

$$\sigma_k(X_1, \ldots, X_n) = X_1^k + X_2^k + \cdots + X_n^k \quad (k = 0, 1, \ldots)$$

Montrer qu'on peut les exprimer en fonction de $s_1, \ldots, s_n$ à l'aide des formules suivantes :

$$\sigma_k - s_1\sigma_{k-1} + s_2\sigma_{k-2} - \cdots + (-1)^{k-1}s_{k-1}\sigma_1 + (-1)^k s_k\sigma_0 = 0 \quad \text{pour } k < n$$
$$\sigma_k - s_1\sigma_{k-1} + \cdots + (-1)^n s_n\sigma_{k-n} = 0 \quad \text{pour } k \geqslant n.$$

Calculer complètement, à l'aide des fonctions symétriques élémentaires, les sommes de Newton σ_k pour $0 \leqslant k \leqslant 6$.

¶ **15.** Soit

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

une équation algébrique à coefficients dans un corps commutatif K. Soient $x_1, \ldots, x_n$ ses racines dans une extension algébriquement close de K (on pourra prendre **C** en supposant que K est un sous-corps de **C**, mais bien entendu cette hypothèse ne simplifie rien !). Soit f un polynôme symétrique à n indéterminées, à coefficients dans K. Montrer qu'il existe un polynôme p à n indéterminées, à coefficients dans K, tel que l'on ait

$$f(x_1, \ldots, x_n) = p(a_{n-1}, \ldots, a_0)$$

et que p ne dépend que de f (utiliser l'*Exercice* 13). Applications :

a) Calculer la somme des puissances 5e des racines de l'équation

$$x^6 - 4x^5 + 3x^3 - 4x^2 + x + 1 = 0.$$

b) Calculer la somme

$$\sum x_i^2 x_j^2 x_k x_h$$

où $x_1, \ldots, x_5$ désignent les racines de l'équation

$$x^5 - 4x^3 + x^2 + 3x + 1 = 0.$$

c) On désigne par x_1, x_2, x_3 les racines de l'équation

$$x^3 + ax^2 + bx + c = 0;$$

former les équations dont les racines sont les quantités suivantes :

i) $x_1 + x_2, x_2 + x_3, x_3 + x_1$;

ii) $x_1^2 - x_2x_3, x_2^2 - x_3x_1, x_3^2 - x_1x_2$

iii) $(x_1 + jx_2 + j^2x_3)^3$, $(x_1 + j^2x_2 + jx_3)^3$ où $j = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$.

¶ **16.** Soit

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

une équation algébrique à coefficients dans un corps commutatif K. On désigne par $x_1, \ldots, x_n$ ses racines (distinctes ou non) dans une extension algébriquement close de K. On appelle **discriminant** de l'équation donnée l'expression

$$D = \prod_{1 \leqslant i < j \leqslant n} (x_i - x_j)^2,$$

a) Montrer qu'il existe un polynôme p à n indéterminées, à coefficients dans K, et indépendant de l'équation (*), tel que l'on ait

$$D = p(a_{n-1}, \ldots, a_0).$$

b) Calculer le discrimimant d'une équation de degré 2, 3 ou 4.

c) Pour que l'équation (*) possède au moins une racine double, il faut et il suffit que son discriminant soit nul.

d) Déterminer les valeurs de λ pour lesquelles les équations suivantes possèdent au moins une racine double :

$$x^3 - 3x + \lambda = 0; \qquad x^3 - 8x^2 + (13 - \lambda)x - 6 - 2\lambda = 0;$$
$$x^4 - 4x^3 + (2 - \lambda)x^2 + 2x - 2 = 0.$$

¶¶ *e*) Montrer que le discriminant de l'équation

$$x^n + px + q = 0$$

est égal à

$$(-1)^{\frac{n(n-1)}{2}} n^n q^{n-1} + (-1)^{\frac{(n-1)(n-2)}{2}} (n-1)^{n-1} p^n.$$

f) On désigne par f le polynôme figurant au premier membre de l'équation (*). Montrer que le discriminant D de l'équation (*) est encore donné par la formule

$$(-1)^{\frac{n(n-1)}{2}} D = \prod_{1 \leqslant i \leqslant n} f'(x_i).$$

g) Montrer que le discriminant de l'équation

$$\frac{x^n}{n!} + \frac{x^{n-1}}{(n-1)!} + \cdots + 1 = 0$$

est égal à

$$(-1)^{\frac{n(n-1)}{2}}.$$

¶¶ *h*) On considère (*Exercice* 5) l'équation cyclotomique

$$\Phi_n(x) = 0.$$

Montrer que son discriminant est égal à

$$(-1)^{\frac{\varphi(n)}{2}} \frac{n^{\varphi(n)}}{\prod_{p|n} p^{\frac{\varphi(n)}{p-1}}}$$

(utiliser la question (*f*) et l'*Exercice* 8).

¶ **20.** Soient K un corps commutatif et f un polynôme à une indéterminée, à coefficients dans K. On se propose de prouver qu'il existe un corps L, extension de K (i.e. dont K est un sous-corps), dans lequel f admet au moins une racine (ce résultat est le premier pas dans la démonstration du théorème de Steinitz).

a) Montrer qu'on peut se ramener au cas où f est irréductible sur K.

b) Dans l'anneau de polynôme $A = K[X]$, on considère l'idéal $I = (f)$ engendré par f et on forme l'anneau quotient $L = A/I$ (§ 8, *Exercice* 7). Montrer que c'est un corps.

c) Soit j l'application de K dans L qui, à chaque $c \in K$, associe la classe mod I du polynôme constant c. Montrer que c'est un isomorphisme de K sur un sous-corps de L (dans ce qui suit, on convient d'identifier chaque $c \in K$ à son image $j(c)$ dans L).

d) Soit $z \in L$ l'image du polynôme X par l'application canonique de K[X] sur L. Montrer que z est racine de f, et que $L = K[z]$. (Ce qui démontre le résultat annoncé).

e) On prend $f(X) = X^2 - d$ où $d \in K$ n'est pas un carré dans K. Montrer que les constructions précédentes se réduisent alors à celles du § 9. On vérifiera en particulier que le corps $\mathbf{C}$ est le quotient de l'anneau $\mathbf{R}[X]$ par l'idéal engendré par le polynôme $X^2 + 1$ (cette méthode de construction de $\mathbf{C}$ est due à Cauchy).

f) On prend $f(X) = X^3 + pX + q$, supposé irréductible sur K. Donner du corps L correspondant une description analogue à celle qu'on a donnée au § 9 pour les anneaux $K[\sqrt{d}]$.

g) Que se passe-t-il, dans les constructions précédentes, si le polynôme f n'est pas irréductible?

¶¶ **21.** Soient $f_1, \ldots, f_n$ des polynômes non constants à une indéterminée à coefficients dans un corps commutatif K. Montrer qu'il existe dans l'anneau $K[X_1, \ldots, X_n]$ un idéal maximal qui contient $f_1(X_1), \ldots, f_n(X_n)$ (utiliser l'*Exercice* 15 du § 27). En raisonnant comme dans l'*Exercice* précédent, en déduire l'existence d'une extension algébrique L de K dans laquelle chaque f_i possède au moins une racine.
(La démonstration complète du théorème de Steinitz est une extension directe du raisonnement de cet *Exercice*; on introduit un anneau de polynômes à une infinité de variables, comportant autant (sic) de variables qu'il y a de polynômes irréductibles à coefficients dans K et de coefficient dominant égal à 1, puis on prend le quotient de cet anneau par un idéal maximal bien choisi)

¶ **22.** Les notations restant celles de l'*Exercice* précédent, montrer que tout idéal premier de l'anneau $K[X_1, \ldots, X_n]$ contenant $f_1(X_1), \ldots, f_n(X_n)$ est maximal (cf. § 26, *Exercice* 3).

¶ **23.** Soit K un corps commutatif. On dit qu'une extension L de K (i.e. un corps commutatif admettant K pour sous-corps) est **algébrique** si tout $x \in L$ est algébrique sur K. Montrer que, pour que K soit algébriquement clos, il faut et il suffit qu'on ait $L = K$ pour toute extension algébrique de K.

24. Un corps algébriquement clos possède toujours une infinité d'éléments.

¶ **25.** (Démonstration du théorème de d'Alembert-Gauss). Cet *Exercice* suppose connues les propriétés des fonctions continues dans le plan (en particulier et tout spécialement le fait qu'une fonction continue positive sur un ensemble compact y atteint effectivement son minimum). On désigne par

$$f(z) = a_0 + \cdots + a_n z^n$$

un polynôme non constant à coefficients complexes; on suppose $a_n \neq 0$.

a) Montrer que le rapport

$$f(z)/a_n z^n$$

tend vers 1 quand $|z|$ augmente indéfiniment, i.e. que pour tout $\varepsilon > 0$ il existe $r > 0$ tel que

$$|z| > r \quad \text{implique} \quad \left| 1 - \frac{f(z)}{a_n z^n} \right| < \varepsilon.$$

b) Soit

$$m = \inf_{z \in \mathbf{C}} |f(z)|;$$

montrer qu'il existe un nombre $r' > 0$ tel que

$$|z| \geqslant r' \quad \text{implique} \quad |f(z)| \geqslant m + 1.$$

En appliquant le théorème du minimum à la fonction continue $|f(z)|$ sur l'ensemble compact $|z| \leqslant r'$, montrer qu'il existe un $z_0 \in \mathbf{C}$ tel que

$$|f(z_0)| = m.$$

[Si le théorème de d'Alembert est vrai, il est clair que $m = 0$; pour montrer que le théorème en question est vrai, il est donc nécessaire, et bien entendu suffisant, de montrer que $m = 0$. C'est le but de la question suivante.]

c) On suppose $m \neq 0$; en remplaçant z par $z - z_0$ et f par $f/f(z_0)$ on se ramène au cas où l'on a

$$f(0) = 1, \qquad |f(z)| \geqslant 1 \qquad \text{pour tout} \quad z \in \mathbf{C}.$$

Soit

$$f(z) = 1 + b_q z^q + b_{q+1} z^{q+1} + \cdots + b_n z^n \qquad \text{avec} \qquad b_q \neq 0;$$

montrer qu'il existe un nombre $M > 0$ tel que

$$|z| \leqslant 1 \quad \text{implique} \quad |f(z) - 1 - b_q z^q| \leqslant M.|z|^{q+1};$$

déduire de là qu'on a $|f(z)| < 1$ (contradiction avec l'hypothèse, ce qui achèvera la démonstration) pourvu que z soit choisi de telle sorte qu'on ait

$$|z| \leqslant 1, \qquad |z| < |b_q|/M, \qquad \operatorname{Arg}(b_q) + q.\operatorname{Arg}(z) = \pi.$$

¶¶ **26.** Soient E un corps commutatif algébriquement clos, L un corps commutatif quelconque, et σ un isomorphisme de L sur un sous-corps L' de E. On considère une extension M de L et on suppose $M = L[z]$ où z est algébrique sur L. Soit

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$$

le polynôme minimal de z sur L; on note

$$f^\sigma(X) = X^n + \sigma(a_{n-1})X^{n-1} + \cdots + \sigma(a_0)$$

le polynôme, à coefficients dans L', qui s'en déduit par σ, et on considère une racine z' de f^σ dans E; soit $M' = L'[z']$. Montrer qu'il existe un et un seul isomorphisme σ' de M sur M' qui coïncide avec σ sur L, et applique z sur z'.
Déduire de là le résultat suivant : soient E une extension algébriquement close d'un corps commutatif K, et L une extension de degré fini de K. Alors il existe un isomorphisme j de L sur un sous-corps de E, tel que $j(x) = x$ pour tout $x \in K$. (Raisonner par récurence sur le degré de L sur K. On peut en fait démontrer que le résultat subsiste pour toute extension *algébrique*, de degré fini ou non, de K).

¶¶ **27.** Soient K un corps commutatif, E une extension algébriquement close de K, et L une extension de degré fini de K; on suppose L *séparable sur* K (§ 26, *Exercice* 4, *h*)) et on pose $n = [L : K]$. Montrer que le nombre d'isomorphismes j de L dans E, tels que $j(x) = x$ pour tout $x \in K$, est exactement n (raisonner comme dans l'*Exercice* 26 en utilisant l'*Exercice* 11 du § 32).
On désigne par $j_1, \ldots, j_n$ les isomorphismes en question. Pour $k \neq h$, on note L_{kh} l'ensemble des $z \in L$ tels que $j_k(z) = j_h(z)$; montrer que c'est un sous-corps de L contenant K, et distinct de L.

On suppose K *infini*; montrer que la réunion des L_{kh} n'est pas L tout entier et qu'il existe un $z \in L$ tel que les n éléments $j_h(z)$ soient deux à deux distincts. En déduire que si L est une extension séparable de degré fini d'un corps K infini, il existe un $z \in L$ tel que $L = K[z]$ (**théorème de l'élément primitif**, démontré d'abord par Dedekind pour les corps de nombres algébriques, i.e. pour $K = \mathbf{Q}$; en fait, il est encore valable pour K fini vu l'*Exercice* 2 ci-dessus).

¶ **28.** On considère l'extension

$$L = \mathbf{Q}[\sqrt{3}, \sqrt[3]{2}]$$

de $\mathbf{Q}$. Construire un nombre algébrique z tel que $L = \mathbf{Q}[z]$.

¶¶ **29.** Soient K un corps commutatif, L une extension séparable et de degré fini n de K, E une extension algébriquement close de K, et $j_1, \ldots, j_n$ les n isomorphismes de L dans E tels que $j_h(x) = x$ pour tout $x \in K$ (*Exercice* 27). On se propose de montrer que

$$\mathrm{Tr}_{L/K}(z) = j_1(z) + \cdots + j_n(z)$$
$$\mathrm{N}_{L/K}(z) = j_1(z) \ldots j_n(z)$$

pour tout $z \in L$.

a) Soit $(a_i)_{1 \leqslant i \leqslant n}$ une base de L sur K. Montrer que la matrice

$$A = (j_k(a_h))_{1 \leqslant k,\, h \leqslant n}$$

(à coefficients dans E) est inversible (utiliser l'*Exercice* 16 des §§ 10, 11 ainsi que la caractérisation des systèmes de Cramer).

b) Pour tout $z \in L$ on pose

$$z a_i = \sum_j \xi_{ij} a_j$$

avec des $\xi_{ij} \in K$; on introduit les matrices

$$U_z = (\xi_{ij})_{1 \leqslant i,\, j \leqslant n}$$

et

$$D_z = \begin{pmatrix} j_1(z) & 0 & \ldots & 0 \\ 0 & j_2(z) & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & j_n(z) \end{pmatrix};$$

montrer qu'on a la relation

$$U_z = A D_z A^{-1}.$$

c) Achever la démonstration en observant que $\mathrm{Tr}_{L/K}(z) = \mathrm{Tr}(U_z)$ et que $\mathrm{N}_{L/K}(z) = \det(U_z)$ (cf. § 26, *Exercice* 4).

[Le lecteur notera que ce raisonnement montre aussi que les valeurs propres dans E de l'endomorphisme

$$u_z : x \to zx$$

de L, où l'on regarde L comme un espace vectoriel de dimension n sur K, sont précisément les $j_k(z)$, $1 \leqslant k \leqslant n$].

30. Démontrer que le polynôme

$$X^{n_1} + X^{n_2} + \ldots + X^{n_k},$$

où

$$n_r \equiv r - 1 \pmod{k},$$

est divisible par le polynôme

$$1 + X + X^2 + \cdots + X^{k-1}.$$

¶ **31.** Pour quelles valeurs de r le polynôme $\Phi_n(X^r)$ est-il divisible par le polynôme $\Phi_n(X)$?

32. Soit f un polynôme à une indéterminée à coefficients dans un corps commutatif. Si $f(X^n)$ est divisible par $X - 1$, alors $f(X^n)$ est divisible par $X^n - 1$.

¶¶ **33.** (Démonstration du Nullstellensatz de Hilbert).

a) Soient L un corps commutatif et A un sous-anneau de L; on suppose qu'il existe des éléments $y_1, \ldots, y_q$ de L, en nombre fini, tels que

$$L = A[y_1, \ldots, y_q],$$

et de plus que chaque y_j vérifie une relation algébrique non triviale à coefficients dans A. Montrer qu'il existe un élément $b \neq 0$ de A tel que

Kcorps des fractions de A $K = A[b^{-1}]$

(choisir b de telle sorte que L soit un $A[b^{-1}]$-module de type fini et appliquer l'*Exercice* 24 du § 19).

b) Montrer que tout idéal premier non nul de l'anneau A contient b.

c) On suppose qu'il existe un sous-corps K de L tel que A soit le sous-anneau de L engendré par K et par un nombre fini d'éléments de L algébriquement indépendants sur K. Montrer qu'alors $A = K$ et que L est une extension algébrique de degré fini de K (observer que, dans un anneau de polynômes sur un corps, l'intersection des idéaux premiers non nuls se réduit à 0).

d) Soient K un corps commutatif et L une extension de K; on suppose qu'il existe un nombre fini d'éléments $z_1, \ldots, z_r$ de L tels que

$$L = K[z_1, \ldots, z_r];$$

montrer qu'alors L est une extension algébrique de degré fini de K, et qu'en particulier $L = K$ si K est algébriquement clos [extraire de la famille $z_1, \ldots, z_r$ les éléments algébriquement indépendants en nombre aussi grand que possible et appliquer *c*) à l'anneau A engendré par K et ces éléments].

e) Soient K un corps commutatif et $\mathfrak{m}$ un idéal maximal de l'anneau de polynômes $K[X_1, \ldots, X_r]$; montrer que l'anneau quotient $L = K[X_1, \ldots, X_r]/\mathfrak{m}$ est un corps, extension algébrique de degré fini de K [appliquer la question *d*), et l'*Exercice* 7 du § 8]. En déduire le Nullstellensatz [Voir une autre démonstration au § 35, *Exercice* 51].

¶¶ **34.** Soit p un nombre premier et soit $k = \mathbf{Z}/p\mathbf{Z}$ le corps des entiers modulo p. Si

$$f(X) = f(X_1, \ldots, X_n)$$

est un polynôme en n variables, à coefficients dans k, on note $S(f)$ la somme des valeurs de f, autrement dit on pose

$$S(f) = \sum_{x_i \in k} f(x_1, \ldots, x_n).$$

a) On suppose que f est un monôme $X_1^{m_1} \ldots X_n^{m_n}$. Montrer que l'on a alors $S(f) = 0$,

sauf si tous les m_i sont divisibles par $p-1$ et $\geqslant 1$, auquel cas on a $S(f) = (-1)^n$. (Se ramener au cas d'une variable.)

b) Utiliser *a*) pour prouver que $S(f) = 0$ si $\deg(f) < n(p-1)$.

c) Soit $\varphi(X) = \varphi(X_1, \ldots, X_n)$ un polynôme à coefficients dans k. On pose

$$f(X) = 1 - \varphi(X)^{p-1}.$$

Montrer que l'on a

$$f(x) = 1 \quad \text{si} \quad \varphi(x) = 0, \qquad x \in k^n$$
$$f(x) = 0 \quad \text{si} \quad \varphi(x) \neq 0, \qquad x \in k^n.$$

En déduire que le nombre $N(\varphi)$ de zéros de φ dans k^n vérifie la congruence

$$N(\varphi) \equiv S(f) \pmod{p}.$$

d) On suppose que $\deg(\varphi) < n$. Déduire de *b*) et *c*) que l'on a $N(\varphi) \equiv 0 \pmod{p}$. En particulier, si φ est sans terme constant, φ a au moins un zéro distinct de $(0, \ldots, 0)$ (*théorème de Chevalley*).

e) Étendre ce qui précède au cas d'un nombre fini d'équations $\varphi_\alpha(x) = 0$, avec $\Sigma \deg \varphi_\alpha < n$. (Prendre pour f le produit des $1 - \varphi_\alpha^{p-1}$.)