ALGÈBRE COMMUTATIVE

Cours à l'Université de Rennes 1 (2006–2007)

Antoine Chambert-Loir

Antoine Chambert-Loir
IRMAR, Université de Rennes 1, Campus de Beaulieu, 35042 Rennes Cedex.
E-mail : antoine.chambert-loir@univ-rennes1.fr
Url : http://perso.univ-rennes1.fr/antoine.chambert-loir

Version du 9 octobre 2006
La version la plus à jour est disponible sur le Web à l'adresse http://perso.univ-rennes.fr/antoine.chambert-loir/2006-07/g1/

Mais je ne m'arrête point à expliquer ceci plus en détail, à cause que je vous ôterais le plaisir de l'apprendre par vous-même, et l'utilité de cultiver votre esprit en vous exerçant...

René Descartes (1596-1659)

TABLE DES MATIÈRES

CHAPITRE 1

ANNEAUX, IDÉAUX, ALGÈBRES

Ce chapitre introduit les notions d'anneaux et d'idéaux. Ces deux notions formalisent les méthodes de calcul bien connues avec les nombres entiers ou les matrices : on dispose d'une addition, d'une multiplication, de deux symboles 0 *et* 1 *et des règles de calcul usuelles.*

§1.1. Premières définitions

DÉFINITION 1.1.1. — *On appelle anneau un groupe abélien A noté additivement muni d'une loi de multiplication $A \times A \to A$, $(a,b) \mapsto ab$ vérifiant les propriétés suivantes :*

– *il existe un élément $1 \in A$ tel que pour tout $a \in A$, $1a = a1 = a$ (élément neutre pour la multiplication) ;*

– *pour tous a, b et c dans A, $(ab)c = a(bc)$ (associative) ;*

– *pour tous a, b et c dans A, $a(b+c) = ab + ac$ et $(b+c)a = ba + ca$ (distributivité de la multiplication sur l'addition).*

On dit que l'anneau A est commutatif si de plus

– *pour tous a et b dans A, $ab = ba$ (commutativité).*

Comme exemples évidents d'anneaux commutatifs, citons $\mathbf{Z}$, $\mathbf{Z}/n\mathbf{Z}$ pour $n \geqslant 1$, les corps $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, l'anneau $K[X]$ des polynômes à une indéterminée à coefficients dans un corps (voire un anneau commutatif) K. Si A est un anneau, l'ensemble des fonctions d'un ensemble S dans un anneau A muni des lois évidentes ($(f+g)(s) = f(s) + g(s)$ et $(fg)(s) = f(s)g(s)$) est un anneau. L'ensemble des fonctions continues d'un espace topologique dans $\mathbf{R}$ est un anneau, de même l'ensemble des fonctions de classe $\mathscr{C}^k$ d'un ouvert de $\mathbf{R}^n$ dans $\mathbf{R}$ ou $\mathbf{C}$ ($k \in \mathbf{N} \cup \{\infty\}$).

Voici des exemples non commutatifs bien connus :

Exemples 1.1.2. — a) Soit A un anneau et soit $\mathrm{M}_n(A)$ l'ensemble des matrices $n \times n$ à coefficients dans A muni des règles de calcul habituelles : la somme de deux matrices

est obtenue en ajoutant terme à terme, le produit des matrices $P = (p_{i,j})$ et $Q = (q_{i,j})$ est la matrice $R = (r_{i,j})$ dont le terme (i, j) est donné par

$$r_{i,j} = \sum_{k=1}^{n} p_{i,k} q_{k,j}.$$

Si $n \geqslant 2$, ou si A n'est pas commutatif, l'anneau $\mathrm{M}_n(A)$ n'est pas commutatif.

b) Si K est un corps (pour l'instant commutatif), l'ensemble $\mathrm{End}_K(V)$ des endomorphismes d'un K-espace vectoriel V est un anneau, non commutatif dès que $\dim V \geqslant 2$. En fait, $\mathrm{End}_K(V)$ est aussi un K-espace vectoriel et sa multiplication est K-linéaire. On dit que c'est une *K-algèbre*.

c) Soit G un groupe abélien. Si φ et ψ sont deux endomorphismes de G, l'application $g \mapsto \varphi(g) + \psi(g)$ est encore un endomorphisme de G qu'on note $\varphi + \psi$; cela munit $\mathrm{End}(G)$ d'une structure de groupe commutatif, d'élément neutre l'application $g \mapsto 0$. La composition des endomorphismes $(\varphi, \psi) \mapsto \varphi \circ \psi$ est une loi associative et distributive par rapport à l'addition ; l'application identique de G en est un élément neutre. Ces lois munisent ainsi l'ensemble $\mathrm{End}(G)$ des endomorphismes du groupe abélien G d'un structure d'anneau.

Voici un exemple un peu moins connu.

Exemple 1.1.3. — Soit A un anneau et soit G un groupe. Le groupe abélien $A^{(G)}$ des fonctions de G dans A de support fini est muni d'un produit de convolution défini par la formule

$$(\varphi * \psi)(g) = \sum_{h \in G} \varphi(h)\psi(h^{-1}g).$$

Le produit de convolution est bien défini : la somme est finie, et la convolée de deux fonctions de support fini est encore de support fini. En outre, le produit de convolution est associatif, l'élément neutre est la fonction (« de Dirac ») qui vaut 1 en l'élément neutre de G et 0 ailleurs. Cela munit $A^{(G)}$ d'une structure d'anneau. Surtout lorsque A est un anneau commutatif, on l'appelle l'*algèbre du groupe* G (à coefficients dans A).

Les axiomes des anneaux permettent un calcul analogue à celui dont on a l'habitude dans les entiers ou les matrices. Si a est un élément d'un anneau A et si n est un entier positif ou nul, on définit a^n par récurrence en posant $a^0 = 1$ et, si $n \geqslant 1$, $a^n = a(a^{n-1})$. On prendra garde que $a^n b^n$ et $(ab)^n$ sont en général distincts, à moins que a et b ne commutent, c'est-à-dire que l'on ait $ab = ba$.

PROPOSITION 1.1.4 (Formule du binôme). — *Soit A un anneau, soit a et b des éléments de A tels que $ab = ba$. Alors, pour tout entier $n \geqslant 0$,*

$$(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

Démonstration. — La démonstration, standard, procède par récurrence sur n. Pour $n = 0$, les deux membres valent 1. Supposons la formule vraie pour n, alors

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)(a+b)^n = (a+b)\sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k} \\
&= \sum_{k=0}^{n}\binom{n}{k}a^{k+1}b^{n-k} + \sum_{k=0}^{n}\binom{n}{k}ba^k b^{n-k} \\
&= \sum_{k=0}^{n}\binom{n}{k}a^{k+1}b^{n-k} + \sum_{k=0}^{n}\binom{n}{k}a^k b^{n+1-k} \\
&= \sum_{k=1}^{n+1}\binom{n}{k-1}a^k b^{n+1-k} + \sum_{k=0}^{n}\binom{n}{k}a^k b^{n+1-k} \\
&= \sum_{k=0}^{n+1}\left(\binom{n}{k-1} + \binom{n}{k}\right)a^k b^{n+1-k} \\
&= \sum_{k=0}^{n+1}\binom{n+1}{k}a^k b^{n+1-k}
\end{aligned}$$

puisque $\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$ pour tout couple d'entiers (n,k). Cela conclut la démonstration par récurrence sur n. □

Un *sous-anneau* B d'un anneau A est un sous-groupe de A pour l'addition qui contient 1 et est stable par la multiplication, de sorte que muni des lois induites par les lois de A, B est un anneau dont les éléments neutres sont encore 0 et 1.

L'intersection d'une famille de sous-anneaux d'un anneau A est un sous-anneau de A.

Soit A un anneau et S une partie de A. L'intersection de tous les sous-anneaux de A qui contiennent S est un sous-anneau de A qu'on appelle le *sous-anneau de A engendré par S*. Si S est de la forme $B \cup T$ où B est un sous-anneau de A, on note aussi $B[T]$ le sous-anneau de A engendré par S. Si les éléments de T commutent deux à deux, le sous-anneau engendré par T dans A est commutatif.

Soit A un anneau. L'ensemble Z des éléments $a \in A$ tels que $ax = xa$ pour tout $x \in A$ est un sous-anneau *commutatif* de A, appelé *centre* de A.

DÉFINITION 1.1.5. — *Soit A et B deux anneaux. Un* homomorphisme d'anneaux *$f : A \to B$ est une application vérifiant les propriétés suivantes*

- *on a $f(0) = 0$ et $f(1) = 1$;*
- *pour tous a et b dans A, on a $f(a+b) = f(a) + f(b)$ et $f(ab) = f(a)f(b)$.*

Le mot *morphisme* est un synonyme pour homomorphisme. Un endomorphisme d'un anneau A est un homomorphisme de A dans A. Si A est un anneau, l'application

identique $\mathrm{id}_A\colon A \to A$ est un homomorphisme d'anneaux. La *composition* de deux homomorphismes d'anneaux est encore un homomorphisme d'anneaux. Cela permet de définir la *catégorie des anneaux*.

Conformément aux définitions de théorie des catégories, on dit qu'un homomorphisme d'anneaux $f\colon A \to B$ est un *isomorphisme* s'il existe un homomorphisme d'anneaux $g\colon B \to A$ tel que $f \circ g = \mathrm{id}_B$ et $g \circ f = \mathrm{id}_A$. Le morphisme g est alors appelé homomorphisme réciproque de f. On note $f\colon A \xrightarrow{\sim} B$ pour signifier que l'homomorphisme $f\colon A \to B$ est un isomorphisme ; si A et B sont *isomorphes*, c'est-à-dire s'il existe un isomorphisme $A \xrightarrow{\sim} B$, on écrit $A \simeq B$. Si A est un anneau, un *automorphisme* de A est un isomorphisme de A sur A. L'ensemble des automorphismes d'un anneau est un groupe pour la composition.

PROPOSITION 1.1.6. — *Un homomorphisme d'anneaux est un isomorphisme si et seulement si il est bijectif.*

Démonstration. — Si $f\colon A \to B$ est un isomorphisme, son homomorphisme réciproque est en particulier une bijection réciproque de f, donc f est bijectif. Réciproquement, supposons que f est bijectif et notons g sa bijection réciproque. Il nous faut alors prouver que g est un homomorphisme d'anneaux de B dans A.

Comme $f(0) = 0$, $g(0) = 0$. Si a et $b \in B$,

$$f(g(a+b)) = a + b = f(g(a)) + f(g(b)) = f(g(a) + g(b))$$

et

$$f(g(ab)) = ab = f(g(a))f(g(b)) = f(g(a)g(b)).$$

Comme f est bijectif, $g(a+b) = g(a) + g(b)$ et $g(ab) = g(a)g(b)$. □

Exemples 1.1.7. — *a*) Soit A un anneau et soit a un élément de A qui est inversible, c'est-à-dire qu'il existe un élément $b \in A$ tel que $ab = ba = 1$. Alors, l'application $x \mapsto axb$ est un automorphisme de A, appelé *automorphisme intérieur*. Tout automorphisme de $\mathrm{M}_n(\mathbf{C})$ est un automorphisme intérieur (exercice 8).

b) Soit $A = \mathbf{C}[X_1, \ldots, X_n]$ l'anneau des polynômes en n variables à coefficients dans $\mathbf{C}$. Soit $Q_1, \ldots, Q_n$ des éléments de A. L'application de A dans lui-même qui à un polynôme P associe le polynôme $P(Q_1, \ldots, Q_n)$ dans laquel on substitue le polynôme Q_i à l'indéterminée X_i est un endomorphisme d'anneaux. Soit σ une permutation de $\{1, \ldots, n\}$ et choisissons $Q_i = X_{\sigma(i)}$; notons Φ_σ l'endomorphisme de A ainsi défini. On a $\Phi_{\sigma\tau}(X_i) = X_{\sigma(\tau(i))} = \Phi_\sigma(X_{\tau(i)}) = \Phi_\sigma(\Phi_\tau(X_i))$; on en déduit que $\Phi_{\sigma\tau}(P) = \Phi_\sigma \circ \Phi_\tau(P)$ pour tout polynôme $P \in A$. Par suite, l'application $\sigma \mapsto \Phi_\sigma$ est un homomorphisme de groupes du groupe symétrique $\mathfrak{S}_n$ dans $\mathrm{Aut}(\mathbf{C}[X_1, \ldots, X_n])$.

Si $f : A \to B$ est un homomorphisme d'anneaux, l'image $f(A)$ de A par f est un sous-anneau de B. L'image réciproque $f^{-1}(C)$ d'un sous-anneau C de B est un sous-anneau de A.

Exercices. — 1) a) Soit A un anneau. Notons A^{o} le groupe abélien A muni de la multiplication définie par $a \bullet b = ba$. Alors, A^{o} est un anneau, appelé *anneau opposé* à A.

b) Soit A l'anneau des matrices $n \times n$ à coefficients dans $\mathbf{C}$. Montrer que l'application qui à une matrice associe sa transposée est un isomorphisme de l'anneau A sur l'anneau opposé.

2) a) Soit A un anneau et soit (B_i) une famille de sous-anneaux de A. Montrer que l'intersection des B_i est un sous-anneau de A.

b) Soit A un anneau, soit B un sous-anneau de A et I un idéal bilatère de A. Soit R l'ensemble des sommes $a+b$, pour $a \in B$ et $b \in I$. Montrer que R est un sous-anneau de A.

3) Soit A un anneau et soit S une partie de A.

a) Montrer que l'ensemble des éléments de A qui commutent à tout élément de S est un sous-anneau de A.

b) Déterminer ce sous-anneau lorsque A est l'anneau des endomorphismes d'un K-espace vectoriel de dimension finie et que S est formé d'un endomorphisme diagonalisable.

c) Traiter le cas où S est une matrice de $\mathrm{M}_n(\mathbf{R})$ de polynôme minimal X^n.

4) Soit α un nombre complexe racine d'un polynôme unitaire à coefficients entier P de degré d, disons $P = X^d + a_{d-1}X^{d-1} + \cdots + a_0$. Montrer que l'ensemble des éléments de $\mathbf{C}$ de la forme $c_0 + c_1\alpha + \cdots + c_{d-1}\alpha^{d-1}$, pour $c_0, \ldots, c_{d-1} \in \mathbf{Z}$, est un sous-anneau de $\mathbf{C}$. Montrer que l'hypothèse que P est unitaire est nécessaire.

5) Soit $\mathbf{Z}[\sqrt{2}]$ et $\mathbf{Z}[\sqrt{3}]$ les sous-anneaux de $\mathbf{C}$ engendrés par $\mathbf{Z}$, et respectivement par $\sqrt{2}$ et $\sqrt{3}$.

a) Montrer que $\mathbf{Z}[\sqrt{2}] = \{a + b\sqrt{2}\,;\, a, b \in \mathbf{Z}\}$ et que $\mathbf{Z}[\sqrt{3}] = \{a + b\sqrt{3}\,;\, a, b \in \mathbf{Z}\}$.

b) Montrer que les seuls automorphismes de $\mathbf{Z}[\sqrt{2}]$ sont l'identité et l'application qui applique $a + b\sqrt{2}$ sur $a - b\sqrt{2}$.

c) Montrer qu'il n'existe pas d'homomorphisme d'anneaux de $\mathbf{Z}[\sqrt{2}]$ dans $\mathbf{Z}[\sqrt{3}]$.

d) Quels sont les automorphismes de $\mathbf{Z}[i]$? de $\mathbf{Z}[\sqrt[3]{2}]$?

6) Soit K un corps commutatif et soit V un K-espace vectoriel de dimension finie. Montrer que le centre de l'anneau $\mathrm{End}_K(V)$ est formé des homothéties $x \mapsto ax$, pour $a \in K$.

7) Soit V un espace vectoriel sur un corps commutatif k.

a) Soit (V_i) une famille de sous-espace vectoriels de V telle que $V = \bigoplus V_i$. Pour $x = \sum x_i$, avec $x_i \in V_i$, on pose $p_j(x) = x_j$. Montrer que pour tout j, p_j est un projecteur de V d'image V_j et de noyau $\bigoplus_{i \neq j} V_i$. Montrer que $p_j \circ p_i = 0$ si $i \neq j$ et que $\mathrm{id}_V = \sum p_i$.

b) Inversement, soit (p_i) une famille de projecteurs de V telle que $p_i \circ p_j = 0$ pour $i \neq j$ et $\mathrm{id}_V = \sum p_i$. Soit V_i l'image de p_i. Montrer que V est somme directe des V_i et que p_i est le projecteur sur V_i de noyau la somme des V_j pour $j \neq i$.

8) [*Automorphismes de $M_n(\mathbf{C})$*] Soit A l'anneau des matrices $n \times n$ à coefficients complexes et soit φ un automorphisme de A. Soit Z le centre de A ; c'est l'ensemble des matrices scalaires.

a) Montrer que φ induit par restriction un automorphisme de Z.

On supposera dans la suite que $\varphi|_Z = \mathrm{id}_Z$. Notons $E_{i,j}$ les matrices élémentaires (pour $1 \leqslant i, j \leqslant n$) et posons $B_{i,j} = \varphi(E_{i,j})$.

b) Montrer que $B_{i,i}$ est la matrice d'un projecteur p_i de $\mathbf{C}^n$, que $p_i \circ p_j = 0$ si $i \neq j$ et que $\mathrm{id}_{\mathbf{C}^n} = \sum p_i$.

c) En utilisant l'exercice 7, montrer qu'il existe une base $(f_1, \ldots, f_n)$ de $\mathbf{C}^n$ telle que p_i soit le projecteur sur $\mathbf{C}f_i$ parallèlement au sous-espace vectoriel $\sum_{j\neq i} \mathbf{C}f_j$.

d) Montrer qu'il existe des éléments $\lambda_i \in \mathbf{C}^*$ tels que, posant $e_i = \lambda_i f_i$, on ait $B_{ij}(e_k) = 0$ si $k \neq j$ et $B_{ij}(e_j) = e_i$. En déduire qu'il existe une matrice $B \in \mathrm{GL}_n(\mathbf{C})$ telle que $\varphi(M) = BMB^{-1}$ pour toute matrice M de $M_n(\mathbf{C})$.

e) Qu'en est-il si l'on ne suppose pas que φ est l'identité sur Z ?

9) Soit A un anneau et soit G un groupe. Soit Z le centre de l'anneau A.

a) Si $g \in G$, on note δ_g la fonction de G dans A qui vaut 1 en g et 0 ailleurs. Calculer le produit $\delta_g * \delta_{g'}$ dans l'anneau de groupe $A^{(G)}$.

b) Montrer que le centre de l'anneau $A^{(G)}$ est formé des fonctions $f : G \to Z$ de support fini qui sont constantes sur chaque classe de conjugaison de G.

10) Un opérateur différentiel sur $\mathbf{C}[X]$ est une application $\mathbf{C}$-linéaire de $\mathbf{C}[X]$ dans lui-même de la forme

$$P \mapsto \sum_{i=0}^{n} p_i(X) \frac{d^i}{dX^i} P,$$

où les p_i sont des polynômes. Montrer que l'ensemble des opérateurs différentiels, muni de l'addition et de la composition, sur $\mathbf{C}[X]$ est un anneau.

11) Soit $f : A \to B$ un homomorphisme d'anneaux.

a) Soit R l'ensemble des couples $(a, b) \in A \times A$ tels que $f(a) = f(b)$. Montrer que R, muni de l'addition et de la multiplication terme à terme, est un anneau.

b) On dit que f est un *monomorphisme* si pour tout anneau C et tout couple (g, g') d'homomorphismes d'anneaux de C dans A tel que $f \circ g = f \circ g'$, on a $g = g'$.

Montrer qu'un homomorphisme est un monomorphisme si et seulement s'il est injectif.

c) On dit que f est un *épimorphisme* si pour tout anneau C et tout couple (g, g') d'homomorphismes d'anneaux de B dans C tel que $g \circ f = g' \circ f$, on a $g = g'$.

Montrer qu'un homomorphisme surjectif est un épimorphisme. Montrer que l'homomorphisme d'inclusion de $\mathbf{Z}$ dans $\mathbf{Q}$ est un épimorphisme.

§1.2. Éléments simplifiables, inversibles ; anneaux à division

Certains éléments d'un anneau ont des propriétés particulières intéressantes par rapport à la multiplication, ce qui justifie quelques définitions.

DÉFINITION 1.2.1. — *Soit A un anneau. On dit qu'un élément $a \in A$ est* simplifiable à gauche *si la relation $ab = 0$ dans A entraîne $b = 0$, et qu'il est* diviseur de zéro à gauche *sinon. On dit qu'il est simplifiable à droite si la relation $ba = 0$ dans A entraîne $b = 0$, et qu'il est diviseur de zéro à droite sinon.*

On dit qu'un élément est simplifiable *s'il est simplifiable à droite et à gauche.*

On dit que A est intègre *si A est un anneau commutatif, non nul, et si tout élément non nul de A est simplifiable.*

Dans un anneau commutatif, un élément qui n'est pas simplifiable est aussi appelé *diviseur de zéro.*

DÉFINITION 1.2.2. — *Soit A un anneau et soit a un élément de A.*

On dit que a est inversible à droite *s'il existe $b \in A$ tel que $ab = 1$; on dit alors que b est un inverse à droite de a. On dit de même que a est* inversible à gauche *s'il existe $b \in A$ tel que $ba = 1$; on dit alors que b est un inverse à gauche de a. On dit enfin que a est* inversible *s'il est inversible à droite et à gauche.*

Supposons que a soit inversible à droite ; soit b un inverse à droite de a, de sorte que $ab = 1$. Si $ca = 0$, alors $cab = 0$, d'où $c = 0$; cela démontre que a est simplifiable à droite. De même, un élément inversible à gauche est simpliable à gauche.

Supposons que a soit inversible ; soit b un inverse à droite et c un inverse à gauche. On a $b = (ca)b = c(ab) = c$. Cela entraîne que les inverses à droites et à gauches de a sont égaux à un même élément appelé tout simplement inverse de a et souvent noté a^{-1}. Dans un anneau commutatif, un élément inversible à droite est aussi inversible à gauche, et réciproquement.

On dit que deux éléments a et b d'un anneau commutatif A sont *associés* s'il existe un élément inversible $u \in A^\times$ tel que $a = bu$. La relation « être associé » est une relation d'équivalence.

Soit $A^\times$ l'ensemble des éléments inversibles d'un anneau A.

PROPOSITION 1.2.3. — *L'ensemble des éléments inversibles d'un anneau A est un groupe pour la multiplication. On l'appelle le* groupe des unités *de A.*

Un homomorphisme d'anneaux $f : A \to B$ induit par restriction un homomorphisme de groupes de $A^\times$ dans $B^\times$.

Démonstration. — Soit a et b deux éléments de A, d'inverses a^{-1} et b^{-1}. Alors, $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a{-}1 = aa^{-1} = 1$, si bien que ab est inversible à droite, d'inverse $b^{-1}a^{-1}$. De même, $(b^{-1}a^{-1})(ab) = 1$, donc ab est aussi inversible à gauche. La multiplication de A définit ainsi une loi interne sur $A^\times$. De plus, 1 est inversible et est un élément neutre pour cette loi. Enfin, si $a \in A^\times$, son inverse pour cette loi n'est autre que a^{-1}. Ainsi, $A^\times$ est un groupe pour la multiplication.

Soit $f : A \to B$ un homomorphisme d'anneaux. Soit $a \in A^\times$; soit b l'inverse de a. Comme $ab = ba = 1$, on a $1 = f(1) = f(a)f(b) = f(b)f(a)$. Par suite, $f(a)$ est inversible, d'inverse $f(b)$. L'application f induit donc par restriction une application de $A^\times$ dans $B^\times$. Cette application applique un produit sur le produit des images, c'est donc un homomorphisme de groupes. □

DÉFINITION 1.2.4. — *On dit qu'un anneau A est un* anneau à division *(ou parfois un* corps gauche*), s'il n'est pas l'anneau nul et si tout élément non nul de A est inversible. On dit que c'est un* corps *si c'est un anneau à division et qu'il est commutatif.*

L'existence d'anneaux à division non commutatifs n'est pas évidente. Citons notamment le théorème de Wedderburn selon lequel une algèbre à division finie est commutative, c'est-à-dire un corps, voir l'exercice 22. Le plus connu des anneaux à division non commutatifs est peut-être le corps des quaternions, découvert par Hamilton en 1843.

Exemple 1.2.5. — Le groupe abélien sous-jacent à $\mathbf{H}$ est $\mathbf{R}^4$, dont on note $(1, i, j, k)$ la base canonique. La multiplication $\mathbf{H} \times \mathbf{H} \to \mathbf{H}$ est caractérisée par le fait qu'elle est $\mathbf{R}$-bilinéaire, associative, que 1 est élement neutre, et par les relations $i^2 = j^2 = k^2 = -1$ et $ij = k$. On a $jk = -kj = i$, $ki = -ik = j$ et $ji = -k$.

Soit $q = a1 + bi + cj + dk$ un quaternion ; on pose $\overline{q} = a - bi - cj - dk$. Si q et q' sont des quaternions, on a $\overline{qq'} = \overline{q'}\,\overline{q}$ et $q\overline{q} = a^2 + b^2 + c^2 + d^2$; c'est un nombre réel positif, nul si et seulement si $q = 0$. Si $q \neq 0$, q est inversible et son inverse est le quaternion $(q\bar{q})^{-1}\bar{q}$.

Soit $q = a1 + bi + cj + dk$ un quaternion. On a $i^{-1}qi = -iqi = a1 + bi - cj - dk$, $j^{-1}qj = a1 - bi + cj - dk$ et $k^{-1}qk = a1 - bi - cj + dk$. Par suite, le centre de $\mathbf{H}$ est formé des éléments $a1$, pour $a \in \mathbf{R}$; c'est un sous-corps isomorphe à $\mathbf{R}$.

Notons que l'ensemble des quaternions de la forme $a + bi$, pour a et $b \in \mathbf{R}$ est un sous-corps de $\mathbf{H}$ isomorphe à $\mathbf{C}$. Plus généralement, si (u_1, u_2, u_3) est un vecteur unitaire de $\mathbf{R}^3$, $u = u_1 i + u_2 j + u_3 k$ est un élément de $\mathbf{H}$ tel que $u^2 = -1$ et l'ensemble des quaternions de la forme $a + bu$, pour a et $b \in \mathbf{R}$ est un sous-corps de $\mathbf{H}$ isomorphe à $\mathbf{C}$. Observons aussi que l'équation $x^2 + 1 = 0$ a une infinité de solutions dans $\mathbf{H}$, contrairement à ce qui se passe dans un corps commutatif.

THÉORÈME 1.2.6 (Frobenius, 1878). — *Soit A un $\mathbf{R}$-espace vectoriel de dimension finie muni d'une loi de composition $\mathbf{R}$-bilinéaire qui en fait un anneau à division. Alors A est isomorphe à $\mathbf{R}$, $\mathbf{C}$ ou $\mathbf{H}$.*

On remarquera que l'énoncé est faux sans l'hypothèse que A est de dimension finie (considérer le corps $\mathbf{R}(X)$ des fractions rationnelles) ou que la multiplication fait de A un anneau à division (considérer l'anneau produit $\mathbf{R} \times \mathbf{R}$). Il est de même faux si l'on ne suppose pas que la multiplication est $\mathbf{R}$-bilinéaire (*cf.* B. DESCHAMPS, « À propos d'un théorème de Frobenius », *Ann. math. Blaise Pascal* **8** (2001), p. 61–66). La démonstration ci-dessous suit assez fidèlement un article de R. PALAIS, « The classification of real division algebras », *Amer. Math. Monthly* **75** (1968), p. 366–368.

Démonstration. — On identifie $\mathbf{R}$ au sous-anneau de A formé des $x1_A$ pour $x \in \mathbf{R}$ et 1_A l'élément neutre de A pour la multiplication.

Supposons que $A \neq \mathbf{R}$.

Soit α un élément de $A \setminus \mathbf{R}$. L'anneau $\mathbf{R}[\alpha]$ engendré par R et α est commutatif ; c'est un sous-espace vectoriel de A, il est de dimension finie. Par conséquent, c'est un corps (commutatif). Le polynôme minimal de α dans $\mathbf{R}[\alpha]$ est irréductible. Il est donc de degré $\leqslant 2$. Comme $\alpha \notin \mathbf{R}$, il est de degré 2, de la forme $X^2 + 2aX + b$. Alors, $(\alpha + a)^2 = a^2 - b$ et l'élément $i = (\alpha + a)/\sqrt{b - a^2}$ de $\mathbf{R}[\alpha]$ vérifie $i^2 = -1$. Observons que $\mathbf{R}[\alpha] = \mathbf{R}[i]$ est isomorphe à $\mathbf{C}$.

Supposons d'abord que A est commutatif et montrons que l'on a $A = \mathbf{R}[i]$. Considérons, sinon, un élément α' de A qui n'est pas dans $\mathbf{R}[i]$. Le même argument que ci-dessus fournit un élément $i' = (\alpha' + a')/\sqrt{b' - (a')^2}$ de A tel que $\mathbf{R}[i'] = \mathbf{R}[\alpha']$. Comme $\alpha' \notin \mathbf{R}[i]$, $i' \neq \pm i$. Le polynôme $X^2 + 1$ a ainsi au moins quatre racines distinctes dans le corps commutatif A, ce qui est absurde.

Traitons maintenant le cas général. Le sous-corps commutatif $\mathbf{R}[i]$ permet de considérer A comme un $\mathbf{C}$-espace vectoriel. Soit alors $\varphi\colon A \to A$ l'application définie par $\varphi(x) = xi$. C'est une application $\mathbf{C}$-linéaire et l'on a $\varphi^2 = -\mathrm{id}_A$. Comme le polynôme $X^2 + 1$ est scindé à racines simples dans $\mathbf{C}$, A est la somme des espaces propres pour les valeurs propres i et $-i$. Autrement dit, A est somme directe des sous-espaces A_+ et A_-, où A_+ est l'ensemble des $x \in A$ tels que $\varphi(x) = ix$ et A_- celui des $x \in A$ tels que $\varphi(x) = -ix$.

On constate que A_+ est stable par multiplication (si $xi = ix$ et $yi = iy$, alors $(xy)i = xiy = ixy$) et par inverse (si $xi = ix$, alors $x^{-1}i = ix^{-1}$). C'est donc un sous-corps de A. L'inclusion $\mathbf{R}[i] \subset A_+$ est évidente ; montrons que l'on a égalité. Considérons un élément $\beta \in A_+$. Le sous-anneau de A_+ engendré par $\mathbf{R}[i]$ et β est un corps commutatif ; il est donc égal à $\mathbf{R}[i]$ ce qui entraîne $\beta \in \mathbf{R}[i]$.

Supposons maintenant que $A \neq A_+$ et considérons un élément non nul $\beta \in A_-$. L'application $x \mapsto x\beta$ est $\mathbf{R}[i]$-linéaire injective, donc bijective. Si $xi = ix$, alors $x\beta i = x(-i\beta) = -xi\beta = -ix\beta$, donc $A_+\beta \subset A_-$; inversement, si $xi = -ix$, soit $y \in A$ tel que $y = x\beta$, alors $yi = x\beta i = -xi\beta = ix\beta$, d'où l'autre inclusion.

Par un argument analogue, $A_-\beta = A_+$. En particulier, $\beta^2 \in \mathbf{R}[i] \cap \mathbf{R}[\beta] = \mathbf{R}$, car ces deux espaces vectoriels $\mathbf{R}[i]$ et $\mathbf{R}[\beta]$ sont distincts, de dimension 2 et contiennent $\mathbf{R}$. Supposons $\beta^2 > 0$. Alors, β^2 a quatre racines carrées dans le corps $\mathbf{R}[\beta]$, à savoir $\pm\sqrt{\beta^2}$ et $\pm\beta$, ce qui contredit le fait qu'une équation polynomiale de degré 2 dans un corps ait au plus deux solutions. Donc $\beta^2 < 0$ et $j = (-\beta^2)^{-1/2}\beta$ est un élément de A_- tel que $j^2 = -1$.

Posons $k = ij$. L'espace vectoriel A est de dimension 4 et $(1, i, j, k)$ en est une base. On a $k^2 = ijij = i(-ij)j = -i^2j^2 = -1$; de même, la table de multiplication de A coïncide avec celle de $\mathbf{H}$. L'isomorphie de A et $\mathbf{H}$ est ainsi manifeste. □

DÉFINITION 1.2.7. — *Soit A un anneau. On dit que a est nilpotent s'il existe $n \geqslant 1$ tel que $a^n = 0$.*

Exercices. — 12) Soit $n \geqslant 2$ un entier. Déterminer les éléments nilpotents et les éléments inversibles de $\mathbf{Z}/n\mathbf{Z}$.

13) a) Quels sont les éléments inversibles de $\mathbf{Z}/n\mathbf{Z}$, pour $n \in \mathbf{Z}$? Pour quels entiers n cet anneau est-il intègre ?

b) Soit n et m des entiers non nuls. Montrer que l'application canonique de $\mathbf{Z}/nm\mathbf{Z}$ dans $\mathbf{Z}/n\mathbf{Z}$ est un homomorphisme d'anneaux. Montrer qu'il induit une surjection de $(\mathbf{Z}/mn\mathbf{Z})^\times$ sur $(\mathbf{Z}/n\mathbf{Z})^\times$.

c) Exhiber un homomorphisme d'anneaux $f : A \to B$ qui soit surjectif mais tel que l'homomorphisme de groupes de $A^\times$ dans $B^\times$ déduit de f par restriction ne le soit pas.

14) Soit K un corps et A un anneau non nul. Montrer que tout homomorphisme d'anneaux de K dans A est injectif.

15) a) Soit K un corps commutatif, soit V un K-espace vectoriel et soit A l'anneau $\mathrm{End}_K(V)$ des endomorphismes de V. Les éléments de A inversibles à gauche sont les endomorphismes injectifs, les éléments inversibles à droite sont les endomorphismes surjectifs.

b) Donner un exemple d'anneau (non commutatif) et d'élément qui possède une infinité d'inverses à droite.

16) [*Anneau produit*] Soit A et B deux anneaux. On munit le groupe abélien $A \times B$ d'une loi interne en définissant pour a et $a' \in A$, b et $b' \in B$, $(a,b) \cdot (a',b') = (aa', bb')$.

a) Montrer que cette loi confère à $A \times B$ une structure d'anneau. Quel est l'élément neutre pour la multiplication ?

b) Déterminer les éléments simplifiables (à droite ou à gauche), resp. inversibles (à droite ou à gauche), resp. nilpotents, de l'anneau $A \times B$.

c) Montrer que les éléments $e = (1,0)$ et $f = (0,1)$ de $A \times B$ vérifient $e^2 = e$ et $f^2 = f$. On dit que ce sont des *idempotents*.

17) Soit A un anneau non nul.

a) Soit a un élément de A qui possède un unique inverse à droite. Montrer que a est simplifiable puis que a est inversible.

b) Si tout élément non nul de A est inversible à gauche, A est un anneau à division.

c) On suppose que A est fini. Montrer qu'un élément simplifiable à gauche est inversible à droite. Si tout élément de A est simplifiable à gauche, A est donc un anneau à division. Si A est commutatif, tout idéal premier de A est maximal.

d) Même question lorsqu'on suppose que A est une K-algèbre de dimension finie comme K-espace vectoriel, K étant un corps commutatif. (Cela signifie que la multiplication de A est K-bilinéaire.)

e) On suppose que tout élément non nul de A est simplifiable à gauche et que l'ensemble des idéaux à droite de A est fini. Montrer que A est un anneau à division. (*Montrer que tout élément non nul x est inversible à droite en introduisant les idéaux à droite $x^n A$ pour $n \geqslant 1$.*)

18) Soit A un anneau et soit $e \in A$ un idempotent.

a) Montrer que $1-e$ est un idempotent de A.

b) Montrer que $eAe = \{eae\,;\, a \in A\}$ est un sous-groupe abélien de A et que la multiplication de A le munit d'une structure d'anneau.

c) Expliciter le cas particulier où $A = M_n(k)$, k étant un corps commutatif, et e une matrice de rang r, disons avec des 1 en début de diagonale et des 0 sinon.

19) Soit A un anneau.

a) Soit $a \in A$ un élément nilpotent. Si $n \geqslant 0$ est tel que $a^{n+1} = 0$, calculer $(1+a)(1-a+a^2-\cdots+(-1)^n a^n)$. En déduire que $1+a$ est inversible dans A.

b) Soit $x \in A$ un élément inversible et $y \in A$ un élément nilpotent tel que $xy = yx$; montrer que $x+y$ est inversible.

c) Si x et y sont deux éléments nilpotents de A qui commutent, montrer que $x+y$ est nilpotent. (Si n et m sont deux entiers tels que $x^{n+1} = y^{m+1} = 0$, on utilisera la formule du binôme pour calculer $(x+y)^{n+m+1}$.)

20) Soit A un anneau, soit a et b des éléments de A tels que $1-ab$ soit inversible dans A.

a) Montrer que $1-ba$ est inversible dans A et calculer son inverse. (Commencer par le cas où ab est nilpotent.)

b) Si $A = M_n(k)$, où k est un corps commutatif, montrer que ce résultat équivaut au fait que ab et ba ont même polynôme caractéristique.

21) Soit A un anneau commutatif et $f = a_0 + a_1X + \cdots + a_nX^n \in A[X]$.

a) Montrer que f est nilpotent si et seulement si tous les a_i sont nilpotents.

b) Montrer que f est inversible dans $A[X]$ si et seulement a_0 est inversible dans A et $a_1, \ldots, a_n$ sont nilpotents. (*Si* $g = f^{-1} = b_0 + b_1X + \cdots + b_mX^m$, *montrer par récurrence sur* k *que* $a_n^{k+1} b_{m-k} = 0$.)

c) Montrer que f est diviseur de zéro si et seulement si il existe $a \in A$, $a \neq 0$ tel que $af = 0$. (*Si* $fg = 0$ *avec* g *de degré minimal, montrer que pour tout* k, $a_k g = 0$.)

22) Cet exercice propose une démonstration du fameux théorème de Wedderburn : *tout anneau à division fini est commutatif*. Soit donc F un anneau à division fini, qu'on ne suppose pas commutatif. Un sous-anneau de F qui est un corps sera appelé sous-corps.

a) Soit Z le *centre* de F. Montrer que Z est un sous-corps de F. On note q son cardinal. Montrer qu'il existe un entier $n \geqslant 1$ tel que $\operatorname{card} F = q^n$.

b) Soit $x \in F$. Montrer que l'ensemble C_x des $a \in F$ tels que $ax = xa$ est un sous-corps de F. Montrer qu'il existe un entier n_x qui divise n et tel que $\operatorname{card} C_x = q^{n_x}$. (Remarquer que la multiplication à gauche par les éléments de C_x munit F d'une structure de C_x-espace vectoriel.)

c) Si $x \in F^*$, calculer en fonction de n_x le cardinal de la classe de conjugaison $\mathscr{C}(x)$ de x dans F^* (l'ensemble des éléments de F^* de la forme axa^{-1}, pour $a \in F^*$).

d) Si $x \notin Z$, en déduire que le cardinal de $\mathscr{C}(x)$ est un multiple de $\Phi_n(q)$. (Φ_n désigne le n-ième polynôme cyclotomique.)

e) Montrer à l'aide de l'équation aux classes que $\Phi_n(q)$ divise $q^n - q$. En déduire que $n = 1$, donc que F est commutatif.

§1.3. Idéaux

DÉFINITION 1.3.1. — *On appelle* idéal à gauche *d'un anneau A tout sous-groupe (pour l'addition) $I \subset A$ tel que pour tout $a \in I$ et tout $b \in A$, $ba \in I$.*

On appelle idéal à droite *d'un anneau A tout sous-groupe $I \subset A$ tel que pour tout $a \in I$ et tout $b \in A$, $ab \in I$.*

On dit que $I \subset A$ est un idéal bilatère *si c'est un idéal à droite et un idéal à gauche.*

Dans un anneau commutatif, idéaux à droite, à gauche et bilatères coïncident ; on parle alors tout simplement d'*idéal*. Remarquons que 0 et A sont des idéaux bilatères de A. Pour tout $a \in A$, l'ensemble Aa formé des éléments xa de A pour $x \in A$, est un idéal à gauche ; l'ensemble aA formé des ax, pour $x \in A$, est un idéal à droite. Si A est commutatif, on note souvent (a) cet idéal.

Comme -1 est un élément de A, pour prouver qu'une partie I de A est un idéal à gauche, il suffit d'établir les faits suivants :

- $0 \in I$;
- si $a \in I$ et $b \in I$, $a + b \in I$;
- si $a \in A$ et $b \in I$, $ab \in I$.

Exemple 1.3.2. — *Si K est un anneau à division, les seuls idéaux à gauche (ou à droite) de K sont* (0) *et K.* En effet, soit I un idéal à gauche de K distinct de 0 et soit a un élément non nul de I. Soit b un élément de K. Comme $a \neq 0$, on peut considérer l'élément ba^{-1} de K et, par définition d'un idéal à gauche, $(ba^{-1})a \in I$. On a donc $b \in I$, d'où $I = K$.

Les anneaux $\mathbf{Z}$ et $K[X]$, pour K un corps commutatif, possèdent une *division euclidienne. Si a et b sont des entiers relatifs, avec $b \neq 0$, il existe un unique couple d'entiers (q, r) tel que $a = bq + r$ et et $0 \leqslant r < |b|$.* De même, *si A et B sont des polynômes à coefficients dans un corps commutatif K, avec $B \neq 0$, il existe un unique couple (Q, R) de polynômes tel que $A = BQ + R$ et* $\deg R < \deg B$.

Exemple 1.3.3. — Si I est un idéal de $\mathbf{Z}$, il existe un unique entier $n \geqslant 0$ tel que $I = (n)$.

Démonstration. — Si $I = (0)$, $n = 0$ convient.

Supposons maintenant $I \neq (0)$. Si $I = (n)$, on constate que les éléments strictement positifs de I sont $\{n; 2n; 3n; \ldots\}$ et que n est le plus petit d'entre eux — ce qui montre l'unicité d'un éventuel entier n comme dans l'énoncé.

Notons donc n le plus petit élément de $I \cap \mathbf{N}^*$. Comme $n \in I$, $an \in I$ pour tout $a \in \mathbf{Z}$ et $(n) \subset I$. Réciproquement, soit a est un élément de I. La *division euclidienne* de a par n s'écrit $a = qn + r$, avec $q \in \mathbf{Z}$ et $0 \leqslant r \leqslant n - 1$. Comme $a \in I$ et comme $qn \in I$, $r = a - qn$ appartient à I. Comme n est le plus petit élément strictement positif de I et comme $r < n$, on a nécessairement $r = 0$. Par suite, $a = qn \in (n)$ et $I \subset (n)$. Ainsi, $I = (n)$. □

Exemple 1.3.4. — Si I est un idéal de $K[X]$, il existe un polynôme P tel que $I = (P)$. En outre, la condition que P soit nul ou unitaire détermine P de manière unique.

Démonstration. — La démonstration est analogue : si $I = 0$, on choisit $P = 0$. Sinon, soit P est un élément non nul de I, unitaire, dont le degré est minimal. Tout multiple de P appartient à I, d'où $(P) \subset I$. Inversement, pour $A \in I$, la division euclidienne de A par P s'écrit $A = PQ + R$, avec $\deg R < \deg P$. Comme A et P appartiennent à I, $A - PQ$ aussi, donc $R \in I$. Par minimalité du degré de P, $R = 0$, d'où $A \in (P)$. □

On dispose d'un certain nombre d'opérations intéressantes sur les idéaux.

1.3.5. Intersection. — Si I et J sont deux idéaux à gauche de A, l'ensemble $I \cap J$ est encore un idéal à gauche de A. Plus généralement, l'*intersection* d'une famille d'idéaux à gauche de A est encore un idéal à gauche de A.

Démonstration. — Soit $(I_s)_{s\in S}$ une famille d'idéaux de A et posons $I = \bigcap_s I_s$. (Si $S = \varnothing$, on a $I = A$.) L'intersection d'une famille de sous-groupes est encore un sous-groupe, donc I est un sous-groupe de A. Soit maintenant $x \in I$ et $a \in A$ arbitraires et montrons que $ax \in I$. Pour tout s, $x \in I_s$ et I_s étant un idéal à gauche, on a donc $ax \in I_s$. Par suite, ax appartient à tous les I_s donc $ax \in I$. □

Un énoncé analogue est valable pour les idéaux à droite et les idéaux bilatères.

1.3.6. Idéal engendré par une partie. — Si S est une partie de A, il existe un plus petit idéal à gauche I de A contenant S, qu'on appelle *idéal à gauche engendré* par S. Cela signifie que I est un idéal contenant S et que si J est un idéal contenant S, alors J contient déjà I. De plus, I est l'ensemble des combinaisons linéaires presque nulle $\sum_{s\in S} a_s s$.

Démonstration. — En effet, il suffit de définir I comme l'intersection des idéaux à gauche de A qui contiennent S. C'est un idéal à gauche d'après la proposition précédente. Notons d'autre part J l'ensemble des combinaisons linéaires presque nulles $\sum_{s\in S} a_s s$, pour $(a_s) \in A^{(S)}$.

Si (a_s) est une famille presque nulle d'éléments de A, $\sum_{s\in S} a_s s$ est un élement de tout idéal à gauche de A contenant S, donc de I. Cela montre que $J \subset I$.

Réciproquement, montrons que J est un idéal à gauche de A. Il contient $0 = \sum_{s\in S} 0s$; si $\sum a_s s$ et $\sum b_s s$ sont des éléments de J, la famille $(a_s + b_s)_{s\in S}$ est une famille presque nulle d'éléments de A et $\sum (a_s + b_s)s \in J$; enfin, si $a \in A$ et si $x = \sum a_s s \in J$, on a $ax = a(\sum a_s s) = \sum (aa_s)s \in J$ et J est bien un idéal de A.

Comme J contient S (si $t \in S$, $t = \sum_{s\in S} a_s t$ avec $a_t = 1$ et $a_s = 0$ si $s \neq t$). Par suite, I est contenu dans J, d'où finalement l'égalité. □

Par des arguments similaires, il existe un plus petit idéal à droite (*resp.* bilatère) de A contenant S ; c'est l'intersection des idéaux à droite (*resp.* bilatère) de A qui

contiennent S. Ce sont respectivement l'ensemble des combinaisons linéaires $\sum_{s\in S} sa_s$ et $\sum_{s\in S} a_s s b_s$, pour (a_s) et (b_s) des familles presque nulles d'éléments de A.

PROPOSITION 1.3.7. — *Le* noyau *d'un morphisme d'anneaux $f : A \to B$ est l'ensemble des $a \in A$ tels que $f(a) = 0$. C'est un* idéal bilatère *de A que l'on note* $\ker(f)$.

Démonstration. — Un morphisme d'anneaux étant un morphisme de groupes abéliens, $\ker(f)$ est un sous-groupe de A. De plus, si $x \in \ker f$ et si $a \in A$, on a $f(ax) = f(a)f(x) = f(a)0 = 0$ donc $ax \in \ker f$. De même, si $x \in \ker f$ et $a \in A$, $f(xa) = f(x)f(a) = 0$, donc $xa \in \ker f$. Il en résulte que $\ker f$ est un idéal à droite et à gauche de A. □

1.3.8. Image, image réciproque. — Soit $f : A \to B$ un morphisme d'anneaux et soit J un idéal à gauche de B ; l'image réciproque de J par f,

$$f^{-1}(J) = \{a \in A;\ f(a) \in J\}$$

est un idéal à gauche de A.

Démonstration. — Comme $f(0) = 0 \in J$, $0 \in f^{-1}(J)$. Si a et $b \in f^{-1}(J)$, $f(a+b) = f(a) + f(b) \in J$ puisque $f(a)$ et $f(b) \in J$ et que J est un idéal de B. Enfin, si $a \in A$ et $b \in f^{-1}(J)$, on a $f(ab) = f(a)f(b) \in J$ puisque $f(b) \in J$. □

En revanche, l'image d'un idéal à gauche par un morphisme d'anneaux n'est pas forcément un idéal. Si $f : A \to B$ est un morphisme d'anneaux et si I est un idéal à gauche de A, on notera $Bf(I)$, voire BI, l'idéal à gauche engendré dans B par $f(I)$.

1.3.9. Somme d'idéaux. — Soit I et J deux idéaux (à gauche, à droite, bilatère) de A. L'ensemble des sommes $a + b$ avec $a \in I$ et $b \in J$ est un idéal (à gauche, à droite, bilatère) de A, noté $I + J$. C'est aussi l'idéal (...) de A engendré par la partie $I \cup J$. Plus généralement, si $(I_s)_{s\in S}$ est une famille d'idéaux (...) de A, l'ensemble des sommes (presque nulles) $\sum_s a_s$, où pour tout s, $a_s \in I_s$, est un idéal (...) de A noté $\sum_s I_s$. C'est aussi l'idéal (...) de A engendré par la partie $\bigcup_s I_s$.

Démonstration. — Démontrons le résultat pour des idéaux à gauche. Comme $0 = \sum_s 0$ et comme $0 \in I_s$ pour tout s, $0 \in \sum_s I_s$. Ensuite, si $a = \sum_s a_s$ et $b = \sum_s b_s$ sont deux éléments de $\sum_s I_s$, on a $a + b = \sum_s (a_s + b_s)$ où pour tout s, $a_s + b_s \in I_s$, presque tous les termes de cette somme étant nuls. Donc $a + b \in \sum_s I_s$. Finalement, si $a = \sum_s a_s$ appartient à I_s et $b \in A$, on a $ba = \sum_s (ba_s)$. Pour tout s, $ba_s \in I_s$, donc $ba \in \sum_s I_s$. Ainsi, $\sum_s I_s$ est bien un idéal à gauche de A.

Pour montrer que c'est l'idéal à gauche de A engendré par la partie $\bigcup_s I_s$, nous devons établir deux inclusions. Tout d'abord, si $t \in S$ et $a \in I_t$, on a $a = \sum_s a_s$ avec $a_s = 0$ si $s \neq t$ et $a_t = a$. Donc $a \in \sum_s I_s$ et l'idéal $\sum_s I_s$ contient I_t. Par définition de l'idéal $\langle \bigcup_s I_s \rangle$ (plus

petit idéal à gauche qui contient la partie $\bigcup_s I_s$), on a ainsi

$$\langle \bigcup_s I_s \rangle \subset \sum_s I_s.$$

Dans l'autre sens, si I est un idéal à gauche contenant $\bigcup_s I_s$, montrons que I contient $\sum_s I_s$. Soit alors $a = \sum_s a_s$ un élément de $\sum_s I_s$. Tous les termes de cette somme appartiennent à I. Par définition d'un idéal à gauche, a appartient à I et I contient $\sum_s I_s$. □

1.3.10. Produit d'idéaux. — Soit A un anneau et soit I et J deux idéaux bilatères de A. L'ensemble des produits ab avec $a \in I$ et $b \in J$ n'est pas forcément un idéal de A. L'idéal IJ est par définition l'idéal bilatère engendré par ces produits.

Soit K l'ensemble des combinaisons linéaires $\sum a_s b_s$, où $a_s \in I$ et $b_s \in J$. C'est une partie de IJ. Montrons que K est un idéal bilatère de A. C'est un sous-groupe abélien de manière évidente. De plus, soit $x = \sum a_s b_s \in K$ et soit $a \in A$. On a

$$ax = a\big(\sum a_s b_s\big) = \sum (a a_s) b_s;$$

comme I est un idéal à gauche, $aa_s \in AI$ pour tout s, donc $ax \in K$. Enfin, la relation

$$xa = \big(\sum a_s b_s\big) a = \sum a_s (b_s a)$$

montre que $xa \in K$ puisque, J étant un idéal à droite, $b_s a \in J$ pour tout s. Comme K contient les produits ab, pour $a \in I$ et $b \in J$, on a l'inclusion $IJ \subset K$ et, finalement, $IJ = K$.

Comme I et J sont des idéaux bilatères, pour tout $a \in I$ et tout $b \in J$, le produit ab appartient tant à I qu'à J ; il en résulte que $IJ \subset I \cap J$.

1.3.11. (Nil)radical. — Le *nilradical* d'un anneau *commutatif* A est l'ensemble de ses éléments nilpotents. C'est un idéal de A.

Plus généralement, on définit le *radical* d'un idéal I de A par la formule

$$\sqrt{I} = \{a \in A ; \text{il existe } n \geqslant 1,\ a^n \in I\}.$$

C'est un idéal de A qui contient I. Par définition même, le nilradical de A est donc égal au radical de l'idéal nul.

Démonstration. — Comme $0^1 = 0 \in I$, $0 \in \sqrt{I}$. Si $a \in \sqrt{I}$ et $b \in \sqrt{I}$, choisissons n et $m \geqslant 1$ tels que $a^n \in I$ et $b^m \in I$. Alors, on a d'après la formule du binôme

$$(a+b)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} a^k b^{n+m-k}.$$

Dans cette somme, tous les termes appartiennent à I : c'est vrai de ceux correspondant à $k \geqslant n$ puisque $a^k = a^n a^{n-k}$ et $a^n \in I$; de même, si $k \leqslant n$, $n+m-k \geqslant m$ et $b^{n+m-k} = b^m b^{n-k}$ appartient à I. On a donc $(a+b)^{n+m} \in I$, d'où $a+b \in \sqrt{I}$. Enfin, si $a \in \sqrt{I}$ et $b \in A$, choisissons $n \geqslant 1$ tel que $a^n \in I$. Alors, $(ba)^n = b^n a^n \in I$ et $ba \in \sqrt{I}$. □

Exercices. — 23) Soit K un corps commutatif, soit V un K-espace vectoriel et soit A l'anneau des endomorphismes de V.

a) Pour tout sous-espace vectoriel W de K, l'ensemble N_W des endomorphismes dont le noyau contient W est un idéal à gauche de A, l'ensemble I_W des endomorphismes dont l'image est contenue dans W est un idéal à droite de W.

b) Si V est de dimension finie, les idéaux à droite (*resp.* à gauche) sont tous de cette forme.

c) Si V est de dimension finie, les seuls idéaux bilatères de A sont (0) et A.

d) L'ensemble des endomorphismes de rang fini de V (c'est-à-dire dont l'image est de dimension finie) est un idéal bilatère de A. Il est distinct de A si V est de dimension infinie.

24) Quel est le radical de l'idéal (12) dans $\mathbf{Z}$?

25) Soit A un anneau commutatif et soit a, b deux éléments de A. S'ils sont associés, c'et-à-dire s'il existe un élément inversible u de A tel que $a = bu$, montrer que les idéaux $(a) = aA$ et $(b) = bA$ sont égaux. Réciproquement, si A est intègre et si $(a) = (b)$, montrer que a et b sont associés.

26) Soit A un anneau et soit I un idéal à droite de A.

a) Montrer que l'idéal à gauche engendré par I dans A est un idéal bilatère.

b) Montrer que l'ensemble J des éléments $a \in A$ tels que $xa = 0$ pour tout $x \in I$ (l'annulateur à droite de I) est un idéal bilatère de A.

27) Montrer qu'un anneau intègre possédant un nombre fini d'idéaux à gauche est un anneau à division. (*Montrer que tout élément non nul x est inversible à gauche en introduisant les idéaux à gauche Ax^n pour $n \geqslant 1$.*)

28) Soit A un anneau commutatif et soit I, J et L des idéaux de A. Démontrer les assertions suivantes :

a) $I \cdot J$ est contenu dans $I \cap J$;

b) on a $(I \cdot J) + (I \cdot L) = I \cdot (J + L)$;

c) $(I \cap J) + (I \cap L)$ est contenu dans $I \cap (J + L)$;

d) si J est contenu dans I, on a $J + (I \cap L) = I \cap (J + L)$;

e) soit K un corps. Supposons que l'on ait $A = K[X, Y]$. Posons $I = (X)$, $J = (Y)$ et $L = (X + Y)$. Déterminer $(I \cap J) + (I \cap L)$ et $I \cap (J + L)$, puis les comparer.

29) Soit A, B des anneaux commutatifs et soit $f : A \to B$ un homomorphisme d'anneaux. Pour tout idéal I de A, on note $f_*(I)$ l'idéal de B engendré par $f(I)$ et on l'appelle extension de I dans B. Pour tout idéal J de B, on appelle contraction de J l'idéal $f^{-1}(J)$.

Étant donné un idéal I de A et un idéal J de B, montrer les assertions suivantes :

a) I est contenu dans $f^{-1}(f_*(I))$ et J contient $f_*(f^{-1}(J))$;

b) on a $f^{-1}(J) = f^{-1}\big(f_*(f^{-1}(J)\big)$ et $f_*(I) = f_*\big(f^{-1}(f_*(I)\big)$.

Soit $\mathscr{C}$ l'ensemble des idéaux de A qui sont des contractions d'idéaux de B et $\mathscr{E}$ l'ensemble des idéaux de B qui sont des extensions d'idéaux de A.

c) on a $\mathscr{C} = \{I; I = f^{-1}\big(f_*(I)\big)\}$ et $\mathscr{E} = \{J; J = f_*\big(f^{-1}(I)\big)\}$;

d) l'application f_* définit une bijection de $\mathscr{C}$ sur $\mathscr{E}$; quel est son inverse ?

Soit I_1 et I_2 deux idéaux de A, et J_1 et J_2 deux idéaux de B. Montrer les assertions suivantes :
e) on a $f_*(I_1+I_2) = f_*(I_1) + f_*(I_2)$ et $f^{-1}(J_1+J_2)$ contient $f^{-1}(J_1) + f^{-1}(J_2)$;
f) $f_*(I_1 \cap I_2)$ est contenu dans $f_*(I_1) \cap f_*(I_2)$ et l'on a $f^{-1}(J_1 \cap J_2) = f^{-1}(J_1) \cap f^{-1}(J_2)$;
g) on a $f_*(I_1 \cdot I_2) = f_*(I_1) \cdot f_*(I_2)$ et $f^{-1}(J_1 \cdot J_2)$ contient $f^{-1}(J_1) \cdot f^{-1}(J_2)$;
h) $f_*(\sqrt{I})$ est contenu dans $\sqrt{f_*(I)}$ et l'on a $f^{-1}(\sqrt{J}) = \sqrt{f^{-1}(J)}$.

30) Soit I et J deux idéaux d'un anneau commutatif A. On suppose que $I+J=A$. Montrer que pour tout entier n, $I^n + J^n = A$.

31) Soit A un anneau.

a) Montrer par un contre-exemple que l'ensemble des éléments nilpotents de A ne forme pas un sous-groupe abélien. (On pourra choisir $A = M_2(\mathbf{C})$.)

b) Soit N l'ensemble des éléments $a \in A$ tels que ax soit nilpotent pour tout $x \in A$. Montrer que N est un idéal bilatère de A dont tout élément est nilpotent.

c) Soit I un idéal bilatère de A dont tout élément est nilpotent. Montrer que $I \subset N$.

32) Soit A un anneau commutatif, soit I un idéal de A et soit S une partie de A. On définit le *conducteur* de S dans I par la formule

$$J = (I : S) = \{a \in A ; \text{ pour tout } s \in S,\ as \in I\}.$$

Montrer que c'est un idéal de A ; c'est le plus grand idéal K de A tel que $KS \subset I$.

§1.4. Algèbres ; polynômes

DÉFINITION 1.4.1. — *Soit k un anneau commutatif. Une* k-algèbre *est un anneau A muni d'un morphisme d'anneaux $i : k \to A$ dont l'image est contenue dans le centre de A.*

Formellement, une k-algèbre est le couple $(A, i : k \to A)$. On dira cependant souvent « soit A une k-algèbre » en sous-entendant le morphisme i. Si $x \in k$ et $a \in A$, on commetra ainsi l'abus d'écriture en notant xa au lieu de $i(x)a$. Noter cependant que i n'est pas forcément injectif. Noter aussi que A n'est pas forcément commutatif.

DÉFINITION 1.4.2. — *Si (A, i) et (B, j) sont des k-algèbres, un* morphisme *de k-algèbres $f : A \to B$ est un morphisme d'anneaux tel que pour tout $x \in k$ et tout $a \in A$, $f(i(x)a) = j(x)f(a)$.*

Exercice 1.4.3. — Vérifier que l'image $f(A)$ d'un morphisme de k-algèbres $f : A \to B$ est une sous-k-algèbre de B.

Exemples 1.4.4. — a) Si k est un sous-anneau d'un anneau commutatif A, l'injection naturelle $k \hookrightarrow A$ munit A d'une structure de k-algèbre.

b) Tout anneau est de manière unique une $\mathbf{Z}$-algèbre. En effet, si A est un anneau, il existe un unique morphisme $i : \mathbf{Z} \to A$. (On a nécessairement $i(0) = 0$, $i(1) = 1$; par récurrence, $i(n)$ est défini pour $n \geqslant 1$ et enfin, $i(n) = -i(-n)$ si $n \leqslant 0$.)

c) Soit K une algèbre à division et soit $i\colon \mathbf{Z} \to K$ l'homomorphisme canonique. Si i n'est pas injectif, son noyau est de la forme $p\mathbf{Z}$, pour un nombre premier p et l'image de i est un sous-corps commutatif K_0 de K de cardinal p. Si i est injectif, son image est isomorphe à $\mathbf{Z}$ et K contient l'ensemble des fractions a/b, pour a et b dans $i(\mathbf{Z})$, $b \neq 0$, qui est un sous-corps K_0 de K isomorphe à $\mathbf{Q}$. Le sous-corps K_0 est appelé sous-corps premier de K ; on dit que K est de caractéristique p si K_0 est un corps à p éléments, et de caractéristique zéro si K_0 est infini.

c) L'anneau $k[X]$ des polynômes à coefficients dans k est une k-algèbre de manière naturelle.

1.4.5. Construction de l'anneau des polynômes.— Soit A un anneau et soit I un ensemble. L'ensemble $\mathbf{N}^{(I)}$ est l'ensemble des multi-indices indexés par I : ses éléments sont des familles (n_i) formés d'entiers positifs ou nuls, presque tous nuls. Lorsque I est fini de cardinal d, $\mathbf{N}^{(I)}$ s'identifie naturellement à $\mathbf{N}^d$. Soit $\mathscr{P}_I$ l'ensemble $R^{(\mathbf{N}^I)}$ formé des familles $(a_m)_{m\in\mathbf{N}^I}$ d'éléments de A, indexées par $\mathbf{N}^{(I)}$ dont presque tous les termes sont égaux à 0. Muni de l'addition terme à terme, c'est un groupe abélien. Soit $P = (p_m)$ et $Q = (q_m)$ des éléments de $\mathscr{P}_I$. Si $m \in \mathbf{N}^{(I)}$, il n'y a qu'un nombre fini de couples de multiindices (m', m'') tels que $m = m' + m''$; on peut alors poser

$$r_m = \sum_{m'+m''=m} p_{m'} q_{m''};$$

la famille (r_m) est presque nulle, donc définit un élément de $\mathscr{P}_I$.

On vérifie (un peu laborieusement si I est infini) que cette loi $(P,Q) \mapsto R$ est associative et fait de $\mathscr{P}_I$ un anneau.

Si $i \in I$, notons X_i l'élement de $\mathscr{P}_I$ dont l'unique terme non nul est celui correspondant au multiindice δ_i (qui vaut 1 en i et 0 ailleurs), et vaut 1. Si $P = (p_m)$, on constate que l'on a

$$P = \sum_{m\in\mathbf{N}^{(I)}} p_m \prod_{i\in I} X_i^{m_i}.$$

L'anneau $\mathscr{P}_I$ est appelé anneau des polynômes d'indéterminées $(X_i)_{i\in I}$ à coefficients dans A. On le note $A[(X_i)_{i\in I}]$. Si $I = \{1,\dots,n\}$, on le note plutôt $A[X_1,\dots,X_n]$; si I est un singleton, on le note $A[T]$, où T est l'indéterminée.

Si A est un anneau commutatif, c'est un anneau commutatif, donc une A-algèbre.

Pour $m \in \mathbf{N}^{(I)}$, l'expression $\prod_{i\in I} X_i^{m_i}$ est parfois notée X^m et est appelée monôme ; m_i est son degré en X_i et $\sum m_i$ son degré total. Soit P un polynôme dans $A[(X_i)]$, si $P = \sum a_m X^m$, les monômes de P sont les $a_m X^m$ avec $a_m \neq 0$. Pour $i \in I$, on appelle degré en X_i de P, et l'on note $\deg_{X_i}(P)$, la borne supérieure des degrés en X_i des monômes non nuls de P. De même, le degré total de P, noté $\deg(P)$, est la borne supérieure des degrés totaux des monômes non nuls de P. Ces bornes supérieures sont prises dans $\mathbf{N} \cup \{-\infty\}$: les degrés du polynôme nul sont égaux à $-\infty$.

On a $\deg_{X_i}(P+Q) \leqslant \max(\deg_{X_i}(P), \deg_{X_i}(Q))$, avec égalité si ces deux degrés sont distincts. De plus, on a $\deg_{X_i}(PQ) \leqslant \deg_{X_i}(P) + \deg_{X_i}(Q)$. Si A est intègre, on a égalité (voir ci-dessous). Des relations analogues valent pour le degré total.

PROPOSITION 1.4.6. — *Soit A un anneau intègre. Soit P et $Q \in A[T]$ des polynômes non nuls. Alors,* $\deg(PQ) = \deg(P) + \deg(Q)$. *En particulier, $PQ \neq 0$.*

Démonstration. — Notons $P = p_0 + p_1 T + \cdots + p_n T^n$ et $Q = q_0 + \cdots + q_m T^m$ les coefficients de P, avec $n = \deg P$ et $m = \deg Q$, de sorte que que $p_n \neq 0$ et $q_m \neq 0$. Alors,

$$PQ = p_0 q_0 + (p_0 q_1 + p_1 q_0) T + \cdots + (p_{n-1} q_m + p_n q_{m-1}) T^{n+m-1} + p_n q_m T^{n+m}.$$

Comme A est intègre, $p_n q_m \neq 0$ et le degré de PQ est égal à $n+m$, ce qu'il fallait démontrer. □

COROLLAIRE. — *Soit A est un anneau intègre, il en est de même de l'anneau des polynômes $A[(X_i)]$. En outre, pour tous polynômes P, Q, on a la relation* $\deg_{X_i}(PQ) = \deg_{X_i}(P) + \deg_{X_i}(Q)$.

Démonstration. — Nous devons démontrer que le produit de deux polynômes non nuls n'est pas nul et que son degré en la variable X_i est la somme des degrés. Pour ce faire, nous pouvons supposer qu'il n'y a qu'un nombre fini de variables, puis raisonner par récurrence sur le nombre de variables. Soit A' l'anneau des polynômes à coefficients dans A en les variables X_j, pour $j \neq i$; par récurrence, c'est un anneau intègre. Grâce à l'isomorphisme $A[(X_j)_{j\in I}] \simeq A'[X_i]$, le corollaire découle donc de la proposition précédente. □

La notion de degré d'un polynôme intervient aussi dans le théorème de division euclidienne :

THÉORÈME 1.4.7. — *Soit A un anneau et soit P et Q deux polynômes de $A[X]$. On suppose que $Q \neq 0$ et que le coefficient du terme de plus haut degré de Q est inversible*[(1)]. *Alors, il existe un unique couple de polynômes (R, S) dans $A[X]$ vérifiant les propriétés*

- $P = RQ + S$;
- $\deg S < \deg Q$.

Démonstration. — On commence par l'unicité. Si $P = RQ + S = R'Q + S'$, alors $Q(R' - R) = S' - S$ est de degré au plus $\max(\deg S, \deg S') < \deg Q$. Supposons $R \neq R'$, c'est-à-dire $R' - R \neq 0$. Alors, si $uX^{\deg Q}$ et aX^m sont les termes de plus haut degré dans Q et $R' - R$ respectivement, le terme de plus haut degré dans $Q(R' - R)$ est donné par $auX^{m+\deg Q}$. Comme u est inversible et $a \neq 0$, $au \neq 0$. Ainsi, $Q(R' - R)$ est de degré $m + \deg Q \geqslant \deg Q$. Cette contradiction montre que $R = R'$, puis $S = P - RQ = P - R'Q = S'$.

(1) Rappelons à ce propos qu'un polynôme dont le coefficient dominant est égal à 1 est dit *unitaire*.

Montrons maintenant l'existence du couple (R,S) comme dans le théorème. Notons toujours $uX^{\deg Q}$ le terme de plus haut degré de Q. On raisonne par récurrence sur le degré de P. Si $\deg P < \deg Q$, il suffit de poser $R=0$ et $S=P$. Sinon, soit $aX^{\deg P}$ le terme de plus haut degré de P. Alors, $P' = P - au^{-1}X^{\deg P - \deg Q}Q$ est un polynôme de degré au plus $\deg P$ mais dont le coefficient du terme de degré $\deg P$ est égal à $a - au^{-1}u = 0$. Ainsi, $\deg P' < \deg P$. Par récurrence, il existe deux polynômes R' et S' dans $A[X]$ tels que

$$P' = R'Q + S' \quad \text{et} \quad \deg S' < \deg Q.$$

Alors, on a

$$P = P' + au^{-1}X^{\deg P - \deg Q}Q = (R' + au^{-1}X^{\deg P - \deg Q})Q + S'.$$

Il suffit maintenant de poser $R = R' + au^{-1}X^{\deg P - \deg Q}$ et $S' = S$. Le théorème est donc démontré. □

La k-algèbre des polynômes jouit d'une *propriété universelle* importante :

PROPOSITION 1.4.8. — *Soit k un anneau commutatif. Soit A une k-algèbre et soit $n \geqslant 1$ un entier non nul. Pour tout n-uplet $(a_1,\dots,a_n)$ d'éléments de A qui commutent deux à deux, il existe un unique homomorphisme de k-algèbres $f\colon k[X_1,\dots,X_n]$ tel que pour tout $i \in \{1,\dots,n\}$, $f(X_i) = a_i$.*

Démonstration. — Si un tel morphisme existe, il doit vérifier

$$f(\lambda X_1^{m_1}\dots X_n^{m_n}) = \lambda f(X_1)^{m_1}\dots f(X_n)^{m_n} = \lambda a_1^{m_1}\dots a_n^{m_n}.$$

Par suite, si $P = \sum_{\mathbf{m}} \lambda_{\mathbf{m}} X_1^{m_1}\dots X_n^{m_n}$, on doit avoir

$$f(P) = \sum_{\mathbf{m}} \lambda_{\mathbf{m}} a_1^{m_1}\dots a_n^{m_n},$$

ce qui prouve qu'il existe au plus un tel morphisme de k-algèbres, et que s'il existe, il est défini par cette dernière formule. Réciproquement, il est facile de prouver, en utilisant le fait que les a_i commutent deux à deux, que cette formule définit un morphisme de k-algèbres. □

Un exemple d'un tel morphisme est fourni par la théorie des polynômes d'endomorphismes. On choisit pour k un corps, pour A l'anneau des endomorphismes d'un k-espace vectoriel V, voire l'anneau $\mathrm{M}_n(k)$ des matrices $n \times n$ à coefficients dans k. Alors, pour tout élément a de A et tout polynôme $P \in k[X]$, on peut calculer $P(a)$ et ces éléments obéissent aux règles de calcul usuelles, qui ne font rien d'autre que traduire le fait que l'application de $k[X]$ dans A donnée par $P \mapsto P(a)$ est un homomorphisme d'anneaux.

Ce morphisme est parfois appelé, surtout lorsque $A = k$, morphisme d'*évaluation* en le point $(a_1,\dots,a_n)$. L'image d'un polynôme P est notée $P(a_1,\dots,a_n)$. Il en résulte par exemple un morphisme de k-algèbres $k[X_1,\dots,X_n] \to \mathscr{F}(k^n,k)$ des polynômes dans

la k-algèbre des fonctions de k^n dans k. Les fonctions qui sont dans l'image de ce morphisme sont tout naturellement appelées *fonctions polynomiales*.

1.4.9. Algèbre engendrée par une partie. — Soit A une k-algèbre et soit S une partie de A. La k-algèbre $k[S]$ est par définition la plus petite sous-k-algèbre de A qui contient S. C'est l'ensemble des combinaisons linéaires de la forme $\lambda s_1^{m_1} \dots s_n^{m_n}$ pour $\lambda \in k$, les s_i dans S et les m_i dans $\mathbf{N}$.

Si $S = \{a_1, \dots, a_n\}$, $k[S]$ est aussi notée $k[a_1, \dots, a_n]$. Si de plus les a_i commutent deux à deux, c'est l'image du morphisme d'évaluation $k[X_1, \dots, X_n] \to A$ en $(a_1, \dots, a_n)$.

Démonstration. — Notons φ ce morphisme d'évaluation. Comme $\varphi(X_i) = a_i$, $\operatorname{im}\varphi$ est une sous-k-algèbre de A qui contient les a_i, donc $\operatorname{im}\varphi$ contient $k[a_1, \dots, a_n]$. Réciproquement, toute sous-k-algèbre de A qui contient $\{a_1; \dots; a_n\}$ contient les éléments de A de la forme $\lambda a_1^{m_1} \dots a_n^{m_n}$ et aussi leurs combinaisons linéaires. Par suite, $k[a_1, \dots, a_n]$ contient $\operatorname{im}\varphi$. On a ainsi égalité. □

Exercices. — 33) Utiliser la propriété universelle des anneaux de polynômes pour démontrer qu'il existe un unique morphisme de k-algèbres $\varphi : k[X, Y] \to k[X][Y]$ tel que $\varphi(X) = X$ et $\varphi(Y) = Y$ et que c'est un isomorphisme.

34) Soit M un monoïde, c'est-à-dire un ensemble muni d'une loi associative et possédant un élément neutre 1. Soit A un anneau. Si $m \in M$, on note e_m l'élément de A^M dont toutes les coordonnées sont nulles sauf celle d'indice m qui vaut 1.

a) Montrer que le groupe abélien $A^{(M)}$ possède une unique structure d'anneau telle que $(ae_m)(a'e_{m'}) = (aa')e_{mm'}$ pour m et m' dans M, a et a' dans A.

b) Lorsque M est un groupe, on retrouve l'anneau du groupe. Lorsque M est le monoïde $\mathbf{N}$, pour l'addition, on retrouve l'anneau des polynômes en une indéterminée.

c) Lorsque M est le groupe $\mathbf{Z}/n\mathbf{Z}$, construire un isomorphisme d'anneaux de $A^{(M)}$ sur l'anneau quotient $A[T]/(T^n - 1)$.

35) On dit qu'un anneau A possède une division euclidienne à droite s'il existe une application $\varphi : A \setminus \{0\} \to \mathbf{N}$ de sorte que pour tout couple (a, b) d'éléments de A, $b \neq 0$, il existe un couple (q, r) d'éléments de A tels que $a = qb + r$ avec $r = 0$ ou $\varphi(r) < \varphi(b)$.

Si A possède une division euclidienne à droite, tout idéal à gauche de A est de la forme Aa. (Soit I un idéal à gauche de A ; si $I \neq 0$, soit a un élément non nul de I tel que $\varphi(a)$ soit minimal. Montrer que $I = Aa$.) C'est en particulier le cas des anneaux de polynômes $K[X]$, lorsque K est un anneau à division.

36) Soit A un anneau, soit P et Q des polynômes à coefficients dans A en une indéterminée X, de degrés m et n respectivement. Soit a le coefficient dominant de Q et $\mu = \max(1 + m - n, 0)$. Montrer qu'il existe un couple de polynômes (R, S) tel que $a^\mu P = QR + S$ et $\deg S < n$. Montrer que ce couple est unique si A est intègre, ou si, plus généralement, a est simplifiable.

37) Soit k un corps et $A = k[X_1, \dots, X_n]$; un idéal de A est dit monomial s'il est engendré par des monômes.

a) Montrer qu'un monôme M appartient à un idéal monomial $I = (M_\alpha)_{\alpha \in E}$ si et seulement si c'est un multiple d'un des monômes M_α.

b) Montrer que les deux propriétés suivantes sont équivalentes :

a) I est un idéal monomial

b) $P \in I$ si et seulement si chaque monôme de P appartient à I.

c) Montrer que si I et J sont des idéaux monomiaux de A, il en est de même des idéaux $I + J$, $I.J$, $I \cap J$, $I : J$ et $\sqrt{I}$. Donner des systèmes de générateurs monomiaux de ces idéaux en fonctions de ceux de I et J.

38) Soit k un corps et soit $I = (M_\alpha)_{\alpha \in E}$ un idéal monomial de $k[X_1, \dots, X_n]$. On veut montrer qu'il existe une partie finie $F \subset E$ telle que $I = (M_\alpha)_{\alpha \in F}$. On va procéder par récurrence sur le nombre n d'indéterminées.

a) Traiter le cas $n = 1$.

b) On fixe dans la suite $n \geqslant 2$ et on suppose que l'assertion est vraie s'il y a $< n$ indéterminées.

Soit $i \in \{1, \dots, n\}$, on définit

$$\begin{aligned} \varphi_i : k[X_1, \dots, X_n] &\to k[X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_n] \\ P(X_1, \dots X_n) &\mapsto P(X_1, \dots, X_{i-1}, 1, X_{i+1}, \dots, X_n) \end{aligned}$$

En utilisant l'hypothèse de récurrence remarquer qu'il existe une partie finie $F_i \subset E$ telle que pour tout $\alpha \in E$ le monôme $\varphi_i(M_\alpha)$ peut s'écrire $\varphi_i(M_\alpha) = M'_\alpha \times \varphi_i(M_\beta)$ pour un $\beta \in F_i$.

c) Soit F_0 l'ensemble des $\alpha \in E$ tels que pour tout $i \in \{1, \dots, n\}$, on ait

$$\deg_{X_i} M_\alpha < \max\{\deg_{X_i} M_\beta ;\ \beta \in F_i\}\}$$

et $F = \bigcup_{i=0}^{n} F_i$. Montrer que $I = (M_\alpha)_{\alpha \in F}$.

39) Soit A un anneau, I un ensemble et M l'ensemble $\mathbf{N}^{(I)}$ des multiindices indexés par I. Soit $\mathscr{F}_I = A^M$ l'ensemble des familles d'éléments de A indexées par M ; muni de l'addition terme à terme, c'est un groupe abélien.

a) Montrer que les formules donnant la multiplication des polynômes s'étendent à $\mathscr{F}_I$ et le munissent d'une structure d'anneau. L'anneau des polynômes $\mathscr{P}_I$ en est un sous-anneau.

Si X_i désigne l'indéterminée d'indice i, un élément de $\mathscr{F}_I$ est une série infinie $\sum_m a_m X_1^{m_1} \dots X_n^{m_n}$. On l'appelle l'anneau des séries formelles en les indéterminées (X_i). Si $I = \{1, \dots, n\}$, on le note $A[[X_1, \dots, X_n]]$, et $A[[X]]$ si I est un singleton et que l'indéterminée est notée X.

b) Supposons que k soit un anneau commutatif. Pour toute k-algèbre A et toute famille $(a_1, \dots, a_n)$ d'éléments nilpotents de A qui commutent deux à deux, montrer qu'il existe un unique homomorphisme $\varphi : k[[X_1, \dots, X_n]] \to A$ tel que $\varphi(X_i) = a_i$.

c) On suppose encore que k est un anneau commutatif. Montrer qu'un élément $\sum a_n X^n$ de $k[[X]]$ est inversible si et seulement si a_0 est un élément inversible de k.

40) Soit k un corps. Notons Φ l'homomorphisme d'évaluation de $k[X_1,\dots,X_n]$ dans $\mathscr{F}(k^n,k)$

a) Soit $A_1,\dots,A_n$ des parties de k. Soit $P\in k[X_1,\dots,X_n]$ un polynôme en n variables tel que $\deg_{X_i}(P)<\operatorname{card}(A_i)$ pour tout i. Si $P(a_1,\dots,a_n)=0$ pour tout $(a_1,\dots,a_n)\in A_1\times\cdots\times A_n$, montrer que $P=0$.

b) Si k est un corps infini, montrer que Φ est injectif. Montrer qu'il n'est pas surjectif.

c) On suppose maintenant que k est un corps fini. Montrer que Φ est surjectif ; donner en particulier un antécédent explicite de tout élément de $\mathscr{F}(k^n;k)$ (penser aux polynômes interpolateurs de Lagrange). Montrer que Φ n'est pas injectif ; si $q=\operatorname{card}(k)$, montrer que son noyau est engendré par les polynômes $X_i^q-X_i$, pour $1\leqslant i\leqslant n$.

§1.5. Anneaux quotients

Étant donnés un anneau et une relation d'équivalence convenable sur cet anneau, l'objectif est de munir l'ensemble des classes d'équivalence d'une structure d'anneau. Cela revient en fait à « rendre nuls » les éléments d'un idéal de l'anneau sans modifier les autres règles de calcul.

A. Construction

Rappelons qu'une relation $\mathscr{R}$ sur un ensemble X est dite *relation d'équivalence* si elle est réflexive (pour tout x, $x\mathscr{R}x$), symétrique (si $x\mathscr{R}y$, alors $y\mathscr{R}x$) et transitive (si $x\mathscr{R}y$ et $y\mathscr{R}z$, alors $x\mathscr{R}z$). L'ensemble des classes d'équivalence de X pour la relation $\mathscr{R}$ est noté $X/\mathscr{R}$.

Soit maintenant A un anneau. On peut alors chercher les relations d'équivalence sur A qui sont *compatibles avec la structure d'anneau.* On veut ainsi que soient satisfaite la propriété :

$$\text{si } x\mathscr{R}y \text{ et } x'\mathscr{R}y', \text{ alors } x+x'\mathscr{R}y+y' \text{ et } xx'\mathscr{R}yy'.$$

Notons alors I la classe d'équivalence de 0. Si $x\mathscr{R}y$, comme $y\mathscr{R}y$, on a donc $x-y\mathscr{R}0$, soit $x-y\in I$, et réciproquement. Ainsi, $\mathscr{R}$ est définie par $x\mathscr{R}y$ si et seulement si $x-y\in I$.

Montrons d'autre part que I est un idéal bilatère de A. On a déjà $0\in I$. De plus, si $x\in I$ et $y\in I$, $x\mathscr{R}0$ et $y\mathscr{R}0$, donc $(x+y)\mathscr{R}0$, ce qui prouve que $x+y\in I$. Enfin, si $x\in I$ et $a\in A$, $x\mathscr{R}0$, d'où $ax\mathscr{R}a0$ et $xa\mathscr{R}0a$; comme $a0=0a=0$, on a bien $ax\in I$ et $xa\in I$.

Dans l'autre sens, les calculs ci-dessus montrent que l'on a le théorème suivant.

THÉORÈME 1.5.1. — *Soit A un anneau et soit I un idéal bilatère de A. La relation $\mathscr{R}$ sur A définie par $x\mathscr{R}y$ si et seulement si $x-y\in I$ est une relation d'équivalence compatible avec la structure d'anneau. L'ensemble quotient $A/\mathscr{R}$ possède une unique structure d'anneau telle que la surjection canonique* $\mathrm{cl}:A\to A/\mathscr{R}$ *soit un homomorphisme d'anneaux. Cet homomorphisme est surjectif de noyau I.*

L'*anneau quotient* $A/\mathscr{R}$ est noté A/I. L'homomorphisme $\mathrm{cl}:A\to A/I$ est aussi appelé *surjection canonique.*

Soit a un élément du centre de A ; remarquons que $\mathrm{cl}(a)$ appartient au centre de A/I. En effet, si $x \in A/I$, il existe $b \in A$ tel que $x = \mathrm{cl}(b)$; alors, $\mathrm{cl}(a)x = \mathrm{cl}(a)\,\mathrm{cl}(b) = \mathrm{cl}(ab) = \mathrm{cl}(ba)$ car a est central, donc $\mathrm{cl}(a)x = \mathrm{cl}(b)\,\mathrm{cl}(a) = xa$. Par suite, si k est un anneau et $i : k \to A$ un homomorphisme d'anneaux dont l'image est contenue dans le centre de A, de sorte que (A, i) est une k-algèbre, la composition $\mathrm{cl} \circ i : k \to A \to A/I$ munit A/I d'une (mieux, de l'unique) structure de k-algèbre pour laquelle la surjection canonique est un homomorphisme de k-algèbres.

B. Théorème de factorisation

L'importance de la structure d'anneau quotient vient de sa propriété universelle, manifestée dans le *théorème de factorisation* que nous démontrons maintenant.

THÉORÈME 1.5.2. — *Soit A et B deux anneaux et soit $f : A \to B$ un homomorphisme d'anneaux. Si I est un idéal bilatère de A contenu dans* $\ker f$*, il existe un unique homomorphisme d'anneaux $\bar{f} : A/I \to B$ tel que $f = \bar{f} \circ \mathrm{cl}$.*

Une façon visuelle et commode d'écrire cette dernière égalité est de dire que le diagramme

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle \mathrm{cl}}\downarrow & \nearrow_{\bar{f}} & \\ A/I & & \end{array}$$

est *commutatif*.

Démonstration. — Nécessairement, $\bar{f}$ doit être tel que $\bar{f}(\mathrm{cl}(a)) = f(a)$ pour tout $a \in A$. Comme tout élément de A/I est de la forme $\mathrm{cl}(a)$ pour un certain $a \in A$, cela montre qu'il existe au plus un homomorphisme d'anneaux $\bar{f} : A/I \to B$ tel que $f = \bar{f} \circ \mathrm{cl}$.

Montrons maintenant l'existence de $\bar{f}$. Soit x un élément de A/I. On sait qu'il existe $a \in A$ tel que $x = \mathrm{cl}(a)$. Si a' est un autre représentant de x, donc tel que $x = \mathrm{cl}(a')$, on a $a' - a \in I$, donc, puisque $I \subset \ker f$, $f(a' - a) = 0$ et par conséquent, $f(a) = f(a')$. On peut ainsi poser $\bar{f}(x) = f(a)$ — le résultat est indépendant du représentant a choisi. Il reste à montrer que $\bar{f}$ est un homomorphisme d'anneaux.

Comme $\mathrm{cl}(0_A) = 0_{A/I}$ et $\mathrm{cl}(1_A) = 1_{A/I}$, on a bien $f(0_{A/I}) = 0_B$ et $f(1_{A/I}) = 1_B$. De plus, si $x = \mathrm{cl}(a)$ et $y = \mathrm{cl}(b)$ sont deux éléments de A/I, on a $x + y = \mathrm{cl}(a + b)$ et

$$\begin{aligned} \bar{f}(x + y) = \bar{f}(\mathrm{cl}(a + b)) = f(a + b) = f(a) + f(b) = \bar{f}(\mathrm{cl}(a)) + \bar{f}(\mathrm{cl}(b)) \\ = f(x) + f(y) \end{aligned}$$

et, de même,

$$\bar{f}(xy) = f(ab) = f(a)f(b) = \bar{f}(x)\bar{f}(y).$$

Il en résulte que $\bar{f}$ est un homomorphisme d'anneaux. Le théorème est ainsi démontré. □

Le noyau de $\bar{f}$ sera calculé à la proposition 1.5.5. Notamment, on montrera que $\bar{f}$ *est injectif si et seulement si* $I = \ker f$. Soit $f : A \to B$ un homomorphisme d'anneaux. On a vu (page 4) que $f(A)$ est un sous-anneau de B. Ainsi, on peut décomposer f en

$$A \xrightarrow{\mathrm{cl}} A/\ker f \xrightarrow{\bar{f}} f(A) \hookrightarrow B$$

c'est-à-dire en la composition d'un homomorphisme surjectif, d'un isomorphisme et d'un homomorphisme injectif.

Soit A un anneau et soit I un idéal de A. On s'intéresse maintenant aux idéaux de l'anneau A/I. Soit $\mathscr{J}$ un idéal à gauche de A/I. On sait que $\mathrm{cl}^{-1}(\mathscr{J})$ est un idéal à gauche de A. Par construction, il contient I puisque pour tout $a \in I$, $\mathrm{cl}(a) = 0$ est un élément de $\mathscr{J}$.

La propriété importante est donnée par la proposition :

PROPOSITION 1.5.3. — *Soit A un anneau et soit I un idéal bilatère de A. L'application* cl^{-1} *:*

$$\begin{array}{ccc} \textit{idéaux à gauche de } A/I & \to & \textit{idéaux à gauche de } A \textit{ contenant } I \\ \mathscr{J} & \mapsto & \mathrm{cl}^{-1}(\mathscr{J}) \end{array}$$

est une bijection.

Un résultat analogue vaut pour les idéaux à droite et les idéaux bilatères.

Autrement dit, pour tout idéal à gauche J de A qui contient I, il existe un unique idéal $\mathscr{J}$ de A/I tel que $J = \mathrm{cl}^{-1}(\mathscr{J})$. *De plus, on a* $\mathscr{J} = \mathrm{cl}(J)$ (image de l'idéal J par la surjection canonique, laquelle image se trouve être encore un idéal à gauche dans ce cas).

Démonstration. — Commencer par construire la bijection réciproque. Si J est un idéal de A, montrons d'abord que $\mathrm{cl}(J)$ est un idéal à gauche de A. On a bien $0 = \mathrm{cl}(0) \in \mathrm{cl}(J)$. D'autre part, si x et y appartiennent à $\mathrm{cl}(J)$, soit a et b des éléments de J tels que $x = \mathrm{cl}(a)$ et $y = \mathrm{cl}(b)$. Alors, $x+y = \mathrm{cl}(a)+\mathrm{cl}(b) = \mathrm{cl}(a+b)$; comme J est un idéal à gauche de A, $a+b$ appartient à J et $x+y$ appartient bien à $\mathrm{cl}(J)$. Enfin, soit x un élément de $\mathrm{cl}(J)$ et y un élément de A/I. Choisissons encore $a \in J$ et $b \in A$ tels que $x = \mathrm{cl}(a)$ et $y = \mathrm{cl}(b)$. On a $yx = \mathrm{cl}(b)\,\mathrm{cl}(a) = \mathrm{cl}(ba) \in \mathrm{cl}(J)$ puisque, J étant un idéal à gauche de A, $ba \in J$.

Si $\mathscr{J}$ est un idéal à gauche de A/I, on a

$$\boxed{\mathrm{cl}(\mathrm{cl}^{-1}(\mathscr{J})) = \mathscr{J}.}$$

Montrons les deux inclusions. Un élément x de $\mathrm{cl}(\mathrm{cl}^{-1}(\mathscr{J}))$ est de la forme $x = \mathrm{cl}(a)$ pour $a \in \mathrm{cl}^{-1}(\mathscr{J})$. On a donc $x \in \mathscr{J}$. Réciproquement, si $x \in \mathscr{J}$, soit $a \in A$ tel que $x = \mathrm{cl}(a)$. Alors, $\mathrm{cl}(a) = x \in \mathscr{J}$, donc a appartient à $\mathrm{cl}^{-1}(\mathscr{J})$ et x appartient bien à $\mathrm{cl}(\mathrm{cl}^{-1}(\mathscr{J}))$.

Enfin, si J est un idéal à gauche de A, on a

$$\boxed{\mathrm{cl}^{-1}(\mathrm{cl}(J)) = I + J.}$$

Là encore, montrons les deux inclusions. Si $x \in I+J$, on peut écrire $x = a+b$ avec $a \in I$ et $b \in J$. Il en résulte $\mathrm{cl}(x) = \mathrm{cl}(a)+\mathrm{cl}(b) = \mathrm{cl}(b) \in \mathrm{cl}(J)$. Donc $x \in \mathrm{cl}^{-1}(\mathrm{cl}(J))$. Dans l'autre sens, soit $x \in \mathrm{cl}^{-1}(\mathrm{cl}(J))$. Par définition, $\mathrm{cl}(x) \in \mathrm{cl}(J)$ et il existe $a \in J$ tel que $\mathrm{cl}(x) = \mathrm{cl}(a)$. On a alors $\mathrm{cl}(x-a) = 0$, ce qui signifie que $x-a \in I$. Finalement, $x = (x-a)+a$ appartient à $I+J$, ainsi qu'il fallait démontrer.

Si de plus J contient I, alors $I+J = J$ et les deux formules établies montrent que l'application cl^{-1} définit une bijection de l'ensemble des idéaux à gauche de A/I sur l'ensemble des idéaux à gauche de A contenant I, dont la bijection réciproque est donnée par cl. □

Lorsque J est un idéal à gauche de A qui contient I, l'idéal $\mathrm{cl}(J)$ de A/I est aussi noté J/I. Cette notation intervient notamment lorsque l'homomorphisme cl est omis des notations. L'expression « soit J/I un idéal de $A/I\ldots$ » sous-entendra toujours que J est un idéal de A contenant I.

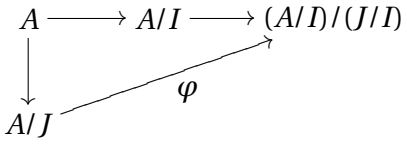
PROPOSITION 1.5.4. — *Soit A un anneau, soit I un idéal bilatère de A et soit J un idéal bilatère de A contenant I. La composition des surjections canoniques $A \to A/I \to (A/I)/(J/I)$ a pour noyau J. Il en résulte un isomorphisme canonique*

$$A/J \simeq (A/I)/(J/I).$$

En résumé, un quotient d'un quotient est encore un quotient.

Démonstration. — La composée de deux homomorphismes surjectifs étant encore surjectif, le morphisme $A \to (A/I)/(J/I)$ est surjectif. Un élément $a \in A$ appartient au noyau si et seulement si $\mathrm{cl}(a) \in A/I$ appartient au noyau de l'homomorphisme $A/I \to (A/I)/(J/I)$, c'est-à-dire $\mathrm{cl}(a) \in (J/I)$. Comme $J/I = \mathrm{cl}(J)$, cela signifie que $a \in \mathrm{cl}^{-1}(\mathrm{cl}(J)) = J$ puisque J contient I.

Le théorème de factorisation affirme alors l'existence d'un unique homomorphisme $\varphi : A/J \to (A/I)/(J/I)$ rendant le diagramme



commutatif. Cet homomorphisme est surjectif. Soit $x \in A/J$ un élément tel que $\varphi(x) = 0$. Soit $a \in A$ tel que $x = \mathrm{cl}_J(a)$. Par définition de φ, on a $\varphi(x) = \mathrm{cl}_{J/I} \circ \mathrm{cl}\, I(a) = 0$, c'est-à-dire $a \in J$. Ainsi, $x = 0$ et l'homomorphisme φ est injectif. C'est donc un isomorphisme □

La dernière partie de la démonstration peut être généralisée en un complément important au théorème de factorisation

PROPOSITION 1.5.5. — *Soit $f : A \to B$ un morphisme d'anneaux et soit I un idéal bilatère de A contenu dans* $\ker f$. *Soit $\bar{f} : A/I \to B$ l'homomorphisme fourni par le théorème de factorisation. Alors, le noyau de $\bar{f}$ est égal à* $(\ker f)/I$.

Démonstration. — En effet, si $\bar{f}(x) = 0$, soit $a \in A$ tel que $x = \mathrm{cl}(a)$. On a alors $f(a) = 0$, d'où $a \in \ker f$ et $x = \mathrm{cl}(a) \in \mathrm{cl}(\ker f) = (\ker f)/I$. Réciproquement, si $x \in (\ker f)/I$, il existe $a \in \ker f$ tel que $x = \mathrm{cl}(a)$. On a alors $\bar{f}(x) = f(a) = 0$ et $x \in \ker \bar{f}$. □

C. Lemme chinois

Deux idéaux bilatères I et J d'un anneau A sont dits comaximaux si $I + J = A$. Ils donnent lieu à la forme générale du *théorème chinois*.

THÉORÈME 1.5.6. — *Soit A un anneau, I et J deux idéaux bilatères de A qui sont comaximaux.*

L'homomorphisme canonique $A \to (A/I) \times (A/J)$ donné par $a \mapsto (\mathrm{cl}_I(a), \mathrm{cl}_J(a))$ est surjectif; son noyau est l'idéal bilatère $I \cap J$. Il en résulte, par passage au quotient, un isomorphisme

$$\boxed{A/(I \cap J) \simeq A/I \times A/J.}$$

COROLLAIRE 1.5.7. — *Soit I et J deux idéaux bilatères comaximaux d'un anneau A; pour tout couple (x, y) d'éléments de A, il existe $a \in A$ tel que $a \in x + I$ et $a \in y + J$.*

Démonstration. — Considérons le diagramme d'anneaux

$$\begin{array}{ccc} & A & \\ \swarrow & & \searrow \\ A/(I \cap J) & \xrightarrow{\varphi} & A/I \times A/J \end{array}$$

dans lequel on doit montrer l'existence d'un unique flèche φ, dessinée en traits pointillés, qui le rende commutatif et qui soit un isomorphisme. Or, le morphisme $A \to A/I \times A/J$ envoie $a \in A$ sur $(\mathrm{cl}_I(a), \mathrm{cl}_J(a))$. Son noyau est donc $I \cap J$. D'après la propriété universelle des anneaux quotients, il existe un unique morphisme φ rendant le diagramme commutatif; pour tout $a \in A$, on a $\varphi(\mathrm{cl}_{I\cap J}(a)) = (\mathrm{cl}_I(a), \mathrm{cl}_J(a))$.

Montrons que φ est un isomorphisme. Comme $I+J = A$, il existe $x \in I$ et $y \in J$ tels que $x + y = 1$. Alors, on a les égalités $1 = \mathrm{cl}_I(x + y) = \mathrm{cl}_I(y)$ dans A/I et $1 = \mathrm{cl}_J(x + y) = \mathrm{cl}_J(x)$ dans A/J. Par suite, $\varphi(x) = (\mathrm{cl}_I(x), \mathrm{cl}_J(x)) = (0, \mathrm{cl}_J(x + y)) = (0, 1)$ tandis que $\varphi(y) = (1, 0)$. Si a et b sont dans A, il en résulte que

$$\varphi(bx + ay) = (0, \mathrm{cl}(b)) + (\mathrm{cl}(a), 0) = (\mathrm{cl}(a), \mathrm{cl}(b)).$$

Tout élément de $A/I \times A/J$ étant de la forme $(\mathrm{cl}(a), \mathrm{cl}(b))$, φ est surjectif. □

Remarque 1.5.8. — Soit I et J des idéaux d'un anneau commutatif A tels que $I + J = A$; on a $I \cap J = IJ$.

On a déjà remarqué l'inclusion $IJ \subset I \cap J$, vraie sans supposer que l'anneau commutatif ni les idéaux I et J comaximaux. Inversement, soit $a \in I \cap J$. Puisque $I + J = A$, il existe $x \in I$ et $y \in J$ tels que $x + y = 1$. On a donc $a = (x + y)a = xa + ya$. Comme $x \in I$ et $a \in J$, $xa \in IJ$; comme $ya = ay$, que $y \in J$ et $a \in I$, $ya = ay \in IJ$. Par suite, $a \in IJ$.

Exercices. — 41) Soit n un entier $\geqslant 1$. On note $s : \mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$ la surjection canonique.

a) Étant donné un entier m, montrer que $s(m)$ est inversible dans l'anneau $\mathbf{Z}/n\mathbf{Z}$ si et seulement si n et m sont premiers entre eux.

b) Montrer que l'anneau $\mathbf{Z}/n\mathbf{Z}$ est intègre si et seulement si n est premier.

c) Si n est premier, montrer que l'anneau $\mathbf{Z}/n\mathbf{Z}$ est un corps.

d) Déterminer l'idéal $\sqrt{n\mathbf{Z}}$.

42) Soit A un anneau commutatif, soit a et b deux éléments de A. Montrer les assertions suivantes :

a) l'anneau $A[X]/(X - a)$ est isomorphe à A ;

b) l'anneau $A[X, Y]/(Y - b)$ est isomorphe à $A[X]$;

c) l'anneau $A[X, Y]/(X - a, Y - b)$ est isomorphe à A.

43) Soit K un corps. On pose $A = K[X, Y]/(X^2, XY, Y^2)$.

a) Déterminer les éléments inversibles de A ;

b) déterminer tous les idéaux principaux de A ;

c) déterminer tous les idéaux de A.

44) Soit A un anneau et soit I l'idéal bilatère engendré par les $xy - yx$ pour $x, y \in A$.

a) Montrer que l'anneau A/I est commutatif.

b) Soit J un idéal bilatère de A tel que A/J soit un anneau commutatif. Montrer que $I \subset J$.

45) a) Soit K un corps commutatif et $P \in K[X]$ un polynôme à coefficients dans K. Montrer que l'anneau $K[X]/(P)$ est un corps si et seulement si P est irréductible dans $K[X]$.

b) Montrer que le polynôme $X^2 + 1$ est irréductible dans $\mathbf{Z}[X]$. L'anneau $A = \mathbf{Z}[X]/(X^2 + 1)$ est-il un corps ? (Définir un isomorphisme de A sur l'anneau $\mathbf{Z}[i]$.)

c) Montrer que le polynôme $X^2 + 1$ est irréductible dans $\mathbf{F}_p[X]$ si et seulement si $p \equiv 3 \pmod 4$.

d) Quel est le cardinal de l'anneau A/pA ? Pour quels nombres premiers p est-il un corps ? Sinon, et si p est impair, construire un isomorphisme de A/pA sur $\mathbf{F}_p \times \mathbf{F}_p$. Que se passe-t-il pour $p = 2$?

46) Soit A un anneau, soit I un idéal de A. On note $I[X]$ l'ensemble des polynômes $P \in A[X]$ dont tous les coefficients appartiennent à I.

a) Montrer que $I[X]$ est un idéal à gauche de $A[X]$.

b) Si I est un idéal bilatère de A, montrer que $I[X]$ est un idéal bilatère de $A[X]$ et construire un isomorphisme de l'anneau $A[X]/I[X]$ sur l'anneau $(A/I)[X]$.

47) Soit A un anneau, soit I un idéal bilatère de A et soit $M_n(I)$ l'ensemble des matrices de $M_n(A)$ dont tous les coefficients appartiennent à I.

a) Montrer que $M_n(I)$ est un idéal bilatère de $M_n(A)$ et construire un isomorphisme d'anneaux de $M_n(A)/M_n(I)$ sur $M_n(A/I)$.

b) Inversement, montrer que tout idéal bilatère de $M_n(A)$ est de la forme $M_n(I)$, pour I un idéal bilatère de A.

§1.6. Anneaux de fractions (cas commutatif)

Au paragraphe précédent, nous avons d'une certaine façons « forcé » des éléments d'un anneau à être nuls ; nous voulons maintenant effectuer une opération opposée : rendre *inversibles* les éléments d'une partie convenable. *Dans tout ce paragraphe, nous nous restreignons au cas d'un anneau commutatif.*

DÉFINITION 1.6.1. — *Soit A un anneau. Une partie S de A est dite* multiplicative *si elle vérifie les propriétés :*

– $1 \in S$;
– *pour tous a et b dans S, $ab \in S$.*

Étant donnés un anneau commutatif A et une partie multiplicative S de A, nous allons construire un anneau $S^{-1}A$ et un homomorphisme $i : A \to S^{-1}A$ tel que $i(S)$ est formé d'éléments inversibles dans $S^{-1}A$. Donnons d'abord quelques exemples :

Exemple 1.6.2. — a) Si $A = \mathbf{Z}$ et $S = \mathbf{Z} \setminus \{0\}$, l'anneau $S^{-1}A$ sera égal à $\mathbf{Q}$ et $i : \mathbf{Z} \to \mathbf{Q}$ l'injection usuelle. Plus généralement, si A est un anneau intègre, $S = A \setminus \{0\}$ est une partie multiplicative et l'anneau $S^{-1}A$ est le corps des fractions de A.

b) Si S est formé d'éléments inversibles, alors $S^{-1}A = A$.

c) Si $A = \mathbf{Z}$ et $S = \{1; 10; 100; \ldots\}$ est l'ensemble des puissances de 10 dans $\mathbf{Z}$, alors $S^{-1}A$ sera l'ensemble des nombres décimaux, c'est-à-dire l'ensemble des nombres rationnels qui peuvent s'écrire sous la forme $a/10^n$ avec $a \in \mathbf{Z}$ et $n \in \mathbf{N}$.

Ainsi, ce qu'on veut imiter, c'est tout simplement le *calcul de fractions* que l'on apprend au collège.

A. Construction

Sur l'ensemble $A \times S$, définissons la relation d'équivalence $\sim$ par :

$$(a, s) \sim (b, t) \quad \text{si et seulement s'il existe } u \in S \text{ tel que } \quad u(at - bs) = 0.$$

C'est en effet une relation d'équivalence.

– pour tout $(a, s) \in A \times S$, puisque $1 \in S$ et $1(as - as) = 0$, $(a, s) \sim (a, s)$. La relation est réflexive ;

– si $(a,s)\sim(b,t)$, choisissons $u\in S$ tel que $u(at-bs)=0$. Alors, $u(bs-at)=0$, d'où $(b,t)\sim(a,s)$. La relation est symétrique ;

– enfin, si $(a,s)\sim(b,t)$ et $(b,t)\sim(c,u)$, choisissons v et $w\in S$ tels que $v(at-bs)=w(bu-ct)=0$. Comme

$$t(au-cs)=u(at-bs)+s(bu-ct),$$

on a $vwt(au-cs)=0$. Puisque v, w et t appartiennent à S, $vwt\in S$ et $(a,s)\sim(c,u)$. La relation est donc transitive.

On désigne par $S^{-1}A$ l'ensemble des classes d'équivalence (on trouve parfois la notation A_S) ; la classe du couple (a,s) est notée a/s. On note $i:A\to S^{-1}A$ l'application qui à $a\in A$ associe la classe $a/1$. L'ensemble $A\times S$ n'est pas un anneau. En revanche, nous allons munir $S^{-1}A$ d'une structure d'anneau de sorte que i est un homomorphisme d'anneaux. La définition provient des formules habituelles pour la somme et le produit de fractions. L'élément 1 de $S^{-1}A$ est par définition $1/1$, l'élément 0 est $0/1$. On définit ensuite

$$(a/s)+(b/t)=(at+bs)/st,\quad (a/s)\cdot(b/t)=(ab/st).$$

Vérifions d'abord que cette définition a un sens : si $(a,s)\sim(a',s')$, il faut montrer que

$$(at+bs,st)\sim(a't+bs',s't)\quad\text{et}\quad(ab,st)\sim(a'b,s't).$$

On a alors

$$(at+bs)s't-(a't+bs')st=t^2(as'-a's).$$

Choisissons $u\in S$ tel que $u(as'-a's)=0$; il en résulte que

$$u\big((at+bs)s't-(a't+bs')st\big)=0$$

et donc $(at+bs,st)\sim(a't+bs',s't)$. De même,

$$u(abs't-a'bst)=ubt(as'-a's)=0$$

et donc $(ab,st)\sim(a'b,st)$. Plus généralement, si $(a,s)\sim(a',s')$ et $(b,t)\sim(b',t')$, on a, en répétant ces vérifications (ou en remarquant la commutativité des opérations),

$$(a,s)+(b,t)\sim(a',s')+(b,t)\sim(a',s')+(b',t').$$

La vérification que ces lois confèrent une structure d'anneau commutatif à $S^{-1}A$ est un peu longue mais sans surprise et ne sera pas faite ici. Par exemple, la distributivité de l'addition sur la multiplication se démontre ainsi : si a/s, b/t et c/u sont trois éléments de $S^{-1}A$,

$$\frac{a}{s}\left(\frac{b}{t}+\frac{c}{u}\right)=\frac{a(bu+ct)}{stu}=\frac{abu}{stu}+\frac{act}{stu}=\frac{ab}{st}+\frac{ac}{su}=\frac{a}{s}\frac{b}{t}+\frac{a}{s}\frac{c}{u}.$$

L'application $i:A\to S^{-1}A$ telle que $i(a)=a/1$ pour tout $a\in A$ est un homomorphisme d'anneaux. En effet, $i(0)=0/1=0$, $i(1)=1/1=1$, et pour tous a et b dans A, on

a

$$i(a+b) = (a+b)/1 = a/1 + b/1 = i(a) + i(b)$$

et

$$i(ab) = (ab)/1 = (a/1)(b/1) = i(a)i(b).$$

Enfin, si $s \in S$, on a $i(s) = s/1$ et $i(s)(1/s) = s/s = 1$. Donc pour tout $s \in S$, $i(s)$ est inversible dans $S^{-1}A$.

B. Exemples

a) Soit A un anneau commutatif intègre. La partie $S = A \setminus \{0\}$ est une partie multiplicative de A. L'anneau $S^{-1}A$ est alors un *corps*, appelé *corps des fractions* de A.

Démonstration. — Comme A est intègre, $1 \neq 0$ et $1 \in S$. D'autre part, si a et b sont deux éléments non nuls de A, on a par définition $ab \neq 0$. Ainsi, S est une partie multiplicative de A.

Un élément de $S^{-1}A$ est de la forme a/s avec $a \in A$ et $s \neq 0$. S'il est nul, il existe un élément $b \in A \setminus \{0\}$ tel que $ab = 0$. Puisque A est intègre, on a alors $a = 0$. En particulier, $1/1 \neq 0$ dans $S^{-1}A$. Si a/s n'est au contraire pas nul, on a $a \neq 0$ et s/a est un élément de $S^{-1}A$ tel que $(a/s)(s/a) = as/as = 1$. Par suite, a/s est inversible. Nous avons donc prouvé que $S^{-1}A$ est un corps. □

b) Soit A un anneau commutatif et soit $s \in A$ un élément non nilpotent. Alors, la partie $S = \{1; s; s^2; \ldots\}$ est une partie multiplicative qui ne contient pas 0 et l'anneau localisé $S^{-1}A$ est non nul (voir la remarque a) ci-dessous). On le note en général A_s.

c) Soit $f : A \to B$ un homomorphisme d'anneaux commutatifs. Si S est une partie multiplicative de A, $f(S)$ est une partie multiplicative de B. Si T est une partie multiplicative de B, $f^{-1}(T)$ est une partie multiplicative de A. Lorsque le morphisme f est implicite, par exemple lorsque B est explictement une A-algèbre, on s'autorisera l'abus d'écriture $S^{-1}B$ pour $T^{-1}B$.

d) Si I est un idéal d'un anneau commutatif A, l'ensemble $S = 1 + I$ des éléments $a \in A$ tels que $a - 1 \in I$ est une partie multiplicative. C'est l'image réciproque de la partie multiplicative $\{1\}$ de A/I par la surjection canonique $A \to A/I$.

e) On dit qu'un idéal I d'un anneau commutatif A est un *idéal premier* si les propriétés équivalentes suivantes sont satisfaites :

(i) il est distinct de A et la condition $ab \in I$ entraîne que $a \in I$ ou $b \in I$;
(ii) le complémentaire $S = A \setminus I$ est une partie multiplicative non vide de A ;
(iii) l'anneau quotient A/I est intègre.

L'équivalence des deux premières assertions est immédiate par passage au complémentaire. Que A/I soit intègre signifie que $I \neq A$ (un anneau intègre n'est pas nul) et que le produit de deux éléments n'appartenant pas à I n'appartient pas à I. Si I est un idéal premier de A, l'anneau de fractions $(A \setminus I)^{-1}A$ est souvent noté A_I.

Remarques 1.6.3. — a) À quelle condition l'anneau $S^{-1}A$ peut-il être nul ? Il résulte de la définition qu'une fraction a/s est nulle dans $S^{-1}A$ si et seulement s'il existe $t \in S$ tel que $t(a1 - s0) = at = 0$. Dire que $S^{-1}A$ est l'anneau nul signifie alors que $1/1 = 1 = 0 = 0/1$, et donc qu'il existe $s \in S$ tel que $s \cdot 1 = s = 0$, autrement dit que $0 \in S$. On peut donc affirmer que *l'anneau $S^{-1}A$ est nul si et seulement si* 0 *appartient à S*.

Cela justifie *a posteriori* l'interdiction de diviser par zéro : si l'on s'autorisait cela, les règles du calcul de fractions rendraient toute fraction égale à 0 !

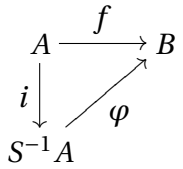
b) La définition de la relation d'équivalence dans la construction de l'anneau localisé peut sembler surprenante puisqu'elle est plus faible que l'« égalité du produit en croix » $at = bs$. Lorsque l'anneau est intègre et $0 \notin S$, ou plus généralement lorsque tous les éléments de S sont simplifiables, c'est équivalent. En revanche, dans le cas général, l'égalité du produit en croix ne fournirait pas une relation d'équivalence.

C. Propriété universelle

L'importance de cette construction vient de la *propriété universelle* qu'elle vérifie :

THÉORÈME 1.6.4. — *Soit A un anneau commutatif et S une partie multiplicative de A. Notons $i : A \to S^{-1}A$ l'homomorphisme d'anneaux que nous venons de construire. Alors, pour tout anneau B et tout homomorphisme $f : A \to B$ tel que $f(S) \subset B^\times$, il existe un unique homomorphisme $\varphi : S^{-1}A \to B$ tel que $f = \varphi \circ i$.*

On peut résumer cette dernière formule en disant que le diagramme



est commutatif.

Démonstration. — Si un tel φ existe, il doit vérifier

$$\varphi(a/s)f(s) = \varphi(a/s)\varphi(i(s)) = \varphi(a/s)\varphi(s/1) = \varphi(a/1) = \varphi(i(a)) = f(a)$$

et donc

$$\varphi(a/s) = f(s)^{-1}f(a)$$

où $f(s)^{-1}$ désigne l'inverse de $f(s)$ dans B. Cela prouve qu'il existe un plus un tel homomorphisme φ. Pour montrer son existence, il suffit de vérifier que la formule indiquée définit un homomorphisme d'anneaux $\varphi : S^{-1}A \to B$ tel que $\varphi \circ i = f$.

Tout d'abord, si $(a/s) = (b/t)$, soit $u \in S$ tel que $uta = usb$. Alors, $f(u)f(ta) = f(u)f(sb)$, d'où $f(ta) = f(sb)$, car $f(u)$ est inversible dans B. Comme A est commutatif, on a en fait $f(at) = f(ta) = f(sb) = f(bs)$, donc $f(a)f(t) = f(s)f(b)$ puis $f(s)^{-1}f(a) = f(b)f(t)^{-1}$; de même, $f(t)f(b) = f(b)f(t) = f(bt)$ d'où $f(b)f(t)^{-1} =$

$f(t)^{-1}f(b)$. Par conséquent, $f(s)^{-1}f(a) = f(t)^{-1}f(b)$ ce qui démontre que φ est bien défini. Quant à la vérification des axiomes d'un homomorphisme d'anneaux, on a

$$\varphi(0) = f(0/1) = f(1)^{-1}f(0) = 0 \quad \text{et} \quad \varphi(1) = f(1/1) = f(1)^{-1}f(1) = 1.$$

Puis,

$$\begin{aligned}\varphi(a/s) + \varphi(b/t) &= f(s)^{-1}f(a) + f(t)^{-1}f(b) = f(st)^{-1}\big(f(at) + f(bs)\big)\\ &= f(st)^{-1}f(at+bs) = \varphi((at+bs)/st) = \varphi((a/s) + (b/t)).\end{aligned}$$

Enfin,

$$\begin{aligned}\varphi(a/s)\varphi(b/t) &= f(s)^{-1}f(a)f(t)^{-1}f(b) = f(st)^{-1}f(ab)\\ &= \varphi(ab/st) = \varphi((a/s)(b/t)).\end{aligned}$$

L'application φ est donc un homomorphisme et le théorème est démontré. □

Remarque 1.6.5. — Si A est un anneau et S une partie multiplicative de A, on peut montrer de manière formelle l'existence et l'unicité d'un anneau A_S, muni d'un homomorphisme d'anneaux $i\colon A \to A_S$, vérifiant la propriété universelle : pour tout homomorphisme d'anneaux $f\colon A \to B$ tel que $f(S) \subset B^\times$, il existe un unique homomorphisme d'anneaux $\tilde{f}\colon A_S \to B$ tel que $f = \tilde{f} \circ i$. Toutefois, on ne peut rien en dire en général. Par exemple, Malcev a construit en 1937 un anneau intègre A ne possédant pas d'homomorphisme dans un corps (1 devrait s'appliquer sur 0 !). Si l'anneau vérifie une certaine condition, dite de Ore, on peut vérifier que la construction à l'aide de fractions que nous avons présenter fournit un anneau qui est solution de ce problème universel ; voir l'exercice 59.

On peut aussi construire l'anneau localisé comme un quotient.

PROPOSITION 1.6.6. — *Soit A un anneau commutatif, a un élément de A et $S = \{1; a; a^2; \ldots\}$ la partie multiplicative de A formée des puissances de a. L'homomorphisme canonique*

$$\varphi\colon A[X] \to S^{-1}A, \quad P \mapsto P(1/a)$$

est surjectif, de noyau l'idéal $(1-aX)$. Il en résulte un isomorphisme

$$\bar{\varphi}\colon A[X]/(1-aX) \simeq S^{-1}A.$$

Démonstration. — Un élément de $S^{-1}A$ s'écrit b/a^n pour un certain $n \geqslant 1$ et un élément $b \in A$. On a ainsi $b/a^n = \varphi(bX^n)$ et φ est bien surjectif. Son noyau contient certainement $1-aX$ puisque $\varphi(1-aX) = 1 - a/a = 0$. Il contient par suite l'idéal $(1-aX)$. Il en résulte par la propriété universelle des anneaux quotients un homomorphisme bien défini $\bar{\varphi}\colon A[X]/(1-aX) \to S^{-1}A$. Nous allons montrer que $\bar{\varphi}$ est un isomorphisme. D'après la proposition 1.5.5, il en résultera que $\ker\varphi = (1-aX)$.

Définissons donc l'inverse de $\bar{\varphi}$. Soit g l'homomorphisme canonique $A \to A[X]/(1-aX)$ tel que pour tout $b \in A$, $b \mapsto \mathrm{cl}(b)$, la classe du polynôme constant b. Dans l'anneau $A[X]/(1-aX)$, on a $\mathrm{cl}(aX) = 1$ et donc $\mathrm{cl}(a)$ est inversible, d'inverse $\mathrm{cl}(X)$. La propriété universelle de la localisation affirme qu'il existe un unique morphisme $\psi : S^{-1}A \to A[X]/(1-aX)$ tel que pour tout $b \in A$, $\psi(b/1) = g(b)$. Par construction, si $b \in A$ et $n \geqslant 1$, $\psi(b/a^n) = b\,\mathrm{cl}(X^n) = \mathrm{cl}(bX^n)$.

Finalement, montrons que ψ est l'inverse de $\bar{\varphi}$. Si $P \in A[X]$, $\psi(\bar{\varphi}(\mathrm{cl}(P))) = \psi(P(1/a))$. Par suite, si $P = \sum b_n X^n$, on a

$$\begin{aligned}\psi(\bar{\varphi}(\mathrm{cl}(P))) &= \psi(\varphi(P)) = \psi(P(1/a)) \\ &= \psi\Big(\sum (b_n/a^n)\Big) = \sum \psi(b_n/a^n) \\ &= \sum \mathrm{cl}(bX^n) = \mathrm{cl}\Big(\sum b_n X^n\Big) = \mathrm{cl}(P)\end{aligned}$$

et $\psi \circ \bar{\varphi} = \mathrm{id}$. Enfin,

$$\bar{\varphi}(\psi(b/a^n)) = \bar{\varphi}(\mathrm{cl}(bX^n)) = \varphi(aX^n) = b/a^n$$

et $\bar{\varphi} \circ \psi = \mathrm{id}$. L'homomorphisme $\bar{\varphi}$ est donc un isomorphisme, ce qu'il fallait démontrer. □

La généralisation au cas d'une partie multiplicative quelconque est laissée en exercice (exercice 57).

D. Localisation et quotient

Enfin, étudions brièvement les idéaux de $S^{-1}A$. Un premier résultat est le suivant :

PROPOSITION 1.6.7. — *Soit A un anneau commutatif. Pour tout idéal $\mathscr{I}$ de $S^{-1}A$, il existe un idéal I de A tel que $\mathscr{I} = i(I)(S^{-1}A)$. On peut en fait prendre $I = i^{-1}(\mathscr{I})$.*

Démonstration. — Il faut montrer que

$$\boxed{\mathscr{I} = i(i^{-1}(\mathscr{I}))(S^{-1}A).}$$

Comme $i(i^{-1}(\mathscr{I})) \subset \mathscr{I}$, l'idéal engendré par $i(i^{-1}(\mathscr{I}))$ est contenu dans $\mathscr{I}$, d'où l'inclusion

$$i(i^{-1}(\mathscr{I}))(S^{-1}A) \subset \mathscr{I}.$$

Réciproquement, si $x \in \mathscr{I}$, choisissons $a \in A$ et $s \in S$ tels que $x = a/s$. On a alors $sx \in I$ et comme $sx = a/1 = i(a)$, a appartient à $i^{-1}(\mathscr{I})$. Il en résulte que $sx \in i(i^{-1}(\mathscr{I}))$, puis $x = (sx)(1/s)$ appartient à $i(i^{-1}(\mathscr{I}))(S^{-1}A)$, ce qui établit l'autre inclusion. □

L'idéal $i(I)S^{-1}A$ sera aussi noté $IS^{-1}A$, en omettant le morphisme i. Il sera aussi noté $S^{-1}I$, cette dernière notation étant celle qui sera utilisée dans le cas plus général de la localisation des modules.

PROPOSITION 1.6.8. — *Soit A un anneau commutatif, soit S une partie multiplicative de A et soit I un idéal de A. Soit $T = \mathrm{cl}(S) \subset A/I$ l'image de S par la surjection canonique $A \to A/I$. Il existe un unique isomorphisme*

$$\varphi : S^{-1}A/IS^{-1}A \xrightarrow{\sim} T^{-1}(A/I)$$

tel que pour tout $a \in A$, $\varphi(\mathrm{cl}(a/1)) = \mathrm{cl}(a)/1$.

Dit plus abstraitement, les deux anneaux $S^{-1}A/IS^{-1}A$ et $T^{-1}(A/I)$ sont des A-algèbres : un quotient ou un localisé d'une A-algèbre sont des A-algèbres. La proposition affirme alors qu'il existe un *unique isomorphisme de A-algèbres* entre ces deux anneaux.

Démonstration. — On peut donner une démonstration explicite, mais la méthode la plus élégante (et la plus abstraite) utilise les propriétés universelles des quotients et des localisés. Considérons le morphisme d'anneaux composé

$$A \to A/I \to T^{-1}(A/I), \quad a \mapsto \mathrm{cl}(a)/1.$$

Par ce morphisme, un élément $s \in S$ a pour image $\mathrm{cl}(s)/1$ qui est inversible dans $T^{-1}(A/I)$, d'inverse $1/\mathrm{cl}(s)$. La propriété universelle de la la localisation affirme qu'il existe un unique homomorphisme d'anneaux

$$\varphi_1 : S^{-1}A \to T^{-1}(A/I)$$

par lequel $a/1$ a pour image $\mathrm{cl}(a)/1$.

Par cet homomorphisme, un élément $a/1$ avec $a \in I$ a pour image

$$\varphi_1(a/1) = \varphi_1(a)/1 = \mathrm{cl}(a)/1 = 0$$

puisque $a \in I$ et donc $\mathrm{cl}(a) = 0$ dans A/I. Par suite, le noyau de φ_1 contient l'image de I dans $S^{-1}A$; il contient automatiquement l'idéal $IS^{-1}A$ qui est engendré par I dans $S^{-1}A$. D'après la propriété universelle des anneaux quotients, il existe un unique homomorphisme d'anneaux

$$\varphi : S^{-1}A/IS^{-1}A \to T^{-1}(A/I)$$

tel que pour tout $a/s \in S^{-1}A$, $\varphi(\mathrm{cl}(a/s)) = \mathrm{cl}(a)/\mathrm{cl}(s)$.

Nous avons montré qu'il existe un unique morphisme de A-algèbres $\varphi : S^{-1}A/IS^{-1}A \to T^{-1}(A/I)$. On peut aussi résumer ces constructions par le diagramme commutatif

$$\begin{array}{ccc} & S^{-1}A & \longrightarrow S^1A/IS^{-1}A \\ A \nearrow & & \downarrow \varphi \\ & \searrow^{\varphi_1} & \\ & A/I & \longrightarrow T^{-1}(A/I). \end{array}$$

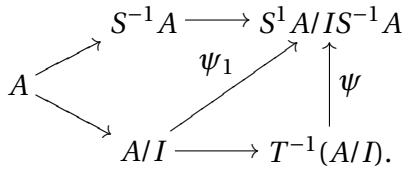
Reprenons ce diagramme dans l'autre sens. Le noyau du morphisme de A-algèbres $A \to S^{-1}A/IS^{-1}A$ contient I, d'où un unique morphisme de A-algèbres

$$\psi_1 \colon A/I \to S^{-1}A/IS^{-1}A$$

(donc vérifiant que pour tout $a \in A$, $\psi_1(\mathrm{cl}(a)) = \mathrm{cl}(a/1)$). Si $s \in S$, $\psi_1(\mathrm{cl}(s)) = \mathrm{cl}(s/1)$ est inversible, d'inverse $\mathrm{cl}(1/s)$. Ainsi, l'image de T par ψ_1 est formée d'éléments inversibles dans $S^{-1}A/IS^{-1}A$. Il existe donc un unique morphisme de A-algèbres

$$\psi : T^{-1}(A/I) \to S^{-1}A/IS^{-1}A$$

(c'est-à-dire tel que pour tout $a \in A$, $\psi(\mathrm{cl}(a)/1) = \mathrm{cl}(a/1)$). Ces constructions sont synthétisées par le diagramme commutatif



Finalement, si $a \in A$ et $s \in S$, on a $\varphi(\mathrm{cl}(a/s)) = \mathrm{cl}(a)/\mathrm{cl}(s)$ dans $T^{-1}(A/I)$ et $\psi(\mathrm{cl}(a)/\mathrm{cl}(s)) = \mathrm{cl}(a/s)$ dans $S^{-1}A/IS^{-1}A$ d'où il résulte que $\varphi \circ \psi$ et $\psi \circ \varphi$ sont l'identité. □

Cette dernière proposition reviendra plus tard sous le vocable *exactitude de la localisation.*

Exercices. — 48) Soit A un anneau commutatif et soit S une partie multiplicative de A.

a) Montrer que l'homomorphisme canonique $i : A \to S^{-1}A$ est injectif si et seulement si tout élément de S est simplifiable.

b) Plus généralement, déterminer le noyau de l'homomorphisme i.

49) Soit A un anneau commutatif et soit S une partie multiplicative de A.

a) Quels sont les éléments inversibles de l'anneau des nombres décimaux ?

b) Montrer qu'un élément $a \in A$ est inversible dans $S^{-1}A$ si et seulement s'il existe $b \in A$ tel que $ab \in S$.

c) Si T est une partie multiplicative de A qui contient S, construire un homomorphisme d'anneaux de $S^{-1}A$ dans $T^{-1}A$.

d) Soit $\tilde{S}$ l'ensemble des éléments de A dont l'image est inversible dans $S^{-1}A$. Montrer que l'homomorphisme d'anneaux canonique de $S^{-1}A$ dans $\tilde{S}^{-1}A$ est un isomorphisme. On donnera une démonstration explicite ainsi qu'une démonstration utilisant la propriété universelle.

50) a) Soit A un anneau commutatif, soit t un élément de A et soit $S = \{1, t, t^2, \ldots\}$ la partie multiplicative engendrée par t. On note A_t l'anneau de fractions $S^{-1}A$. Montrer que les propriétés suivantes sont équivalentes :

(1) Le morphisme canonique $i : A \to A_t$ est surjectif ;
(2) la suite décroissante d'idéaux $(t^nA)_n$ est stationnaire ;
(3) pour n assez grand, l'idéal t^nA est engendré par un idempotent.

(*Pour voir que* (2) *implique* (3)*, montrer par récurrence sur k qu'une relation de la forme* $t^n = t^{n+1}a$ *implique* $t^n = t^{n+k}a^k$*, puis que* $t^n a^n$ *est un idempotent.*)

b) Soit S une partie multiplicative de A formée d'éléments s tels que les morphismes $A \to A_s$ soient surjectifs. Montrer que le morphisme $A \to S^{-1}A$ est surjectif.

c) Soit A un anneau qui est fini, ou qui est un espace vectoriel de dimension finie sur un sous-corps (ou plus généralement, un anneau *artinien*). Montrer que la condition (2) est vérifiée pour tout élément t de A.

51) Soit a et b des entiers $\geqslant 1$.

a) Montrer qu'il existe des entiers m et n tels que m soit premier à b, chaque diviseur premier de n divise b, et tels que $a = mn$. (Attention, n *n'est pas* le pgcd de a et b).

b) Montrer que l'anneau $(\mathbf{Z}/a\mathbf{Z})_b$ est isomorphe à $\mathbf{Z}/n\mathbf{Z}$. On exhibera un homomorphisme de $\mathbf{Z}/n\mathbf{Z}$ sur $(\mathbf{Z}/a\mathbf{Z})_b$ dont on montrera que c'est un isomorphisme.

52) a) Montrer que l'anneau $\mathbf{Z}[i]$ est isomorphe à l'anneau $\mathbf{Z}[X]/(X^2+1)$.

b) Soit a un entier. En considérant $\mathbf{Z}[i]/(a+i)$ comme un quotient de $\mathbf{Z}[X]$, définir un isomorphisme

$$\mathbf{Z}[i]/(a+i) \xrightarrow{\sim} \mathbf{Z}/(a^2+1)\mathbf{Z}.$$

c) Plus généralement, soit a et b deux entiers premiers entre eux. Montrer que l'image de b dans $\mathbf{Z}[i]/(a+ib)$ est inversible. Exprimer cet anneau comme un quotient de $\mathbf{Z}_b[X]$ puis définir un isomorphisme

$$\mathbf{Z}[i]/(a+ib) \quad \xrightarrow{\sim} \mathbf{Z}/(a^2+b^2)\mathbf{Z}.$$

(*Noter que si* $1 = au + bv$*, alors* $1 = (a+bi)u + b(v-ui)$.)

53) a) Soit A un sous-anneau de $\mathbf{Q}$. Montrer qu'il existe une partie multiplicative S de $\mathbf{Z}$ telle que $A = S^{-1}\mathbf{Z}$.

b) Soit $A = \mathbf{C}[X,Y]$ l'anneau des polynômes en deux indéterminées X et Y sur $\mathbf{C}$, soit $B = A[Y/X]$ le sous-anneau du corps des fractions rationnelles $\mathbf{C}(X,Y)$ engendré par A et Y/X.

Montrer que l'unique homomorphisme d'anneaux de $\mathbf{C}[T,U]$ dans B qui applique T sur X et U sur Y/X est un isomorphisme. En déduire que $A^\times = B^\times = \mathbf{C}^\times$, puis que B n'est pas un localisé de A.

54) Soit K un corps et soit $\varphi : K[U,V] \to K[X]$ l'homomorphisme d'anneaux défini par les égalités $\varphi(U) = X^3$, $\varphi(V) = -X^2$ et $\varphi(a) = a$ pour tout a dans K.

a) Quels sont les noyau et image de φ ? Soit A l'image de φ.

b) Montrer que A est intègre et que son corps des fractions est isomorphe à $K(X)$.

c) Montrer que l'anneau A n'est pas principal.

55) Soit A un anneau (commutatif) et soit S une partie multiplicative de A qui ne contient pas 0.

a) Si A est principal, montrer que $S^{-1}A$ est un anneau principal.

b) La réciproque est-elle vraie ?

56) Soit B l'ensemble des fractions rationnelles à coefficients réels de la forme $P/(X^2+1)^n$, où $P \in \mathbf{R}[X]$ est un polynôme, $n \in \mathbf{N}$. Soit A la partie de B formée de ces fractions $P/(X^2+1)^n$ où $n \geqslant 1$ et où P est de degré $\leqslant 2n$.

a) Montrer que A et B sont des sous-anneaux de $\mathbf{R}(X)$.

b) Quels sont leurs éléments inversibles ?

c) Montrer que B est un anneau principal. Montrer que l'idéal de A engendré par $1/(X^2+1)$ et $X/(X^2+1)$ n'est pas principal.

57) Soit A un anneau commutatif, soit S une partie multiplicative de A.

a) On suppose qu'il existe s et $t \in S$ tels que S soit l'ensemble des $s^n t^m$ lorsque n et m parcourent $\mathbf{N}$. Montrer que l'homomorphisme $A[X,Y] \to S^{-1}A, \quad P(X,Y) \mapsto P(1/s, 1/t)$ est surjectif et que son noyau contient l'idéal $(1-sX, 1-tY)$ engendré par $1-sX$ et $1-tY$ dans $A[X,Y]$. En déduire un isomorphisme $A[X,Y]/(1-sX, 1-tY) \simeq S^{-1}A$.

b) Plus généralement, soit $\langle 1-sX_s\rangle_{s\in S}$ l'idéal de l'anneau de polynômes (en une infinité de variables) $A[(X_s)_{s\in S}]$ engendré par les polynômes $1-sX_s$, lorsque s parcourt S. Alors, l'homomorphisme canonique

$$A[(X_s)_{s\in S}] \to S^{-1}A, \quad P \mapsto P((1/s)_s)$$

induit un isomorphisme

$$A[(X_s)_{s\in S}]/\langle 1-sX_s\rangle_{s\in S} \simeq S^{-1}A.$$

58) Soit A un anneau commutatif et soit S une partie multiplicative de A ne contenant pas 0. On note $\mathfrak{r}(A)$ l'ensemble des éléments nilpotents de A ; on dit que A est *réduit* si $\mathfrak{r}(A) = 0$.

a) Si A est intègre, montrer que $S^{-1}A$ est intègre.

b) Si A est réduit, montrer que $S^{-1}A$ est réduit.

c) On note $f : A \to S^{-1}A$ l'homomorphisme naturel $a \mapsto a/1$. Plus généralement, montrer que $\mathfrak{r}(S^{-1}A)$ est l'idéal engendré par l'image de $\mathfrak{r}(A)$ dans $S^{-1}A$.

59) Soit A un anneau et soit S une partie multiplicative de A formée d'éléments simplifiables.

On dit qu'un anneau A_S est un anneau de fractions à droite pour S s'il existe un homomorphisme injectif $i : A \to A_S$ vérifiant les conditions suivantes :

(i) pour tout $s \in S$, $i(s)$ est inversible dans A_S ;
(ii) tout élément de A_S est de la forme $i(a)\,i(s)^{-1}$ pour $a \in A$ et $s \in S$.

a) Supposons que A admette un anneau de fractions à droite pour S. Montrer que pour tout $a \in A$ et tout $s \in S$, il existe $a' \in A$ et $s' \in S$ tels que $as' = sa'$ (condition de Ore).

b) On suppose inversement que cette condition est satisfaite. On définit une relation $\sim$ sur $A \times S$ par « $(a,s) \sim (b,t)$ si et seulement s'il existe c et $d \in A$ et $u \in S$ tels que $u = sc = td$ et $ac = bd$. » Montrer qu'il existe, sur l'ensemble quotient A_S, une unique structure d'anneau tel que l'application i qui à $a \in A$ associe la classe de $(a,1)$ soit un homomorphisme et tel que tout $s \in S$ soit inversible dans A_S, d'inverse la classe de $(1,s)$. En déduire que A_S est un anneau de fractions à droite pour S.

c) Soit I un ensemble de cardinal au moins 2, soit K un corps commutatif et soit $A = K\{I\}$ l'algèbre du monoïde des mots sur I. Montrer que A n'admet pas de corps des fractions à droite.

§1.7. Idéaux maximaux

DÉFINITION 1.7.1. — *Soit A un anneau. On dit qu'un idéal à gauche I de A est maximal s'il est maximal parmi les idéaux à gauche de A qui sont distincts de A.*

Autrement dit, I est maximal si l'on a $I \neq A$ et si les seuls idéaux à gauche de A contenant I sont A et I.

On a une définition analogue pour les idéaux à droite et les idéaux bilatère.

Lorsque l'anneau A n'est pas commutatif, on prendra garde qu'un idéal bilatère peut être maximal en tant qu'idéal à gauche, mais pas en tant qu'idéal à droite, voire qu'il peut être maximal en tant qu'idéal bilatère mais pas en tant qu'idéal à droite ou à gauche.

Exemples 1.7.2. — a) Les idéaux de $\mathbf{Z}$ sont de la forme $n\mathbf{Z}$, avec $n \in \mathbf{Z}$; si n divise m, alors $m\mathbf{Z} \subset n\mathbf{Z}$. Par suite, les idéaux maximaux de $\mathbf{Z}$ sont les idéaux $p\mathbf{Z}$, où p est un nombre premier.

De même, si K est un corps (commutatif), les idéaux maximaux de l'anneau $K[X]$ des polynômes en une indéterminée sont les idéaux engendrés par un polynôme irréductible. Si K est algébriquement clos, ce sont donc les idéaux $(X-a)$, pour $a \in K$.

Plus généralement, les idéaux maximaux d'un anneau (commutatif) principal A sont de la forme πA, où π est un élément irréductible de A.

b) Soit K un corps (commutatif) et soit V un K-espace vectoriel de dimension finie. Les idéaux à gauche de $\mathrm{End}(V)$ sont les idéaux I_W, pour W un sous-espace vectoriel de V, où I_W est l'ensemble des endomorphismes dont le noyau contient W. Si $W \subset W'$, $I_{W'} \subset I_W$. Par suite, les idéaux à gauche maximaux de $\mathrm{End}(V)$ sont les idéaux I_W, où W est une droite de V. Les seuls idéaux bilatères de $\mathrm{End}(V)$ sont (0) et $\mathrm{End}(V)$. Le seul idéal bilatère maximal est donc l'idéal nul.

c) Un idéal à gauche maximal d'un anneau est un idéal à droite maximal de l'anneau opposé.

Concernant l'existence d'idéaux maximaux, on a le résultat général suivant, conséquence du théorème de Zorn (th. A.2.1).

THÉORÈME 1.7.3 (Krull). — *Soit A un anneau et soit I un idéal à gauche de A distinct de A. Il existe un idéal maximal de A qui contient I.*

En particulier, tout anneau non nul possède au moins un idéal à gauche maximal (prendre $I = 0$).

L'énoncé analogue pour les idéaux à droite et les idéaux bilatères est vrai et se démontre de la même façon.

Démonstration. — Soit $\mathscr{I}$ l'ensemble des idéaux à gauche de A qui contiennent I et qui sont distincts de A. Munissons $\mathscr{I}$ de l'ordre donné par l'inclusion.

Montrons que $\mathscr{I}$ est un ensemble inductif. Soit en effet (J_i) une famille totalement ordonnée d'idéaux à gauche de A tels que $I \subset J_i \subsetneq A$; soit J la réunion des idéaux J_i (si la famille n'est pas vide, $J = I$ sinon). Montrons que l'on a $J \in \mathscr{I}$. Remarquons que J contient I par construction ; comme 1 n'appartient à J_i pour aucun indice i, $1 \notin J$ et $J \neq A$. Enfin, J est un idéal à gauche de A : si $x \in J$ et $y \in J$, il existe des indices i et j tels que $x \in J_i$ et $y \in J_j$. Commme la famille (J_i) est totalement ordonnée, on a $J_i \subset J_j$ ou $J_j \subset J_i$. Dans le premier cas, $x + y \in J_j$, dans le second, $x + y \in J_i$; par suite, $x + y \in J$. Enfin, si $x \in J$ et $a \in A$, soit i tel que $x \in J_i$; puisque J_i est un idéal à gauche, $ax \in J_i$, d'où $ax \in J$.

D'après le théorème de Zorn (théorème A.2.1), l'ensemble $\mathscr{I}$ possède un élément maximal $\mathfrak{m}$. Par définition de l'ordre de $\mathscr{I}$, $\mathfrak{m}$ est un idéal à gauche de A distinct de A qui contient I et qui est maximal pour cette propriété. Ainsi, $\mathfrak{m}$ un idéal à gauche maximal de A contenant I, d'où le théorème. □

COROLLAIRE 1.7.4. — *Soit A un anneau. Pour qu'un élément de A soit inversible à gauche (*resp. *à droite), il faut et il suffit qu'il n'appartienne à aucun idéal maximal à gauche (*resp. *à droite) de A.*

Démonstration. — Soit a un élément de A. Dire que a est inversible à gauche signifie que l'idéal Aa est égal à A; aucun idéal maximal de A ne peut contenir a. Dans le cas contraire, il existe un idéal à gauche maximal de A qui contient Aa et cet idéal maximal contient a. □

PROPOSITION 1.7.5. — *Soit A un anneau commutatif. Un idéal I de A est maximal si et seulement si l'anneau A/I est un corps. (En particulier, un idéal maximal de A est un idéal premier.)*

Démonstration. — Supposons que A/I soit un corps. Ses idéaux sont alors l'idéal nul et l'anneau tout entier ; les idéaux de A qui contiennent I sont donc I et A, ce qui entraîne que I est un idéal maximal. Inversement, si I est un idéal maximal, cet argument entraîne que les seuls idéaux de A/I sont lui-même et l'idéal nul. Soit x un élément non nul de A/I. L'idéal (x) engendré par x, n'étant pas nul, est donc égal à A/I ; il existe par suite $y \in A/I$ tel que $xy = 1$, si bien que x est inversible. Cela démontre que A/I est un corps. □

Dans le cas des anneaux de polynômes sur un corps algébriquement clos, le théorème suivant dû à Hilbert, fournit une description précise des idéaux maximaux.

THÉORÈME 1.7.6 (Théorème des zéros de Hilbert). — *Soit K un corps algébriquement clos. Les idéaux maximaux de $K[X_1, \ldots, X_n]$ sont les idéaux $(X_1 - a_1, \ldots, X_n - a_n)$, pour $(a_1, \ldots, a_n) \in K^n$.*

Démonstration. — Montrons tout d'abord que, pour tout $(a_1,\dots,a_n)\in K^n$, l'idéal $(X_1-a_1,\dots,X_n-a_n)$ est un idéal maximal de $K[X_1,\dots,X_n]$. Soit $\varphi\colon K[X_1,\dots,X_n]\to K$ l'homomorphisme d'évaluation en $(a_1,\dots,a_n)$, défini par $\varphi(P)=P(a_1,\dots,a_n)$. Il est surjectif ; l'isomorphisme $K\simeq K[X_1,\dots,X_n]/\ker(\varphi)$ et le fait que K soit un corps entraîne que $\ker(\varphi)$ est un idéal maximal de $K[X_1,\dots,X_n]$. Il suffit donc de montrer que ce noyau est précisément égal à l'idéal $(X_1-a_1,\dots,X_n-a_n)$. Une inclusion est évidente : si $P=(X_1-a_1)P_1+\cdots+(X_n-a_n)P_n$, $\varphi(P)=0$. Soit inversement $P\in K[X_1,\dots,X_n]$. Par division euclidienne de P par X_1-a_1 par rapport à la variable X_1, il existe un polynôme P_1 et un polynôme $R_1\in K[X_2,\dots,X_n]$ tel que

$$P=(X_1-a_1)P_1+R_1(X_2,\dots,X_n).$$

Continuons le procédé en divisant par X_2-a_2, etc. : il existe des polynômes $P_1,\dots,P_n$, P_i ne faisant intervenir que les variables $X_i,\dots,X_n$, et un polynôme constant R_n, tels que

$$P=(X_1-a_1)P_1+\cdots+(X_n-a_n)P_n+R_n.$$

En évaluant en $(a_1,\dots,a_n)$, on obtient

$$\varphi(P)=P(a_1,\dots,a_n)=R_n.$$

Si $\varphi(P)=0$ =, on a donc $R_n=0$ et P appartient à l'idéal $(X_1-a_1,\dots,X_n-a_n)$.

Nous nous contenterons de démontrer la réciproque sous l'hypothèse supplémentaire que le corps K n'est pas dénombrable. Soit I un idéal maximal de $K[X_1,\dots,X_n]$ et soit L l'anneau quotient $K[X_1,\dots,X_n]/I$. C'est un corps ; notons x_i la classe de X_i dans L. L'image de K par l'homomorphisme canonique est un sous-corps de L que l'on identifie à K.

Le corps L possède une structure naturelle de K-espace vectoriel et, à ce titre, est engendré par la famille dénombrable des $x_1^{i_1}\dots x_n^{i_n}$: un élément de L est la classe d'un polynôme, donc combinaison linéaire de classes de monômes. En outre, $\mathbf{N}^n$ est dénombrable.

Soit f un élément non nul de L et soit $\varphi\colon K[T]\to L$ l'homomorphisme d'anneaux donné par $\varphi(P)=P(f)$. Supposons qu'il soit injectif. Alors, φ s'étend en un homomorphisme de corps, toujours noté φ, de $K(T)$ dans L. En particulier, les éléments $1/(f-a)$, images des fractions rationnelles $1/(T-a)$ qui sont linéairement indépendantes sur K dans $K(T)$ (décomposition en éléments simples), sont linéairement indépendants sur K dans L. Mais ceci contredit le lemme ci-dessous : une famille libre de L est de cardinal dénombrable, alors que K ne l'est pas. Par suite, l'homomorphisme φ n'est pas injectif. Soit $P\in K[T]$ un polynôme non nul de degré minimal tel que $P(f)=0$. Le polynôme P n'est pas constant ; comme K est algébriquement clos, il est de la forme $c\prod_{i=1}^m(T-c_i)$, pour des éléments $c_i\in K$ et $c\in K^*$. On a ainsi $c\prod_{i=1}^n(f-c_i)=0$ dans L. Comme L est un corps, f est égal à l'un des c_i. Cela montre que $L=K$.

En particulier, il existe, pour tout $i \in \{1,\dots,n\}$, un élément $a_i \in K$ tel que $x_i = a_i$. Cela entraîne les relations $X_i - a_i \in I$, si bien que l'idéal I contient l'idéal $(X_1 - a_1, \dots, X_n - a_n)$. Comme ce dernier idéal est maximal, on a égalité, ce qu'il fallait démontrer. □

Et une variante topologique de l'énoncé précédent :

THÉORÈME 1.7.7 (Gelfand). — *Soit X un espace topologique. Pour tout $x \in X$, l'ensemble $\mathfrak{m}_x$ des fonctions continues sur X qui s'annulent en x est un idéal maximal de l'anneau $\mathscr{C}(X)$.*

Si X est un espace métrique compact, l'application de X dans l'ensemble des idéaux maximaux de $\mathscr{C}(X)$ ainsi définie est une bijection.

Démonstration. — Soit $\varphi_x : \mathscr{C}(X) \to \mathbf{R}$ l'homomorphisme d'évaluation en x, donné par $f \mapsto f(x)$. Il est surjectif, son noyau est $\mathfrak{m}_x$, ce qui démontre que $\mathfrak{m}_x$ est un idéal maximal de $\mathscr{C}(X)$.

Supposons que X soit un espace métrique. Pour tout point $x \in X$, la fonction $y \mapsto d(x,y)$ appartient à $\mathfrak{m}_x$ mais ne s'annule en aucun autre point de X, d'où l'injectivité de l'application considérée.

Soit I un idéal de $\mathscr{C}(X)$ qui n'est contenu dans aucun des idéaux maximaux $\mathfrak{m}_x$, pour $x \in X$. Pour tout $x \in X$, il existe donc une fonction continue $f_x \in I$ telle que $f_x(x) \neq 0$. Par continuité, l'ensemble U_x des points de X où f_x n'est pas nulle est un voisinage ouvert de x. Ces ouverts U_x recouvrent X. Puisque X est compact, il existe un ensemble fini $S \subset X$ tel que les U_s, pour $s \in S$, recouvrent X. Posons alors $f = \sum_{s\in S}(f_s)2$. C'est une fonction positive, jamais nulle car les f_s n'ont pas de zéro commun. Donc f est inversible dans $\mathscr{C}(X)$. Par construction $f \in I$; on a donc $I = \mathscr{C}(X)$. Par conséquent, tout idéal strict de $\mathscr{C}(X)$ est contenu dans l'un des $\mathfrak{m}_x$ et ces idéaux épuisent l'ensemble des idéaux maximaux de $\mathscr{C}(X)$. □

Terminons par quelques compléments, dans le cas d'un anneau commutatif, sur les idéaux premiers d'un anneau et par une caractérisation des éléments nilpotents d'un anneau commutatif. Rappelons (p. 31) qu'un idéal P d'un anneau commutatif est dit premier si l'anneau quotient A/P est intègre, ou, ce qui est équivalent, si le produit de deux éléments n'appartenant pas à P n'appartient pas à P.

Soit $f : A \to B$ un homomorphisme d'anneaux et soit Q un idéal premier de B. Posons $P = f^{-1}(Q)$; c'est le noyau de l'homomorphisme de A dans B/Q, composé de f et de l'homomorphisme canonique de B sur B/Q. Par suite, f définit par passage au quotient un homomorphisme *injectif* de A/P dans B/Q. En particulier, A/P est intègre et l'idéal P est premier. On aurait pu démontrer ce fait plus élémentairement : soit a et b des éléments de A tels que $ab \notin P$. Alors, $f(ab) = f(a)f(b)$ n'appartient pas à Q, donc $f(a) \notin Q$ ou $f(b) \notin Q$. Dans le premier cas, $a \notin P$, dans le second, $b \notin P$.

PROPOSITION 1.7.8. — *Soit A un anneau commutatif. L'intersection des idéaux premiers de A coïncide avec le nilradical de A (*i.e. *l'ensemble des éléments nilpotents de A).*

Démonstration. — Nous devons montrer qu'un élément $a \in A$ est nilpotent si et seulement s'il appartient à tout idéal premier de A.

Soit $a \in A$ et soit P un idéal premier de A. Si $a \notin P$, la définition d'un idéal premier entraîne que $a^n \notin P$, par récurrence sur n. A fortiori, $a^n \neq 0$ et a n'est pas nilpotent. Autrement dit, un élément nilpotent appartient à tout idéal premier de A.

Inversement, soit a un élément de A qui n'est pas nilpotent. L'ensemble $S = \{1, a, a^2, \ldots\}$ des puissances de a est une partie multiplicative de A qui ne contient pas 0. L'anneau localisé $S^{-1}A$ est donc distinct de 0 ; soit M un idéal maximal de cet anneau et soit P l'ensemble des éléments $x \in A$ tels que $x/1 \in P$. Par définition, P est l'image réciproque de M par l'homomorphisme canonique de A dans $S^{-1}A$. C'est donc un idéal premier. Comme $a/1$ est inversible dans $S^{-1}A$, $a/1 \notin M$ et $a \notin P$. Nous avons ainsi trouvé un idéal premier de A qui ne contient pas a, ce qui termine la démonstration de la proposition. □

Exercices. — 60) a) L'ensemble des fonctions à support compact, l'ensemble des fonctions qui s'annulent pour tout entier assez grand, sont des idéaux stricts de l'anneau des fonctions continues sur $\mathbf{R}$. Ils ne sont contenus dans aucun idéal $\mathfrak{m}_x$.

b) Soit A l'anneau des fonctions holomorphes sur un voisinage du disque unité fermé. Montrer que tout idéal de A est engendré par un polynôme $P \in \mathbf{C}[z]$ dont les racines sont de modules $\leqslant 1$. Les idéaux maximaux de A sont les idéaux $(z-a)$, pour $a \in \mathbf{C}$ tel que $|a| \leqslant 1$.

c) Soit K une partie compacte et connexe de $\mathbf{C}$ et soit $\mathscr{H}$ l'anneau des fonctions holomorphes sur K (c'est-à-dire sur un voisinage ouvert de K). Montrer que l'anneau $\mathscr{H}$ est intègre et que ses idéaux sont principaux (on dit que $\mathscr{H}$ est un anneau principal).

61) Soit A un anneau non nul et soit $\mathfrak{m}$ l'ensemble des éléments non inversibles de A. On suppose que $\mathfrak{m}$ est un sous-groupe abélien de A.

a) Montrer que pour tout $a \in A$, l'un des éléments a ou $1-a$ est inversible.

b) Montrer que $\mathfrak{m}$ est un idéal bilatère de A.

c) Montrer que $\mathfrak{m}$ est l'unique idéal à gauche maximal de A. (On dit qu'un tel anneau est *local*.)

d) Inversement, si A est un anneau qui possède un unique idéal à gauche maximal, montrer que cet idéal est égal à $\mathfrak{m}$.

62) Soit A un anneau commutatif local (voir l'exercice 61). Soit I et J deux idéaux de A et $a \in A$ un élément non diviseur de 0 tel que $IJ = (a)$.

a) Montrer qu'il existe $x \in I$ et $y \in J$ tels que $xy = a$. Justifier que x et y ne sont pas diviseurs de 0.

b) En déduire que $I = (x)$ et $J = (y)$.

63) Soit A l'anneau produit des corps $\mathbf{Z}/p\mathbf{Z}$, pour p parcourant l'ensemble des nombres premiers. Soit I l'ensemble des familles $(a_p) \in A$ où $a_p = 0$ pour presque tout nombre premier p. Notons B l'anneau A/I.

a) Soit $\mathfrak{m}$ un idéal maximal de A qui ne contient pas I. Montrer qu'il existe un nombre premier q tel que $\mathfrak{m}$ soit l'ensemble des familles (a_p), avec $a_q = 0$. Déterminer l'anneau quotient $A/\mathfrak{m}$.

b) Soit p un nombre premier. Montrer que $pB = B$.

c) Montrer que l'anneau B possède une unique structure de $\mathbf{Q}$-algèbre.

d) Pour tout idéal maximal $\mathfrak{m}$ de A contenant I, le corps $A/\mathfrak{m}$ est de caractéristique zéro.

64) Si I est un idéal de $\mathbf{C}[X_1,\dots,X_n]$, on note $\mathscr{V}(I)$ l'ensemble des $(x_1,\dots,x_n) \in \mathbf{C}^n$ tels que $P(x_1,\dots,x_n) = 0$ pour tout $P \in I$. Si Z est une partie de $\mathbf{C}^n$, on note $\mathscr{I}(Z)$ l'ensemble des $P \in \mathbf{C}[X_1,\dots,X_n]$ tels que $P(x) = 0$ pour tout $x \in Z$.

a) Si $I \subset I'$, $\mathscr{V}(I') \subset \mathscr{V}(I)$. En outre, $I \subset \mathscr{I}(\mathscr{V}(I))$.

b) Si $Z \subset Z'$, $\mathscr{I}(Z') \subset \mathscr{I}(Z)$. Montrer aussi que $Z \subset \mathscr{V}(\mathscr{I}(Z))$.

c) Pour que $\mathscr{V}(I)$ soit vide, il faut et il suffit que I soit égal à $\mathbf{C}[X_1,\dots,X_n]$.

d) Soit $P \in \mathscr{I}(\mathscr{V}(I))$ et soit J l'idéal de $\mathbf{C}[X_1,\dots,X_n,T]$ engendré par I et le polynôme $1 - TP(X_1,\dots,X_n)$. Montrer que $\mathscr{V}(J) = 0$. En déduire qu'il existe des polynômes $P_i \in I$, Q et $Q_i \in \mathbf{C}[X_1,\dots,X_n,T]$ tels que $1 = (1-TP)Q + \sum Q_i P_i$. Montrer alors qu'il existe m tel que $P^m \in I$. (*Poser d'abord formellement $T = 1/P$ puis chasser les dénominateurs.*)

e) Montrer que $\mathscr{I}(\mathscr{V}(I))$ est égal à $\sqrt{I}$ (l'ensemble des éléments de $\mathbf{C}[X_1,\dots,X_n]$ dont une puissance appartient à I).

65) a) Soit I et J des idéaux d'un anneau commutatif A et soit P un idéal premier de A tel que $IJ \subset P$. Montrer que l'on a $I \subset P$ ou $J \subset P$.

b) Soit $f : A \to B$ un homomorphisme d'anneaux. Si $I \subset B$ est un idéal premier de B, montrer que $f^{-1}(I)$ est un idéal premier de B.

c) Soit S une partie multiplicative de A et soit $f : A \to S^{-1}A$ l'homomorphisme canonique. Montrer que l'application $I \mapsto f^{-1}(I)$ induit une bijection de l'ensemble des idéaux premiers de $S^{-1}A$ sur l'ensemble des idéaux premiers de A qui sont disjoints de S.

66) Soit k un corps. Soit A l'anneau $k^{\mathbf{N}}$ et N l'ensemble $k^{(\mathbf{N})}$ des suites $(x_n) \in A$ telles que $x_n = 0$ pour n assez grand.

a) Montrer que N est un idéal de A. Justifier qu'il existe un idéal maximal $\mathfrak{m}$ de A qui contient N. On pose alors $K = A/\mathfrak{m}$.

b) Montrer que K est une extension de k, de cardinal non dénombrable.

c) Si k est algébriquement clos, montrer qu'il en est de même de K.

d) Soit I un idéal de $k[X_1,\dots,X_n]$ et soit J le sous-K-espace vectoriel de $K[X_1,\dots,X_n]$ engendré par les éléments de I. Si $I \neq (1)$, montrer que $J \neq (1)$.

e) Utiliser le cas du théorème des zéros de Hilbert prouvé dans le cours et la construction précédente pour en déduire le cas général.

§1.8. Anneaux principaux, anneaux euclidiens

Soit A un anneau commutatif. Rappelons qu'un idéal de A est dit principal s'il est de la forme aA, où a est un élément de A. On note aussi (a) l'idéal aA.

Pour que l'idéal principal aA soit contenu dans l'idéal bA, il faut et il suffit qu'il existe $c \in A$ tel que $a = bc$. Soit A un anneau commutatif intègre et soit a, b des éléments de A tels que $aA = bA$. Il existe donc des éléments c et $d \in A$ tels que $a = bc$ et $b = ad$, d'où $a = a(cd)$ et $b = (cd)$. Si $a \neq 0$, $b \neq 0$; en simplifiant par a, on voit que $cd = 1$, donc que c et d sont inversibles. Autrement dit, pour que des éléments non nuls a et b de l'anneau commutatif intègre A engendrent le même idéal, il faut et il suffit qu'il existe un élément inversible $u \in A$ tel que $b = au$.

Remarquons aussi que l'idéal aA est l'annulateur du A-module A/aA, car l'anneau A est supposé commutatif. Si les A-modules A/aA et A/bA sont isomorphes, ils ont même annulateur, donc $aA = bA$ et il existe un élément inversible $u \in A$ tel que $a = bu$. La réciproque est évidente.

DÉFINITION 1.8.1. — *On dit qu'un anneau (commutatif) est un* anneau principal *s'il est intègre et si tout idéal est principal.*

Exemples 1.8.2. — a) L'anneau $\mathbf{Z}$ est principal, de même que l'anneau $k[X]$ des polynômes en une variable à coefficients dans un corps (commutatif) k. La division euclidienne des entiers montre en effet qu'un idéal non nul de $\mathbf{Z}$ est en effet engendré par son plus petit élément strictement positif. De même, un idéal non nul de $k[X]$ est engendré par un de ses éléments non nuls de degré minimal.

b) L'idéal (X, Y) de l'anneau des polynômes en deux variables à coefficients dans un corps k n'est pas principal : un générateur serait un polynôme P qui divise à la fois X et Y. Ce polynôme serait une constante non nulle ; il existerait ainsi Q et $R \in k[X, Y]$ tels que $1 = XQ(X, Y) + YR(X, Y)$, ce qui est absurde, le second membre n'ayant pas de terme constant.

DÉFINITION 1.8.3. — *On dit qu'un anneau commutatif intègre A est* euclidien *s'il existe une application $\delta : A \setminus \{0\} \to \mathbf{N}$, appelée* jauge[(2)]*, et vérifiant les deux propriétés suivantes :*

– *pour tous a et b dans $A \setminus \{0\}$, $\delta(ab) \geqslant \max(\delta(a), \delta(b))$;*

– *pour tous a et b dans A, $b \neq 0$, il existe q et $r \in A$ tels que $a = bq + r$ et $r = 0$ ou $\delta(r) < \delta(b)$.*

Exemples 1.8.4. — a) L'anneau des entiers relatifs (pour la valeur absolue), l'anneau des polynômes en une indéterminée à coefficients dans un corps commutatif (pour le degré) sont des anneaux euclidiens.

(2) Le terme consacré, employé par exemple par Bourbaki et Wedderburn, est *stathme*.

b) L'anneau $\mathbf{Z}[i]$ des entiers de Gauss est euclidien, avec la jauge δ définie par $\delta(z) = z\bar{z} = |z|^2$.

c) *Un anneau euclidien est principal.* En effet, soit A un anneau euclidien pour une jauge $\delta : A \to \mathbf{N}$ et soit I un idéal non nul de A. Soit b un élément non nul de I tel que $\delta(a)$ soit minimal. Pour $a \in I$, considérons une division euclidienne $a = bq + r$ de a par b ; on a $\delta(r) < \delta(b)$ et $r = a - bq \in I$. Par suite, $r = 0$ et $a \in (b)$, d'où $I = (b)$.

d) Il existe des anneaux principaux qui ne sont euclidiens pour aucune application δ ; par exemple l'ensemble des nombres complexes de la forme $a + b\frac{1+i\sqrt{19}}{2}$, avec a et $b \in \mathbf{Z}$. (Voir D. PERRIN, *Cours d'algèbre*, Ellipses, p. 53–55 ; la démonstration que cet anneau n'est pas euclidien est reprise dans l'exercice 75.)

e) La première propriété des jauges entraîne que $\delta(a) \leqslant \delta(b)$ si a divise b. En particulier, la jauge du pgcd d'une famille d'éléments non nuls est inférieure à la jauge de chacun des éléments. De même, si u est inversible, $\delta(a) = \delta(au)$ pour tout élément non nul de A. Cette propriété n'est toutefois pas nécessaire pour impliquer que l'anneau A est euclidien : on peut toujours modifier une application qui vérifierait la seconde propriété pour en faire une jauge, voir l'exercice 72.

Exercices. — 67) On pose $A = \mathbf{C}[X, Y]/(XY - 1)$. On note x l'image de X dans A.

a) Montrer que x est inversible dans A. Montrer que tout élément a non nul de A peut s'écrire de façon unique sous la forme $a = x^m P(x)$, où m est dans $\mathbf{Z}$ et où P est un polynôme à coefficients dans $\mathbf{C}$ dont le terme constant est non nul. On note $e(a)$ le degré de P.

b) Soit a et b deux éléments de A, avec $b \neq 0$. Montrer qu'il existe des éléments q et r dans A tels que $a = bq + r$ avec $r = 0$ ou bien $e(r) < e(b)$.

c) En déduire que A est principal.

68) Soit K un compact de $\mathbf{C}$ et $\mathscr{H}$ l'anneau des fonctions holomorphes sur K (c'est-à-dire sur un voisinage ouvert de K). Montrer que $\mathscr{H}$ est principal.

69) a) Montrer que l'idéal $(2, X)$ de $\mathbf{Z}[X]$ n'est pas principal.

b) Soit A un anneau commutatif tel que l'anneau $A[X]$ soit principal. Montrer que A est un corps.

70) Soit A l'ensemble des nombres réels de la forme $a + b\sqrt{2}$, avec a et $b \in \mathbf{Z}$. Soit K l'ensemble des nombres réels de la forme $a + b\sqrt{2}$ avec a et $b \in \mathbf{Q}$.

a) Montrer que K est un sous-corps de $\mathbf{R}$ et que A est un sous-anneau de K. Montrer aussi que $(1, \sqrt{2})$ est une base de A comme $\mathbf{Z}$-module et une base de K comme $\mathbf{Q}$-espace vectoriel.

b) Pour $x = a + b\sqrt{2} \in K$, on pose $\delta(x) = \left|a^2 - 2b^2\right|$. Montrer que $\delta(xy) = \delta(x)\delta(y)$ pour tous $x, y \in K$.

c) Pour $x = a + b\sqrt{2} \in K$, on pose $\{x\} = \{a\} + \{b\}\sqrt{2}$, où $\{t\}$ désigne le nombre entier le plus proche d'un nombre réel t, choisi inférieur à t en cas de litige. Montrer que $\delta(x - \{x\}) \leqslant \frac{1}{2}$.

d) Montrer que A est euclidien pour δ.

71) Soit K l'ensemble des nombres complexes de la forme $a+b\frac{1+i\sqrt{3}}{2}$, où a et $b \in \mathbf{Q}$, et soit A l'ensemble des éléments de K où a et $b \in \mathbf{Z}$.

a) Montrer que K est un sous-corps de $\mathbf{C}$ et que A est un sous-anneau de K.

b) Montrer que A est un anneau euclidien pour l'application $z \mapsto |z|^2$.

72) Soit A un anneau intègre et soit $\delta : A \setminus \{0\} \to \mathbf{N}$ une application qui vérifie la seconde propriété des jauges des anneaux euclidiens, à savoir : pour tous a et b dans A, $b \neq 0$, il existe q et $r \in A$ tels que $a = bq+r$ et tels que $r = 0$ ou $\delta(r) < \delta(b)$. Pour $a \in A$, on pose $\delta'(a) = \min_{b\neq 0} \delta(ab)$.

Montrer que δ' est une jauge sur A et donc que A est un anneau euclidien.

73) [*PAS FINI*] Soit A un anneau, non nécessairement commutatif et soit a, b des éléments non nuls de A.

Soit $f : A/aA \to A/bA$ un isomorphisme de A-modules à droite.

a) Montrer qu'il existe $u \in A$ tel que $f(\mathrm{cl}(x)) = \mathrm{cl}(ux)$ pour tout $x \in A$.

b) Montrer qu'il existe $v \in A$ tel que $ua = bv$.

c) Montrer qu'il existe x et $y \in A$ tels que $1 = u + bx = v + ay$. (...)

74) Soit A un anneau euclidien, de jauge δ.

a) Soit $a \in A$ un élément non nul, non inversible de jauge minimale. Montrer que pour tout $x \in A$ qui n'est pas multiple de a, il existe un élément inversible $u \in A$ tel que $1-ux$ soit multiple de a.

b) Soit n le nombre d'éléments inversibles de A. Montrer qu'il existe un idéal maximal $\mathfrak{m} \subset A$ tel que le cardinal de $A/\mathfrak{m}$ soit inférieur ou égal à $n+1$.

75) Soit A le sous-anneau de $\mathbf{C}$ engendré par $\varepsilon = (1+i\sqrt{19})/2$.

a) Montrer que $\varepsilon^2 = \varepsilon - 5$. En déduire que A est un $\mathbf{Z}$-module libre de base $(1, \varepsilon)$.

b) Montrer que pour tout $a \in A$, $|a|^2$ est entier. En déduire qu'un élément $a \in A$ est inversible si et seulement si $|a|^2 = 1$. En déduire que $A^\times = \{-1, +1\}$.

c) Soit $\mathfrak{m}$ un idéal maximal de A. Montrer qu'il existe un nombre premier p tel que $p \in \mathfrak{m}$. Montrer que $A/\mathfrak{m}$ a pour cardinal p^2 si $P = X^2 - X + 5$ est irréductible dans $\mathbf{Z}/p\mathbf{Z}$, et pour cardinal p sinon.

d) Montrer que le polynôme X^2-X+5 est irréductible dans les corps $\mathbf{Z}/2\mathbf{Z}$ et $\mathbf{Z}/3\mathbf{Z}$; en déduire que le cardinal de $A/\mathfrak{m}$ est au moins égal à 4.

e) Montrer que A n'est pas un anneau euclidien.

§1.9. Anneaux factoriels

DÉFINITION 1.9.1. — *Soit A un anneau intègre. On dit qu'un élément non nul $a \in A$ est* irréductible *s'il n'est pas inversible et si la relation $a = bc$ avec b et $c \in A$ entraîne que b ou c est inversible.*

Exemples 1.9.2. — Les éléments irréductibles de $\mathbf{Z}$ sont les nombres premiers et leurs opposés. Soit k un corps commutatif ; les éléments irréductibles de $k[X]$ sont les polynômes irréductibles c'est-à-dire lespolynômes de degré $\geqslant 1$ qui ne s'écrivent pas comme produit de deux polynômes de degrés $\geqslant 1$. L'élément 0 n'est jamais irréductible : il s'écrit 0×0 et 0 n'est pas inversible (car A est intègre, donc $1 \neq 0$).

PROPOSITION 1.9.3 (Lemme de Gauss). — *Soit A un anneau principal qui n'est pas un corps. Pour qu'un idéal de A soit maximal, il faut et il suffit qu'il soit engendré par un élément irréductible.*

Démonstration. — Soit I un idéal maximal d'un anneau principal A et soit a un générateur de I. Comme A n'est pas un corps, $I \neq 0$ et $a \neq 0$. Soit b et c des éléments de A tels que $a = bc$. Si $b \notin I$, on a $I + (b) = A$, car I est un idéal maximal, donc $(b) = A$ car $I = (a) \subset (b)$; par suite, b est inversible. Sinon, $b \in I$; il existe $u \in A$ tel que $b = au$, d'où $a = auc$ et $cu = 1$ en simplifiant par a ; par suite, b est inversible.

Inversement, soit a un élément irréductible de A et montrons que l'idéal $I = aA$ est un idéal maximal de A. Soit x un élément de A qui n'est pas multiple de a et posons $J = I + (x)$. Soit b un générateur de J ; comme $a \in I$, il existe $c \in A$ tel que $a = bc$. Si c était inversible, on aurait $(a) = (b) = I + (x)$, d'où $x \in (a)$, ce qui n'est pas. Comme a est irréductible, l'élément b est alors inversible, si bien que $J = A$. Cela démontre que I est un idéal maximal de A. □

DÉFINITION 1.9.4. — *Soit A un anneau intègre. On dit que A est un anneau* factoriel *s'il vérifie les deux propriétés suivantes :*

a) *toute suite croissante d'idéaux principaux de A est stationnaire ;*

b) *pour tout élément irréductible a de A, l'idéal principal (a) engendré par a est un idéal premier.*

La première condition va permettre d'écrire un élément comme produit d'éléments irréductibles. Elle est automatique si l'anneau A est noethérien. La seconde, la plus importante, va garentir l'unicité d'une décomposition en facteurs irréductibles, à des modifications mineures près.

Explicitons un peu cette seconde condition. Soit p un élément irréductible de A. Par définition, l'idéal (p) est premier si et seulement si le produit d'éléments a et b dans A ne peut appartenir à (p) sans que l'un des deux y appartienne. Autrement dit : si ab est multiple de p, a ou b est multiple de p.

Exemples 1.9.5. — *a*) La prop. 1.9.3 entraîne qu'un élément irréductible engendre un idéal maximal. Compte-tenu du lemme 1.9.6 ci-dessous, un anneau principal est factoriel.

b) Nous verrons plus tard que si A est un anneau factoriel, il en est de même de l'anneau $A[X_1, \ldots, X_n]$ des polynômes à coefficients dans A. C'est en particulier le cas des anneaux de polynômes à coefficients dans un corps, ou dans l'anneau $\mathbf{Z}$.

LEMME 1.9.6. — *Toute suite croissante d'idéaux d'un anneau principal est stationnaire.*[(3)]

[(3)] En d'autres termes, un anneau principal est *noethérien.*

Démonstration. — Soit A un anneau principal, soit (I_n) une suite croissante d'idéaux de A. Soit I la réunion des I_n ; c'est un idéal de A car la réunion est croissante. Comme A est principal, il existe un élément $a \in I$ tel que $I = (a)$. Soit alors $n \in \mathbf{N}$ tel que $a \in I_n$. Pour $m \geqslant n$, on a $I = (a) \subset I_n \subset I$, d'où l'égalité. □

THÉORÈME 1.9.7. — *Soit A un anneau factoriel et soit a un élément non nul de A.*

a) *Il existe des éléments irréductibles $p_1, \ldots, p_n \in A$ et un élément inversible $u \in A$ tels que $a = up_1 \ldots p_n$ (*existence d'une décomposition en facteurs irréductibles*).*

b) *Considérons deux décompositions de a en facteurs irréductibles, disons $a = up_1 \ldots p_n = vq_1 \ldots q_m$. Alors $n = m$ et il existe une permutation σ de $\{1, \ldots, n\}$ et des éléments inversibles u_i, pour $1 \leqslant i \leqslant n$, tels que $q_i = u_i p_{\sigma(i)}$ pour tout i (*unicité de la décomposition en facteurs irréductibles*).*

C'est la définition classique d'un anneau factoriel !

Démonstration. — Si a est inversible, l'assertion *a*) est évidente (avec $n = 0$ et $u = a$). Sinon, il existe un idéal maximal contenant (a), donc un élément irréductible $p_1 \in A$ tel que $aA \subset p_1 A$. Soit a_1 l'élément de A tel que $a = p_1 a_1$. On a ainsi $(a) \subsetneq (a_1)$. Si a_1 n'est pas inversible, on peut réitérer l'argument, de sorte à obtenir des éléments irréductibles $p_1, \ldots, p_n$ et des éléments $a_1, \ldots, a_n \in A$ tels que $a = p_1 \ldots p_n a_n$. Si a_n est inversible, l'assertion *a*) est démontrée. Si l'on peut réiterer l'argument à l'infini, la suite d'idéaux $(a) \subset (a_1) \subset \ldots$ est strictement croissante, donc non stationnaire, ce qui contredit le premier axiome d'un anneau factoriel.

Soit $a = up_1 \ldots p_n = vq_1 \ldots q_m$ deux décompositions de a en produit d'éléments irréductibles. Si $m = 0$, $a = v$ est inversible ; il en est alors de même de $up_1 \ldots p_n$, ce qui implique $n = 0$ et $a = u = v$. Supposons $m \geqslant 1$. Comme q_m divise $up_1 \ldots p_m$ et que l'idéal (q_m) est premier, q_m divise l'un des facteurs u, p_1, …, p_n. Comme u est inversible, il existe un entier $j \in \{1, \ldots, n\}$ tel que q_m divise p_j. Comme p_j est irréductible, p_j et q_m ne diffèrent que par multiplication par un élément inversible. Il existe un élément inversible $u_m \in A^\times$ tel que $q_m = u_m p_j$. Posons $b = a/q_m$. Il possède deux décompositions en produit d'éléments irréductibles, à savoir $vq_1 \ldots q_{m_1}$ et $(u/u_m)p_1 \ldots \widehat{p_j} \ldots p_n$, où le chapeau sur p_j signifie que ce facteur est omis du produit. Par récurrence, $m - 1 = n - 1$, il existe une permutation σ de $\{1, \ldots, m-1\}$ sur $\{1, \ldots, \widehat{j}, \ldots, n\}$, des éléments inversibles u_i tels que $q_i = u_i p_{\sigma(i)}$ pour $1 \leqslant i \leqslant m-1$. On a donc $m = n$ et l'application σ de $\{1, \ldots, m\}$ sur $\{1, \ldots, n\}$ qui étend σ et telle que $\sigma(m) = j$ est une permutation telle que $q_i = u_i p_{\sigma(i)}$ pour tout i compris entre 1 et n. Cela démontre l'assertion d'unicité par récurrence sur m. □

Remarque 1.9.8. — Inversement, soit A un anneau intègre vérifiant la conclusion du théorème.

Si $a \in A$ n'est pas nul, notons $f(a)$ le nombre de facteurs irréductibles dans une décomposition de a en produit d'éléments irréductibles. Il ne dépend pas de la décomposition choisie.

Soit a, b, c des éléments de A tels que $a = bc$ et $a \neq 0$. Par la propriété d'unicité, on voit que $f(a) = f(b) + f(c)$. Soit (a_n) une suite d'éléments de A telle que la suite d'idéaux $(a_0), (a_1), \ldots$, soit croissante. Il existe ainsi pour tout entier n un élément $b_n \in A$ tel que $a_n = b_n a_{n+1}$ et $f(a_{n+1}) \leqslant f(a_n)$; la suite $(f(a_n))_n$ est donc une suite décroissante d'entiers naturels. Elle est donc stationnaire. De plus, si $f(a_n) = f(a_{n+1})$, b_n est une unité et les idéaux (a_n) et (a_{n+1}) sont égaux. Cela démontre que la suite d'idéaux $((a_n))_n$ est elle-même stationnaire.

Soit p un élément irréductible de A et soit a, b, c des éléments de A tels que $ab = pc$. Si $c = 0$, $pc = 0$ et a ou b est nul. Supposons $c \neq 0$; alors $a \neq 0$ et $b \neq 0$. Choisissons-en des décompositions en facteurs irréductibles $a = up_1 \ldots p_n$, $b = vq_1 \ldots q_m$, $c = wr_1 \ldots r_s$. Alors, ab possède deux décompositions irréductibles $uvp_1 \ldots p_n q_1 \ldots q_m$ et $wpr_1 \ldots r_s$. L'assertion d'unicité implique que le facteur irréductible p qui apparaît dans la seconde décomposition invervient aussi dans la première. Il existe donc élément inversible α de A et, ou bien un élément $i \in \{1, \ldots, n\}$ tel que $p = \alpha p_i$, ou bien un élément $j \in \{1, \ldots, m\}$ tel que $p = \alpha q_j$. Dans le premier cas, a est multiple de p, dans le second, b est multiple de p. Par suite, l'idéal (p) est un idéal premier.

Ces remarques montrent que l'anneau A est factoriel.

Remarque 1.9.9. — Certains anneaux possèdent des éléments irréductibles privilégiés, les nombres premiers dans $\mathbf{Z}$, les polynômes irréductibles unitaires dans un anneau de polynômes, par exemple. Soit A un anneau factoriel. Voyons comment normaliser la décomposition en facteurs irréductibles de sorte à disposer, pour tout élément non nul de A, d'une décomposition en facteurs irréductibles bien définie.

Choisissons une famille (π_i) d'éléments irréductibles de A telle que

– si $i \neq j$, π_i et π_j ne sont pas associés ;
– tout élément irréductible de A est associé à l'un des π_i.[(4)]

Alors, tout élément non nul de A s'écrit de manière unique sous la forme $u \prod_i \pi_i^{r_i}$ où u est un élément inversible de A et les r_i des entiers positifs ou nuls, seul un nombre fini d'entre eux étant nuls. De manière équivalente, l'application $A^\times \times \mathbf{N}^{(I)}$ dans $A \setminus \{0\}$ qui associe à $(u, (r_i))$ le produit $u \prod_i \pi_i^{r_i}$ est un isomorphisme de monoïdes.

Un autre intérêt de cette normalisation est qu'un élément $a = u \prod_i \pi_i^{r_i}$ divise un élément $b = v \prod_i \pi_i^{s_i}$ si et seulement si pour tout i, $r_i \leqslant s_i$. (En effet, si $c \in A$ est tel que $b = ac$, soit $c = w \prod_i \pi_i^{t_i}$ la décomposition en facteurs irréductibles de c, on a alors

$$b = v \prod_i \pi_i^{s_i} = uw \prod_i \pi_i^{r_i + t_i},$$

d'où, par unicité, $s_i = r_i + t_i \geqslant r_i$ pour tout i. Réciproquement, il suffit de poser $c = vu^{-1} \prod_i \pi_i^{s_i - r_i}$.)

1.9.10. Ppcm, pgcd. — Soit A un anneau factoriel.

Soit (a_n) une famille d'éléments non nuls de A. On va définir leur ppcm et leur pgcd. Pour simplifier, on suppose avoir normalisé la décomposition en facteurs irréductibles

(4) Une telle famille existe, il suffit de choisir, à l'aide du théorème de Zorn, une famille maximale d'éléments irréductibles de A deux à deux non associés.

comme ci-dessus. Pour tout n, notons $a_n = u_n \prod_i \pi_i^{r_{n,i}}$ la décomposition en facteurs irréductibles de a_n. Pour tout i, on pose $r_i = \min(r_{n,i})$; c'est un entier naturel, nul pour presque tout i, ce qui permet de poser $\mathrm{pgcd}((a_n)) = \prod_i \pi_i^{r_i}$. Comme $r_i \leqslant r_{n,i}$ pour tout i, c'est un diviseur de chacun des a_n.

Soit b un élément non nul de A; notons $b = v \prod_i \pi_i^{s_i}$ sa décomposition en facteurs irréductibles. Pour que b divise a_n, il faut et il suffit que $s_i \leqslant r_{n,i}$ pour tout i ; pour que b divise tous les a_n, il faut et il suffit que $s_i \leqslant r_i$ pour tout i, c'est-à-dire que b divise $\mathrm{pgcd}((a_n))$. Cela justifie d'appeler $\mathrm{pgcd}((a_n))$ le *plus grand diviseur commun* des a_n. l'expression « plus grand » étant à prendre au sens de la divisibilité.

Pour tout i, posons $m_i = \max(r_{n,i})$. Si la suite (m_i) est une suite d'entiers naturels dont presque tous les termes sont nuls, nous pouvons poser $\mathrm{ppcm}((a_n)) = \prod \pi_i^{m_i}$. Sinon, posons $\mathrm{ppcm}((a_n)) = 0$. Dans tous les cas, c'est un multiple de chacun des a_n.

Soit b un élément non nul de A; notons $b = v \prod_i \pi_i^{s_i}$ sa décomposition en facteurs irréductibles. Pour que b soit multiple de a_n, il faut et il suffit que $s_i \geqslant r_{n,i}$ pour tout i ; pour que b soit multiple de tous les a_n, il faut et il suffit que $s_i \geqslant m_i$ pour tout i. Si l'un des m_i est infini, ou si la suite (m_i) n'est pas presque nulle, cette condition n'est pas réalisée et aucun élément non nul de A n'est multiple de tous les a_n. Dans le cas contraire, on voit en revanche que b est multiple de $\mathrm{ppcm}((a_n))$, et inversement. Là encore, cela justifie d'appeler $\mathrm{ppcm}((a_n))$ le *plus petit multiple commun* des a_n. l'expression « plus petit » étant aussi à prendre au sens de la divisibilité.

DÉFINITION 1.9.11. — *Des éléments d'un anneau factoriel A sont dits* premiers entre eux *si leur pgcd est égal à* 1.

Soit (a_n) une famille d'éléments de A. Alors, pour $x \in A$, on a la relation

$$\mathrm{pgcd}((xa_n)) = x\,\mathrm{pgcd}(a_n).$$

Cela se démontre aisément en considérant les décompositions en facteurs irréductibles des a_n, la formule se ramène en effet à la formule $\min(r_n) + s = \min(r_n + s)$. Inversement, si $d = \mathrm{pgcd}((a_n))$, il existe pour tout n un élément $b_n \in A$ tel que $a_n = d\,b_n$ et l'on a $\mathrm{pgcd}((b_n)) = 1$. Les b_n sont donc premiers entre eux.

PROPOSITION 1.9.12. — *Soit A un anneau factoriel et soit (a_n) une famille d'éléments de A. L'idéal engendré par* $\mathrm{pgcd}((a_n))$ *est le plus petit idéal principal contenant l'idéal engendré par les a_n. L'idéal engendré par* $\mathrm{ppcm}((a_n))$ *est le plus grand idéal principal contenu dans l'idéal $\bigcap_n (a_n)$.*

En particulier, si A est un anneau principal, deux éléments a et b sont premiers entre eux si et seulement si les idéaux (a) et (b) sont comaximaux.

Démonstration. — Compte tenu du fait que l'inclusion d'idéaux $(a) \subset (b)$ équivaut à ce que a soit multiple de b, c'est une simple reformulation de ce qui a été dit plus haut. □

Remarque 1.9.13. — Si l'on ne fixe pas une forme particulière pour la décomposition en facteurs irréductibles, le ppcm et le pgcd de deux éléments sera bien défini à multiplication par un élément inversible près.

COROLLAIRE 1.9.14 (Théorème de Bézout). — *Soit A un anneau principal, soit (a_n) une famille d'éléments de A et soit d son pgcd. il existe des éléments $u_n \in A$, presque tous nuls, tels que $d = \sum u_n a_n$.*

Exercices. — 76) Soit A l'ensemble des nombres complexes de la forme $a + b\mathrm{i}\sqrt{5}$, où a et $b \in \mathbf{Z}$.

a) Montrer que A est un sous-anneau de $\mathbf{C}$.

b) Montrer que les seuls éléments inversibles de A sont 1 et -1.

c) Montrer que 2, 3, $1 + \mathrm{i}\sqrt{5}$ et $1 - \mathrm{i}\sqrt{5}$ sont irréductibles dans A.

d) En observant que $2 \cdot 3 = (1 + \mathrm{i}\sqrt{5})(1 - \mathrm{i}\sqrt{5})$, montrer que A n'est pas un anneau principal.

77) Soit A un anneau principal.

a) Soit a un élément non nul de A. Démontrer que $A/(a)$ est de longueur finie ; calculer sa longueur en termes de la décomposition en facteurs irréductibles de a.

b) Utiliser le théorème de Jordan-Hölder pour donner une seconde démonstration de l'unicité de la décomposition en facteurs irréductibles.

78) Cet exercice est la base de l'algorithme de Berlekamp pour factoriser des polynômes sur des corps finis.

Soit P un polynôme non constant à coefficients dans le corps fini $\mathbf{F}_p$. On suppose que P est *séparable* c'est-à-dire que P et P' sont premiers entre eux.

Notons R_P l'anneau $\mathbf{F}_p[X]/(P)$. Soit $P = \prod_{i=1}^{r} P_i$ la factorisation de P en polynômes irréductibles de $\mathbf{F}_p[X]$. Notons $n_i = \deg P_i$.

a) Montrer que l'anneau R_{P_i} est isomorphe au corps fini $\mathbf{F}_{p^{n_i}}$.

b) Si $A \in R_P$, on désigne par $\rho_i(A)$ le reste de la division euclidienne de A par P_i. Montrer que l'application $A \mapsto (\rho_1(A), \ldots, \rho_r(A))$ définit un isomorphisme d'anneaux $R_P \simeq \prod_{i=1}^{r} R_{P_i}$.

c) Si $A \in R_P$, posons $t(A) = A^p - A$. Montrer que t est un endomorphisme $\mathbf{F}_p$-linéaire de R_P (vu comme un $\mathbf{F}_p$-espace vectoriel) et qu'il correspond, par les isomorphismes précédents, à l'application

$$\prod_{i=1}^{r} \mathbf{F}_{p^{n_i}} \to \prod_{i=1}^{r} \mathbf{F}_{p^{n_i}}, \qquad (a_1, \ldots, a_r) \mapsto (a_1^p - a_1, \ldots, a_r^p - a_r).$$

d) Montrer que le noyau de t est un sous-espace vectoriel de R_P de dimension r.

e) Soit a un élément du noyau de t. Montrer qu'il existe un polynôme unitaire $Q \in \mathbf{F}_p[X]$ de degré minimal tel que $Q(a) = 0$. Montrer que le polynôme Q est séparable et scindé sur $\mathbf{F}_p$.

f) (*suite*) Si $a \notin \mathbf{F}_p$, montrer que Q n'est pas irréductible. D'une factorisation partielle $Q = Q_1 Q_2$, montrer comment obtenir une factorisation partielle non triviale de P.

79) Soit p un nombre premier et considérons le polynôme $P = X^n + X + p$, où $n \geqslant 2$.

a) Supposons $p \neq 2$. Montrer que toute racine complexe de P vérifie $|z| > 1$.

b) Toujours pour $p \neq 2$, montrer que P est irréductible dans $\mathbf{Z}[X]$.

c) Supposons maintenant $p = 2$. Si n est pair, montrer que P est irréductible dans $\mathbf{Z}[X]$. Si n est impair, montrer que $X + 1$ divise P et que $P/(X + 1)$ est irréductible dans $\mathbf{Z}[X]$.

d) Plus généralement, tout polynôme $P = a_n X^n + \cdots + a_1 X + a_0$ tel que $|a_0|$ soit un nombre premier strictement supérieur à $|a_1| + \cdots + |a_n|$ est irréductible.

80) Soit n un entier $\geqslant 2$ et S le polynôme $X^n - X - 1$. Le but du problème est de montrer, en suivant Selmer (*Math. Scand.* **4** (1956), p. 287–302) que S est irréductible dans $\mathbf{Z}[X]$.

a) Montrer que S a n racines distinctes dans $\mathbf{C}$.

b) Pour tout polynôme $P \in \mathbf{Q}[X]$ tel que $P(0) \neq 0$, on pose

$$\varphi(P) = \sum_{j=1}^{m} \Big(z_j - \frac{1}{z_j}\Big),$$

où $z_1, \ldots, z_m$ sont les racines complexes de P, répétées suivant leur multiplicité.

Calculer $\varphi(P)$ en fonction des coefficients de P. Calculer $\varphi(S)$.

Si P et Q sont deux polynômes de $\mathbf{Q}[X]$ tels que $P(0)Q(0) \neq 0$, montrer que $\varphi(PQ) = \varphi(P) + \varphi(Q)$.

c) Si z est une racine de S, montrer l'inégalité

$$2\Re\Big(z - \frac{1}{z}\Big) > \frac{1}{|z|^2} - 1.$$

(Poser $z = re^{i\theta}$ et évaluer $\cos(\theta)$ en fonction de r.)

d) Si $x_1, \ldots, x_m$ sont des nombres réels strictement positifs tels que $\prod_{j=1}^{m} x_j = 1$. Montrer l'inégalité $\displaystyle\sum_{j=1}^{m} x_j \geqslant m$.

e) Soit P et Q deux polynômes de $\mathbf{Z}[X]$ de degrés non nuls tels que $S = PQ$. Montrer que $|P(0)| = 1$ puis que $\varphi(P)$ est un entier strictement positif. En déduire une contradiction, et donc que S est un polynôme irréductible dans $\mathbf{Z}[X]$.

§1.10. Factorialité des anneaux de polynômes

Il est difficile de mentionner les anneaux factoriels sans discuter un théorème de Gauss selon lequel les anneaux de polynômes à coefficient dans un anneau factoriel sont eux-mêmes factoriels.

Soit donc A un anneau factoriel. Tout d'abord, on rappelle que *les éléments inversibles de $A[X]$ sont les polynômes constants égaux à un élément inversible de $A^\times$*. Comme A est intègre, rappelons que l'on a $\deg(PQ) = \deg(P) + \deg(Q)$, si P et Q sont deux polynômes de $A[X]$. Par suite, si $PQ = 1$, $\deg(P) = \deg(Q) = 0$, P et Q sont des éléments de A, inverses l'un de l'autre dans A, et *a fortiori* inversibles dans $A[X]$. (Voir aussi l'exercice 21.)

DÉFINITION 1.10.1. — *Soit A un anneau factoriel et soit P un polynôme dans $A[X]$. Le* contenu *de P, noté* $\mathrm{ct}(P)$*, est par définition le pgcd des coefficients de P. Un polynôme est dit* primitif *si son contenu est* 1*, c'est-à-dire si ses coefficients sont premiers entre eux.*

Comme d'habitude lorsqu'il s'agit de pgcd, le contenu est défini à multiplication par un élément inversible de A près.

PROPOSITION 1.10.2. — *Soit A un anneau factoriel et soit P et Q deux polynômes de $A[X]$. Alors,* $\mathrm{ct}(PQ) = \mathrm{ct}(P)\,\mathrm{ct}(Q)$.

Démonstration. — Les coefficients de P sont tous divisibles par $\mathrm{ct}(P)$ et les coefficients du polynôme $P_1 = P/\mathrm{ct}(P)$ sont premiers entre eux ; le polynôme P_1 est donc primitif. De même, il existe un polynôme primitif $Q_1 \in A[X]$ tel que $Q = \mathrm{ct}(Q)Q_1$. Alors, $PQ = \mathrm{ct}(P)\,\mathrm{ct}(Q)P_1Q_1$ et $\mathrm{ct}(PQ)$ est ainsi égal à $\mathrm{ct}(P)\,\mathrm{ct}(Q)\,\mathrm{ct}(P_1Q_1)$. Il suffit donc de montrer que P_1Q_1 est encore un polynôme primitif.

Soit π un élément irréductible de A et montrons que π ne divise pas tous les coefficients de P_1Q_1. Comme P_1 est primitif, la réduction $\mathrm{cl}(P_1)$ de P_1 modulo π est un polynôme non nul à coefficients dans l'anneau $A/(\pi)$. De même, $\mathrm{cl}(Q_1)$ est un polynôme non nul à coefficients dans $A/(\pi)$. Or, π est irréductible dans A qui est un anneau factoriel. Par suite, $A/(\pi)$ est un anneau intègre et l'anneau de polynômes $(A/(\pi))[X]$ est aussi intègre (corollaire 1.4.5). Il en résulte que le produit $\mathrm{cl}(P_1)\,\mathrm{cl}(Q_1) = \mathrm{cl}(P_1Q_1)$ est encore non nul dans $(A/\pi)[X]$. Cela signifie exactement que π ne divise pas tous les coefficients de P_1Q_1, ce qu'on voulait démontrer. □

Cette proposition fondamentale va nous permettre de déterminer les éléments irréductibles de $A[X]$.

PROPOSITION 1.10.3. — *Soit A un anneau factoriel et soit K son corps des fractions. Les éléments irréductibles de $A[X]$ sont*

– *les éléments irréductibles de A ;*

– *les polynômes primitifs de $A[X]$ qui sont irréductibles en tant que polynômes de $K[X]$.*

Démonstration. — On commence par montrer que ces éléments sont irréductibles, puis on montrera qu'il n'y en a pas d'autres.

Soit donc a un élément de A qui est irréductible et soit P et Q deux polynômes de $A[X]$ tels que $a = PQ$. Alors, $\deg(P) + \deg(Q) = \deg(PQ) = 0$, donc P et Q sont tous deux de degré 0, c'est-à-dire des éléments de A. Comme a est irréductible dans A, P ou Q est inversible dans A, donc aussi dans $A[X]$ et a est bien irréductible dans $A[X]$.

Soit maintenant $P \in A[X]$ un polynôme primitif qui est irréductible dans $K[X]$. Si $P = QR$ avec Q et R dans $A[X]$, cela fournit *a fortiori* une décomposition dans $K[X]$ si bien que Q ou R est inversible dans $K[X]$, autrement dit, Q ou R est constant. Supposons

pour fixer les notations que R est un élément de A, noté a ; on a donc $P = aQ$. Par suite, le contenu de P vaut

$$\mathrm{ct}(P) = \mathrm{ct}(aQ) = a\,\mathrm{ct}(Q)$$

et a est nécessairement inversible dans A donc dans $A[X]$. Ainsi, P est irréductible dans $A[X]$.

Réciproquement, soit P un élément irréductible de $A[X]$. Il existe un polynôme primitif $P_1 \in A[X]$ tel que $P = \mathrm{ct}(P)P_1$. Par suite, $\mathrm{ct}(P) = 1$ ou P_1 est inversible dans $A[X]$.

Supposons d'abord que P n'est pas primitif. Alors, P_1 est inversible dans $A[X]$, ce qui signifie que P_1 est un polynôme constant, inversible dans A. Il reste à montrer que $\mathrm{ct}(P)$ est irréductible, mais s'il ne l'était pas, on pourrait écrire $\mathrm{ct}(P) = ab$ où ni a ni b n'est inversible dans A. Cela fournirait une factorisation $P = a(bP_1)$ comme produit de deux éléments non inversibles, ce qui contredit l'hypothèse que P est irréductible.

Supposons maintenant que P_1 n'est pas inversible dans $A[X]$, c'est-à-dire $\deg(P) > 0$. On a déjà vu que $\mathrm{ct}(P) = 1$, donc $P = P_1$ et il faut montrer que P est irréductible dans $K[X]$. Soit $P = QR$ une factorisation de P en produit de deux éléments de $K[X]$. On peut écrire $Q = qQ_1$ et $R = rR_1$, où q et r sont deux éléments de K et Q_1 et R_1 sont deux polynômes primitifs de $A[X]$. On a ainsi $P = (qr)Q_1R_1$. Écrivons alors $qr = a/b$ où a et b sont deux éléments de A. On a $bP = aQ_1R_1$. Par suite, ces deux polynômes ont même contenu, b et a respectivement[(5)], c'est-à-dire $qr \in A^\times$. Comme P est irréductible dans $A[X]$, cette factorisation montre que Q_1 ou R_1 est inversible dans $A[X]$, donc dans $K[X]$; par suite, $Q = qQ_1$ ou $R = rR_1$ est inversible dans $K[X]$. □

THÉORÈME 1.10.4 (Gauss). — *Si A est un anneau factoriel, $A[X]$ est un anneau factoriel.*

Démonstration. — Soit (P_n) une suite d'éléments de $A[X]$ telle que la suite d'idéaux $((P_n))$ soit croissante. Pour $n \geqslant m$, P_m est multiple de P_n, donc $\mathrm{ct}(P_m)$ est multiple de $\mathrm{ct}(P_n)$. Par suite, la suite $((\mathrm{ct}(P_n))$ est croissante. Comme l'anneau A est factoriel, cette suite d'idéaux est stationnaire. De même, pour $n \geqslant m$, $\deg(P_n) \leqslant \deg(P_m)$, donc la suite d'entiers naturels $(\deg(P_n))$ est décroissante ; elle est donc stationnaire.

Soit N un entier tel que $\deg(P_n) = \deg(P_N)$ et $\mathrm{ct}(P_n) = \mathrm{ct}(P_N)$ pour $n \geqslant N$. Soit n un entier tel que $n \geqslant N$; comme P_n divise P_N, il existe un polynôme Q tel que $P_N = QP_n$. On a alors $\deg(Q) = 0$ et $\mathrm{ct}(Q) = 1$, ce qui entraîne que Q est un polynôme constant, de terme constant $\mathrm{ct}(Q)$, donc inversible. Par suite, les idéaux (P_n) et (P_N) coïncident, ce qui démontre que la suite d'idéaux principaux (P_n) est stationnaire.

Montrons maintenant que les éléments irréductibles de $A[X]$ engendrent des idéaux premiers ou, ce qui est équivalent, que si un élément irréductible de $A[X]$ divise un produit, il divise l'un des facteurs.

(5) à multiplication par un élément inversible de $A^\times$ bien entendu

Soit d'abord π un élément irréductible de A qui divise un produit PQ de deux polynômes de $A[X]$. Il s'ensuit que π divise $\mathrm{ct}(PQ) = \mathrm{ct}(P)\,\mathrm{ct}(Q)$. Par suite π divise $\mathrm{ct}(P)$ ou $\mathrm{ct}(Q)$ et donc il divise P ou Q.

Soit maintenant un polynôme primitif $\Pi \in A[X]$, irréductible dans $K[X]$ qui divise un tel produit PQ. Il divise par conséquent l'un des facteurs dans $K[X]$, dison P pour fixer les notations : $P = R\Pi$ avec $R \in K[X]$. On écrit alors $R = (a/b)R_1$ où $R_1 \in A[X]$ est primitif, et a et b sont deux éléments de A premiers entre eux. On a alors $bP = bR\Pi = aR_1\Pi$. L'égalité des contenus montre que $a = b\,\mathrm{ct}(P)$ et donc $a/b = \mathrm{ct}(P)$ appartient à A. On a donc $R \in A[X]$, ce qui prouve que Π divise P dans $A[X]$. □

COROLLAIRE 1.10.5 (Gauss). — *Si A est un anneau factoriel, $A[X_1,\dots,X_n]$ est un anneau factoriel. En particulier, si k est un corps, $k[X_1,\dots,X_n]$ est un anneau factoriel.*

Démonstration. — C'est immédiat par récurrence sur n en utilisant l'isomorphisme

$$A[X_1,\dots,X_n] \simeq (A[X_1,\dots,X_{n-1}])[X_n].$$

□

Exercices. — 81) [*Critère d'irréductibilité d'Eiseinstein*] Soit A un anneau factoriel et K son corps des fractions. Soit

$$f(X) = \sum_{0 \leqslant k \leqslant n} a_k X^k$$

un polynôme de degré $n \geqslant 1$ à coefficients dans A. Soit p un élément irréductible de A. On suppose que p ne divise pas a_n, que p divise a_k si $0 \leqslant k < n$ et que p^2 ne divise pas a_0. Montrer que f est irréductible dans $K[X]$.

82) Soit $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ un polynôme unitaire dans $\mathbf{Z}[X]$ tel que $a_0 \neq 0$ et

$$|a_{n-1}| > 1 + |a_{n-2}| + \cdots + |a_0|.$$

a) À l'aide du théorème de Rouché en théorie des fonctions d'une variable complexe, montrer que P a exactement une racine complexe de valeur absolue $\geqslant 1$.

b) Montrer que P est irréductible dans $\mathbf{Z}[X]$ (*théorème de Perron*).

83) On considère l'anneau $\mathbf{C}[X,Y]$ des polynômes à coefficients dans $\mathbf{C}$ en les indéterminées X et Y. Soit I l'idéal de $\mathbf{C}[X,Y]$ engendré par l'élément $Y^2 - X^3 + X$ et A l'anneau $\mathbf{C}[X,Y]/I$. On note x et y les classes de X et Y dans A.

Le but de l'exercice est de montrer que A n'est pas un anneau factoriel.

a) Montrer que A est intègre.

b) Montrer que l'homomorphisme canonique $\mathbf{C}[T] \to A$ tel que $T \mapsto x$ est injectif. En déduire que le sous-anneau $\mathbf{C}[x]$ de A engendré par $\mathbf{C}$ et x est isomorphe à l'anneau des polynômes

$\mathbf{C}[T]$. Le degré d'un élément de $\mathbf{C}[x]$ sera par définition le degré du polynôme de $\mathbf{C}[T]$ dont il est l'antécédent.

c) Soit a un élément de A. Montrer qu'il existe des éléments p et q uniques dans $\mathbf{C}[x]$ tels que l'on ait $a = p + qy$.

d) Montrer que l'application $\sigma : A \to A$ définie par $\sigma(p+qy) = p - qy$ est un automorphisme de A qui fixe les éléments de $\mathbf{C}[x]$.

e) Pour tout a dans A, on pose $N(a) = a\sigma(a)$. Vérifier que pour tout a, $N(a)$ appartient à $\mathbf{C}[x]$, que $N(1) = 1$ et que le degré de $N(a)$ est différent de 1. Montrer que pour tous a et b dans A, on a $N(ab) = N(a)N(b)$.

f) Déduire des questions 2, 3 et 5 que $\mathbf{C} \setminus \{0\}$ est l'ensemble des unités de A.

g) Montrer que x, y, $1-x$ et $1+x$ sont irréductibles dans A.

h) Montrer que A n'est pas factoriel.

84) Si $n \geqslant 1$, soit $\Phi_n \in \mathbf{C}[X]$ l'unique polynôme unitaire dont les racines sont simples, égales aux racines primitives n^{e} de l'unité dans $\mathbf{C}$.

a) Montrer que $\prod_{d|n} \Phi_d = X^n - 1$. En déduire par récurrence que pour tout n, $\Phi_n \in \mathbf{Z}[X]$.

b) Si p est un nombre premier, calculer $\Phi_p(X)$. Montrer qu'il existe des entiers $a_1, \ldots, a_{p-1}$ tels que $\Phi_p(1+X) = X^{p-1} + pa_1X^{p-2} + \cdots + pa_{p-1}$, avec $a_{p-1} = 1$. À l'aide du critère d'Eisenstein de l'exercice 81, en déduire que Φ_p est irréductible dans $\mathbf{Q}[X]$.

c) Soit n un entier, $n \geqslant 2$ et soit ζ une racine primitive n^{e} de l'unité. On va montrer que Φ_n est irréductible dans $\mathbf{Q}[X]$. Soit P le polynôme minimal de ζ. Montrer que $P \in \mathbf{Z}[X]$ et qu'il divise Φ_n dans $\mathbf{Z}[X]$.

Soit p un nombre premier ne divisant pas n. Montrer qu'il existe $b \in \mathbf{Z}[\zeta]$ tel que $P(\zeta^p) = pb$.

d) Montrer que ζ^p est une racine primitive n^{e} de l'unité. Si $P(\zeta^p) \neq 0$, montrer en dérivant le polynôme $X^n - 1$ que $n\zeta^{p(n-1)} \in p\mathbf{Z}[\zeta]$. En déduire une contradiction et donc que pour tout nombre premier p premier à n, $P(\zeta^p) = 0$.

e) Montrer que Φ_n est irréductible dans $\mathbf{Q}[X]$.

85) Soit K un corps et soit $E = K(X)$ le corps des fractions rationnelles à coefficients dans K.

a) Montrer qu'il existe deux K-automorphismes de E, uniques, α et β tels que $\alpha(X) = 1/X$ et $\alpha(X) = 1 - X$. Montrer que le sous-groupe G de $\mathrm{Gal}(E/K)$ engendré par α et β est fini, isomorphe au groupe symétrique $\mathfrak{S}_3$.

b) Soit F le corps E^G formé des fractions rationnelles $P \in K(X)$ telles que $\alpha(P) = \beta(P) = P$. Montrer que F contient la fraction

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

c) Montrer que l'extension $K(f) \subset E$ est finie de degré 6. En déduire que $F = K(f)$.

86) Soit $K \subset \mathbf{C}(T)$ un sous-corps contenant $\mathbf{C}$ mais distinct de $\mathbf{C}$.

a) Montrer que l'extension $K \subset \mathbf{C}(T)$ est algébrique, finie.

b) On note $n = [\mathbf{C}(T) : K]$ son degré. Montrer que le polynôme minimal de T sur K est de la forme

$$f(X) = X^n + k_1X^{n-1} + \cdots + k_n$$

et qu'il existe $j \in \{1;\dots;n\}$ tel que $k_j \notin \mathbf{C}$.

c) On fixe un tel entier j et on note $u = k_j = g/h$ où $g, h \in \mathbf{C}[T]$ sont deux polynômes premiers entre eux. Soit $m = \max(\deg g, \deg h)$. Montrer que $m \geqslant n$. Montrer aussi qu'il existe $q \in K[X]$ tel que $g(X) - uh(X) = q(X)f(X)$.

d) Montrer qu'il existe des polynômes $c_0, \dots, c_n \in \mathbf{C}[T]$ premiers entre eux tels que pour tout i, $c_i/c_0 = k_i$.

On pose $f(X,T) = c_0(T)X^n + \cdots + c_n(T)$. Montrer que $f(X,T)$ est irréductible dans $\mathbf{C}[X,T]$.

e) Montrer qu'il existe $q \in \mathbf{C}[X,T]$ tel que

$$g(X)h(T) - g(T)h(X) = q(X,T)f(X,T).$$

En déduire que $m = n$ et donc que $K = \mathbf{C}(u)$ (*théorème de Lüroth*).

87) Soit A un anneau commutatif.

a) Soit P et $Q \in A[X]$ des polynômes. On suppose que les coefficients de P, resp. ceux de Q, engendrent l'idéal (1). Montrer qu'il en est de même des coefficients de PQ. (*Adapter la démonstration du lemme de Gauss : observer que l'hypothèse entraîne que modulo chaque idéal maximal de A, P et Q sont non nuls.*)

b) Montrer qu'il existe des polynômes $W_i \in \mathbf{Z}[P_0,\dots,P_n,Q_0,\dots,Q_n,U_0,\dots,U_n,V_0,\dots,V_n]$ (pour $0 \leqslant i \leqslant 2n$) tels que si $P = \sum p_i X^i$, $Q = \sum q_i X^i$ sont des polynômes de degrés au plus n, $1 = \sum p_i u_i$ et $1 = \sum q_i v_i$ des relations de Bézout pour les coefficients de P et de Q, alors, notant $PQ = \sum r_i X^i$, on a la relation de Bézout

$$1 = \sum_{i=0}^{2n} r_i W_i(p_0,\dots,p_n,q_0,\dots,q_n,u_0,\dots,u_n,v_0,\dots,v_n)$$

pour les coefficients de PQ. (Calculer les W_i pour $n = 1$ ne semble pas une mince affaire...)

c) Pour $P \in A[X]$, notons $\mathrm{ict}(P)$ l'idéal de A engendré par les coefficients de P. La première question entraîne que $\mathrm{ict}(PQ) = A$ si $\mathrm{ict}(P) = \mathrm{ict}(Q) = A$. Lorsque A est principal, $\mathrm{ict}(P)$ est l'idéal engendré par le contenu de P et l'on a donc $\mathrm{ict}(PQ) = \mathrm{ict}(P)\,\mathrm{ict}(Q)$ d'après le lemme de Gauss. Montrer cependant que $\mathrm{ict}(PQ) \neq \mathrm{ict}(P)\,\mathrm{ict}(Q)$ en général, par exemple lorsque $A = \mathbf{C}[U,V]$, $P = UX + V$ et $Q = VX + U$.

CHAPITRE 2

MODULES

Le modules sont aux anneaux ce que les espaces vectoriels sont aux corps. Ce chapitre d'introduction aux modules en donne la définition et les premières propriétés. On montre aussi comment construire des modules par passage au quotient ou par localisation. Le produit tensoriel sera introduit plus tard dans le cours.

§2.1. Premiers pas

DÉFINITION 2.1.1. — *Soit A un anneau. Un* A-module à droite *est un groupe abélien M muni d'une loi d'action*

$$M \times A \to M, \qquad (a, m) \mapsto ma$$

vérifiant les propriétés suivantes : pour tous $a, b \in A$ et tous $m, n \in M$, on a

- $m(a+b) = ma + mb$ *et* $(m+n)a = ma + na$ *(distributivité) ;*
- $m(ab) = (ma)b$ *(associativité) ;*
- $m1 = m$ *(élément neutre).*

Un A-module à gauche *est un groupe abélien M muni d'une application (multiplication externe, ou loi d'action)*

$$A \times M \to M, \qquad (a, m) \mapsto am$$

vérifiant les propriétés suivantes : pour tous $a, b \in A$ et tous $m, n \in M$, on a

- $(a+b)m = am + bm$ *et* $a(m+n) = am + an$ *(distributivité) ;*
- $(ab)m = a(bm)$ *(associativité) ;*
- $1m = m$ *(élément neutre).*

Exemples 2.1.2. — a) Soit A un anneau ; la multiplication $A \times A \to A$ munit le groupe abélien A de deux structures de modules, l'une à gauche et l'autre à droite. La première est notée A_s, la seconde A_d (pour senestre et dextre !). Soit I un idéal à gauche de A ; la multiplication de A, $A \times I \to I$, munit I d'une structure de A-module à gauche. De

même, si I est un idéal à droite de A, la multiplication $I \times A \to I$ le munit d'une structure de A-module à droite.

b) Si A est un anneau commutatif, un module à droite est aussi un module à gauche, pour la même loi d'action à l'échange des facteurs près.

c) Un groupe abélien possède une unique structure de $\mathbf{Z}$-module.

d) Lorsque A est un corps commutatif, la notion de A-module (à droite ou à gauche, cela n'a pas d'importance) coïncide avec la notion étudiée dans les premières années d'université. Cette terminologie est conservée lorsque A est un anneau à division ; on parle ainsi d'espace vectoriel à droite ou à gauche sur A.

e) Si $f : A \to B$ est un homomorphisme d'anneaux, la multiplication externe $B \times A \to B$ définie par $(b, a) \mapsto bf(a)$ munit B d'une structure de A-module à droite.

f) Plus généralement, si $f : A \to B$ est un homomorphisme d'anneaux et si M est un B-module à droite, la multiplication externe $M \times A \to M$ définie par $(m, a) \mapsto mf(a)$ munit M d'une structure de A-module à droite.

g) Soit A un anneau et soit M un A-module à gauche. Muni de la loi d'action $A^{\mathrm{o}} \times M \to M$, $(m, a) \mapsto am$, M est un A^{o}-module à droite. Cette correspondance permet de déduire d'un énoncé pour des modules à droite un énoncé analogue pour les modules à gauche.

h) Soit A et B des anneaux. Un (A, B)-bimodule est un groupe abélien M muni de d'une structure de A-module à gauche et d'une structure de B-module à droite telles que l'on ait $a(mb) = (am)b$ pour tout $a \in A$, tout $m \in M$ et tout $b \in B$. Cela revient à la donnée d'une structure de $A \times B^{\mathrm{o}}$-module à gauche, ou à la donnée d'une structure de $A^{\mathrm{o}} \times B$-module à droite.

Dans la suite, j'entendrai par A-module (sans précision) un A-module à droite et la plupart des propriétés ne seront démontrées que pour ceux-ci. L'explicitation et la démonstration de l'énoncé analogue pour les modules à gauche est laissé au lecteur consciencieux.

Remarque 2.1.3. — Soit A un anneau et soit M un A-module à gauche. Si $a \in A$, notons $\mu_a : M \to M$ l'application définie par $\mu_a(m) = am$. C'est un endomorphisme de M en tant que groupe abélien. De plus, l'application $a \mapsto \mu_a$ définit un homomorphisme d'anneaux $A \to \mathrm{End}(M)$. En effet, si a, $b \in A$ et $m \in M$, $\mu_{ab}(m) = (ab)m = a(bm) = \mu_a(bm) = \mu_a \circ \mu_b(m)$, d'où $\mu_{ab} = \mu_a \circ \mu_b$.

Inversement, soit M un groupe abélien et $\mu : A \to \mathrm{End}(M)$ un homomorphisme d'anneaux. Définissons une loi d'action $A \times M \to M$ par $(a, m) \mapsto \mu(a)(m)$. On constate que cela définit une structure de A-module à gauche sur M telle que la multiplication par un élément a de A soit $\mu(a)$.

Ainsi, M étant un groupe abélien, se donner une structure de A-module à gauche sur M équivaut à se donner un homomorphisme d'anneaux $A \to \mathrm{End}(M)$. Tout groupe abélien M est par conséquent muni d'une structure canonique de $\mathrm{End}(M)$-module à

gauche. De même, tout A-module M est muni d'une structure canonique de $\mathrm{End}_A(M)$-module à gauche.

Une structure de A-module à droite sur M équivaut à la donnée d'un homomorphisme d'anneaux $A \to \mathrm{End}(M)^{\mathrm{o}}$.

DÉFINITION 2.1.4. — *Soit A un anneau et soit M un A-module à droite. Un* sous-module *de M est une partie N de M vérifiant :*

- *N est un sous-groupe abélien de M ;*
- *pour tout $a \in A$ et tout $m \in N$, $ma \in N$.*

Il y a une définition analogue pour les modules à gauche.

Exemples 2.1.5. — a) Si M est un A-module, la partie de M réduite à 0 en est un sous-module. De même, M est un sous-module de lui-même.

b) Si A est un anneau, les idéaux à gauche de A sont les sous-A-modules de A_s, les idéaux à droite de A sont les sous-A-modules de A_d.

c) Si A est un anneau à division, les sous-modules d'un A-espace vectoriel en sont les sous-espaces vectoriels.

LEMME 2.1.6. — *Soit M un A-module à droite et soit N une partie de M. Pour montrer que N est un sous-module de M, il suffit de montrer les propriétés suivantes :*

- *$0 \in N$;*
- *si $a \in A$ et $m \in N$, $ma \in N$;*
- *si $m \in N$ et $n \in N$, $m+n \in N$.*

Démonstration. — En effet, la seconde propriété appliquée à $a = -1$ et $m \in N$ montre que $-m \in N$. Jointe aux deux autres propriétés, on constate que N est un sous-groupe abélien de M. La seconde propriété implique alors que c'en est un sous-module. □

DÉFINITION 2.1.7. — *Soit A un anneau et soit M et N deux A-modules. Un* homomorphisme *de M dans N est une application $f : M \to N$ telle que pour tous a et b dans A et tous m et n dans M, on a*

$$f(ma+nb) = f(m)a + f(n)b.$$

On note $\mathrm{Hom}_A(M,N)$ *l'ensemble des homomorphismes de M dans N.*

Un homomorphisme de M dans M est appelé endomorphisme *de M. On note* $\mathrm{End}_A(M)$ *l'ensemble des endomorphismes du A-module M.*

Les expressions « application A-linéaire » voire « application linéaire » sont synonymes d'« homomorphisme de A-modules ».

Soit A un anneau et soit M, N, P trois A-modules. Si $f : M \to N$ et $g : N \to P$ sont des homomorphismes, leur composé $g \circ f : M \to P$ est un homomorphisme de A-modules.

On dit qu'un homomorphisme de A-modules $f\colon M \to N$ est un homomorphisme est un isomorphisme s'il existe un homomorphisme $g\colon N \to M$ tel que $f \circ g = \mathrm{id}_N$ et $g \circ f = \mathrm{id}_M$.

PROPOSITION 2.1.8. — *Pour qu'un homomorphisme de A-modules soit un isomorphisme, il faut et il suffit qu'il soit bijectif.*

Démonstration. — Si $f : M \to N$ est un isomorphisme, de réciproque g, il est clair que g est la bijection réciproque de f.

Inversement, soit $f : M \to N$ un homomorphisme bijectif et soit g sa bijection réciproque. Alors, g est un homomorphisme. En effet, si n, $n' \in N$ et a, $a' \in A$, on a

$$f\big(g(n)a + g(n')a'\big) = f(g(n))a + f(g(n'))a' = na + n'a'$$

donc $g(n)a + g(n')a' = g(na + n'a')$, ce qui établit la linéarité de g. □

DÉFINITION 2.1.9. — *Soit $f : M \to N$ un homomorphisme de A-modules. On appelle* noyau *de f, noté* $\ker f$*, l'ensemble des $m \in M$ tels que $f(m) = 0$.*

PROPOSITION 2.1.10. — *Soit $f : M \to N$ un homomorphisme de A-modules.*

Si M' est un sous-module de M, $f(M')$ est un sous-module de N. Si N' est un sous-module de N, $f^{-1}(N')$ est un sous-module de M.

En particulier, le noyau $\ker f$ *et l'image* $\mathrm{im}\, f = f(M)$ *de f sont des sous-modules (de M et N respectivement).*

Démonstration. — Montrons que $f(M')$ est un sous-module de N. Comme $f(0_M) = 0_N$ et $0_M \in M'$, $0_N \in f(M')$. D'autre part, si n et $n' \in f(M')$, il existe m et $m' \in M'$ tels que $n = f(m)$ et $n' = f(m')$. Par suite,

$$n + n' = f(m) + f(m') = f(m + m') \in f(M').$$

Enfin, si $n = f(m)$ appartient à $f(M')$ et si $a \in A$, $na = f(m)a = f(ma)$ appartient à $f(M')$ puisque $ma \in M'$.

Montrons que $f^{-1}(N')$ est un sous-module de M. Comms $f(0_M) = 0_N \in N'$, $0_M \in f^{-1}(N')$. D'autre part, si m et $m' \in f^{-1}(N')$ et si a et $b \in A$, on a

$$f(ma + m'b) = f(m)a + f(m')b \in N'$$

puisque $f(m)$ et $f(m')$ appartiennent à N' et que N' est un sous-module de N. Donc $ma + m'b$ appartient à $f^{-1}(N')$. □

Exemple 2.1.11. — Soit A un anneau et soit M, N deux A-modules à droite. L'ensemble $\mathrm{Hom}(M,N)$ des homomorphismes de groupes abéliens de M dans N est un groupe abélien, la somme de deux homomorphismes f et g étant l'homomorphisme $f + g$ défini par $m \mapsto f(m) + g(m)$. Si f et g sont des homomorphismes de A-modules, alors $f + g$ en est un également, en vertu de la formule

$$(f + g)(ma) = f(ma) + g(ma) = f(m)a + g(m)a = (f(m)a + g(m)a) = (f + g)(m)a,$$

pour $a \in A$ et $m, n \in M$. De même, l'application nulle est un homomorphisme de A-modules, de même que $-f$, pour tout $f \in \mathrm{Hom}_A(M,N)$. Il en résulte que $\mathrm{Hom}_A(M,N)$ est un sous-groupe abélien de $\mathrm{Hom}(M,N)$.

Lorsque $M = N$, $\mathrm{End}_A(M)$ est en outre un anneau, la multiplication étant donnée par la composition des homomorphismes. C'est un sous-anneau de $\mathrm{End}(M)$.

Supposons que A soit commutatif. Soit $f \in \mathrm{Hom}_A(M,N)$ et soit $a \in A$. Alors, l'application af définie par $m \mapsto f(m)a$ est un homomorphisme de A-modules, car

$$(fa)(mb) = f(bm)a = f(m)ba = f(m)ab = (fa)(m)b,$$

pour tout $m \in M$ et tous $a, b \in A$. Le groupe abélien $\mathrm{Hom}_A(M,N)$ est ainsi muni d'une structure de A-module.

Si l'anneau A n'est pas commutatif, l'application $m \mapsto f(m)a$ n'est pas forcément A-linéaire ; on ne peut par suite pas toujours munir le groupe abélien $\mathrm{Hom}_A(M,N)$ d'une structure de A-module. Supposons cependant que N soit un (B,A)-bimodule. On peut alors munir $\mathrm{Hom}_A(M,N)$ d'une structure de B-module à gauche en définissant, si $f \in \mathrm{Hom}_A(M,N)$ et $b \in B$, l'application linéaire bf par $(bf)(m) = bf(m)$. (Il est clair que bf est un endomorphisme de groupes abéliens ; les égalités $bf(ma) = b(f(ma)) = b \cdot f(m) \cdot a = (bf(m))a$ montrent qu'il est A-linéaire.) On a $(bb')f = b(b'f)$.

De même, si M est un (B,A)-bimodule, on peut munir $\mathrm{Hom}_A(M,N)$ d'une structure de B-module à droite en définissant, pour $f \in \mathrm{Hom}_A(M,N)$, l'application fb par $(fb)(m) = f(bm)$. Si b, $b' \in B$ et $f \in \mathrm{Hom}_A(M,N)$, on a $(fbb')(m) = f(bb'm)$; d'autre part, $(fb)b'$ applique m sur $(fb)(b'm) = f(bb'm)$, d'où la relation $fbb' = (fb)b'$, d'où l'assertion.

DÉFINITION 2.1.12. — *Soit A un anneau et soit M un A-module à droite. Le dual de M, noté $M^\vee$, est le groupe abélien* $\mathrm{Hom}_A(M,A)$*, muni de la structure de A-module à gauche pour laquelle $(a\varphi)(m) = \varphi(m)a$. Ses éléments sont appelés* formes linéaires.

Exercices. — 1) Soit M un A-module. Montrer que $(-1)m = -m$.

2) Soit A un anneau et soit M un A-module à droite.

a) Montrer que l'ensemble $(0 : M)$ des $a \in A$ tels que $ma = 0$ pour tout $m \in M$ est un idéal bilatère de A (*annulateur de M*). On le note aussi $\mathrm{ann}(M)$.

b) Plus généralement, soit N un sous-A-module de M. Montrer que l'ensemble $(N : M)$ des $a \in A$ tels que $ma \in N$ pour tout $m \in M$ est un idéal bilatère de A.

3) Soit A et B deux anneaux et $f : A \longrightarrow B$ un homomorphisme d'anneaux.

a) Soit M un B-module à droite. Montrer que l'on définit un A-module à droite en munissant le groupe abélien M de la multiplication $(M, B) \to M$ définie par $(m, b) \mapsto mf(b)$. Ce A-module est noté f_*M.

b) Soit $u\colon M \to N$ un homomorphisme de B-modules à droite ; montrer que u définit un homomorphisme de A-modules de $f_*M \to f_*N$.

c) Montrer que l'application $\mathrm{Hom}_B(M,N) \to \mathrm{Hom}_A(f_*M, f_*N)$ ainsi définie est un homomorphisme injectif de groupes abéliens. Donner un exemple où il n'est pas surjectif.

d) Soit M un B-module à droite. Déterminer l'annulateur du module f_*M en fonction de celui de M.

4) Soit A et B des anneaux et $f : A \to B$ un homomorphisme d'anneaux. Le groupe additif de B est muni de la structure de A-module à droite déduite de f.

a) On suppose que l'image de f est contenue dans le centre de B (de sorte que B est une A-algèbre). Montrer que la multiplication de B est A-bilinéaire (c'est-à-dire que les applications $x \mapsto xb$ et $x \mapsto bx$, pour $b \in B$ fixé, sont A-linéaires).

b) Inversement, si la multiplication de B est A-bilinéaire, montrer que l'image de f est contenue dans le centre de B.

5) Soit M et N deux A-modules.

a) Soit $u \in \mathrm{End}_A M$. Montrer qu'il existe une unique structure de $A[X]$-module sur M telle que $X \cdot m = u(m)$ (et $1 \cdot m = m$) pour tout $m \in M$. On notera M_u le $A[X]$-module M muni de cette structure.

Montrer que cette application $u \mapsto M_u$ induit une bijection entre les structures de $A[X]$-module sur M et les endomorphismes $u \in \mathrm{End}\, M$.

b) Soit $u \in \mathrm{End}_A M$ et $v \in \mathrm{End}_A N$. Déterminer tous les homomorphismes de $A[X]$ modules de M_u dans N_v.

c) Si $M = N$, à quelle condition $M_u \simeq M_v$?

d) Comment pouvez-vous interpréter les résultats de l'exercice lorsque $A = k$ est un corps et $M = k^n$ est l'espace vectoriel standard de dimension n sur k ?

§2.2. Opérations sur les modules

PROPOSITION 2.2.1. — *Soit A un anneau, soit M un A-module à droite et soit $(N_s)_{s\in S}$ une famille de sous-modules de M. Alors, l'*intersection *$N = \bigcap_s N_s$ est un sous-module de M.*

Démonstration. — Comme $0 \in N_s$ pour tout s, $0 \in N$. Soit m et n deux éléments de N. Pour tout s, m et n appartiennent au sous-module N_s, donc $m+n$ aussi et $m+n$ appartient à leur intersection N. Enfin, soit $m \in N$ et $a \in A$. Pour tout s, $m \in N_s$, donc $ma \in N_s$ et finalement, $ma \in N$. Ainsi, N est un sous-A-module de M. □

PROPOSITION 2.2.2. — *Soit A un anneau, soit M un A-module à droite et soit X une partie de M. Il existe un plus-petit sous-A-module $\langle X\rangle$ de M contenant X : c'est l'intersection de la famille (non vide) des sous-modules de M qui contiennent X. C'est aussi l'ensemble des sommes $\sum_{x\in X} xa_x$ où (a_x) est une famille presque nulle d'éléments de A.*

On dit que $\langle X\rangle$ est le sous-module de M engendré par X.

Démonstration. — Il existe des sous-modules de M qui contiennent X, par exemple M lui-même. Par suite, l'intersection $\langle X\rangle$ de ces sous-modules est un sous-module de M et contient X. Par construction, $\langle X\rangle$ est contenu dans tout sous-module de M qui contient X. C'est ainsi le plus petit d'entre eux.

Si $(a_x)_x$ est une famille presque nulle d'éléments de A, $\sum_{x\in X} xa_x$ est une combinaison linéaire d'éléments de $\langle X\rangle$, donc appartient à $\langle X\rangle$. Ceci prouve que l'ensemble $\langle X\rangle'$ des telles combinaisons linéaires est contenu dans $\langle X\rangle$. Réciproquement, il suffit de montrer que cet ensemble est un sous-module de M. Comme il contient X, on aura l'autre inclusion. Tout d'abord, $0 = \sum_x x0$ appartient à $\langle X\rangle'$. Par ailleurs, si m et n sont deux éléments de $\langle X\rangle'$, il existe deux familles presque nulles $(a_x)_x$ et $(b_x)_x$ telles que $m = \sum_x xa_x$ et $n = \sum_x xb_x$. Alors, la famille $(a_x + b_x)_x$ est presque nulle et l'on a

$$m + n = \Big(\sum_x xa_x\Big) + \Big(\sum_x xb_x\Big) = \sum_x x(a_x + b_x)$$

donc $m + n$ appartient à $\langle X\rangle'$. Enfin, si $m \in \langle X\rangle'$ et $a \in A$, soit $(a_x)_x$ une famille presque nulle telle que $m = \sum_x xa_x$. On a alors $ma = \sum_x x(a_x a)$, donc $ma \in \langle X\rangle'$. □

DÉFINITION 2.2.3. — *Soit A un anneau, M un A-module à droite et soit $(M_s)_s$ une famille de sous-module de M. La* somme *des M_s, $\sum_s M_s$, est le sous-module de M engendré par la réunion $\bigcup_s M_s$ des M_s.*

C'est aussi l'ensemble des combinaisons linéaires $\sum_s m_s$ où $(m_s)_s$ est une famille presque nulle d'éléments de M telle que $m_s \in M_s$ pour tout s. En effet, ce dernier ensemble est un sous-module de M qui contient $\bigcup_s M_s$, et contenu dans tout sous-module de M qui contient les M_s.

DÉFINITION 2.2.4. — *Soit A un anneau et soit (M_s) une famille de A-modules. Le* produit *des M_s est l'ensemble $\prod_s M_s$ muni des lois :*

$$(m_s)_s + (n_s)_s = (m_s + n_s)_s, \qquad (m_s)_s a = (m_s a)_s$$

qui en font un A-module.

La somme directe *des M_s est le sous-module $\bigoplus_s M_s$ de $\prod M_s$ formé des éléments $(m_s)_s$ tels que pour tout s sauf pour un nombre fini, $m_s = 0$.*

Remarque 2.2.5. — Si tous les M_s sont égaux à un même module M, on a $\prod_s M_s = M^S$. Le sous-module $\bigoplus M_s$ est noté $M^{(S)}$.

LEMME 2.2.6. — *Pour tout t, définissons des applications*

$$i_t\colon M_t \to \bigoplus_s M_s, \qquad p_t\colon \prod_s M_s \to M_t$$

définis par $i_t(m) = (m_s)$ où $m_t = m$ et $m_s = 0$ si $s \neq t$ et $p_t((m_s)) = m_t$. Ce sont des homomorphismes de A-modules.

Démonstration. — Soit m, n dans M_t, a et b dans A. Alors,

$$i_t(ma+nb) = (0,\dots,0,ma+nb,0,\dots)$$

(dans le membre de droite, le $ma+nb$ est dans la composante indexée par t)

$$\begin{aligned} &= (0,\dots,0,m,0,\dots)a + (0,\dots,0,n,0,\dots,0)b \\ &= i_t(m)a + i_t(n)b. \end{aligned}$$

Par suite, i_t est un homomorphisme de A-modules. La démonstration que p_t est un homomorphisme est laissée en exercice. □

Produits et des sommes directes de modules satisfont une *propriété universelle* que nous énonçons maintenant.

THÉORÈME 2.2.7. — *Soit A un anneau et soit (M_s) une famille de A-modules à droite.*

a) Pour tout A-module M et toute famille (f_s) de morphismes $f_s\colon M \to M_s$, il existe un unique morphisme $f\colon M \to \prod_s M_s$ tel que pour tout s, $p_s \circ f = f_s$.

b) Pour tout A-module M et toute famille (f_s) de morphismes $f_s\colon M_s \to M$, il existe un unique morphisme $f\colon \bigoplus_s M_s \to M$ tel que pour tout s, $f \circ i_s = f_s$.

Démonstration. — a) Supposons que $f\colon M \to \prod_s M_s$ vérifie $p_s \circ f = f_s$. Alors, si $f(m) = (m_s)_s$, on a nécessairement

$$m_s = p_s((m_s)_s) = p_s(f(m)) = (p_s \circ f)(m) = f_s(m),$$

ce qui montre que f, s'il existe, est unique. Réciproquement, définissons $f(m)$ comme la famille $(f_s(m))_s$. Il faut montrer que l'application ainsi définie $f\colon M \to \prod_s M_s$ est un homomorphisme de A-modules. Or, pour tous a et b dans A et tous m et n dans M, on a

$$\begin{aligned} f(ma+nb) &= \big(f_s(ma+nb)\big)_s = \big(f_s(m)a + f_s(n)b\big)_s \\ &= \big(f_s(m)\big)_s a + \big(f_s(n)\big)_s b = f(m)a + f(n)b, \end{aligned}$$

ce qui prouve que f est un homomorphisme de A-modules.

b) Supposons que $f\colon \bigoplus_s M_s \to M$ vérifie $f \circ i_s = f_s$. Alors, l'image par f d'un élément $(0,\dots,0,m,0,\dots) = i_s(m)$ (où $m \in M_s$ est dans la composante indexée par s) est nécessairement égale à $f_s(m)$. Un élément de $\bigoplus M_s$ est une famille $(m_s)_s$ avec $m_s \in M_s$, tous

les m_s étant nuls, sauf un nombre fini. Par suite, un tel élément est égal à $\sum_s i_s(m_s)$ (la somme est en fait finie) et son image par f est égale à

$$f(\sum_s i_s(m_s)) = \sum_s (f \circ i_s)(m_s) = \sum_s f_s(m_s),$$

ce qui montre l'unicité. Réciproquement, l'application $f : \bigoplus M_s \to M$ définie par

$$f((m_s)_s) = \sum_s f_s(m_s) \qquad \text{(somme finie)}$$

est un homomorphisme de A-modules qui vérifie $f \circ i_s = f_s$ pour tout s. En effet, si a et b sont dans A et $(m_s)_s$, $(n_s)_s$ sont deux éléments de $\bigoplus_s M_s$, on a

$$\begin{aligned} f((m_s)_s a + (n_s)_s b) &= f((m_s a + n_s b)_s) \\ &= \sum_s f_s(m_s a + n_s b) = \sum_s \big(f_s(m_s)a + f_s(n_s)b\big) \\ &= \big(\sum_s f_s(m_s)\big)a + \big(\sum_s f_s(n_s)\big)b \\ &= f((m_s)_s)a + f((n_s)_s)b. \end{aligned}$$

□

Remarque 2.2.8. — Ce théorème peut se reformuler ainsi : pour tout A-module à droite M, les applications canoniques

$$\mathrm{Hom}_A(\bigoplus_s M_s, M) \to \prod_s \mathrm{Hom}_A(M_s, M), \qquad f \mapsto (f \circ i_s)_s$$

et

$$\mathrm{Hom}_A(M, \prod_s M_s) \to \prod_s \mathrm{Hom}_A(M, M_s), \qquad f \mapsto (p_s \circ f)_s$$

sont des isomorphismes.

Soit M un A-module et soit (M_s) une famille de sous-modules de M. On dispose alors d'un homomorphisme de A-modules $\bigoplus_s M_s \to \sum_s M_s$, définie par $(m_s) \mapsto \sum m_s$, pour toute famille presque nulle (m_s). Cet homomorphisme est surjectif. On dit que les M_s sont en somme directe si c'est un isomorphisme.

Dans le cas d'une famille (M_1, M_2) à 2 éléments, le noyau de cet homorphisme est l'ensemble des couples $(m, -m)$, où $m \in M_1 \cap M_2$. Par suite, M_1 et M_2 sont en somme directe si et seulement si $M_1 \cap M_2 = 0$. La situation est un peu plus compliquée pour des familles à plus de 2 éléments ; c'est déjà le cas pour les espaces vectoriels, voir pour mémoire l'exercice 10.

Soit M un A-module. Soit N un sous-module de M ; un *supplémentaire* de N est un sous-module P de M tel que N et P soient en somme directe et que l'on ait $M = N + P$. Contrairement à ce qui se passe pour les espaces vectoriels, tout sous-module n'a pas forcément de supplémentaire.

DÉFINITION 2.2.9. — *Soit A un anneau, M un A-module à droite et I un idéal à droite de A. On définit le sous-module MI de M comme l'ensemble des combinaisons linéaires $\sum m_i a_i$ où pour tout i, $a_i \in I$ et $m_i \in M$.*

Exercices. — 6) a) La réunion de deux sous-modules n'est en général pas un sous-module. Donner un exemple (on pourra se placer dans le cadre des espaces vectoriels).

b) Si $(M_n)_{n\in\mathbf{N}}$ est une famille de sous-modules d'un A-module M telle que $M_n \subset M_p$ si $n \leqslant p$, montrer que $\bigcup_n M_n$ est un sous-A-module de M.

c) Soit k un corps, soit V un k-espace vectoriel et soit $(W_i)_{1\leqslant i\leqslant n}$ une famille de sous-espaces vectoriels de V telle que $W = \bigcup_i W_i$ soit un sous-espace vectoriel. Si k est infini ou, plus généralement, si k a au moins n éléments, montrer qu'il existe un entier i tel que $W = W_i$.

d) Soit V_1, V_2 et V_3 les ensembles des $(x, y) \in \mathbf{Z}^2$ tels que x soit pair, resp. $x+y$ soit pair, resp. y soit pair. Montrer que ce sont des sous-modules de $\mathbf{Z}^2$, distincts de $\mathbf{Z}^2$, et que $\mathbf{Z}^2 = V_1 \cup V_2 \cup V_3$.

7) Soit M un A-module et $M_1, \ldots, M_r$ des sous-A-modules de M dont M est la somme directe. Soit $I_1 = (0 : M_1), \ldots, I_r = (0 : M_r)$ leurs annulateurs. On suppose que les I_α sont deux à deux comaximaux.

On pose : $I = \bigcap_{\alpha=1}^r I_\alpha$ et $J_\alpha = \bigcap_{\beta\neq\alpha} I_\beta$.

a) Montrer que pour tout α, I_α et J_α sont des idéaux bilatères comaximaux de A.

Pour tout α, soit N_α le sous-module de M engendré par les M_β, pour $\beta \neq \alpha$. Si J est un idéal de A, on notera $(0 : J)$ le sous-A-module de M égal à $\{m \in M ;\ ma = 0 \text{ pour tout } a \in J\}$.

Montrer les formules suivantes :

b) $J_\alpha = (0 : N_\alpha)$ et $N_\alpha = (0 : J_\alpha)$;

c) $N_\alpha = MI_\alpha$ et $MJ_\alpha = M_\alpha = \bigcap_{\beta\neq\alpha} N_\beta$.

8) Soit M un A-module et $m \in M$ un élément dont l'annulateur est réduit à (0). Montrer l'équivalence des propriétés suivantes :

a) mA possède un supplémentaire dans M ;

b) il existe une forme linéaire f sur M telle que $f(m) = 1$.

Montrer qu'alors $M = mA \oplus \ker f$.

9) Soit $f : M \to N$ un homomorphisme de A-modules.

a) Montrer qu'il existe $g : N \to M$ tel que $g \circ f = \mathrm{id}_M$ si et seulement si f est injectif et $\mathrm{im}(f)$ admet un supplémentaire dans N.

b) Montrer qu'il existe $g : N \to M$ tel que $f \circ g = \mathrm{id}_N$ si et seulement si f est surjectif et $\ker(f)$ admet un supplémentaire dans M.

10) Soit A un anneau, soit M un A-module et soit $(M_i)_{i\in I}$ une famille de sous-modules de M dont la somme est égale à M.

a) Pour que les M_i soient en somme directe, il faut et il suffit que Pour tout $i \in I$, l'intersection des sous-modules M_i et $\sum_{j\neq i} M_j$ soit réduite à 0.

b) Donner un exemple de module M, de famille (M_1, M_2, M_3) de sous-modules dont la somme est égale à M et telle que $M_i \cap M_j = 0$ pour tout couple (i, j) avec $i \neq j$, mais qui ne soit pas en somme directe.

§2.3. Quotients de modules

Soit A un anneau et soit M un A-module. On s'intéresse aux relations d'équivalence sur M qui sont compatibles avec la structure de module, c'est-à-dire que pour tous m, m', n et n' dans M,

$$\text{si } m \sim m' \text{ et } n \sim n', \text{ alors } am + bn \sim am' + bn'.$$

Soit N l'ensemble des $m \in M$ tels que $m \sim 0$. Comme une relation d'équivalence est réflexive, $0 \in N$. Si m et n appartiennent à N, on a $m \sim 0$, $n \sim 0$ et donc pour tous a et b dans A, $am + bn \sim (a0 + b0) = 0$, c'est-à-dire $am + bn \in N$. Cela prouve que N est un sous-module de M. De plus, si m et n sont deux éléments de M tels que $m \sim n$, on a $m + (-n) \sim n + (-n)$, d'où $m - n \in N$.

Réciproquement, soit N un sous-A-module de M et soit $\sim$ la relation d'équivalence sur M définie par $m \sim n$ si et seulement si $m - n \in N$. Notons M/N l'ensemble des classes d'équivalence et $\mathrm{cl}_N \colon M \to M/N$ l'application canonique.[(1)] Les calculs qui précèdent montrent le théorème suivant.

THÉORÈME 2.3.1. — *Soit A un anneau, M un A-module et N un sous-module de M. La relation $\sim$ sur M définie par $m \sim n$ si et seulement si $m - n \in N$ est une relation d'équivalence sur M compatible avec la structure de module. L'ensemble quotient M/N possède une unique structure de A-module telle que l'application* $\mathrm{cl} \colon M \to M/N$ *est un homomorphisme de A-modules.*

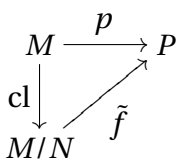
L'homomorphisme cl *est surjectif et de noyau N.*

On démontre maintenant un *théorème de factorisation*, propriété universelle des modules quotients.

THÉORÈME 2.3.2. — *Soit A un anneau, M un A-module et N un sous-module de M. Pour tout A-module P et tout homomorphisme $f \colon M \to P$ tel que $N \subset \ker f$, il existe un unique homomorphisme de modules $\tilde{f} \colon M/N \to P$ tel que $f = \tilde{f} \circ \mathrm{cl}$.*

De plus, $\mathrm{im}\, \tilde{f} = \mathrm{im}\, f$ *et* $\ker \tilde{f} = \mathrm{cl}(\ker f)$. *En particulier, $\tilde{f}$ est injectif si et seulement si* $\ker f = N$.

On peut représenter l'égalité du théorème en disant que le diagramme



(1) S'il n'y a pas de confusion possible, on pourra noter simplement cl cette application.

est commutatif. L'intérêt de ce théorème est qu'il permet de factoriser un homomorphisme de A-modules $f : M \to N$ en la composition

$$M \xrightarrow{\mathrm{cl}} M/\ker f \xrightarrow{\tilde{f}} \operatorname{im} f \hookrightarrow N$$

d'un homomorphisme surjectif, d'un isomorphisme et d'un homomorphisme injectif.

Démonstration. — Nécessairement, on doit avoir $\tilde{f}(\mathrm{cl}(m)) = f(m)$ pour tout m dans M. Comme tout élément de M/N est de la forme $\mathrm{cl}(m)$ pour un certain $m \in M$, cela montre qu'il existe au plus un homomorphisme de A-modules $\tilde{f} : M/N \to P$ tel que $\tilde{f} \circ \mathrm{cl} = f$.

Montrons l'existence de $\tilde{f}$. Soit $x \in M/N$ et soit deux éléments m et m' de M tels que $x = \mathrm{cl}(m) = \mathrm{cl}(m')$. Alors, $m - m' \in N$ et donc, puisque $N \subset \ker f$, $f(m - m') = 0$. On a alors $f(m) = f(m')$ et l'on peut définir $\tilde{f}$ en posant $\tilde{f}(x) = f(m)$ — cela ne dépend en effet pas de l'élément $m \in M$ choisi parmi ceux qui vérifient $x = \mathrm{cl}(m)$. Il reste à montrer que $\tilde{f}$ est un homomorphisme de A-modules. Or, soit x et $y \in M/N$, soit a et b dans A. Choisissons $m \in M$ tel que $x = \mathrm{cl}(m)$ et $n \in M$ tel que $y = \mathrm{cl}(n)$. Alors, $ax + by = a\,\mathrm{cl}(m) + b\,\mathrm{cl}(n) = \mathrm{cl}(am + bn)$ et

$$\tilde{f}(ax + by) = \tilde{f}(\mathrm{cl}(am + bn)) = f(am + bn) = af(m) + bf(n) = a\tilde{f}(x) + b\tilde{f}(y).$$

Ainsi, $\tilde{f}$ est un homomorphisme de A-modules.

On a évidemment $\operatorname{im} f \subset \operatorname{im} \tilde{f}$. D'autre part, si p appartient à $\operatorname{im} \tilde{f}$, choisissons $x \in M/N$ tel que $p = \tilde{f}(x)$ puis $m \in M$ tel que $x = \mathrm{cl}(m)$. Alors, $p = \tilde{f}(\mathrm{cl}(m)) = f(m)$ appartient à $\operatorname{im} f$, d'où l'autre inclusion et finalement l'égalité $\operatorname{im} f = \operatorname{im} \tilde{f}$.

Enfin, si $\tilde{f}(x) = 0$, on peut écrire $x = \mathrm{cl}(m)$ avec $m \in M$ et la relation $\tilde{f} \circ \mathrm{cl} = f$ implique $f(m) = 0$, d'où $x \in \mathrm{cl}(\ker f)$. Dans l'autre sens, si $x = \mathrm{cl}(m)$ avec $m \in \ker f$, on a $\tilde{f}(x) = \tilde{f}(\mathrm{cl}(m)) = f(m) = 0$, donc $x \in \ker \tilde{f}$. Ainsi, $\ker \tilde{f} = \mathrm{cl}(\ker f)$. □

La proposition suivante décrit les sous-modules d'un module quotient tel que M/N.

PROPOSITION 2.3.3. — *Soit A un anneau, M un A-module, N un sous-module de M. L'application* cl^{-1} *:*

$$\begin{array}{ccc} \textit{sous-modules de } M/N & \to & \textit{sous-modules de } M \textit{ contenant } N \\ \mathscr{P} & \mapsto & \mathrm{cl}^{-1}(\mathscr{P}) \end{array}$$

est une bijection.

Ainsi, pour tout sous-module P de M qui contient N, il existe un unique sous-module $\mathscr{P}$ de M/N tel que $P = \mathrm{cl}^{-1}(\mathscr{P})$. De plus, on $\mathscr{P} = \mathrm{cl}(P)$. *Le sous-module* $\mathrm{cl}(P)$ *de M/N sera noté P/N.* Cette notation est cohérente. En effet, la restriction de cl à P est un homomorphisme $\mathrm{cl}|P : P \to M/N$ de noyau $P \cap N = N$ et d'image $\mathrm{cl}(P)$. D'après le théorème de factorisation, $\mathrm{cl}|_P$ induit un isomorphisme $P/N \to \mathrm{cl}(P)$.

Démonstration. — La démonstration est une conséquence immédiate des deux formules suivantes : si P est un sous-module de M,

$$\boxed{\mathrm{cl}^{-1}(\mathrm{cl}(P)) = P + N}$$

et si $\mathscr{P}$ est un sous-module de M/N,

$$\boxed{\mathrm{cl}(\mathrm{cl}^{-1}(\mathscr{P})) = \mathscr{P}.}$$

En effet, si $P \subset N$, $P + N = P$ et ces formules montrent que l'application cl^{-1} comme dans l'énoncé admet cl comme bijection réciproque.

Montrons la première formule. Si $m \in \mathrm{cl}^{-1}(\mathrm{cl}(P))$, on a $\mathrm{cl}(m) \in \mathrm{cl}(P)$. Il existe donc $p \in P$ tel que $\mathrm{cl}(m) = \mathrm{cl}(p)$ et par suite, $\mathrm{cl}(m - p) = 0$. Cela signifie que $n = m - p \in N$ et $m = p + n$ appartient à $P + N$. Réciproquement, si $m = p + n$ appartient à $P + N$, $\mathrm{cl}(m) = \mathrm{cl}(p + n) = \mathrm{cl}(p)$ appartient à $\mathrm{cl}(P)$, donc $m \in \mathrm{cl}^{-1}(\mathrm{cl}(P))$.

Montrons la seconde formule. Par définition, on a $\mathrm{cl}(\mathrm{cl}^{-1}(\mathscr{P})) \subset \mathscr{P}$. Réciproquement, si $x \in \mathscr{P}$, soit $m \in M$ tel que $x = \mathrm{cl}(m)$. Alors, $\mathrm{cl}(m) \in \mathscr{P}$, autrement dit, $m \in \mathrm{cl}^{-1}(\mathscr{P})$ et donc $x = \mathrm{cl}(m) \in \mathrm{cl}(\mathrm{cl}^{-1}(\mathscr{P}))$. □

Enfin, nous pouvons calculer le « quotient d'un quotient ».

PROPOSITION 2.3.4. — *Soit A un anneau, N, P, M trois A-modules tels que $N \subset P \subset M$. Alors, on a un isomorphisme canonique*

$$(M/N)/(P/N) \simeq (M/P)$$

tel que pour tout $m \in M$, $\mathrm{cl}_{P/N}(\mathrm{cl}_N(m)) \mapsto \mathrm{cl}_P(m)$.

Démonstration. — Considérons l'homomorphisme composé

$$\varphi \colon M \to (M/N) \to (M/N)/(P/N), \qquad m \mapsto \mathrm{cl}_{P/N}(\mathrm{cl}_N(m)).$$

Il est surjectif, comme composé de deux homomorphismes surjectif. Un élément m est dans son noyau si et seulement si $\mathrm{cl}_N(m) \in \ker \mathrm{cl}_{P/N} = P/N = \mathrm{cl}_N(P)$, c'est-à-dire $m \in P$ puisque P contient N. Ainsi, $\ker\varphi = P$ et le théorème de factorisation 2.3.2 affirme l'existence d'un unique homomorphisme bijectif $\tilde{\varphi} \colon M/P \to (M/N)/(P/N)$ tel que $\tilde{\varphi}(\mathrm{cl}_P(m)) = \mathrm{cl}_{P/N}(\mathrm{cl}_N(m))$. C'est l'isomorphisme cherché. □

Exercices. — 11) Soit A un anneau intègre et M un A-module. On dit que $x \in M$ est de torsion si $(0 : x) \neq 0$. On note $T(M)$ l'ensemble des éléments de torsion de M. Si $T(M) = 0$ on dit que M est sans torsion.

a) Montrer que l'ensemble des éléments de torsion de M est un sous-module de M. Donner un contre-exemple lorsque l'hypothèse que A est un anneau intègre n'est pas vérifiée.

b) Montrer que $M/T(M)$ est sans torsion.

c) Montrer que si $f : M \to N$ est un morphisme de A-modules alors $f(T(M)) \subset T(N)$. Donner un exemple où l'inclusion est stricte.

d) Soit $g \colon N \to P$ un second morphisme de A-modules tel que $\ker g = \mathrm{im}\, f$. Montrer que $\ker g \cap T(N) = f(T(M))$.

12) Soit A un anneau, M un A-module et N un sous-A-module de M.

a) Montrer que si M est de type fini, M/N l'est aussi.

b) Montrer que si N et M/N sont de type fini alors M est de type fini.

13) Soit A un anneau, soit I un idéal bilatère de A et soit M un A-module à droite.

a) Montrer qu'il existe une unique structure de A/I-module à droite sur le A-module M/MI de sorte que l'on ait $\mathrm{cl}_{MI}(m)\,\mathrm{cl}_I(a) = \mathrm{cl}_{MI}(ma)$, pour tout $m \in M$ et tout $a \in A$.

b) Si M est un A-module libre, montrer que M/MI est un A/I-module libre.

14) Soit A un anneau, soit M un A-module et soit N un sous-module de M.

a) Montrer que les conditions suivantes sont équivalentes : 1) N possède un supplémentaire dans M ; 2) N est le noyau d'un projecteur de M ; 3) N est l'image d'un projecteur de M.

b) Soit p_0 et p deux projecteurs de M d'image N, soit u l'application $p - p_0$. Montrer que l'image de u est contenue dans N et que son noyau contient N ; en déduire, par passage au quotient, une application linéaire $\bar{u}\colon M/N \to N$.

c) Soit p_0 un projecteur de M ; montrer que l'application $p \mapsto \bar{u}$ est une bijection de l'ensemble des projecteurs de M d'image N sur $\mathrm{Hom}_A(M/N, N)$.

15) Soit A un anneau, soit M un A-module à droite et soit N un sous-module de A.

a) Si M/N est un A-module libre, montrer que N possède un supplémentaire dans M.

b) Retrouver ainsi le fait que tout sous-espace vectoriel d'un espace vectoriel possède un supplémentaire.

16) Soit A un anneau et T une matrice $n \times m$ à coefficients dans A. Cette matrice représente un homomorphisme de modules $u : A^m \longrightarrow A^n$. Posons $M = \mathrm{coker}\, u = A^n/\mathrm{im}(u)$.

a) Montrer que $(0 : M) = (\mathrm{im}(u) : A^n)$.

b) Montrer que si $m \geqslant n$ alors les mineurs maximaux de T (c'est à dire les déterminants des sous matrices $n \times n$ de T) appartiennent à $(0 : M)$. (*Traiter tout d'abord le cas $m = n$.*)

17) Soit A un anneau et $u : A^n \to A^n$ un morphisme de matrice M_u dans la base canonique de A^n. Posons $M = \mathrm{coker}\, u = A^n/\mathrm{im}(u)$ et soit $u^* : A^n \to A^n$ dont la matrice M_{u^*} est la matrice transposée des cofacteurs de M_u. Enfin pour $k \in \{1, \ldots, n\}$ soit J_k l'idéal engendré par les mineurs $k \times k$ de M_u (c'est-à-dire les déterminants des sous-matrices $k \times k$ de M_u). Remarquer que $J_n = (\det(M_u))$ et que J_{n-1} est engendré par les coefficients de M_{u^*}.

a) Soit $a \in (0 : M)$ et $\mu_a : A^n \to A^n$, $x \longmapsto ax$; montrer qu'il existe un morphisme $v : A^n \to A^n$ tel que $\mu_a = u \circ v$, et que $\det(M_u) M_v = a M_{u^*}$.

b) Montrer que $(0 : M) \subset (J_n : J_{n-1})$.

On suppose désormais que $\det(M_u)$ n'est pas diviseur de zéro.

c) Montrer que u^* est injectif.

d) Soit $a \in (J_n : J_{n-1})$; montrer qu'il existe $w : A^n \to A^n$ tel que $au^* = \det(M_u) w$. Montrer alors que $u \circ w = \mu_a$.

e) Montrer que $(0 : M) = (J_n : J_{n-1})$.

§2.4. Générateurs, bases ; modules libres, modules de type fini

DÉFINITION 2.4.1. — *Soit A un anneau et soit M un A-module à droite.*

On dit qu'une famille $(m_i)_{i \in I}$ d'éléments de M est :

– génératrice *si le sous-module de M engendré par les m_i est égal à M ;*

– libre *si pour toute famille presque nulle $(a_i)_{i\in I}$ d'éléments de A, la relation $\sum_{i\in I} m_i a_i = 0$ implique que $a_i = 0$ pour tout $i \in I$;*

– liée *si elle n'est pas libre ;*

– *une* base *de M si pour tout élément m de M, il existe une unique famille presque nulle $(a_i)_{i\in I}$ dans A telle que $m = \sum m_i a_i$.*

Une sous-famille d'une famille libre est libre ; une famille contenant une sous-famille génératrice est génératrice. Lorsque l'anneau n'est pas nul, une famille libre est constituée d'éléments distincts deux à deux (sous peine de voir surgir la combinaison linéaire $x - y = 0$ si $x = y$). Par suite, seules les familles $(m_i)_{i\in I}$ telles que l'application $i \mapsto m_i$ soit *injective* sont intéressantes en pratique. Cela justifie notamment que l'on définisse, par abus de langage, les notions de *partie génératrice*, *partie libre* et *base* comme des parties S de M telle que la famille $(s)_{s\in S}$ soit respectivement génératrice, libre, une base.

PROPOSITION 2.4.2. — *Soit A un anneau, M un A-module à droite et soit S une partie de M. Soit φ_S l'homomorphisme canonique*

$$A_d^{(S)} \to M, \qquad (a_s)_{s\in S} \mapsto \sum_{s\in S} a a_s.$$

Alors,

– *φ_S est injectif si et seulement si S est libre ;*
– *φ_S est surjectif si et seulement si S est génératrice ;*
– *φ_S est un isomorphisme si et seulement si S est une base.*

Démonstration. — Le noyau de φ_S est l'ensemble des familles (a_s) telles que $\sum_s s a_s = 0$. Dire que S est libre équivaut donc à dire que $\ker\varphi_S = (0)$, c'est-à-dire que φ_S est injectif.

L'image de φ_S est l'ensemble des combinaisons linéaires d'éléments de S. Par suite, $\operatorname{im}\varphi_S = \langle S\rangle$ et φ_S est surjectif si et seulement si S est génératrice.

Enfin, la définition du fait que S est une base revient exactement à dire que φ_S est bijectif, donc un isomorphisme. □

COROLLAIRE 2.4.3. — *Une base est une partie libre et génératrice.*

DÉFINITION 2.4.4. — *Un module qui possède une base est dit* libre. *Un module qui possède une partie génératrice finie est dit* de type fini.

PROPOSITION 2.4.5. — *Soit M un A-module, soit N un sous-module de M.*

a) *Si M est de type fini, M/N est de type fini.*
b) *Si N et M/N sont de type fini, alors M est de type fini.*
c) *Si N et M/N sont des A-modules libres, alors M est un A-module libre.*

Par contre, il peut arriver que M soit de type fini mais que N ne le soit pas ; il peut arriver que M soit libre, mais que N, ou M/N, ne soit pas libre.

Plus précisément, nous allons démontrer les assertions suivantes :

a) *si M possède une famille génératrice de cardinal r, M/N aussi ;*

b) *si N et M/N possèdent des familles génératrices de cardinaux r et s, M possède une famille génératrice de cardinal $r+s$.*

c) *Si N et M/N ont des bases de cardinaux r et s, M possède une base de cardinal $r+s$.*

Démonstration. — *a*) Les images dans M/N d'une famille génératrice de M engendrent M/N, car l'homomorphisme canonique $M \to M/N$ est surjectif. Par suite, M/N est de type fini si M l'est.

b) Soit $(n_1,\dots,n_r)$ une famille génératrice de N et soit $(m_1,\dots,m_s)$ une famille finie d'éléments de M telle que $(\mathrm{cl}(m_1),\dots,\mathrm{cl}(m_s))$ engendre M/N. Montrons que la famille $(m_1,\dots,m_s,n_1,\dots,n_r)$ engendre M.

Soit $m \in M$. Par hypothèse, $\mathrm{cl}(m)$ est combinaison linéaire de $\mathrm{cl}(m_1),\dots,\mathrm{cl}(m_s)$. Il existe donc des éléments $a_i \in A$ tels que $\mathrm{cl}(m) = \sum_{i=1}^{s} \mathrm{cl}(m_i)a_i$, ce qui entraîne que $n = m - \sum_{i=1}^{s} m_i a_i$ appartient à N. Il existe alors des éléments $b_j \in A$ tels que $n = \sum_{j=1}^{r} n_j b_j$. Alors, $m = \sum_{i=1}^{s} m_i a_i + \sum_{j=1}^{r} n_j b_j$ est bien combinaison linéaire des m_i et des n_j.

c) Supposons en outre que $(n_1,\dots,n_r)$ soit une base de N et que $(\mathrm{cl}(m_1),\dots,\mathrm{cl}(m_s))$ soit une base de M/N et montrons que $(m_1,\dots,m_s,n_1,\dots,n_r)$ est une base de M. On a déjà démontré que cette famille engendre M, il reste à prouver qu'elle est libre. Soit donc $0 = \sum_{i=1}^{s} m_i a_i + \sum_{j=1}^{r} n_j b_j$ une relation de dépendance linéaire entre ces éléments. Son image dans M/N est une relation de dépendance linéaire $0 = \sum_{i=1}^{s} \mathrm{cl}(m_i)a_i$ entre les $\mathrm{cl}(m_i)$ qui forment une famille libre. On a donc $a_i = 0$ pour tout i. Par suite, $0 = \sum_{j=1}^{r} n_j b_j$; comme la famille $(n_1,\dots,n_r)$ est libre, $b_j = 0$ pour tout j. La relation de dépendance linéaire considérée était donc triviale, ce qu'il fallait démontrer. □

COROLLAIRE 2.4.6. — *Soit M un A-module (à droite) et soit $M_1,\dots,M_n$ des sous-modules de M qui sont de type fini. Leur somme $\sum_{i=1}^{n} M_i$ est un A-module de type fini.*

En particulier, la somme directe d'une famille finie de modules de type fini est de type fini.

Démonstration. — Par récurrence, il suffit de traiter le cas de deux modules. La seconde projection $\mathrm{pr}_2 : M_1 \oplus M_2 \to M_2$ est une application linéaire surjective, son noyau est isomorphe à M_1. Comme M_1 et M_2 sont de type fini, $M_1 \oplus M_2$ est de type fini. L'homomorphisme canonique de $M_1 \oplus M_2$ dans M déduit des injections de M_1 et M_2 dans M a pour image $M_1 + M_2$. Par suite, $M_1 + M_2$ est de type fini. □

Remarque 2.4.7. — Soit M un A-module de type fini qui est libre. Alors, toute partie génératrice de M possède une sous-famille finie.

Soit en effet $(m_1,\dots,m_n)$ une famille génératrice de M et $(e_i)_{i\in I}$ une famille génératrice arbitraire de M. Pour $j\in\{1,\dots,n\}$, on peut écrire $m_j=\sum_{i\in I}^n e_i a_{ij}$, où $(a_{ij})_i$ est une famille d'éléments de A tous nuls, sauf pour un nombre fini d'entre eux. L'ensemble I_0 des éléments de I tels que $a_{ij}\neq 0$ pour un j au moins est donc réunion de n ensembles finis, donc est fini. Par construction, chacun des m_j est combinaison linéaire d'éléments de la sous-famille $(e_i)_{i\in I_0}$, si bien que cette famille engendre M.

Si la famille $(e_i)_{i\in I}$ est une base, aucune de ses sous-familles strictes n'engendre M, donc $I=I_0$. Nous avons démontré qu'une base d'un module de type fini est finie. On parlera de module libre de type fini.

Lorsque l'anneau A est commutatif, ou que A est un anneau à division, nous verrons au paragraphe suivant que le cardinal d'une base d'un module libre de type fini est indépendant du choix de cette base.

Soit M un A-module libre et soit $(e_i)_{i\in I}$ une base de M. L'application $A^{(I)}\to M$ donnée par $(a_i)\mapsto\sum e i a_i$ est un isomorphisme de A-modules, si bien que M hérite de la *propriété universelle* des modules somme directe. Ainsi, si N est un A-module, se donner une application linéaire u de M dans N équivaut à se donner les images $u(e_i)$ des vecteurs de base. L'application u est alors donnée par $u(\sum e_i a_i)=\sum u(e_i)a_i$.

En particulier, pour tout i, il existe une unique forme linéaire φ_i sur M qui applique e_i sur 1 et les autres vecteurs de base sur 0. Si $m=\sum_{i\in I} e_i a_i$ est un élément de M, on a $\varphi_i(m)=a_i$.

La famille $(\varphi_i)_{i\in I}$ est une base du module dual $M^\vee$. En effet, si φ est une forme linéaire sur M et si $m=\sum_i e_i a_i$ est un élément de M, on a $\varphi(m)=\sum_i\varphi(e_i)a_i$, donc $\varphi(m)=\sum_i\varphi(e_i)\varphi_i(m)$, ce qui démontre que $\varphi=\sum\varphi(e_i)\varphi_i$; la famille (φ_i) est donc génératrice. Inversement, si $\varphi=\sum a_i\varphi_i=0$, on a $0=\varphi(e_i)=a_i$, si bien que la famille (φ_i) est libre. On l'appelle la *base duale* de la base $(e_i)_{i\in I}$.

Un autre intérêt des modules libres est de permettre du calcul matriciel. Soit $\Phi=(a_{i,j})\in M_{m,n}(A)$ une matrice à m lignes et n colonnes à coefficients dans A. On lui associe une application $\varphi\colon A^n\to A^m$ par la formule $\varphi(x_1,\dots,x_n)=(\sum_{j=1}^n a_{i,j}x_j)_{1\leqslant i\leqslant m}$. C'est un homomorphisme de groupes abéliens. En outre, pour tout $a\in A$, on a

$$\varphi((x_1,\dots,x_n)a)=\varphi(x_1,\dots,x_n)a,$$

si bien que φ est un homomorphisme de A-modules à droite. Inversement, tout homomorphisme φ de A-modules à droite est de cette forme : soit e_j l'élément de A^n dont la coordonnée j est égale à 1 et les autres sont nulles ; posons $\varphi(e_j)=(a_{1,j},\dots,a_{m,j})$. Si $x=(x_1,\dots,x_n)\in A^n$, on a $x=\sum_{j=1}^n e_j x_j$, donc

$$\varphi(x)=\sum_{j=1}^n\varphi(e_j)x_j=(\sum_{j=1}^n a_{i,j}x_j).$$

Par suite, φ est donné par la matrice $(a_{i,j})$.

Si $\Phi' = (b_{j,k}) \in M_{n,p}$ est une matrice à n lignes et p colonnes, la matrice $\Phi'' = \Phi\Phi'$ possède m lignes et p colonnes ; son coefficient $c_{i,k}$ d'indice (i,k) est donné par la formule

$$c_{i,k} = \sum_{j=1}^{n} a_{i,j} b_{j,k}.$$

L'homomorphisme $\varphi'' \colon A^p \to A^m$ qui lui est associé vérifie

$$\varphi''(x_1,\dots,x_p) = (\sum_k c_{i,k}x_k)_{1\leqslant i\leqslant m} = (\sum_{j,k} a_{i,j}b_{j,k}x_k)_i = (\sum_j a_{i,j}y_j)_i,$$

où $(y_1,\dots,y_n) = \varphi'(x_1,\dots,x_p)$. On a donc

$$\varphi''(x_1,\dots,x_p) = \varphi(y_1,\dots,y_n) = \varphi(\varphi'(x_1,\dots,x_p)),$$

si bien que $\varphi'' = \varphi \circ \varphi'$.

Cela démontre en particulier que l'application $M_n(A) \to \mathrm{End}(A_d^n)$ qui à une matrice carrée associe l'endomorphisme correspondant de A_d^n est un homomorphisme d'anneaux. Voilà pourquoi nous avons privilégié les modules à droite !

Exercices. — 18) Soit A un anneau et M un A-module. Si $m \in M$, à quelle condition sur $\mathrm{ann}(m)$ la famille $\{m\}$ est-elle libre ?

19) Soit A un anneau commutatif intègre et K son corps des fractions. On suppose $K \neq A$. Montrer que K n'est pas libre comme A-module.

20) Donner des exemples :

a) de modules non-libres ;

b) d'une famille libre à n éléments dans A^n qui ne soit pas une base ;

c) d'une partie génératrice minimale qui ne soit pas une base ;

d) de sous-module n'ayant pas de supplémentaire ;

e) de module libre ayant un sous-module qui ne l'est pas ;

21) [*Extensions de modules libres*] Soit L et M deux A-modules, $f : L \to M$ un homomorphisme d'anneaux.

a) On suppose que $\ker f$ et $\mathrm{im}\, f$ sont de type fini. Montrer que L est de type fini.

b) On suppose que $\ker f \simeq A^p$ et $\mathrm{im}\, f \simeq A^q$. Montrer que $L \simeq A^{p+q}$.

22) [*Bidual*] Soit M un A-module. On note $M^\vee = \mathrm{Hom}_A(M,A)$ son dual et $M^{\vee\vee} = \mathrm{Hom}_A(M^\vee, A)$ son bidual, c'est-à-dire le dual de son dual.

a) Soit $m \in M$. Montrer que l'application

$$\lambda_m : M^\vee \to A, \qquad \varphi \mapsto \varphi(m)$$

est A-linéaire. En déduire un homomorphisme de A-modules $\lambda : M \to M^{\vee\vee}$ donné par $m \mapsto \lambda_m$.

b) Dans cette question et la suivante, on suppose que $M = A^n$, $n \geqslant 1$. Soit $(e_1,\dots,e_n)$ la base canonique de A^n, c'est-à-dire $e_i = (0,\dots,0,1,0,\dots)$, le 1 étant en position i. Soit φ_i l'application linéaire $A^n \to A$ définie par $(a_1,\dots,a_n) \mapsto a_i$. Montrer que $(\varphi_1,\dots,\varphi_n)$ est une base de $M^\vee$.

c) Toujours lorsque $M = A^n$, montrer que λ est un isomorphisme.

Un tel module M pour lequel l'homomorphisme canonique $M \to M^{\vee\vee}$ est un isomorphisme est dit *réflexif*.

d) Donner un exemple de module pour lequel λ n'est pas injectif ; pas surjectif.

23) Soit M un A-module. Soit $f \in \mathrm{End}_A(M)$; on définit sa transposée ${}^{\mathrm{t}}f$ par ${}^{\mathrm{t}}f(\varphi) = \varphi \circ f$, pour tout $\varphi \in M^\vee = \mathrm{Hom}_A(M, A)$.

a) Montrer que l'ensemble des polynômes P de $A[X]$ tels que $P(f) = 0$ est un idéal que l'on notera $I(f)$.

b) Montrer que $I(f) \subset I({}^{\mathrm{t}}f)$.

c) Montrer que si M est réflexif, $I(f) = I({}^{\mathrm{t}}f)$.

24) Montrer qu'un idéal non nul I d'un anneau A est un sous-module libre de A si et seulement si I est principal et engendré par un élément non diviseur de zéro de A.

25) Soit A un anneau, M un A-module de type fini et $\varphi : M \longrightarrow A^n$ un morphisme surjectif de A-modules.

a) Montrer que φ admet un inverse à droite.

b) Montrer que $M \simeq \ker\varphi \oplus \mathrm{im}\,\psi$.

c) Montrer que $\ker\varphi$ est de type fini.

26) Soit A un anneau, soit M un A-module qui est somme directe d'une famille de sous-modules $(M_i)_{i\in I}$ indexée par un ensemble infini I. Soit S une famille génératrice de M.

a) Pour $x \in S$, écrivons $x = \sum_{i\in I} x_i$ et soit $I(x)$ l'ensemble des $i \in I$ tels que $x_i \neq 0$. C'est une partie finie de I. Montrer que la réunion, pour $x \in S$, des parties $I(x)$ est égale à I.

b) Montrer que S est infinie.

c*) Montrer que $\mathrm{card}(S) = \mathrm{card}(I)$.

d) Si M est un A-module libre engendré par une partie finie, montrer que toute base de M est finie.

§2.5. Espaces vectoriels

PROPOSITION 2.5.1. — *Soit K un anneau à division et soit M un K-espace vectoriel à droite. Soit $\mathscr{L} \subset \mathscr{G}$ des parties de M ; on suppose que $\mathscr{L}$ est libre et $\mathscr{G}$ génératrice.*

Soit B une partie de M telle que $\mathscr{L} \subset B \subset \mathscr{G}$. Les assertions suivantes sont équivalentes : (i) B est une base ; (ii) B est maximale parmi les parties libres ; (iii) B est minimale parmi les parties génératrices.

Démonstration. — Supposons que B soit une base de M. Alors, B est libre. De plus, si $m \in \mathscr{G} \setminus B$, il existe une famille presque nulle $(a_b)_{b\in B}$ d'éléments de K telle que $m = \sum ba_b$; la relation de dépendance linéaire $m - \sum ba_b = 0$ montre que la partie $B \cup \{m\}$ n'est pas libre. La partie B est donc libre et maximale.

Elle est génératrice ; montrons qu'elle est minimale. Soit sinon une partie génératrice B' de M telle que $\mathscr{L} \subset B' \subset B$, mais $B' \neq B$. Soit β un élément de $B \setminus B'$. Puisque B' est génératrice, il existe des éléments a_b, pour $b \in B'$, de K tels que $\beta = \sum_{b'\in B} ba_b$.

Posons $a_\beta = -1$ et $a_b = 0$ si b est un élément de $B \setminus B'$ distinct de β. La relation de dépendance linéaire $\sum ba_b = 0$ n'est pas triviale ; cela démontre que B est liée, contrairement à l'hypothèse.

Supposons maintenant que B soit une partie libre maximale. Montrons que B est génératrice. Soit m un élément de $\mathscr{G}$. Par hypothèse, la partie $B \cup \{m\}$ n'est pas libre ; il existe donc des éléments $(a_b)_{b\in B}$ et $a \in K$, presque tous nuls, mais pas tous, tels que $\sum ba_b + ma = 0$. Si $a = 0$, cette relation de dépendance linéaire ne relie que les éléments de B, contrairement à l'hypothèse que B est libre. Donc $a \neq 0$ et $m = -\sum_{b\in B} ba_b a^{-1}$ appartient au sous-espace vectoriel V de M engendré par B. Comme $\mathscr{G}$ est génératrice, $V = M$, ce qui montre que B est une partie génératrice de M. C'est donc une base.

Il reste à montrer qu'une partie génératrice minimale est une base. Si une telle partie B n'était pas libre, il existerait une relation de dépendance linéaire non triviale $\sum ba_b = 0$; soit $\beta \in B$ tel que $a_\beta \neq 0$. On a alors $\beta = -\sum_{b\neq\beta} ba_b a_\beta^{-1}$. Par suite, β appartient au sous-espace vectoriel engendré par les éléments de $B \setminus \{\beta\}$, partie qui est par suite génératrice, contrairement à l'hypothèse que B est minimale. □

Un des résultats fondamentaux de la théorie des espaces vectoriels est le théorème suivant, vraisemblablement bien connu lorsque K est commutatif !

THÉORÈME 2.5.2. — *Soit K un anneau à division et soit M un K-espace vectoriel à droite.*

a) M possède une base.

b) Plus précisément, si L est une partie libre de M et G une partie génératrice de M telles que $L \subset G$, il existe une base B de M telle que $L \subset B \subset G$.

c) Toutes les bases de M sont équipotentes.

Le cardinal commun des bases de M est appelé *dimension* de M ; on le note $\dim_K M$.

Démonstration. — L'assertion *a*) découle de *b*), appliquée à la partie libre $L = \varnothing$ et la partie génératrice $G = M$.

Démontrons donc *b*). Soit $\mathscr{L}$ l'ensemble des parties libres de G qui contiennent L, ordonné par l'inclusion. Cet ensemble n'est pas vide (car L est un élément de $\mathscr{L}$). Soit (L_i) une famille totalement ordonnée de parties libres de G et soit L la réunion des L_i. C'est une partie libre de M. Soit en effet une relation de dépendance linéaire $\sum_{m\in L} ma_m = 0$ entre les éléments de L. Soit J l'ensemble des éléments $m \in L$ tels que $a_m \neq 0$; c'est un ensemble fini. Par récurrence, il existe alors un indice i tel que $J \subset L_i$. Alors, $\sum_{m\in J} ma_m = 0$ est une relation de dépendance linéaire entre les éléments de la partie libre L_i ; comme $a_m = 0$ pour tout $m \in J$, cela entraîne $J = \varnothing$; autrement dit, $a_m = 0$ pour tout $m \in L$ et la partie L est libre. Par suite, $\mathscr{L}$ est inductif.

D'après le théorème de Zorn, il possède un élément maximal B. Un tel élément est une base de M en vertu de la proposition précédente.

c) Il résulte du lemme 2.5.3 ci-dessous que si M est engendré par n éléments, toute famille de $n+1$ éléments de M est liée. Par suite, si M possède une base de cardinal n, le cardinal de toute base est $\leqslant n$. Cela entraîne l'assertion dans le cas où M possède une famille génératrice finie.

Si M possède une libre infinie, ce même lemme entraîne que toute famille génératrice de M est infinie. La démonstration de l'équipotence des bases dans ce cas repose sur l'axiome du choix. Plus précisément, si $(u_i)_{i\in I}$ et $(v_j)_{j\in J}$ sont deux bases de M, il existe d'après le lemme 2.5.4 une injection de I dans J, ainsi qu'une injection de J dans I. Il résulte alors du théorème de Cantor-Bernstein que I et J sont équipotents. □

LEMME 2.5.3. — *Soit K un anneau à division et soit M un K-espace vectoriel à droite. Soit $(m_1,\dots,m_n)$ une famille génératrice de M et $(v_1,\dots,v_p)$ une famille libre dans M. On a l'inégalité $p\leqslant n$.*

Démonstration. — Démontrons ce résultat par récurrence sur n. Si $n=0$, M est engendré par une famille vide, donc $M=0$ et la seule famille libre dans M est la famille vide. Supposons le résultat vrai pour tout K-espace vectoriel engendré par $n-1$ éléments.

Il existe des éléments $a_{ij}\in K$ tels que $v_j=\sum m_i a_{ij}$. Si $a_{nj}=0$ pour tout j, les vecteurs v_j appartiennent au sous-module N engendré par $(m_1,\dots,m_{n-1})$. On a donc $p\leqslant n-1$, d'où $p\leqslant n$. Sinon, il existe un indice j tel que $a_{1j}\neq 0$. Quitte à permuter les indices j, on peut supposer que $j=1$.

Pour $1<j\leqslant p$, posons $w_j=v_j-v_p a_{11}^{-1}a_{1j}$ (a_{11} est inversible, car K est un anneau à division). Un calcul immédiat montre que les w_j appartiennent au sous-module N de M engendré par $v_2,\dots,v_n$. Par ailleurs, la famille $(w_2,\dots,w_p)$ est libre : donnons-nous une relation de dépendance linéaire $\sum w_j\lambda_j=0$. On obtient $-v_1(\sum a_{11}^{-1}a_{1j}\lambda_j)+\sum v_j\lambda_j=0$, relation de dépendance linéaire non triviale s'il existe j tel que $\lambda_j\neq 0$. Par récurrence, $p-1\leqslant n-1$, d'où $p\leqslant n$. □

Le résultat reste vrai en dimension infinie, sous la forme suivante.

LEMME 2.5.4. — *Soit K un anneau à division, soit M un K-espace vectoriel. Soit $(m_i)_{i\in I}$ une famille génératrice de M et soit $(v_j)_{j\in J}$ une famille libre de M ; il existe alors une injection de J dans I.*

Démonstration. — Soit Φ l'ensemble des couples (J',φ), où J' est une partie de J et φ une application de J' dans I tels que la famille $(w_j^{\varphi})_{j\in J}$ définie par $w_j^{\varphi}=m_{\varphi(j)}$ pour $j\in J'$ et $w_j^{\varphi}=v_j$ pour $j\in J\setminus J'$ soit libre. Le couple $(\varnothing,\varnothing)$ est un élément de Φ. On munit Φ de l'ordre pour lequel $(J'_1,\varphi_1)\prec(J'_2,\varphi_2)$ si $J'_1\subset J'_2$ et $\varphi_2|_{J'_1}=\varphi_1$. Il est facile de voir que Φ est inductif : si $(J'_\alpha,\varphi_\alpha)$ est une famille totalement ordonnée d'éléments de Φ, soit J' la réunion des J'_α et soit φ l'application de J' dans I qui coïncide avec φ_α sur J'_α. Elle est bien définie. D'après le théorème de Zorn (théorème A.2.1), Φ possède un élément

maximal (J', φ). Montrons que $J' = J$. Dans le cas contraire, soit k un élément de $J \setminus J'$. D'après le lemme d'échange appliqué à la famille (w_j^{φ}), il existe un élément $i \in I$ tel que la famille (w_j) définie par $w_j = w_j^{\varphi}$ si $j \in J'$, $w_k = u_i$, et $w_j = v_j$ sinon soit libre. Posons $J'' = J' \cup \{k\}$ et soit φ' l'application de J'' dans I telle que $\varphi'(k) = i$ et dont la restriction à J' est égale à φ. Les famille (w'_j) et $(w_j^{\varphi'})$ coïncident, donc (J'', φ') est un élément de Φ tel que $(J', \varphi) \prec (J'', \varphi')$, mais différent, ce qui contredit l'hypothèse que (J', φ) est maximal.

Comme la famille $(v_{\varphi(j)})_{j \in J}$ est libre, l'application φ est injective : c'est une injection de J dans I, cqfd. □

LEMME 2.5.5 (Lemme d'échange). — *Soit K un anneau à division, soit M un K-espace vectoriel. Soit $(u_i)_{i \in I}$ une partie génératrice de M et soit $(v_j)_{j \in J}$ une partie libre de M. Pour tout $k \in J$, il existe un élément $i \in I$ tel que la famille $(v'_j)_{j \in J}$ définie par $v'_k = u_i$ et $v'_j = v_j$ si $j \neq k$ soit libre.*

En d'autre termes, étant données une partie libre et une partie génératrice d'un espace vectoriel, on peut remplacer tout élément de la partie libre par un élément de la partie génératrice sans altérer son caractère libre.

Démonstration. — Posons $J' = J \setminus \{k\}$. Dire que l'élément $i \in I$ ne convient pas signifie exactement que u_i appartient au sous-espace vectoriel M' engendré par la famille $(v_j)_{j \in J'}$. Si le lemme est faux, tous les u_i appartiennent à M', d'où $M' = M$, puisque la famille $(u_i)_{i \in I}$ est génératrice. Mais alors v_k appartient aussi à M', d'où l'existence d'une relation de dépendance linéaire $v_k = \sum_{j \in J'} v_j \lambda_j$, ce qui contredit l'hypothèse que la famille $(v_j)_{j \in J}$ est libre. □

COROLLAIRE 2.5.6. — *Soit A un anneau commutatif et soit M un A-module. Si M est libre, toutes les bases de M ont même cardinal.*

Démonstration. — Soit $\mathfrak{m}$ un idéal maximal de A ; l'anneau quotient $K = A/\mathfrak{m}$ est donc un corps. soit $\mathfrak{m}M$ le sous-module de M engendré par les produits am pour $a \in \mathfrak{m}$ et $m \in M$. Posons $\bar{M} = M/\mathfrak{m}M$. C'est un A-module annulé par $\mathfrak{m}$ car si $a \in \mathfrak{m}$ et $m \in M$, $a\,\mathrm{cl}(m) = \mathrm{cl}(am) = 0$. On le considère donc comme un $A/\mathfrak{m}$-module, c'est-à-dire comme un K-espace vectoriel.

Soit $(e_i)_{i \in I}$ une base de M. Montrons que $(\mathrm{cl}(e_i))$ est une base de $\bar{M}$. Cette famille engendre $\bar{M}$ comme A-module, donc comme $A/\mathfrak{m}$-module, car les e_i engendrent M. Il reste à montrer qu'elle est libre. Soit (a_i) une famille presque nulle d'éléments de A telle que $\sum \mathrm{cl}(e_i)\,\mathrm{cl}(a_i) = 0$; autrement dit, $\sum e_i a_i$ appartient à $\mathfrak{m}M$. Ce module est engendré par les produits $e_i a$, pour $a \in \mathfrak{m}$ et $i \in I$; il existe donc une famille (b_i) d'éléments de $\mathfrak{m}$ telle que $\sum e_i a_i = \sum e_i b_i$. Comme la famille (e_i) est libre, $a_i = b_i$ pour tout i. En particulier, $a_i \in \mathfrak{m}$, donc $\mathrm{cl}(a_i) = 0$ pour tout $i \in I$. La relation de dépendance linéaire considérée est donc triviale, ce qui démontre que la famille $(\mathrm{cl}(e_i))_{i \in I}$ est libre. C'est

une base du K-espace vectoriel $\bar{M}$. On a donc $\operatorname{card} I = \dim \bar{M}$, cardinal commun des bases de M. □

THÉORÈME 2.5.7. — *Soit K un anneau à division. Tout sous-espace vectoriel N d'un K-espace vectoriel M possède un supplémentaire P et l'on a*

$$\dim(N) + \dim(P) = \dim(M).$$

Démonstration. — Soit M un K-espace vectoriel et soit N un sous-espace vectoriel de M. Soit $\mathscr{B}_1$ une base de N. D'après le théorème 2.5.2, il existe une base $\mathscr{B}$ de M qui contient $\mathscr{B}$. La partie $\mathscr{B}_2 = \mathscr{B} \setminus \mathscr{B}_1$ de M est libre et engendre un sous-espace vectoriel P de M tel que $N + P = M$. Soit m un élément de $N \cap P$. On peut donc écrire m comme combinaison linéaire d'éléments de $\mathscr{B}_1$ et de $\mathscr{B}_2$. En soustrayant ces deux relations, on obtient une relation de dépendance linéaire entre les éléments de $\mathscr{B}$, non triviale si $m \neq 0$, alors que $\mathscr{B}$ est une partie libre. Donc $N \cap P = 0$ et P est un supplémentaire de N dans M.

La formule sur les dimensions résulte de ce que $\dim(N)$ est le cardinal de $\mathscr{B}_1$, $\dim(P)$ celui de $\mathscr{B}_2$, donc que $\dim(N) + \dim(P)$ est le cardinal de la réunion (disjointe) $\mathscr{B}_1 \cup \mathscr{B}_2 = \mathscr{B}$, ensemble dont le cardinal est $\dim(M)$. □

Je résiste à l'envie d'énoncer et démontrer tous les résultats classiques qui restent valables avec les mêmes démonstrations (formule de Grassmann, formule du rang, coïncidence en dimension finie des notions d'endomorphisme bijectif, injectif, surjectif, injectif à droite, à gauche).

Exercices. — 27) a) Soit M un sous-$\mathbf{Z}$-module de type fini de $\mathbf{Q}$. Montrer que M est libre de rang 0 ou 1. (*Montrer par récurrence qu'il existe $a \in \mathbf{Q}$ tel que $M = \mathbf{Z}a$.*) En particulier, le $\mathbf{Z}$-module $\mathbf{Q}$ n'est pas de type fini.

b) Quelles sont les parties libres maximales de $\mathbf{Q}$?

c) Le $\mathbf{Z}$-module $\mathbf{Q}$ possède-t-il des parties génératrices minimales ?

28) Soit K un corps, soit V un K-espace vectoriel de dimension infinie et soit A l'anneau des endomorphismes de V. Montrer que le A-module à droite A^2 est isomorphe à A_d.

29) Soit A un anneau et soit $\varphi\colon A^m \to A^n$ un homomorphisme de A-modules à droites libres. Soit Φ la matrice de φ.

Soit $f\colon A \to B$ un homomorphisme d'anneaux. Soit $f(\Phi)$ la matrice dont les composantes sont les images par f des composantes de Φ.

a) Montrer que $f(\Phi)$ est la matrice d'un homomorphisme $\varphi_0\colon B^m \to B^n$ de B-modules à droite.

b) Si φ est un isomorphisme, montrer qu'il en est de même de φ_0. (*Introduire la matrice Φ' de l'isomorphisme réciproque de φ, puis la matrice $f(\Phi')$.*)

c) En déduire que si A est un anneau possédant un homomorphisme dans un corps K, le A-module A^m n'est isomorphe au A-module A^n que si $m = n$. Autrement dit, les cardinaux

des d'un A-module libre de type fini sont égaux à un même entier (qu'on appelle le *rang* du module).

30) a) Soit K un anneau à division, soit V un K-espace vectoriel et soit W un sous-espace vectoriel de V. Montrer que W est l'intersection des noyaux des formes linéaires nulles sur W.

b) Donner un exemple d'anneau A et de A-module M non nul tel que toute forme linéaire sur M soit nulle.

c) Donner un exemple d'anneau intègre A, de A-module libre M, de sous-module N, tel que N ne soit pas l'intersection des noyaux des formes linéaires nulles sur N.

31) Soit K un anneau à division, soit V_1, V_2, V_3, V_4 des K-espaces vectoriels, soit $u\colon E_1 \to E_2$, $v\colon E_3 \to E_4$ et $w\colon E_1 \to E_4$ des applications linéaires.

a) Pour qu'il existe une application linéaire $f\colon E_2 \to E_4$ telle que $f \circ u = w$, il faut et il suffit que $\ker(u) \subset \ker(w)$.

b) Pour qu'il existe une application linéaire $g\colon E_1 \to E_3$ telle que $v \circ g = w$, il faut et il suffit que $\mathrm{im}(w) \subset \mathrm{im}(v)$.

c) Pour qu'il existe une application linéaire $h\colon E_2 \to E_3$ telle que $v \circ h \circ u = w$, il faut et il suffit que $\ker(u) \subset \ker(w)$ et $\mathrm{im}(w) \subset \mathrm{im}(v)$.

§2.6. Localisation des modules (cas d'un anneau commutatif)

Soit A un anneau commutatif et soit M un A-module. Soit S une partie multiplicative de A. Nous allons construire, par un calcul de fractions similaire à celui qui nous a permis de définir l'anneau localisé $S^{-1}A$, un $S^{-1}A$-module $S^{-1}M$ ainsi qu'un homomorphisme de A-modules $M \to S^{-1}M$.

Soit sur l'ensemble $M \times S$ la relation

$$(m,s) \sim (n,t) \quad \Leftrightarrow \quad \text{il existe } u \in S \text{ tel que } u(tm - sn) = 0.$$

On vérifie comme page 29 que c'est une relation d'équivalence, on note $S^{-1}M$ l'ensemble des classes d'équivalence et $m/s \in S^{-1}M$ la classe d'équivalence du couple $(m,s) \in M \times S$.

On définit sur $S^{-1}M$ deux lois : tout d'abord, si m, $n \in M$ et s, $t \in S$,

$$(m/s) + (n/t) = (tm + sn)/(st)$$

et, si $m \in M$, $a \in A$, s et $t \in S$,

$$(a/t)(m/s) = (am)/(ts).$$

THÉORÈME 2.6.1. — *Muni de ces lois, $S^{-1}M$ est un $S^{-1}A$-module. L'application $i\colon M \to S^{-1}M$ telle que $i(m) = (m/1)$ est un homomorphisme de A-modules, $S^{-1}M$ étant considéré comme un A-module grâce à l'homomorphisme canonique d'anneaux $A \to S^{-1}A$.*

La démonstration est laissée en *exercice*. Les calculs sont semblables à ceux fait lors de la localisation des anneaux.

Remarque 2.6.2. — Rappelons quelques exemples de parties multiplicatives. Tout d'abord, si $s \in A$, la partie $S = \{1; s; s^2; \ldots\}$ est multiplicative. La localisation est dans ce cas notée avec un s en indice : $M_s = S^{-1}M$ est un A_s-module. Si $\mathfrak{p}$ est un idéal premier de A, $S = A \setminus \mathfrak{p}$ est aussi une partie multiplicative. On note $A_\mathfrak{p}$ l'anneau localisé et $M_\mathfrak{p}$ le $A_\mathfrak{p}$-module obtenu par calcul de fractions à partir d'un A-module M.

PROPOSITION 2.6.3. — *Soit A un anneau, S une partie multiplicative de A. Soit $f : M \to N$ un homomorphisme de A-modules. Il existe alors un unique homomorphisme de $S^{-1}A$-modules $\tilde{f} : S^{-1}M \to S^{-1}N$ tel que pour tout $m \in M$ et tout $s \in S$, $\tilde{f}(m/s) = f(m)/s$.*

Autrement dit, le diagramme

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ {\scriptstyle i}\downarrow & & \downarrow{\scriptstyle i} \\ S^{-1}M & \xrightarrow{\tilde{f}} & S^{-1}N \end{array}$$

est commutatif.

Démonstration. — Il faut vérifier que cette définition a un sens. Si $m/s = n/t$, soit $u \in S$ tel que $u(tm - sn) = 0$. Alors,

$$\frac{f(m)}{s} = \frac{utf(m)}{uts} = \frac{f(utm)}{uts} = \frac{f(usn)}{uts} = \frac{f(n)}{t},$$

ce qui prouve que $\tilde{f}$ est bien définie. Alors, si m, $n \in M$, s, $t \in S$, on a

$$\begin{aligned} \tilde{f}\big(\frac{m}{s} + \frac{n}{t}\big) = \tilde{f}\big(\frac{tm+sn}{st}\big) &= \frac{f(tm+sn)}{st} \\ &= \frac{tf(m)}{st} + \frac{sf(n)}{st} = \frac{f(m)}{s} + \frac{f(n)}{t} = \tilde{f}(\frac{m}{s}) + \tilde{f}(\frac{n}{t}) \end{aligned}$$

et $\tilde{f}$ est donc additive. Enfin, si $m \in M$, $a \in A$, s et $t \in S$, on a

$$\tilde{f}\big(\frac{a}{t}\,\frac{m}{s}\big) = \tilde{f}\big(\frac{am}{st}\big) = \frac{f(am)}{st} = \frac{af(m)}{st} = \frac{a}{t}\,\frac{f(m)}{s} = \frac{a}{t}\tilde{f}\big(\frac{m}{s}\big)$$

et $\tilde{f}$ est A-linéaire. □

La localisation des modules donne lieu à une propriété universelle du même genre de celle établie pour les anneaux.

THÉORÈME 2.6.4. — *Soit A un anneau, S une partie multiplicative de A, $f : M \to N$ un homomorphisme de A-modules. On suppose que pour tout $s \in S$, l'homomorphisme $\mu_s : N \to N$, $n \mapsto sn$, est un isomorphisme. Alors, il existe un unique homomorphisme de A-modules $\varphi : S^{-1}M \to N$ tel que $\tilde{f}(m/1) = f(m)$ pour tout $m \in M$.*

Démonstration. — En fait, si $\tilde{f}\colon S^{-1}M \to S^{-1}N$ désigne l'homomorphisme fourni par la proposition précédente et $i\colon N \to S^{-1}N$ l'homomorphisme canonique, la propriété voulue pour φ équivaut à l'égalité $i\circ\varphi = \tilde{f}$. Comme i est dans ce cas un isomorphisme, on a $\varphi = i^{-1}\circ\tilde{f}$. □

La localisation se comporte très bien vis à vis des sous-modules ; c'est la deuxième occurence de l'*exactitude de la localisation.*

PROPOSITION 2.6.5. — *Soit A un anneau, S une partie multiplicative de A. Soit M un A-module et N un sous-module de M.*

Alors, l'homomorphisme canonique $S^{-1}N \to S^{-1}M$ provenant de l'injection $N \to M$ est injectif et définit un isomorphisme de $S^{-1}N$ sur un sous-module de $S^{-1}M$, noté encore $S^{-1}N$.

De plus, on a un isomorphisme canonique

$$S^{-1}M/S^{-1}N \simeq S^{-1}(M/N).$$

Démonstration. — Soit $n \in N$ et $s \in S$. L'image de $n/s \in S^{-1}N$ dans $S^{-1}M$ est égale à n/s mais où n est vu comme un élément de M. Elle est nulle si et seulement s'il existe $t \in S$ tel que $tn = 0$ dans M, mais aussi dans N! Par suite, cet homomorphisme est injectif. C'est ainsi un isomorphisme de $S^{-1}M$ sur son image dans $S^{-1}M$.

Considérons maintenant l'homomorphisme égal à la composition des homomorphismes canoniques

$$M \xrightarrow[m\mapsto m/1]{} S^{-1}M \xrightarrow{\mathrm{cl}} S^{-1}M/S^{-1}N.$$

Par construction, un élément n a pour image 0, d'où, par la propriété universelle des modules quotients, un unique homomorphisme $M/N \to S^{-1}M/S^{-1}N$ par lequel $\mathrm{cl}_N(m) \mapsto \mathrm{cl}_{S^{-1}N}(m/1)$. Comme S agit par automorphisme sur le $S^{-1}A$-module $S^{-1}M/S^{-1}N$, on en déduit un unique homomorphisme $\varphi\colon S^{-1}(M/N) \to S^{-1}M/S^{-1}N$ tel que $(\mathrm{cl}_N(m)/1) \mapsto \mathrm{cl}_{S^{-1}N}(m/1)$.

Montrons que φ est un isomorphisme. Il est surjectif car $\mathrm{cl}_N(m)/s$ a pour image $\mathrm{cl}_{S^{-1}N}(m/s)$. Il est injectif : si $\mathrm{cl}_N(m)/s$ a pour image 0, $m/s \in S^{-1}N$. Il existe ainsi $n \in N$ et $t \in S$ tels que $m/s = n/t$. Soit alors $u \in S$ tel que $u(tm - sn) = 0$. Il en résulte l'égalité

$$\frac{\mathrm{cl}_N(m)}{s} = \frac{\mathrm{cl}_N(utm)}{stu} = \frac{\mathrm{cl}_N(sun)}{stu)} = \frac{0}{stu} = 0,$$

d'où l'injectivité. □

PROPOSITION 2.6.6. — *Soit A un anneau, S une partie multiplicative de A et soit M un A-module. Notons $i\colon M \to S^{-1}M$ l'homomorphisme canonique de A-modules.*

Si $\mathcal{N}$ est un sous-$S^{-1}A$-module de $S^{-1}M$, alors $N = i^{-1}(\mathcal{N})$ est un sous-A-module de M tel que $\mathcal{N} = S^{-1}N$.

Démonstration. — Il est clair que $S^{-1}N \subset \mathscr{N}$: si $m \in N$, on a $m/1 \in \mathscr{N}$, donc pour tout $s \in S$, $m/s \in \mathscr{N}$.

Réciproquement, soit $x \in \mathscr{N}$. On peut écrire $x = m/s$ avec $m \in M$ et $s \in S$. Par suite, $sx = m/1$ appartient à N et $x = (sx)/s$ appartient à $S^{-1}N$. □

PROPOSITION 2.6.7. — *Soit A un anneau, S une partie multiplicative de A. Soit M un A-module et soit (N_i) une famille de sous-modules de M. Alors, on a une égalité de sous-modules de $S^{-1}M$:*

$$\sum_i S^{-1}N_i = S^{-1}\sum N_i.$$

Démonstration. — Notons $N = \sum N_i$. Pour tout i, $N_i \subset N$, d'où une inclusion $S^{-1}N_i \subset S^{-1}N$. Par suite, $\sum_i S^{-1}N_i \subset S^{-1}N$. Réciproquement, soit $n/s \in S^{-1}N$. On peut écrire $n = \sum_i n_i$, où pour tout i, $n_i \in N_i$, la somme étant presque nulle. Alors, $n/s = \sum_i (n_i/s)$ appartient à $\sum S^{-1}N_i$ et l'autre inclusion est démontrée. □

Exercices. — 32) Soit A un anneau et M un A-module. Soit I un idéal de A. On suppose que $M_{\mathfrak{m}} = 0$ pour tout idéal maximal $\mathfrak{m}$ contenant I. Montrer que $M = IM$.

33) Soit A un anneau commutatif, soit S une partie multiplicative de A.

a) Soit $(m_1, \ldots, m_n)$ une famille génératrice de M ; montrer que la famille $(m_1/1, \ldots, m_n/1)$ est génératrice dans le $S^{-1}A$-module $S^{-1}N$.

b) Soit $(m_1, \ldots, m_n)$ une partie libre de M ; si S ne contient pas de diviseur de zéro, montrer que la famille $(m_1/1, \ldots, m_n/1)$ dans $S^{-1}M$ est libre.

c) On suppose que A est intègre et que M est engendré par n éléments. Montrer que le cardinal d'une partie libre de M est inférieur ou égal à n. (*Prendre pour S l'ensemble des éléments non nuls de A.*)

§2.7. Longueur

DÉFINITION 2.7.1. — *Soit A un anneau. On dit qu'un A-module à droite est* simple *s'il n'est pas nul et si ses seuls sous-modules sont* 0 *et lui-même.*

Exemples 2.7.2. — a) Le module nul n'est pas simple.

b) Soit A un anneau et soit I un idéal à droite distinct de A. Pour que le A-module A/I soit simple, il faut et il suffit que les seuls idéaux à droite de A qui contiennent I soient I et A, autrement dit que I soit un idéal à droite maximal de A.

c) Soit M un A-module simple et soit m un élément non nul de M. L'ensemble mA des multiples de M est un sous-module non nul de M ; si M est simple, on a donc $mA = M$.

Supposons de plus que A soit un anneau commutatif. Alors, M est isomorphe au A-module A/I, où I est le noyau de l'homomorphisme de A dans M donné par $a \mapsto am$. En particulier, I est un idéal maximal de A. Notons que c'est l'annulateur de I.

d) Supposons que A soit un anneau à division ; un A-module à droite simple n'est autre qu'un A-espace vectoriel de dimension 1.

e) Soit A un anneau et I un idéal bilatère de A. Dans l'identification entre A-modules annulés par I et (A/I)-modules, sous-A-modules et sous-(A/I)-modules se correspondent. Par suite, un A-module annulé par I est simple si et seulement si il est simple en tant que (A/I)-module.

f) Soit M un A-module et soit N un sous-module de M, distinct de M. Les sous-modules de M/N sont en bijection avec les sous-modules de M contenant N. Par suite, M/N est un A-module simple si et seulement si N est un sous-module maximal de M, au sens où les seuls sous-modules de M contenant N sont N et M.

PROPOSITION 2.7.3 (Lemme de Schur). — *Soit A un anneau, soit $u\colon M \to N$ un homomorphisme non nul de A-modules. Si M est simple, u est injectif. Si N est simple, u est surjectif. Si M et N sont tous deux simples, u est un isomorphisme.*

En particulier, l'anneau des endomorphismes d'un A-module simple est un anneau à division.

Démonstration. — L'image de u est un sous-module non nul de N ; si N est simple, $\mathrm{im}(u) = N$ et u est surjectif. Le noyau de u est un sous-module de M, distinct de M ; si M est simple, $\ker(u) = 0$ et u est injectif. Si M et N sont tous deux simples, u est bijectif, donc un isomorphisme.

Soit M un A-module simple. Comme la bijection réciproque d'un endomorphisme bijectif de M est un homomorphisme, il résulte de ce qui précède que tout élément non nul de $\mathrm{End}_A(M)$ est inversible. Autrement dit, $\mathrm{End}_A(M)$ est un anneau à division. □

DÉFINITION 2.7.4. — *Soit A un anneau. La longueur d'un A-module M est la borne supérieure de l'ensemble des entiers n tels qu'il existe une suite $M_0 \subsetneq M_1 \cdots \subsetneq M_n$ strictement croissante de sous-A-modules de M. On la note $\ell_A(M)$ ou $\ell(M)$.*

Exemples 2.7.5. — a) Si M est un A-module simple, sa longueur est 1 puisque les seules suites strictement croissantes de sous-modules de M sont 0, M (suites de longueur 0) et $0 \subset M$ (de longueur 1).

b) Réciproquement, un A-module de longueur 1 est simple. Tout sous-module N de M qui est distinct de 0 et de M fournit en effet une suite $0 \subsetneq N \subsetneq M$ de longueur 2.

c) Si A est un anneau à division, l'expression « suite strictement croissante de sous-modules » se traduit en « suite de sous-espaces vectoriels emboîtés ». À chaque fois, la dimension augmente au moins de 1, et exactement de 1 si la suite est maximale. Par suite, la longueur d'un module sur un anneau à division est sa dimension en tant qu'espace vectoriel.

d) L'anneau $\mathbf{Z}$ n'est pas un $\mathbf{Z}$-module de longueur finie puisque l'on a de suites strictement croissantes arbitrairement longues d'idéaux de $\mathbf{Z}$:

$$2^n\mathbf{Z} \subset 2^{n-1}\mathbf{Z} \subset \cdots \subset \mathbf{Z}.$$

e) Soit I un idéal bilatère de A ; un A-module M annulé par I est aussi un A/I-module (l'homomorphisme $A \to \mathrm{End}(M)$ passe au quotient par A/I) et ses sous-A-modules sont ses sous-A/I-modules. Par suite, M a même longueur (éventuellement infinie) en tant que A-module qu'en tant que A/I-module.

f) Une suite $M_0 \subsetneq \cdots \subsetneq M_n$ est maximale si on ne peut l'étendre en une suite plus longue en insérant un module entre deux éléments de la suite, de sorte à obtenir une suite strictement croissante de sous-modules. Cela revient à dire que $M_0 = 0$, que M_i/M_{i-1} est un A-module simple pour $1 \leqslant i \leqslant n$ et que $M_n = M$. Si un A-module M est de longueur finie, on peut étendre toute suite en une suite de longueur maximale.

LEMME 2.7.6. — *Soit A un anneau, soit M un A-module à droite, soit $M' \subset M''$ et N des sous-modules de M tels que $M' \cap N = M'' \cap N$ et $M' + N = M'' + N$. Alors $M' = M''$.*

Démonstration. — Soit m un élément de M''. Comme $M'' \subset M'' + N$, il existe par hypothèse $m' \in M'$ et $n \in N$ tel que $m = m' + n$. Alors, $n = m - m' \in M'' \cap N$. Par suite, $n \in M' \cap N$ et $m = m' + n$ appartient à M'. Cela démontre que $M'' \subset M'$, d'où l'égalité. □

PROPOSITION 2.7.7. — *Soit A un anneau. Soit M un A-module et N un sous-module de N. Si deux des modules M, N et M/N sont de longueur finie, le troisième l'est aussi et on a l'égalité*

$$\ell_A(M) = \ell_A(N) + \ell_A(M/N).$$

Démonstration. — Si $N_0 \subsetneq N_1 \subsetneq \cdots \subsetneq N_a$ et $M_0/N \subsetneq \cdots \subset M_b/N$ sont des chaînes de sous-modules de N et M/N respectivement,

$$N_0 \subsetneq N_1 \subsetneq \cdots \subsetneq N_a \subsetneq M_1 \subsetneq \cdots \subsetneq M_b$$

est une chaîne de sous-modules de M de longueur $a + b$, d'où, avec la convention habituelle $\infty + n = +\infty$, l'inégalité $\ell(M) \geqslant \ell(N) + \ell(M/N)$. En particulier, si M est de longueur finie, N et M/N aussi.

Réciproquement, on suppose que N et M/N sont de longueur finie et on veut prouver que M est de longueur finie égale à $\ell(N) + \ell(M/N)$. Soit donc $M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_a$ une chaîne de sous-A-modules de M. Pour tout i, il résulte du lemme ci-dessus appliqué, avec $M' = M_i$, $M'' = M_{i+1}$, qu'au moins une des deux inclusions

$$M_i \cap N \subset M_{i+1} \cap N \quad \text{et} \quad M_i + N \subset M_{i+1} + N$$

est stricte. Par conséquent, on construit des suites strictement croissantes de sous-modules de N d'une part, et de M/N d'autre part, dont la somme des longueurs est au

moins égale à a. En particulier, $\ell(N)+\ell(M/N) \geqslant a$. Prenant ensuite la borne supérieure sur a, on a $\ell(N)+\ell(M/N) \geqslant \ell(M)$ et la proposition est démontrée. □

THÉORÈME 2.7.8 (Jordan–Hölder). — *Soit A un anneau et soit M un A-module à droite. Soit $M_0 \subsetneq M_1 \subsetneq \dots M_n$ et $N_0 \subsetneq N_1 \subsetneq \dots N_m$ des suites strictement croissantes de sous-A-modules de M, maximales. Alors, on a $m = n$ et il existe une permutation σ de $\{1,\dots,n\}$ telle que M_i/M_{i-1} soit isomorphe à $N_{\sigma(i)}/N_{\sigma(i)-1}$ pour tout entier $i \in \{1,\dots,n\}$.*

Autrement dit, si $M_0 \subsetneq M_1 \subsetneq \dots M_n$ est une suite maximale, strictement croissante, de sous-modules de M, M est de longueur finie, égale à n et les modules simples (M_i/M_{i-1}) (pour $1 \leqslant i \leqslant n$) de sous-modules ne dépend pas de la suite strictement croissante maximale choisie.

Démonstration. — Pour $1 \leqslant i \leqslant n$ et $0 \leqslant j \leqslant m$, posons $M_{i,j} = M_{i-1}+M_i \cap N_j$. C'est un sous-module de M, compris entre M_{i-1} et M_i ; on a $M_{i,0} = M_{i-1}$ et $M_{i,m} = M_i$. Il existe donc un plus petit entier $\sigma(i) \in \{1,\dots,m\}$ tel que $M_{i,\sigma(i)} = M_i$, autrement dit $M_{i-1}+M_i \cap N_{\sigma(i)} = M_i$ et $M_i \cap N_{\sigma(i)-1} \subset M_{i-1}$. C'est d'ailleurs l'unique entier j tel que $M_{i,j}/M_{i,j-1} \neq 0$.

De même, pour $1 \leqslant j \leqslant m$ et $0 \leqslant i \leqslant n$, posons $N_{j,i} = N_{j-1} + N_j \cap M_i$, Pour tout j, il existe un plus petit entier $\tau(j) \in \{1,\dots,n\}$ tel que $N_{j,i} = N_j$; c'est l'unique entier i tel que $N_{j,i}/N_{j,i-1} \neq 0$.

D'après le lemme de Zassenhaus ci-dessous, $M_{i,j}/M_{i,j-1}$ et $N_{j,i}/N_{j,i-1}$ sont des A-modules isomorphes. Par conséquent, $\tau(\sigma(i)) = i$ et $\sigma(\tau(j)) = j$ pour tout $i \in \{1,\dots,m\}$ et tout $j \in \{1,\dots,n\}$. Cela entraîne que $m = n$, σ est une permutation de $\{1,\dots,n\}$ et que les A-modules M_i/M_{i-1} et $N_{\sigma(i)}/N_{\sigma(i)-1}$ sont isomorphes, d'où le théorème. □

LEMME 2.7.9 (Zassenhaus). — *Soit M un A-module, soit $N' \subset N$ et $P' \subset P$ des sous-modules. On a des isomorphismes de A-modules*

$$\frac{N'+(N\cap P)}{N'+(N\cap P')} \simeq \frac{N\cap P}{(N'\cap P)+(N\cap P')} \simeq \frac{P'+(N\cap P)}{P'+(N'\cap P)}.$$

Démonstration. — Soit f l'application linéaire composée de l'injection j de $N\cap P$ dans $N'+(N\cap P)$ et de la surjection canonique π de ce dernier sous-module sur son quotient par $N'+(N\cap P')$. Montrons que f est surjective. Considérons en effet un élément x de $N'+(N\cap P)$; on peut écrire $x = n_1+n_2$, où $n_1 \in N'$ et $n_2 \in N\cap P$. On a $\pi(n_1) = 0$, donc $\pi(x) = \pi(n_2) = f(n_2)$ appartient à l'image de f. Soit maintenant $x \in N\cap P$ un élément du noyau de f. Par hypothèse, on peut écrire $x = n_1+n_2$, où $n_1 \in N'$ et $n_2 \in N\cap P'$. On a en particulier $n_2 \in P$, donc $n_1 = x-n_2 \in P$. Par suite, $n_1 \in N'\cap P$ et x appartient à la somme des sous-modules $N'\cap P$ et $N\cap P'$ de $N\cap P$. Inversement, ces sous-modules sont contenus dans le noyau de f. On donc $\ker f = (N'\cap P)+(N\cap P')$. Par passage au quotient, f définit ainsi un isomorphisme du second des trois modules du lemme sur

le premier. La symétrie des formules montre que le second et le troisième module du lemme sont isomorphes, cqfd. □

Remarque 2.7.10. — a) Voyons comment la théorie de la longueur permet de retrouver les résultats concernant la dimension des espaces vectoriels. Soit K un anneau à division. Soit M un K-espace vectoriel simple. Soit x un élément non nul de M ; comme xK est un sous-module non nul de M, on a $xK = M$. Par suite, x est une base de M. Les K-modules simples sont les espaces vectoriels non nuls engendrés par un seul élément.

Soit M un K-espace vectoriel. Supposons que M soit engendré par une famille finie $(x_1, \dots, x_n)$. Supposons que cette famille soit minimale ; c'est donc une base de M. Posons alors $M_i = \mathrm{vect}(x_1, \dots, x_i)$. On a ainsi défini une suite croissante $M_0 \subset M_1 \subset \cdots \subset M_n$ de sous-K-espaces vectoriels de M. L'égalité $M_i = M_{i-1}$ signifie exactement que $x_i \in M_{i-1}$; comme la famille $(x_1, \dots, x_n)$ est minimale, cette suite est strictement croissante. De plus, pour tout i, M_i/M_{i-1} est un espace vectoriel non nul et engendré par un élément (la classe de x_i) ; c'est donc un K-module simple. Du théorème de Jordan-Hölder découlent alors deux résultats :

– $\ell_K(M) = n$;
– toute famille génératrice minimale possède exactement n éléments.

Deux bases de M ont ainsi même cardinal.

b) Soit encore K un anneau à division et soit M un K-espace vectoriel à droite de dimension finie. Soit $E = (e_1, \dots, e_n)$ et $F = (f_1, \dots, f_n)$ des bases de M. Posons $M_i = \mathrm{vect}(e_1, \dots, e_i)$ et $N_i = \mathrm{vect}(f_1, \dots, f_i)$, pour $0 \leqslant i \leqslant n$. La démonstration du théorème de Jordan-Hölder fournit une (unique) permutation σ de $\{1, \dots, n\}$ telle que $M_{i-1} + M_i \cap N_{\sigma(i)-1} = M_{i-1}$ et $M_{i-1} + M_i \cap N_{\sigma(i)} = M_i$, pour tout $i \in \{1, \dots, n\}$. Pour tout i, soit x_i un vecteur appartenant à $M_i \cap N_{\sigma(i)}$ mais pas à M_{i-1}. On a $\mathrm{vect}(x_1, \dots, x_i) = M_i$ pour tout i ; par suite, $X = (x_1, \dots, x_n)$ est une base de M et il existe une matrice B_1 triangulaire supérieure telle que $X = EB_1$. Posons $\tau = \sigma^{-1}$. De même, on a $\mathrm{vect}(x_{\tau(1)}, \dots, x_{\tau(i)}) = N_i$ pour tout i. Par suite, il existe une matrice B_2 triangulaire supérieure telle que $(x_{\tau(1)}, \dots, x_{\tau(n)}) = FB_2$. Si P_τ est la matrice de permutation associée à τ, on a de plus $(x_{\tau(1)}, \dots, x_{\tau(n)}) = (x_1, \dots, x_n)P_\tau$. Par suite, $FB_2 = EB_1P_\tau$, d'où $F = EB_1P_\tau B_2^{-1}$. La matrice de passage de la base E à la base F est donc produit d'une matrice triangulaire supérieure, d'une matrice de permutation et d'une matrice triangulaire supérieure.

Dans $\mathrm{GL}(n, K)$, notons B le sous-groupe des matrices triangulaires supérieures et W le sous-groupe des matrices de permutation. Nous avons démontré que l'on a $\mathrm{GL}(n, K) = BWB$: c'est ce qu'on appelle la *décomposition de Bruhat.*

PROPOSITION 2.7.11. — *Soit A un anneau commutatif, S une partie multiplicative de A et soit M un A-module de longueur finie. Alors, $S^{-1}M$ est un $S^{-1}A$-module de longueur finie inférieure ou égale à $\ell_A(M)$.*

Démonstration. — En effet, soit $N = S^{-1}M$ et soit $N_0 \subsetneq N_1 \subsetneq \cdots \subsetneq N_n$ une suite strictement croissante de sous-modules de N. Posons $M_i = N_i \cap M$ (image réciproque de N_i dans M par l'homomorphisme canonique $M \to S^{-1}M$). On a $M_0 \subset \cdots \subset M_n$ et comme $S^{-1}M_i = N_i$ pour tout i (voir la proposition 2.6.6), les inclusions sont strictes. Ainsi, $\ell_A(M) \geqslant n$. En passant à la borne supérieure, on a donc $\ell_A(M) \geqslant \ell_{S^{-1}A}(S^{-1}M)$. □

Exercices. — 34) Le but de l'exercice est de déterminer tous les sous-$\mathbf{Z}$-modules de $\mathbf{Q}$.

Si $a \in \mathbf{Q}$ est non nul, on pose $v_p(a)$ l'exposant de p dans la décomposition de a en facteurs premiers. On pose $v_p(0) = +\infty$. Soit $V = \prod_{p \text{ premier}} (\mathbf{Z} \cup \{-\infty, +\infty\})$ et $v : \mathbf{Q} \to V$ défini par $v(a) = (v_p(a))_p$. On munit V de l'ordre produit : pour deux familles $(a_p)_p$ et $(b_p)_p$ de V, on dit que $(a_p) \leqslant (b_p)$ si pour tout nombre premier p, $a_p \leqslant b_p$.

a) Si x et y sont deux éléments de $\mathbf{Q}$ tels que $x\mathbf{Z} \subset y\mathbf{Z}$, montrer que $v(y) \leqslant v(x)$.

b) Montrer que toute partie de V admet une borne inférieure et une borne supérieure.

c) Soit M un sous-$\mathbf{Z}$-module de $\mathbf{Q}$ qui est de type fini. Montrer qu'il existe $a \in \mathbf{Q}$ tel que $M = a\mathbf{Z}$.

Montrer que $v(a)$ ne dépend pas du choix du générateur a de M choisi. On le note $v(M)$. Montrer alors que

$$M = \{x \in \mathbf{Q} ;\, v(x) \geqslant v(M)\}.$$

d) Si M est un sous-$\mathbf{Z}$-module de $\mathbf{Q}$, on pose

$$v(M) = \inf_{x \in \mathbf{Q}} v(x).$$

Réciproquement, si $w \in V$, on définit

$$M_w = \{x \in \mathbf{Q} ;\, v(x) \geqslant w\}.$$

Montrer que M_w est nul si et seulement si l'une des deux conditions ci-dessous est satisfaite :

(i) il existe p tel que $w_p = +\infty$;

(ii) l'ensemble des p tels que $w_p > 0$ est infini.

e) Montrer que les applications $M \mapsto v(M)$ et $w \mapsto M_w$ définissent deux bijections réciproques entre l'ensemble des sous-$\mathbf{Z}$-modules non nuls de $\mathbf{Q}$ et la partie $V^0 \subset V$ formée des $w \in V$ qui ne vérifient aucune des deux conditions (i) et (ii) ci-dessus.

f) Si $w \in V^0$, montrer que M_w est de type fini si et seulement si

(i) pour tout p, $w_p \neq -\infty$;

(ii) l'ensemble des p tels que $w_p < 0$ est fini.

Montrer qu'alors tout sous-module de M_w est aussi de type fini.

g) Si $w \in V^0$, montrer que M_w contient $\mathbf{Z}$ si et seulement si pour tout p, $w_p \leqslant 0$. Montrer qu'alors, $M_w/\mathbf{Z}$ est artinien si et seulement si l'ensemble des p tels que $w_p < 0$ est fini.

h) Si $w \in V^0$ est tel que M_w contient $\mathbf{Z}$, montrer que $M_w/\mathbf{Z}$ est de longueur finie si et seulement si

(i) pour tout p, $w_p \neq -\infty$;
(ii) l'ensemble des p tels que $w_p < 0$ est fini.

35) Soit M un A-module de longueur finie et soit u un endomorphisme de M.
a) Montrer qu'il existe un plus petit entier n tel que $\ker(u^n) = \ker(u^p)$ pour tout $p \geqslant n$.
b) Montrer que n est le plus petit entier tel que $\mathrm{im}(u^n) = \mathrm{im}(u^p)$ pour tout $p \geqslant n$.
c) Montrer que $\ker(u^n)$ et $\mathrm{im}(u^n)$ sont supplémentaires dans M.
d) Les conditions 1) u est bijectif ; 2) u est injectif ; 3) u est surjectif ; sont équivalentes.

36) Soit M un A-module, soit $(S_1, \ldots, S_n)$ une famille de sous-modules simples de M telle que $M = \sum S_i$.
a) Soit N un sous-module de M. Soit J une partie maximale de $\{1, \ldots, n\}$ telle que N et les S_j, pour $j \in J$, soient en somme directe. Montrer qu'alors, $M = N \oplus \left(\bigoplus_{j\in J} S_j\right)$.
b) Montrer qu'il existe $J \subset \{1, \ldots, n\}$ tel que M soit isomorphe au module $\bigoplus_{j\in J} S_j$.
c) Montrer que tout sous-module de M possède un supplémentaire.

37) Soit A un anneau, soit I un idéal à droite de A.
a) Montrer que l'ensemble B des $a \in A$ tels que $aI \subset I$ est un sous-anneau de A dont I est un idéal bilatère.
b) Définir un isomorphisme de l'anneau des endomorphismes du A-module à droite A/I sur l'anneau B/I.
c) Si I est un idéal à droite maximal, montrer que B/I est un anneau à division.

38) Soit K un corps commutatif.
a) Pour tout polynôme non nul $P \in K[X]$, montrer que la longueur de $K[X]/(P)$ est égal au nombre de facteurs irréductibles de P, comptés avec multiplicité.
b) Si K est algébriquement clos, la longueur d'un $K[X_1, \ldots, X_n]$ module coïncide avec sa dimension comme K-espace vectoriel. (*Utiliser le théorème des zéros de Hilbert.*)

39) Démontrer l'existence et l'unicité de la décomposition d'un entier en facteurs premiers en appliquant le théorème de Jordan-Hölder au module $\mathbf{Z}/n\mathbf{Z}$, où n est un entier strictement positif.

40) Soit A un anneau et soit M un A-module (à droite) de type fini, non nul.
a) Montrer que l'ensemble des sous-modules de M qui sont distincts de M est inductif.
b) Montrer que pour tout sous-module N de M tel que $N \neq M$, il existe un sous-module P de M tel que $N \subset P \subset M$ et tel que M/P soit un A-module simple.
c) Supposons que A possède un unique idéal maximal (à droite) I. Montrer que $\mathrm{Hom}_A(M, A/I) \neq 0$.
d) Posons $A = \mathbf{Z}$ et $M = \mathbf{Q}$. Montrer qu'il n'existe pas de sous-module $P \subset M$ tel que M/P soit simple.

§2.8. Opérations élémentaires sur les matrices

2.8.1. Matrices élémentaires. — Soit A un anneau. Le groupe $\mathrm{GL}_n(A)$ des matrices inversibles $n \times n$ à coefficients dans A contient un certain nombre d'éléments importants.

On note $(e_{i,j})$ la base canonique de $\mathrm{Mat}_n(A)$; $e_{i,j}$ est la matrice dont tous les coefficients sont nuls sauf celui de la ligne i et de la colonne j qui vaut 1. Pour $i, j \in \{1, \dots, n\}$, $i \neq j$, et $a \in A$, on pose $E_{ij}(a) = I_n + ae_{i,j}$, où I_n est la matrice identité. On a la relation

$$E_{ij}(a)E_{ij}(b) = E_{ij}(a+b)$$

qui, jointe à l'identité évidente $E_{ij}(0) = I_n$, entraîne que les matrices $E_{ij}(a)$ sont inversibles. On note $\mathrm{E}_n(A)$ le sous-groupe de $\mathrm{GL}_n(A)$ engendré par ces matrices, dites élémentaires.

Si $\sigma \in \mathfrak{S}_n$, on note P_σ la matrice attachée à σ ; c'est celle de l'application canonique qui applique le i-ième vecteur de base sur le $\sigma(i)$-ième. Autrement dit, si $P_\sigma = (p_{i,j})$, on a $p_{i,j} = 1$ si $i = \sigma(j)$ et $p_{i,j} = 0$ sinon. On a $P_{\sigma\tau} = P_\sigma P_\tau$ et $P_{\mathrm{id}} = I_n$. L'application $\sigma \mapsto P_\sigma$ est un isomorphisme du groupe $\mathfrak{S}_n$ sur un sous-groupe de $\mathrm{GL}_n(A)$ que l'on note W.

Pour $1 \leqslant i \leqslant n$ et $a \in A$, on note enfin $D_i(a)$ la matrice diagonale $I_n + (a-1)e_{i,i}$ dont les coefficients diagonaux sont tous égaux à 1 sauf celui de la ligne i et de la colonne i qui vaut a. On a $D_i(a)D_i(b) = D_i(ab)$ et $D_i(1) = I_n$; si $a \in A^*$, alors $D_i(a)$ appartient à $\mathrm{GL}_n(A)$.

On note $\mathrm{GE}_n(A)$ le sous-groupe de $\mathrm{GL}_n(A)$ engendré par les matrices élémentaires $E_{i,j}(a)$, pour $a \in A$, les matrices de permutation P_σ et les matrices $D_i(a)$, pour $a \in A^*$.

2.8.2. Opérations élémentaires. — Soit M une matrice à n lignes et p colonnes à coefficients dans A.

La multiplication à droite de M par les matrices élémentaires (de $\mathrm{Mat}_p(A)$) correspond aux manipulations classiques sur les colonnes de M. La matrice $ME_{i,j}(a)$ est obtenue en ajoutant la i-ième colonne de M fois a à sa j-ième colonne (opération qu'on symbolise par $C_j \leftarrow C_j + C_i a$). La matrice MP_σ est obtenue en permutant les colonnes de M : la i-ième colonne de M est placée en $\sigma(i)$; la j-ième colonne de MP_σ est la $\sigma^{-1}(j)$-ième de M. La matrice $MD_i(a)$ est obtenue en multipliant la i-ième colonne de M par a (soit encore $C_i \leftarrow C_i a$).

La multiplication à gauche de M par les matrices élémentaires (de $\mathrm{Mat}_n(A)$) correspond, quant à elle, aux opérations classiques sur les lignes de M. La matrice $E_{i,j}(a)M$ est obtenue en ajoutant a fois la j-ième ligne de A à sa i-ième ligne (on note $L_i \leftarrow L_i + aL_j$) ; la i-ième ligne de M est la ligne d'indice $\sigma(i)$ de la matrice $P_\sigma M$; les lignes de $D_i(a)M$ sont celles de M sauf la ligne d'indice i qui est multipliée par i (c'est-à-dire $L_i \leftarrow aL_i$).

THÉORÈME 2.8.3. — *Soit A un anneau euclidien et soit $M \in \mathrm{Mat}_{n,p}(A)$. Il existe une matrice $P \in \mathrm{E}_n(a)$, une matrice $Q \in E_p(A)$ et une matrice $D \in \mathrm{Mat}_{n,p}(A)$ « diagonale » ($d_{ij} = 0$ pour $i \neq j$) et telle d_{ii} divise $d_{i+1,i+1}$ pour tout i tel que $1 \leqslant i < \min(n,p)$ telles que l'on ait $M = PDQ$. En outre, si $M = P'D'Q'$ est une autre décomposition, il existe pour tout entier i tel que $1 \leqslant i \leqslant \min(n,p)$ un élément inversible $u_i \in A$ tel que $d'_{ii} = d_{ii}u_i$.*

Démonstration. — Notons δ la jauge de A. Démontrons l'existence d'une telle décomposition par récurrence sur $\max(n,p)$, puis par récurrence sur le minimum des jauges des coefficients non nuls de A.

Les matrices 2×2 suivantes se déduisent l'une de l'autre par opérations élémentaires :

$$\begin{pmatrix}1&0\\0&1\end{pmatrix},\quad \begin{pmatrix}1&1\\0&1\end{pmatrix},\quad \begin{pmatrix}0&1\\-1&1\end{pmatrix},\quad \begin{pmatrix}0&1\\-1&0\end{pmatrix}.$$

Il existe donc un élément de $\mathrm{E}_2(\mathbf{Z})$ qui applique le échange les deux axes de $\mathbf{Z}^2$. Faisant les mêmes opérations élémentaires sur les lignes et colonnes d'indices i et j, il en résulte qu'il existe, pour toute transposition (i,j), un élément de $\mathrm{E}_n(A)$ qui échange, au signe près, le i-ième et le j-ième vecteurs de base. Soit maintenant (i,j) les coordonnées d'un coefficient non nul de M de jauge minimale ; d'après ce qui précède, on peut effectuer des opérations élémentaires sur les lignes et les colonnes de M de sorte à placer ce coefficient (au signe près) en coordonnées $(1,1)$.

Soit alors $m_{1k}=m_{11}q_k+m'_{1k}$ la division euclidienne de m_{1k} par m_{11}. L'opération sur les colonnes $C_k\leftarrow C_k-C_1q_k$ transforme la matrice M en la matrice $M'=ME_{1k}(-q_k)$ dont le coefficient m_{1k} est devenu m'_{1k}. Si $m'_{1k}\neq 0$, $\delta(m'_{1k})<0$ et on conclut par récurrence car le minimum des jauges des éléments non nuls de M' est inférieur à celui de M. Cela permet de supposer que seul le premier coefficient de la première ligne est non nul. En faisant l'opération analogue sur les lignes, on conclut de même par récurrence, ou on se ramène au cas où seul le premier coefficient de la première colonne n'est pas nul.

S'il existe un coefficient de coordonnées (i,j), avec $i>1$ et $j>1$, qui n'est pas multiple de m_{11}, ajoutons à la première ligne la ligne i (ce qui revient à multiplier à gauche par la matrice $E_{1i}(1)$), ce qui transforme la première ligne en $(m_{11},m_{i2},\dots,m_{i,p})$. En soustrayant de la colonne j la première multipliée par q, où $m_{1j}=m_{11}q+r$ est une division euclidienne, on obtient une matrice dont l'élément $(1,j)$ est égal à r, n'est pas nul par hypothèse, donc est de jauge $<\delta(m_{11})$. On conclut donc par récurrence.

Après ces premières manipulations, on a transformé la matrice M est une matrice P_1MQ_1, de la forme

$$\begin{pmatrix}m_{11}&0&\dots&0\\0&&&\\\vdots&&m_{11}M'&\\0&&&\end{pmatrix},$$

où M' est une matrice de $\mathrm{Mat}_{n-1,p-1}(A)$. Par récurrence, il existe des matrices $P'\in \mathrm{E}_{n-1}(A)$, $Q'\in \mathrm{E}_{p-1}(A)$ et $D'\in \mathrm{Mat}_{n-1,p-1}(A)$, diagonale dont chaque coefficient divise le suivant, telles que $M'=P'D'Q'$. Définissons alors des matrices par blocs

$$P=\begin{pmatrix}1&0\\0&P'\end{pmatrix},\quad D=m_{11}\begin{pmatrix}1&0\\0&D'\end{pmatrix},\quad Q=\begin{pmatrix}1&0\\0&Q'\end{pmatrix}.$$

On a $P_1MQ_1 = PDQ$, donc $M = (P_1)^{-1}PDQ(Q_1)^{-1}$, d'où l'existence d'une décomposition.

L'assertion d'unicité sera démontrée au paragraphe suivant, car elle se généralise au cas des anneaux principaux. □

COROLLAIRE 2.8.4. — *Si A est un anneau euclidien, on a* $\mathrm{SL}_n(A) = \mathrm{E}_n(A)$ *et* $\mathrm{GL}_n(A) = \mathrm{GE}_n(A)$.

Démonstration. — Soit $M \in \mathrm{GL}_n(A)$; soit $M = PDQ$ une décomposition, avec P et $Q \in \mathrm{E}_n(A)$ et D diagonale. Les coefficients diagonaux de D sont inversibles.

Soit λ et μ des éléments inversibles de A. Observons alors que les matrices suivantes se déduisent l'une de l'autre par une opération élémentaire :

$$\begin{pmatrix}\lambda & 0\\ 0 & \mu\end{pmatrix},\ \begin{pmatrix}\lambda & 1\\ 0 & \mu\end{pmatrix},\begin{pmatrix}0 & 1\\ -\lambda\mu & \mu\end{pmatrix},\begin{pmatrix}\lambda\mu & 1-\mu\\ -\lambda\mu & \mu\end{pmatrix},\begin{pmatrix}\lambda\mu & 1-\mu\\ 0 & 1\end{pmatrix},\begin{pmatrix}\lambda\mu & 0\\ 0 & 1\end{pmatrix}.$$

Cela démontre qu'il existe des matrices U et $V \in \mathrm{E}_2(A)$ telles que

$$U\begin{pmatrix}\lambda & \\ & \mu\end{pmatrix}V = \begin{pmatrix}\lambda\mu & \\ & 1\end{pmatrix},$$

Par récurrence, il existe, pour toute famille $(a_1,\dots,a_n)$ d'éléments inversibles de A, des matrices U et $V \in \mathrm{E}_n(A)$ telles que

$$U\begin{pmatrix}a_1 & & & \\ & a_2 & & \\ & & \ddots & \\ & & & a_n\end{pmatrix}V = \begin{pmatrix}a_1a_2\dots a_n & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1\end{pmatrix}.$$

Il existe par conséquent des matrices P' et $Q' \in \mathrm{E}_n(A)$ telles que $M = P'\,\mathrm{diag}(\det(M),1,\dots,1)Q'$. Cela démontre que $\mathrm{GL}_n(A) = \mathrm{GE}_n(A)$.

Si de plus $M \in \mathrm{SL}_n(A)$, on voit que $M \in \mathrm{E}_n(A)$, d'où l'inclusion $\mathrm{SL}_n(A) \subset \mathrm{E}_n(A)$, puis l'égalité puisque l'autre inclusion est évidente. □

2.8.5. Matrices à coefficients dans un anneau principal. — Dans la fin de ce paragraphe, le but est d'étendre le théorème 2.8.3 au cas d'un anneau principal A quelconque. Cependant, les opérations élémentaires sur les lignes et les colonnes ne suffisent plus et il faut faire intervenir, au lieu du groupe $\mathrm{E}_n(A)$, tout le groupe $\mathrm{SL}_n(A)$.

LEMME 2.8.6. — *Soit A un anneau principal, soit a et b des éléments de A non tous deux nuls. Notons d un pgcd de (a,b) ; soit u et $v \in A$ tels que $d = au + bv$. Soit r et $s \in A$ tels que $a = dr$ et $b = ds$. La matrice $\left(\begin{smallmatrix}u & v\\ -s & r\end{smallmatrix}\right)$ est appartient à* $\mathrm{SL}_2(A)$ *et l'on a*

$$\begin{pmatrix}u & v\\ -s & r\end{pmatrix}\begin{pmatrix}a & *\\ b & *\end{pmatrix} = \begin{pmatrix}d & *\\ 0 & *\end{pmatrix}.$$

Démonstration. — On a $d = au + bv = d(ur + vs)$. Comme $d \neq 0$, il en résulte $ur + vs = 1$ ce qui démontre que $\left(\begin{smallmatrix} u & v \\ -s & r \end{smallmatrix}\right) \in \mathrm{SL}_2(A)$. La seconde assertion est immédiate. □

THÉORÈME 2.8.7. — *Soit A un anneau principal et soit $M \in \mathrm{Mat}_{n,p}(A)$. Il existe une matrice $P \in \mathrm{SL}_n(a)$, une matrice $Q \in \mathrm{SL}_p(A)$ et une matrice $D \in \mathrm{Mat}_{n,p}(A)$ « diagonale » ($d_{ij} = 0$ pour $i \neq j$) et telle d_{ii} divise $d_{i+1,i+1}$ pour tout i tel que $1 \leqslant i < \min(n,p)$ telles que l'on ait $M = PDQ$. En outre, si $M = P'D'Q'$ est une autre décomposition, il existe pour tout entier i tel que $1 \leqslant i \leqslant \min(n,p)$ un élément inversible $u_i \in A$ tel que $d'_{ii} = d_{ii}u_i$.*

Démonstration. — La démonstration est analogue à celle du cas euclidien et nous n'indiquerons que les modifications à y apporter. Pour $a \in A$, $a \neq 0$, notons $\ell(a)$ et appelons *taille* de a, la longueur de $A/(a)$, c'est-à-dire le nombre de facteurs irréductibles de a ; Raisonnons maintenant par récurrence sur $\max(n,p)$ puis sur la taille minimale d'un coefficient non nul de M.

On se ramène comme précédemment au cas où l'élément m_{11} est de taille minimale. Si tous les coefficients de la première colonne sont multiples de m_{11}, on se ramène, par des opérations élémentaires sur les lignes, au cas où seul le premier coefficient de cette première colonne n'est pas nul. Sinon, il existe une matrice $P_1 \in \mathrm{SL}_n(A)$ de la forme

$$\begin{pmatrix} u & 0 & \dots & v & 0 & \dots \\ 0 & 1 & & 0 & & \\ \vdots & & \ddots & \vdots & & \\ -s & & & r & & \\ & & & & 1 & \\ & & & & & \ddots \end{pmatrix}$$

telle que le coefficient $(1,1)$ de P_1M soit le pgcd de m_{11} et $m_{1,i}$, où i est choisi de sorte que $m_{1,i}$ n'est pas multiple de m_{11}. Par récurrence, il existe P et $Q \in \mathrm{SL}_n(A)$ telles que PP_1MQ soit diagonale, chaque coefficient diagonal divisant le suivant.

Par multiplication à droite par des matrices analogues, on se ramène aussi au cas où seul le premier coefficient de la première ligne n'est pas nul, la matrice M étant finalement de la forme

$$\begin{pmatrix} m_{11} & 0 & \dots & 0 \\ 0 & & M' & \\ \vdots & & & \\ 0 & & & \end{pmatrix}$$

avec $M' \in \mathrm{Mat}_{n-1,p-1}(A)$. Le même argument que dans le cas euclidien montre que l'on peut supposer que tous les coefficients de M' sont multiples de m_{11}. On conclut alors de la même façon, en appliquant l'hypothèse de récurrence, la matrice M' étant de taille plus petite.

Quant à l'assertion d'unicité, elle résulte de la proposition suivante, plus précise. □

PROPOSITION 2.8.8. — *Soit $P \in \mathrm{GL}_n(A)$, $Q \in \mathrm{GL}_p(A)$ et soit $D \in \mathrm{Mat}_{n,p}(A)$ une matrice diagonale dont les coefficients diagonaux d_i vérifient la relation de divisibilité $d_i | d_{i+1}$ pour $1 \leqslant i < \min(n,p)$. Posons $M = PDQ$.*

Pour tout entier k tel que $1 \leqslant k \leqslant \min(n,p)$, l'idéal engendré par les mineurs de taille k de la matrice M est l'idéal $(d_1 \dots d_k)$.

Démonstration. — Si $M \in \mathrm{Mat}_{n,p}(A)$ est une matrice à n lignes et p colonnes, notons $\mathscr{I}_k(M)$ l'idéal de A engendré par les mineurs $k \times k$ extraits de A.

Lorsqu'on multiplie une matrice M à droite par une matrice Q, les colonnes de la nouvelle matrice $M' = MQ$ sont des combinaisons linéaires des colonnes de M. Par multilinéarité du déterminant, chaque mineur d'ordre k de M' est combinaison linéaire des mineurs d'ordre k de M, d'où l'inclusion $\mathscr{I}_k(MQ) \subset \mathscr{I}_k(M)$. De même, lorsqu'on multiplie une matrice M à gauche par une matrice Q, les lignes de la nouvelle matrice PM sont des combinaisons linéaires des lignes de M et l'on a une inclusion $\mathscr{I}_k(PM) \subset \mathscr{I}_k(M)$.

En combinant ces inclusions, on voit donc que $\mathscr{I}_k(PMQ) \subset \mathscr{I}_k(M)$ lorsque $P \in \mathrm{Mat}_n(A)$ et $Q \in \mathrm{Mat}_p(A)$. Supposons de plus que P et Q soient inversibles : alors $M = P^{-1}(PMQ)Q^{-1}$, d'où $\mathscr{I}_k(M) \subset \mathscr{I}_k(PMQ)$. On a donc l'égalité de ces idéaux.

Revenons aux notations de la proposition, on a donc démontré que $\mathscr{I}_k(M) = \mathscr{I}_k(D)$ et il reste à calculer ce dernier idéal. Si $I \subset \{1,\dots,n\}$ et $J \subset \{1,\dots,p\}$ sont des parties de cardinal k, la matrice extraite D_{IJ} a pour déterminant 0 si $I \neq J$ et $\prod_{i \in I} d_i$ si $I = J$. Ces produits sont tous multiples de $d_1 \dots d_k$, et l'on a égalité pour $I = J = \{1,\dots,k\}$, si bien que $\mathscr{I}_k(D) = (d_1 \dots d_k)$. La proposition est donc démontrée. □

De manière équivalente, soit Δ_k un générateur de l'idéal engendré par les mineurs d'ordre k de M. On a $(\Delta_k) = (d_1 \dots d_k)$. Autrement dit, Δ_{k-1} divise Δ_k et d_k est égal à Δ_k / Δ_{k-1}, à un élément inversible près.

Exercices. — 41) a) Montrer que le matrice de la transposition de $\{1,2\}$ appartient au sous-groupe de $\mathrm{GL}_2(\mathbf{Z})$ engendré par les matrices élémentaires et les matrices $D_i(-1)$.

b) Appartient-elle au sous-groupe engendré par les matrices élémentaires ?

c) En déduire que le sous-groupe W de $\mathrm{GL}_n(\mathbf{Z})$ est contenu dans le sous-groupe engendré par les matrices élémentaires $E_{i,j}(1)$ et les matrices $D_i(-1)$.

42) Soit N un entier naturel.

a) Montrer que le groupe $\mathrm{SL}_n(\mathbf{Z}/N\mathbf{Z})$ est engendré par les matrices élémentaires.

b) Montrer que l'homomorphisme canonique $\mathrm{SL}_n(\mathbf{Z}) \to \mathrm{SL}_n(\mathbf{Z}/N\mathbf{Z})$ est surjectif.

c) L'homomorphisme $\mathrm{GL}_n(\mathbf{Z}) \to \mathrm{GL}_n(\mathbf{Z}/N\mathbf{Z})$ est-il surjectif ?

43) Soit A un anneau euclidien et soit K son corps des fractions.

a) Soit $u = (a_1,\dots,a_n) \in A^n$. Montrer qu'il existe une matrice $M \in \mathrm{E}_n(A)$ telle que Mu soit de la forme $(a,0,\dots,0)$, où $a \in A$ est un générateur de l'idéal $(a_1,\dots,a_n)$.

b) Montrer que le groupe $\mathrm{E}_n(A)$ opère transitivement sur l'ensemble des droites de K^n.

44) Soit $u \in \mathbf{Z}^n$ un vecteur dont les coordonnées sont premières entre elles. Montrer par récurrence sur le plus petit coefficient non nul de u qu'il existe une matrice $M \in \mathrm{SL}_n(\mathbf{Z})$ de première colonne u.

45) Soit A un anneau commutatif.

a) Montrer que le groupe $\mathrm{GE}_n(A)$ est produit semi-direct du sous-groupe distingué $\mathrm{E}_n(A)$ et du sous-groupe formé des matrices $D_1(a)$, pour $a \in A^\times$.

b) Même question en remplaçant GE_n par GL_n et E_n par SL_n.

46) Soit K un anneau à division.

a) Montrer que l'on a $\mathrm{GL}_n(K) = \mathrm{GE}_n(K)$.

Soit D le groupe abélien $K^\times/[K^\times, K^\times]$, quotient de $K^\times$ par le sous-groupe engendré par les commutateurs. Notons $\pi\colon K^\times \to D$ l'application canonique.

b) Montrer qu'il existe un unique homomorphisme de groupes δ de $\mathrm{GE}_n(K)$ dans D qui applique $E_{ij}(a)$ sur $\pi(1)$ pour tous $i, j \in \{1,\dots,n\}$ et $a \in A$ et qui applique $D_i(a)$ sur $\pi(a)$ pour tous $i \in \{1,\dots,n\}$ et $a \in A^\times$.

c) Lorsque K est commutatif, $D = K^\times$. Montrer alors que l'homomorphisme $\delta\colon \mathrm{GL}_n(K) \to K^\times$ n'est autre que le déterminant. Dans le cas général, on l'appelle le *déterminant non commutatif*.

47) Soit A un anneau principal et soit K son corps des fractions.

a) Soit $u = (a_1,\dots,a_n) \in A^n$. Montrer qu'il existe une matrice $M \in \mathrm{SL}_n(A)$ telle que Mu soit de la forme $(a,0,\dots,0)$, où $a \in A$ est un générateur de l'idéal $(a_1,\dots,a_n)$.

b) Montrer que le groupe $\mathrm{SL}_n(A)$ opère transitivement sur l'ensemble des droites de K^n.

c) Soit D_1 et D_2 les droites de $\mathbf{Q}^2$ de vecteurs directeurs $(1,2)$ et $(2,1)$. Montrer qu'il n'existe pas de matrice $M \in \mathrm{GL}_2(\mathbf{Z})$ telle que $M(D_1)$ et $M(D_2)$ soient les deux axes de coordonnées.

d) Il n'existe pas de matrice $M \in \mathrm{GL}_2(k[X,Y])$ qui applique la droite de vecteur directeur (X,Y) sur celle de vecteur directeur $(1,0)$.

48) Soit M une matrice à n lignes et p colonnes ($p \leqslant n$) dont les coefficients sont dans un anneau principal A.

Montrer qu'on peut compléter M en une matrice $P \in GL(n,A)$ si et seulement si le pgcd des mineurs d'ordre p de A est égal à 1.

49) Soit A un anneau principal, K son corps des fractions.

a) Soit x un élément non nul de K^n. Montrer qu'il existe une matrice de $GL_n(A)$ dont la colonne est proportionnelle à x.

b) Démontrer que toute matrice carrée d'ordre n à coefficients dans K est produit d'une matrice de $GL_n(A)$ et d'une matrice triangulaire de $M_n(K)$. (Raisonner par récurrence.)

c) *Application numérique :* $A = \mathbf{Z}$ et

$$M = \begin{pmatrix} 1/2 & 1 & -1/4 \\ 2/5 & 2 & 2/3 \\ 3/4 & 1/7 & -1 \end{pmatrix}.$$

§2.9. Modules de type fini sur un anneau principal

PROPOSITION 2.9.1. — *Soit A un anneau principal, soit M un A-module libre de rang n et soit N un sous-module de M. Alors, N est un A-module libre de rang $\leqslant n$.*

Démonstration. — Il suffit de montrer que tout sous-module N de A^n est libre ; démontrons ceci par récurrence sur n. Si $n = 0$, on a $N = 0$, qui est un module libre de rang 0. Si $n = 1$, N est un idéal de A. Si $N = 0$, N est libre. Comme A est un anneau principal, il existe sinon un élément non nul $d \in A$ tel que $N = dA$. Comme A est intègre, l'application $a \mapsto da$ est un isomorphisme de A sur N, ce qui démontre que N est libre de rang 1.

Soit maintenant n un entier tel que $n \geqslant 2$ et supposons que tout sous-module de A^r, pour $r < n$, soit libre. Soit N un sous-module de A^n. Notons $f : A^n \to A$ la forme linéaire $(a_1, \dots, a_n) \mapsto a_n$; son noyau est le sous-module $M_0 = A^{n-1} \times \{0\}$ de A^n. Par récurrence (ou bien parce que A est principal), l'idéal $N_1 = f(N)$ de A est libre de rang $\leqslant 1$. Le sous-module $N_0 = N \cap M_0$ de M_0 est isomorphe à un sous-module de A^{n-1} ; par récurrence, il est libre de rang $\leqslant n-1$. On conclut à l'aide de la proposition 2.4.5. □

Le théorème suivant est plus précis : il fournit une base d'un module libre sur un anneau principal adaptée à un sous-module donné.

THÉORÈME 2.9.2 (Théorème de la base adaptée). — *Soit A un anneau principal, soit M un A-module libre de rang n et soit N un sous-module de M. Il existe une base $(e_1, \dots, e_n)$ de M, un entier r tel que $0 \leqslant r \leqslant n$ et des éléments $d_1, \dots, d_r$ de A tels que d_i divise d_{i+1} pour $1 \leqslant i < r$ tels que $(d_1 e_1, \dots, d_r e_r)$ soit une base de N.*

En outre, l'entier r et les idéaux (d_i) ne dépendent que de N et pas de la base $(e_1, \dots, e_n)$.

Démonstration. — On peut supposer que $M = A^n$. D'après la proposition précédente, le sous-module N est libre de rang $p \leqslant n$. C'est donc l'image d'un homomorphisme $A^p \to A^n$ que l'on peut étendre (en appliquant les vecteurs de base supplémentaires sur 0) en un homomorphisme $A^n \to A^n$ d'image N. Notons $U \in \mathrm{Mat}_n(A)$ la matrice de cet homomorphisme.

Il existe, en vertu du théorème 2.8.7 des matrices $P \in \mathrm{GL}_n(A)$ et $Q \in \mathrm{GL}_n(A)$ et une matrice diagonale $D \in \mathrm{Mat}_n(A)$ dont chacun des coefficients $d_1, \dots, d_n$ divise le suivant telles que $U = PDQ$. Comme d_i divise d_{i+1}, $d_{i+1} = 0$ si $d_i = 0$; il existe donc un plus grand entier r tel que $d_r \neq 0$.

Soit $(\varepsilon_1, \dots, \varepsilon_n)$ l'image de la base canonique par Q et posons $e_i = P\varepsilon_i$ pour tout i. La famille $(e_1, \dots, e_n)$ est l'image de la base canonique de A^n par la matrice $PQ \in \mathrm{GL}_n(A)$; c'est donc une base de A^n. En outre, l'image du i-ième vecteur de la base canonique de A^n par U est égale à $Qd_i\varepsilon_i = d_i e_i$. Autrement dit, on a trouvé une base $(e_1, \dots, e_n)$ de A^n et des éléments $d_1, \dots, d_r$ tels que d_i divise d_{i+1} pour $1 \leqslant i < r$ et tels que

$(d_1e_1,\dots,d_re_r)$ engendre N. Comme $d_i \neq 0$ pour $i \leqslant r$, cette famille est libre ; c'est donc une base de N.

Considérons $(\varepsilon_1,\dots,\varepsilon_n)$ une base de A^n, $\delta_1,\dots,\delta_p$ des éléments de A tels que δ_i divise δ_{i+1} pour $1 \leqslant i < p$ et $(\delta_1\varepsilon_1,\dots,\delta_p\varepsilon_p)$ soit une base de N. On a déjà $p = r$ car deux bases d'un module libre de rang fini sur un anneau commutatif ont même cardinal. La matrice de l'injection de N dans A^n dans les bases $(e_1,\dots,e_r)$ et $(e_1,\dots,e_n)$ est égale à $D = \operatorname{diag}(d_1,\dots,d_r)$; elle est aussi égale à $P^{-1}\Delta Q$ où P est la matrice de la base $(\varepsilon_1,\dots,\varepsilon_n)$ dans la base $(e_1,\dots,e_n)$, Q la matrice de la base $(\delta_1\varepsilon_1,\dots,\delta_r\varepsilon_r)$ dans la base $(d_1e_1,\dots,d_re_e)$ et Δ la matrice diagonale $\operatorname{diag}(\delta_1,\dots,\delta_r)$. L'assertion d'unicité résulte alors de celle du théorème 2.8.7. □

COROLLAIRE 2.9.3. — *Soit A un anneau principal et soit M un A-module de type fini. Il existe un entier n et des éléments $d_1,\dots,d_n$ de A, non inversibles, tels que d_i divise d_{i+1} pour $1 \leqslant i < n$ de sorte que M soit isomorphe à la somme directe $\bigoplus_{i=1}^n A/(d_i)$.*

S'il existe un isomorphisme $M \simeq \bigoplus_{i=1}^m A/(\delta_i)$, où $\delta_1,\dots,\delta_m$ sont des éléments de A non inversibles tels que δ_i divise δ_{i+1} pour $1 \leqslant i < m$, alors $m = n$ et l'on a $(\delta_i) = (d_i)$ pour tout i.

Démonstration. — Soit $(m_1,\dots,m_n)$ une famille génératrice de M et soit $f\colon A^n \to M$ l'unique homomorphisme qui applique le i-ième vecteur de la base canonique de A^n sur m_i. Il est surjectif. Soit N le noyau de f ; l'homomorphisme f induit, par passage au quotient, un isomorphisme de A^n/N sur M.

Soit $(e_1,\dots,e_n)$ une base de M, $d_1,\dots,d_p$ des éléments de A tels que $(d_1e_1,\dots,d_pe_p)$ soit une base de N et tels que d_i divise d_{i+1} pour $1 \leqslant i < p$. Posons $d_i = 0$ pour $i > p$; si d_{i+1} est inversible, d_i l'est aussi. L'application φ de A^n dans M qui, à $(a_1,\dots,a_n)$ associe $a_1e_1 + \cdots + a_ne_n$ est surjective, car $(e_1,\dots,e_n)$ est une base de A^n. On a $\varphi(a_1,\dots,a_n) = 0$ si et seulement si d_i divise a_i pour tout i. Par passage au quotient, il en résulte un isomorphisme de $\bigoplus_{i=1}^n A/(d_i)$ sur M.

Comme d_i divise d_{i+1}, d_i est inversible si d_{i+1} l'est. Il existe donc un plus petit entier r tel que d_r ne soit pas inversible, $A/(d_i) = 0$ si $i < r$ et l'on a un isomorphisme $M \simeq \bigoplus_{i=r}^n A/(d_i)$, d'où l'assertion d'existence.

L'assertion d'unicité peut être déduite du résultat analogue sur les matrices ; c'est ce que nous ferons au paragraphe sur les idéaux de Fitting. En voici une autre pour l'instant.

Supposons donc donné un isomorphisme $M \simeq \bigoplus_{i=1}^n A/(d_i)$, où $d_1,\dots,d_n$ sont des éléments non inversibles de A tels que d_i divise d_{i+1} pour $1 \leqslant i < n$. Appliquons le lemme suivant avec $a = p^m$ et $b = p$, où p est un élément irréductible arbitraire de A. On obtient que $p^{n-1}M/p^nM$ est isomorphe à une somme directe de modules $A/(p)$, en nombre égal au nombre d'indices i tels que p^n divise d_i. Comme d_i divise d_{i+1} pour $1 \leqslant i < n$, on voit que p^n divise d_i si et seulement si $\dim(p^{n-1}M/p^nM) \geqslant n+1-i$.

Cela détermine les facteurs irréductibles des d_i, ainsi que leurs exposants, et donc les idéaux (d_i). □

LEMME 2.9.4. — *Soit A un anneau principal, soit d un élément de A et soit p un élément irréductible de A. Posons $M = A/(d)$ et posons, pour tout entier $n \geqslant 1$, $M_n = p^{n-1}M/p^nM$. Alors, le A-module M_n est de manière canonique un $A/(p)$-espace vectoriel dont la dimension vaut* 1 *si p^n divise d et zéro sinon.*

Démonstration. — Le module M_n est annulé par la multiplication par p ; l'homomorphisme d'anneaux canonique $A \to \mathrm{End}(M_n)$ se factorise donc par un homomorphisme d'anneaux de $A/(p)$ dans $\mathrm{End}(M_n)$, d'où une structure de (A/p)-espace vectoriel sur M_n, car $A/(p)$ est un corps.

Soit ν la borne supérieure des entiers n tels que p^n divise d. La bijection entre sous-modules de $A/(d)$ et sous-modules de A contenant (d) applique p^nM sur l'idéal $(p^n, d) = (p^{\min(n,\nu)})$. On a alors des isomorphismes (« canoniques »)

$$M_n = p^{n-1}M/p^nM \simeq \frac{p^{\min(n-1,\nu)}A/dA}{p^{\min(n,\nu)}A/dA} \simeq \frac{p^{\min(n-1,\nu)}A}{p^{\min(n,\nu)}A}.$$

Par conséquent, $M_n = 0$ si et seulement si $\min(n,\nu) = \min(n-1,\nu)$, c'est-à-dire si et seulement $\nu \leqslant n-1$, ce qui revient à dire que p^n ne divise pas d. Dans le cas contraire, $\min(n,\nu) = n$, $\min(n-1,\nu) = n-1$ et

$$M_n \simeq p^{n-1}A/p^nA \simeq A/pA.$$

□

DÉFINITION 2.9.5. — *Soit A un anneau principal et soit M un A-module de type fini. Soit $M \simeq \bigoplus_{i=1}^n A/(d_i)$ une décomposition de M, où les d_i sont des éléments non inversibles de A tels que d_i divise d_{i+1} pour* $1 \leqslant i < n$.

Les idéaux (d_1),…, (d_n) sont appelés les facteurs invariants de M. Le nombre de ces idéaux qui sont non nuls est appelé le rang *de M.*

Avec ces notations, on a $d_i = 0$ pour $n-r+1 \leqslant i \leqslant n$ donc M est isomorphe à la somme directe d'un module libre de rang r et du sous-module $\bigoplus_{i=1}^{n-r} A/(d_i)$. Notons que ce dernier sous-module n'est autre que l'ensemble des éléments de M annulés par un élément non nul de A : c'est le sous-module de torsion de M.

COROLLAIRE 2.9.6. — *Pour qu'un module de type fini sur un anneau principal soit libre, il faut et il suffit qu'il soit sans torsion.*

COROLLAIRE 2.9.7. — *Soit A un anneau principal, soit M un A-module libre de type fini et soit N un sous-module de M. Pour que N admette un supplémentaire dans M, il faut et il suffit que le quotient M/N soit sans torsion.*

Démonstration. — Si N possède un supplémentaire P, l'homomorphisme canonique de P dans M/N est un isomorphisme. Comme P est un sous-module du module libre M, il est sans torsion. Par conséquent, M/N est sans torsion.

Supposons inversement que M/N soit sans torsion. C'est alors un module libre puisque c'est un A-module de type fini et que A est principal. Soit $(f_1,\dots,f_r)$ une base de M/N ; pour tout $i \in \{1,\dots,r\}$, soit e_i un élément de M dont la classe est f_i ; soit P le sous-A-module de M engendré par les e_i. Montrons que P est un supplémentaire de N dans M.

Si $m \in N \cap P$, écrivons $m = \sum a_i e_i$; on a $\mathrm{cl}(m) = 0$ car $m \in N$, donc $\sum a_i f_i = 0$, donc $a_i = 0$ pour tout i puisque la famille (f_i) est libre. Par suite, $m = 0$ et $N \cap P = 0$.

Soit $m \in M$; soit $(a_1,\dots,a_r)$ des éléments de A tels que $\mathrm{cl}(m) = \sum a_i f_i$; alors, $p = \sum a_i e_i$ est un élément de P et l'on a $\mathrm{cl}(p) = \mathrm{cl}(m)$. Par suite, $\mathrm{cl}(m-p) = 0$, donc $m - p \in N$, ce qui démontre que $m \in P+N$. On a ainsi $M = P+N$. Le sous-module P est bien un supplémentaire de N dans M. □

Remarque 2.9.8 (Décomposition primaire des modules de torsion)

Soit A un anneau principal. Fixons un ensemble $\mathscr{P}$ d'éléments irréductibles de A tels que tout élément irréductible de A soit égal au produit d'un élément inversible par un élément de $\mathscr{P}$.

Soit M un A-module de torsion. Pour tout élément irréductible $p \in \mathscr{P}$, soit M_p l'ensemble des $m \in M$ pour lesquels il existe $n \geqslant 0$ avec $p^n m = 0$; on l'appelle le *composant p-primaire* de M. Comme les idéaux (p), pour $p \in \mathscr{P}$, sont maximaux, ces sous-modules sont en somme directe d'après le théorème chinois. Soit $m \in M$ et soit a un élément non nul de A tel que $am = 0$. Le sous-module Am de M s'identifie à $A/(a)$; si $a = u\prod_{p\in\mathscr{P}} p^{n_p}$ est la décomposition en facteurs irréductibles de a, le lemme chinois entraîne

$$A/(a) \simeq \bigoplus_{p\in\mathscr{P}} A/(p^{n_p}),$$

ce qui entraîne que m appartient à la somme des M_p.

On a donc $M = \bigoplus_{p\in\mathscr{P}} M_p$, décomposition qu'on appelle la *décomposition primaire de M*.

Soit M un A-module de type fini et supposons que M soit de torsion. Chacun des sous-modules M_p est un A-module de type fini, annulé par une puissance de p ; ses facteurs invariants sont de la forme $(p^{n_1},\dots,p^{n_s})$, où $n_1 \leqslant \cdots \leqslant n_s$ sont des entiers strictement positifs. La détermination des facteurs invariants des M_p entraîne la détermination des M_p, donc de M, et réciproquement.

Exercices. — 50) Soit A un anneau principal et L un A-module libre de rang fini. Soit M un sous-$\mathbf{Z}$-module de L. Montrer qu'il possède un supplémentaire dans L si et seulement si L/M est sans-torsion.

51) Soit M un module libre de type fini sur un anneau principal A.
a) Soit $m \in M$ non nul. Montrer que les propriétés suivantes sont équivalentes :

a) m fait partie d'une base ;
b) il existe $f \in M^*$ tel que $f(m) = 1$;
c) les coordonnées de m dans *toute* base de M sont premières entre elles ;
d) les coordonnées de m dans *une* base de M sont premières entre elles ;
e) si $m = am'$ avec $a \in A$, alors $a \in A^\times$;
f) si $am = a'm'$ avec $a \in A$, $a' \in A$ et $a \neq 0$, alors a est multiple de a'.

On dit qu'un tel vecteur est primitif.
b) Montrer que tout vecteur est multiple d'un vecteur primitif.
c) *Exemple :* $A = \mathbf{Z}$, $M = \mathbf{Z}^4$, $m = (126, 210, 168, 504)$.

52) Soit A un anneau principal et M un A-module de type fini. On note $(d_1, \dots, d_r)$ les facteurs invariants de M.
Montrer que toute famille génératrice d'éléments de M a au moins r éléments.

53) Soit A un anneau principal et L, M deux A-modules de type fini. Montrer que $\mathrm{Hom}_A(L, M)$ est un A-module de type fini.

54) Soit A un anneau principal, soit M un A-module de type fini dont on note $(d_1, \dots, d_n)$ les facteurs invariants, les d_i étant des éléments non inversibles de A tels que d_i divise d_{i+1} pour $1 \leqslant i < n$.
a) Soit m un élément de M. Pour que le sous-module Am engendré par m dans M admette un supplémentaire, il suffit que l'annulateur de m soit égal à (d_n).
b) Lorsque $A = \mathbf{Z}$ et $M = (\mathbf{Z}/p\mathbf{Z}) \oplus (\mathbf{Z}/p^2\mathbf{Z})$, donner une condition nécessaire et suffisante sur un élément $m \in M$ pour que le sous-module Am possède un supplémentaire dans M.

55) Soit $q(x, y) = ax^2 + bxy + cy^2$ une forme quadratique définie positive à coefficients réels.
a) Montrer qu'il existe un élément e_1 de $\mathbf{Z}^2$ tel que $m = q(e_1)$ soit minimal.
b) Montrer qu'il existe un élément e_2 de $\mathbf{Z}^2$ tel que (e_1, e_2) soit une base de $\mathbf{Z}^2$.
c) En écrivant $q(e_2 + ne_1) \geqslant q(e_1)$, montrer que $m \leqslant 2\sqrt{(ac - b^2)/3}$.

56) Les résultats de cet exercice étendent partiellement les énoncés du lemme **??** et de la proposition 2.9.1. S'inspirer de leurs démonstrations pour les résoudre.
a) Soit A un anneau, soit M un A-module (à gauche) et soit N un sous-module de M. Si N et M/N sont de type fini, montrer que M est de type fini. Plus précisément, si N et M/N possèdent des parties génératrices de cardinaux r et s respectivement, montrer que M possède une partie génératrice de cardinal $r + s$.
b) Soit A un anneau tel que tout idéal à gauche de A soit de type fini. Montrer par récurrence sur n que tout sous-module de A_s^n est de type fini.
c) Plus généralement, montrer que tout sous-module d'un A-module (à gauche) de type fini est de type fini.

57) Soit A un anneau commutatif et soit $I_1, \dots, I_n$ des idéaux de A, distincts de A, tels que $I_1 \subset I_2 \subset \cdots \subset I_n$. On pose $M = \bigoplus_{i=1}^n A/I_i$.

a) Soit $\mathfrak{m}$ un idéal maximal de A qui contient I_n. Munir le $A/\mathfrak{m}$-espace vectoriel $M \otimes A/\mathfrak{m}$ est de dimension n.

b) Montrer que toute famille génératrice de M a au moins n éléments.

58) Le but de cet exercice est de donner une autre démonstration du théorème 2.9.2, indépendante de considérations matricielles.

Soit A un anneau principal, soit M un A-module libre de rang fini et soit N un sous-module de M.

a) Montrer qu'il existe une forme linéaire f sur M pour laquelle l'idéal $I = f(N)$ de A soit maximal (c'est-à-dire qu'il n'existe pas $g \in M^\vee$ telle que $f(N) \subsetneq g(N)$). Soit d un générateur de I.

b) Si $N \neq 0$, montrer que f est surjective. On note alors M' le noyau de f et on pose $N' = N \cap M'$.

c) Montrer que pour toute forme linéaire f' sur M' et tout élément $m \in N'$, $f'(m)$ est multiple de d.

d) Démontrer le théorème 2.9.2 par récurrence sur le rang de M. (Appliquer la méthode utilisée pour prouver la prop. 2.9.1.)

§2.10. Application : Groupes abéliens de type fini

Pour nous, les deux exemples fondamentaux d'anneaux principaux sont $\mathbf{Z}$ et $k[X]$, k étant un corps commutatif. Ce paragraphe est consacré à expliciter ce qui se passe dans le cas de l'anneau $\mathbf{Z}$; le cas de l'anneau $k[X]$ fera l'objet du paragraphe suivant.

Rappelons qu'un $\mathbf{Z}$-module de type fini n'est rien d'autre qu'un groupe abélien fini. En outre, un idéal Il résulte alors du théorème des facteurs invariants le théorème suivant.

THÉORÈME 2.10.1. — *Si G est un groupe abélien de type fini, il existe un unique entier $r \geqslant 0$ et une unique famille $(d_1, \dots, d_s)$ de nombres entiers au moins égaux à 2 telle que d_i divise d_{i+1} pour $1 \leqslant i < s$, tels que*

$$G \simeq \mathbf{Z}^r \oplus (\mathbf{Z}/d_1\mathbf{Z}) \oplus \cdots \oplus (\mathbf{Z}/d_s\mathbf{Z}).$$

Ce résultat fournit une « forme normale » pour tout groupe abélien de type fini, permettant de décider de l'isomorphie de deux tels groupes.

Exemple 2.10.2. — Calculons les facteurs invariants des groupes abéliens $(\mathbf{Z}/3\mathbf{Z}) \oplus (\mathbf{Z}/5\mathbf{Z})$ et $(\mathbf{Z}/6\mathbf{Z}) \oplus (\mathbf{Z}/4\mathbf{Z})$.

Comme 3 et 5 sont premiers entre eux, $(\mathbf{Z}/3\mathbf{Z}) \oplus (\mathbf{Z}/5\mathbf{Z})$ est isomorphe à $\mathbf{Z}/15\mathbf{Z}$, d'après le lemme chinois. Ce groupe abélien n'a qu'un facteur invariant, égal à 15.

Les entiers 6 et 4 ne sont pas premiers entre eux, mais on a $6 = 2 \cdot 3$ et 2 et 3 sont premiers entre eux, d'où, toujours d'après le lemme chinois,

$$(\mathbf{Z}/6\mathbf{Z}) \oplus (\mathbf{Z}/4\mathbf{Z}) \simeq (\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/3\mathbf{Z}) \oplus (\mathbf{Z}/4\mathbf{Z}).$$

Il s'agit maintenant de regrouper les facteurs correspondant à des nombres premiers distincts, ce qu'on fait en commençant par les termes d'exposants maximaux. Comme 3 et 4 sont premiers entre eux, on peut les regrouper et

$$(\mathbf{Z}/6\mathbf{Z}) \oplus (\mathbf{Z}/4\mathbf{Z}) \simeq (\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/12\mathbf{Z})$$

groupe abélien dont les facteurs invariants sont $(2, 12)$.

Ce résultat permet aussi la détermination explicite de tous les groupes abéliens finis G de cardinal g donné : il suffit de déterminer toutes les familles d'entiers strictement positifs $(d_1, \dots, d_s)$ tels que d_i divise d_{i+1} pour $1 \leqslant i < s$ et tels que $g = d_1 \dots d_s$. Pour faire le calcul, il est commode en pratique d'écrire la décomposition primaire du groupe abélien G, c'est-à-dire d'écrire G comme produit de sous-groupes G_p annulés par une puissance d'un nombre premier et de déterminer les G_p.

Exemple 2.10.3. — Déterminons tous les groupes abéliens de cardinal 48. Comme $48 = 2^4 \times 3$, un tel groupe est produit d'un groupe de cardinal 16 et d'un groupe de cardinal 3. Ce dernier ne peut être que $\mathbf{Z}/3\mathbf{Z}$. Il reste à faire la liste des groupes abéliens de cardinal 16, donc à trouver les familles $(d_1, \dots, d_s)$ d'entiers au moins 2 telles que d_i divise d_{i+1} pour $1 \leqslant i < s$ et telles que $d_1 \dots d_s = 16$. Faisons-en la liste :

- $d_1 = 2$, $d_2 = 2$, $d_3 = 2$, $d_3 = 2$;
- $d_1 = 2$, $d_2 = 2$, $d_3 = 4$;
- $d_1 = 2$, $d_2 = 4$, mais alors d_3 serait au plus 2, ce cas ne se produit donc pas ;
- $d_1 = 2$, $d_2 = 8$;
- $d_1 = 4$, $d_2 = 4$;
- $d_1 = 8$, mais alors d_2 serait au plus 2, et ce cas ne se produit pas ;
- $d_1 = 16$.

Comme groupes abéliens de cardinal 16, il y a donc les 6 groupes suivants, deux à deux non isomorphes,

$$(\mathbf{Z}/2\mathbf{Z})^4, \quad (\mathbf{Z}/2\mathbf{Z})^2 \oplus (\mathbf{Z}/4\mathbf{Z}), \quad (\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/8\mathbf{Z}), \quad (\mathbf{Z}/4\mathbf{Z})^2, \quad (\mathbf{Z}/16\mathbf{Z}).$$

Les groupes abéliens de cardinal 48 sont les produits des groupes précédents avec $\mathbf{Z}/3\mathbf{Z}$; sous forme normale, ils s'écrivent

$$(\mathbf{Z}/2\mathbf{Z})^3 \oplus (\mathbf{Z}/6\mathbf{Z}), \quad (\mathbf{Z}/2\mathbf{Z})^2 \oplus (\mathbf{Z}/12\mathbf{Z}), \quad (\mathbf{Z}/4\mathbf{Z}) \oplus (\mathbf{Z}/12\mathbf{Z}), \quad (\mathbf{Z}/48\mathbf{Z}).$$

Exercices. — 59) On considère l'ensemble M des triplets $(x, y, z) \in \mathbf{Z}^3$ tels que $x + y + z$ est pair.

a) Montrer que M est un sous-$\mathbf{Z}$-module libre de type fini de $\mathbf{Z}^3$, de rang 3.

b) Donner une base de M sur $\mathbf{Z}$.

c) Montrer que $\mathbf{Z}^3/M$ est un $\mathbf{Z}$-module simple.

60) Soit L l'ensemble des $(x,y,z) \in \mathbf{Z}^3$ tels que

$$x-3y+2z \equiv 0 \pmod 4 \quad \text{et} \quad x+y+z \equiv 0 \pmod 6.$$

a) Montrer que L est un sous-$\mathbf{Z}$-module libre de $\mathbf{Z}^3$. Quel est son rang ? Montrer que $\mathbf{Z}^3/L$ est isomorphe à $(\mathbf{Z}/4\mathbf{Z}) \times (\mathbf{Z}/6\mathbf{Z})$.

b) Déterminer les facteurs invariants (d_1,d_2,d_3) de $L \subset \mathbf{Z}^3$ et calculer une base (e_1,e_2,e_3) de $\mathbf{Z}^3$ telle que (d_1e_1, d_2e_2, d_3e_3) soit une base de L.

61) a) Soit G un groupe abélien fini. Soit n le plus petit entier $\geqslant 1$ tel que $nG = 0$. Montrer qu'il existe $g \in G$ d'ordre n, c'est-à-dire tel que n est le plus petit entier $\geqslant 1$ tel que $ng = 0$.

b) Soit K un corps commutatif et soit G un sous-groupe fini de K^*. Montrer que G est cyclique.

En particulier, le groupe multiplicatif d'un corps fini est cyclique.

62) a) Soit G un groupe abélien fini (donc un $\mathbf{Z}$-module fini). Montrer qu'il existe un élément de G dont l'ordre est multiple de l'ordre de tout élément de G.

b) Déterminer tous les groupes abéliens finis d'ordre 16.

§2.11. Application : Endomorphismes d'un espace vectoriel de dimension finie

Soit k un corps. On va s'intéresser maintenant aux $k[X]$-modules qui sont des k-espaces vectoriels de dimension finie. Pour commencer, rappelons quelques résultats de l'exercice 5. Soit V un k-espace vectoriel et u un endomorphisme de V. On définit alors une structure de $k[X]$-module sur V en posant pour tout polynôme $P \in k[X]$ et tout $v \in V$, $P \cdot v = P(u)(v)$. Si $P = \sum_{n=0}^{d} a_n X^n$, on a ainsi

$$P \cdot v = \sum_{n=0}^{d} a_n u^n(v).$$

On note V_u le $k[X]$-module ainsi obtenu ; l'homomorphisme canonique de $k[X]$ dans $\mathrm{End}(V)$ qui définit cette structure de $k[X]$-module est ainsi donnée par $P \mapsto P(u)$: la théorie que nous allons développer maintenant est une façon sophistiquée et efficace de parler de polynômes d'endomorphismes.

Si V' est un autre k-espace vectoriel et u' un endormorphisme de V', un homomorphisme (de $k[X]$-modules) de V_u dans $V'_{u'}$ est la donnée d'une application k-linéaire $f : V \to V'$ telle que $f \circ u = u' \circ f$.

En particulier, si $V' = V$, les $k[X]$-modules V_u et $V_{u'}$ sont isomorphes si et seulement si il existe $f \in \mathrm{GL}(V)$ telle que $u = f^{-1}u'f$, c'est-à-dire si les endomorphismes u et u' sont *conjugués*. (En termes de matrices, on dit *semblables*.)

DÉFINITION 2.11.1. — *Un $k[X]$-module M est dit cyclique s'il existe un polynôme $P \in k[X]$ non nul tel que $M \simeq k[X]/(P)$.*

LEMME 2.11.2. — *Si V est un k-espace vectoriel, u un endormorphisme de V, le $k[X]$-module V_u est cyclique si et seulement si il existe un vecteur $v \in V$ et un entier $n \geqslant 1$ tels que la famille $(v, u(v), \dots, u^{n-1}(v))$ soit une base de V.*

Démonstration. — Commençons la démonstration par une remarque. Si P est un polynôme non nul, le $k[X]$-module cyclique $k[X]/(P)$ est de dimension finie comme k-espace vectoriel, dimension d'ailleurs égale au degré de P. De plus, si $n = \deg P$, les éléments $\mathrm{cl}(1)$, $\mathrm{cl}(X)$, …, $\mathrm{cl}(X^{n-1})$ en forment une base.

Soit maintenant V un k-espace vectoriel et u un endormorphisme de V. Si V_u est cyclique, l'image de X par un isomorphisme $k[X]/(P) \simeq V_u$ est un élément v de V tel que $(v, u(v), \dots, u^{n-1}(v))$ soit une base de V. Réciproquement, si $v \in V$ est un vecteur tel que la famille $(v, u(v), \dots, u^{n-1}(v))$ soit une base de V, écrivons $u^n(v) = \sum_{p=0}^{n-1} a_p u^p(v)$ dans cette base. Alors l'homomorphisme $\varphi\colon k[X] \to V$, $P \mapsto P(u)(v)$ est surjectif et un polynôme P est dans le noyau si et seulement s'il est multiple du polynôme $\Pi = (X^n - \sum_{p=0}^{n-1} a_p X^p)$. En effet, la division euclidienne de P par Π est un polynôme R de degré $< n$. Si $R \neq 0$ mais si son image par φ est nul, on obtient une relation de dépendance linéaire non triviale entre $(v, \dots, u^{n-1}(v))$, ce qui est absurde. □

Remarque 2.11.3. — Si V_u est un endomorphisme cyclique, la matrice de u dans la base $(v, \dots, u^{n-1}(v))$ est égale à

$$\begin{pmatrix} 0 & & & & a_0 \\ 1 & 0 & & & a_1 \\ & \ddots & \ddots & & \vdots \\ & & 1 & 0 & a_{n-1} \end{pmatrix},$$

c'est-à-dire à la matrice compagnon C_Π du polynôme $\Pi = X^n - a_{n-1}X^{n-1} - \cdots - a_1 X - a_0$. De plus, Π est le polynôme minimal et le polynôme caractéristique de cette matrice.

Les rappels qui précèdent et le corollaire 2.9.3 établissent le théorème suivant.

THÉORÈME 2.11.4. — *Soit k un corps. Soit V un k-espace vectoriel de dimension finie et u un endomorphisme de V. Il existe alors une unique famille $(P_1, \dots, P_r)$ de polynômes unitaires (non constants) dans $k[X]$ tels que P_i divise P_{i+1} pour $1 \leqslant i < r$ et tels que la matrice de u soit semblable à la matrice diagonale par blocs*

$$\begin{pmatrix} C_{P_1} & & & \\ & C_{P_2} & & \\ & & \ddots & \\ & & & C_{P_r} \end{pmatrix}.$$

Les polynômes $(P_1, \dots, P_r)$ sont appelés facteurs invariants de l'endomorphisme u. On constate sur l'expression matricielle ci-dessus P_r est le polynôme minimal de u, tandis que $P_1 \dots P_r$ est son polynôme caractéristique.

COROLLAIRE 2.11.5. — *En particulier deux endomorphismes u et u' sont semblables si et seulement s'ils ont même famille de facteurs invariants.*

Toute la théorie qui précède a un corollaire amusant, facile, mais non trivial si l'on tient à éviter la théorie des facteurs invariants.

COROLLAIRE 2.11.6. — *Soit K un corps et $k \subset K$ un sous-corps. Soit A et B deux matrices de $\mathrm{Mat}_n(k)$ qui soient semblables en tant que matrices de $\mathrm{Mat}_n(K)$, c'est-à-dire qu'il existe $P \in \mathrm{GL}_n(K)$ telle que $B = P^{-1}AP$. Alors, A et B sont semblables sur k : il existe Q dans $\mathrm{GL}_n(k)$ telle que $B = Q^{-1}AQ$.*

Démonstration. — Notons $(P_1, \dots, P_r)$ la famille des facteurs invariants de A en tant que matrice à coefficients dans k. Il existe donc une base de $V = k^n$ dans laquelle la matrice de A est une diagonale-blocs de matrices compagnons de polynômes caractéristiques $(P_1, \dots, P_r)$. La même matrice de changement de base fournit une base de K^n dans laquelle la matrice de A est la même diagonale par blocs. En particulier, les facteurs invariants de A en tant que matrice à coefficients dans K sont aussi les P_i.

Soit maintenant $(Q_1, \dots, Q_s)$ la famille des facteurs invariants de B en tant que matrice à coefficients dans k, ou dans K, puisque c'est la même chose. Puisque A et B sont semblables en tant que matrices à coefficients dans K, on a les égalités $r = s$ et $P_1 = Q_1$, …, $P_r = Q_r$. Par suite, A et B sont semblables en tant que matrices à coefficients dans k. □

THÉORÈME 2.11.7 (Décomposition de Jordan). — *Soit k un corps algébriquement clos. Soit V un k-espace vectoriel de dimension finie et u un endomorphisme de V. Montrer que V possède une base dans laquelle la matrice de u est diagonale par blocs, chaque bloc étant un « bloc de Jordan » de la forme*

$$J_n(\lambda) = \begin{pmatrix} \lambda & 1 & & 0 \\ & \lambda & \ddots & \\ & & \ddots & 1 \\ 0 & & & \lambda \end{pmatrix} \in \mathrm{Mat}_n(k),$$

où λ est une valeur propre de u. En outre, pour que deux endomorphismes u et u' soient semblables, il faut et il suffit que pour tout $\lambda \in k$, les tailles de leurs blocs de Jordan correspondant à λ coïncident.

Démonstration. — Commençons par écrire la décomposition primaire du module V_u. Comme k est algébriquement clos, les polynômes irréductibles unitaires sont les $X - \lambda$, pour $\lambda \in k$. Notons V_λ le sous-module $(X-\lambda)$-primaire de V_u ; c'est l'ensemble des $v \in V$ tels qu'il existe $n \in \mathbf{N}$ tel que $(X-\lambda)^n \cdot v = 0$, c'est-à-dire $(u - \lambda\,\mathrm{id})^n(v) = 0$. Autrement dit, V_λ est le sous-espace caractéristique de u pour la valeur propre λ. (Il est nul si

et seulement si λ n'est pas une valeur propre. Notons aussi que V_λ est un sous-$k[X]$-module de V_u, ce qui équivaut au fait classique que les sous-espaces caractéristiques de u sont stables par u.)

Le $k[X]$-module correspondant à la matrice de Jordan $J_n(\lambda)$ est isomorphe à $k[X]/(X-\lambda)^n$. Par suite, dire que le sous-module V_λ de V est isomorphe comme $k[X]$-module à

$$\bigoplus_{i=1}^{s} k[X]/((X-\lambda)^{n_i}),$$

pour des entiers $n_1,\dots,n_s$ équivaut à dire que la restriction à V_λ de u est isomorphe à la somme de blocs de Jordan de tailles $n_1,\dots,n_s$. De plus, les polynômes $(X-\lambda)^{n_i}$ (ordonnés par degrés croissants) sont les facteurs invariants de V_λ. Cela démontre l'existence de la décomposition de Jordan. Comme deux endomorphismes sont conjugués si et seulement si les $k[X]$-modules associés sont isomorphes, cela démontre aussi l'unicité des tailles des blocs de Jordan dans une décomposition, ainsi que le fait que deux endomorphismes sont semblables si et seulement si pour tout λ, les tailles des blocs de Jordan associés à λ coïncident. □

Nous allons utiliser la proposition 2.8.8 pour calculer les facteurs invariants d'une matrice.

PROPOSITION 2.11.8. — *Soit k un corps et soit A une matrice de $M_n(k)$. Pour tout entier r compris entre 1 et n, soit $\Delta_r \in k[X]$ le pgcd (unitaire) des mineurs d'ordre r de la matrice $X\mathrm{I}_n - A$. Alors, il existe des polynômes unitaires $P_1,\dots,P_n$ dans $k[X]$ tels que*

$$P_1 = \Delta_1, \quad P_1P_2 = \Delta_2, \quad \dots, P_1\dots P_n = \Delta_n.$$

Pour tout entier r tel que $1 \leqslant r < n$, P_r divise P_{r+1} et si r est le plus petit entier tel que $P_r \neq 1$, les facteurs invariants de A sont les polynômes $(P_{r+1},\dots,P_n)$.

Démonstration. — Posons $A = k[X]$. Pour déduire cette proposition du corollaire 2.8.8, Il suffit de remarquer que, notant $(e_1,\dots,e_n)$ la base canonique de A^n, l'homomorphisme

$$\varphi\colon A^n \to A^n, \qquad e_i \mapsto Xe_i - u(e_i)$$

a pour matrice $X\mathrm{I}_n - A$ et que $(k^n)_A$ est isomorphe à $A^n/\operatorname{im}\varphi$. □

Exercices. — 63) Soit A un anneau principal et M un A-module de type fini.

a) Justifier l'existence d'éléments m_i (pour $1 \leqslant i \leqslant s$) de M d'annulateurs (d_i), avec $d_1|\dots|d_s$, tel que

$$M = \bigoplus_{i=1}^{s} Am_i.$$

b) Soit $i \in \{1,\dots,s\}$. Montrer qu'il existe $u_i \in \mathrm{End}_A(M)$ tel que

$$u_i(m_1) = \cdots = u_i(m_{s-1}) = 0, \quad u_i(m_s) = m_i.$$

c) Soit $u \in \mathrm{End}_A(M)$ qui commute à tout autre élément de $\mathrm{End}_A(M)$. Montrer qu'il existe $a \in A$ tel que $u(m) = am$ pour tout m.

d) Soit $u : M \to M$ une application additive telle que pour tout $v \in \mathrm{End}_A(M)$, $u \circ v = v \circ u$. Montrer que u est une homothétie $m \mapsto am$, pour $a \in A$.

e) Soit K un corps commutatif, E un K-espace vectoriel de dimension finie sur K et $u \in \mathrm{End}_K(E)$. Montrer que tout endomorphisme de E qui commute à tout endomorphisme commutant à u est un polynôme en u. (*On pourra utiliser la structure de $K[X]$-module sur E définie par u.*)

64) Soit k un corps.

a) Déterminer, à similitude près, toutes les matrices à coefficients dans k dont le polynôme caractéristique est $X^3(X-1)$.

b) Déterminer, à similitude près, toutes les matrices de $\mathrm{Mat}_4(k)$ dont le polynôme minimal est $X(X-1)$.

c) Déterminer, à similitude près, toutes les matrices de $\mathrm{Mat}_n(k)$ de polynôme minimal $X(X-1)$.

d) Déterminer, à similitude près, tous les endomorphismes u d'un espace vectoriel de dimension finie V tels que $(u-\mathrm{id})^2 = 0$.

§2.12. Modules et anneaux noethériens

PROPOSITION 2.12.1. — *Soit A un anneau et soit M un A-module. Les propriétés suivantes sont équivalentes :*

a) *tout sous-module de M est de type fini ;*
b) *toute suite croissante de sous-modules de M est stationnaire ;*
c) *toute famille de sous-modules de M admet un élément maximal.*

DÉFINITION 2.12.2. — *Un A-module qui vérifie les propriétés ci-dessus est dit* noethérien.

Si A est un A-module à gauche noethérien, on dit que A est un anneau noethérien à gauche. *Si A est un A-module à droite noethérien, on dit de même que A est un anneau* noethérien à droite.

Lorsque A est commutatif, on dit plus simplement noethérien.

Remarque 2.12.3. — Les sous-A-modules à gauche d'un anneau A sont ses idéaux à gauche. Ainsi, un anneau A est noethérien à gauche si et seulement si l'une des propriétés (équivalentes) ci-dessous est satisfaite :

a) tout idéal à gauche de A est de type fini ;
b) toute suite croissante d'idéaux à gauche de A est stationnaire.

En particulier, un anneau principal est noethérien, résultat qu'on avait déjà remarqué (lemme 1.9.6) pour démontrer qu'un anneau principal est factoriel.

Démonstration de la proposition. — *a*) Supposons que tout sous-module de M est de type fini et considérons une suite croissante $(M_n)_{n\in\mathbf{N}}$ de sous-modules de M. Soit $N = \bigcup M_n$ la réunion des M_n. Comme la réunion est croissante, N est un sous-module de M. Par hypothèse, il est de type fini : il existe une partie finie $S \subset N$ telle que $N = \langle S\rangle$. Pour tout $s \in S$, il existe un entier $n_s \in \mathbf{N}$ tel que $s \in M_n$ pour $n \geqslant n_s$. Posons $\nu = \max(n_s)$, de sorte que $S \subset M_\nu$. Par suite, $N = \langle S\rangle$ est contenu dans M_ν. Finalement, la suite d'inclusions $M_\nu \subset M_n \subset N \subset M_\nu$ pour $n \geqslant \nu$ montre que pour $n \geqslant \nu$, $M_n = M_\nu$. La suite est ainsi stationnaire.

b) Supposons que toute suite croissante de sous-modules de M est stationnaire et soit $(M_i)_{i\in I}$ une famille de sous-modules de M. Supposons par l'absurde qu'elle n'admette pas d'élément maximal. Choisissons $i_1 \in I$; ainsi, M_{i_1} n'est pas maximal dans la famille (M_i). Il existe alors $i_2 \in I$ tel que $M_{i_1} \subsetneq M_{i_2}$. Mais M_{i_2} n'est pas non plus maximal, d'où l'existence de $i_3 \in I$, etc. On obtient ainsi une suite strictement croissante de sous-modules de M,

$$M_{i_1} \subsetneq M_{i_2} \subsetneq \dots$$

et une telle suite n'étant par définition pas stationnaire, on a une contradiction. (*Cette partie de la démonstration n'a rien à voir avec les modules, elle est valide dans tout ensemble ordonné.*)

c) Supposons que toute famille de sous-modules de M admet un élément maximal et montrons que tout sous-module de M est de type fini. Soit ainsi N un sous-module de M et considérons l'ensemble $\mathscr{S}_N$ des sous-modules de N qui sont de type fini. Par hypothèse, il admet un élément maximal ; soit N' un tel sous-module. Par définition, $N' \subset N$, N' est de type fini et aucun sous-module de N qui contient strictement N' n'est de type fini. Supposons par l'absurde que $N' \neq N$. Il existe ainsi $m \in N \setminus N'$. Le sous-module $N'' = N' + Am$ de M est de type fini et est contenu dans N. Comme $m \notin N'$, $N'' \neq N'$. Par suite, $N'' \in \mathscr{S}_N$, ce qui est absurde, N' étant maximal dans $\mathscr{S}_N$. Donc $N' = N$ et N est de type fini. □

PROPOSITION 2.12.4. — *Soit A un anneau, soit M un A-module, N un sous-module de A. Alors, M est un A-module noethérien si et seulement si N et M/N sont des A-modules noethériens.*

Démonstration. — Supposons que M est un A-module noethérien. Comme tout sous-module de N est aussi un sous-module de M, tout sous-module de N est de type fini, donc N est noethérien. Si $\mathscr{P}$ est un sous-module de M/N, son image réciproque $\mathrm{cl}^{-1}(\mathscr{P})$ par l'homomorphisme canonique $\mathrm{cl}\colon M \to M/N$ est un sous-module de type fini de M. Comme $\mathscr{P} = \mathrm{cl}(\mathrm{cl}^{-1}(\mathscr{P}))$, $\mathscr{P}$ est l'image d'un module de type fini, donc est de type fini. Ainsi, M/N est noethérien.

Supposons que N et M/N sont des A-modules noethériens. Soit (P_n) une suite croissante de sous-modules de M. Posons $Q_n = P_n \cap N$. Par définition, les suites croissantes

$(\mathrm{cl}(P_n))$ et $(P_n \cap N)$ de sous-modules de M/N (resp. de N) sont stationnaires. Fixons donc ν tel que si $n \geqslant \nu$,

$$\mathrm{cl}(P_n) = \mathrm{cl}(P_\nu) \quad \text{et} \quad P_n \cap N = P_\nu \cap N.$$

Nous allons montrer que pour $n \geqslant \nu$, $P_n = P_\nu$, ce qui établira que la suite (P_n) est stationnaire.

Fixons donc $n \geqslant \nu$ et soit $p \in P_n$. On a $\mathrm{cl}(p) \in \mathrm{cl}(P_n) = \mathrm{cl}(P_\nu)$, si bien qu'il existe $p' \in P_\nu$ tel que $\mathrm{cl}(p) = \mathrm{cl}(p')$. Alors, $p - p'$ appartient à P_n et vérifie $\mathrm{cl}(p-p') = 0$, d'où $p - p' \in P_n \cap N$. Par suite, $p - p' \in P_\nu \cap N$ et $p = p' + (p - p')$ appartient à P_ν. Ainsi, $P_n \subset P_\nu$, d'où l'égalité. $\mathrm{cl}(P_n) = \mathrm{cl}(P_\nu)$ si $n \geqslant \nu$. □

COROLLAIRE 2.12.5. — *Si $M_1, \ldots, M_n$ sont des A-modules noethériens, $M_1 \oplus \cdots \oplus M_n$ est un A-module noethérien.*

COROLLAIRE 2.12.6. — *Soit A un anneau noethérien à gauche et soit n un entier naturel. Tout sous-module du A-module à gauche A^n est de type fini.*

PROPOSITION 2.12.7. — *Soit A un anneau commutatif et soit S une partie multiplicative de A. Si M est un A-module noethérien, $S^{-1}M$ est un $S^{-1}A$-module noethérien.*

Démonstration. — Soit $\mathscr{N}$ un sous-$S^{-1}A$-module de $S^{-1}M$. D'après la proposition 2.6.6, il existe un sous-module N de M tel que $\mathscr{N} = S^{-1}N$. Comme M est un A-module noethérien, N est de type fini et par suite, $\mathscr{N}$ est de type fini. Ainsi, $S^{-1}M$ est un $S^{-1}A$-module noethérien. □

COROLLAIRE 2.12.8. — *Soit A un anneau noethérien à gauche.*

Si I est un idéal bilatère de A, l'anneau quotient A/I est noethérien à gauche. Si A est commutatif et que S est une partie multiplicative de A, l'anneau localisé $S^{-1}A$ est noethérien.

Démonstration. — D'après la proposition 2.12.4, A/I est un A-module à gauche noethérien. Mais un sous-A-module à gauche de A/I n'est autre qu'un idéal à gauche de A/I. Par suite, A/I est un A/I-module à gauche noethérien. C'est donc un anneau noethérien à gauche.

Autre démonstration. — Soit $\mathscr{J}$ un idéal de A/I. Par la surjection canonique $\mathrm{cl}\colon A \to A/I$, il lui correspond un idéal $J = \mathrm{cl}^{-1}(\mathscr{J})$ de A qui contient I. Puisque A est un anneau noethérien, J est de type fini, $J = (a_1, \ldots, a_r)$. Alors, $\mathscr{J} = \mathrm{cl}(J) = (\mathrm{cl}(a_1), \ldots, \mathrm{cl}(a_r))$ est de type fini.

D'après la proposition 2.12.7, $S^{-1}A$ est un $S^{-1}A$-module noethérien. Par définition, c'est donc un anneau noethérien. □

Le théorème suivant a été démontré par D. Hilbert lorsque $A = \mathbf{Z}$.

THÉORÈME 2.12.9 (Hilbert). — *Si A est un anneau (disons commutatif) noethérien, l'anneau $A[X]$ est noethérien.*

Démonstration. — Soit I un idéal de $A[X]$. Si $n \geqslant 0$, soit I_n l'ensemble des coefficients du terme de degré n des polynômes de I qui sont de degré $\leqslant n$. Alors, I_n est un idéal de A. En effet, si x et $y \in I_n$, il existe P et Q dans I de degrés $\leqslant n$ dont les coefficients de X^n sont x et y respectivement. Alors, si a et $b \in A$, le coefficient de X^n dans le polynôme $aP + bQ$ est $ax + by$, et $aP + bQ$ est un polynôme de O de degré $\leqslant n$. De plus, comme le polynôme nul appartient à I, $0 \in I_n$.

Remarquons que la suite (I_n) est stationnaire : si $P \in I$ est de degré $\leqslant n$, $XP \in I$ est de degré $\leqslant n+1$ le coefficient de X^{n+1} dans XP est celui de X^n dans P. Ainsi, $I_n \subset I_{n+1}$.

Comme A est noethérien, la suite $(I_n)_n$ est stationnaire. Soit $\nu \in \mathbf{N}$ tel que $I_n = I_\nu$ pour $n \geqslant \nu$.

Les idéaux I_n pour $n \leqslant \nu$ sont de type fini. Choisissons ainsi pour $n \leqslant \nu$ une famille finie de polynômes $(P_{n,1}, \ldots, P_{n,r(n)})$ dans I, de degrés n, dont les coefficients $a_{n,j}$ dominants engendrent I_n.

Soit $J \subset A[X]$ l'idéal engendré par les P_{nj} pour $0 \leqslant n \leqslant \nu$ et $1 \leqslant j \leqslant r(n)$.

On a $J \subset I$ et nous allons montrer par récurrence sur le degré d'un élément de I que $I = J$.

Un polynôme $P \in I$ de degré $\leqslant 0$ est constant et appartient à I_0. Il appartient ainsi à J. Supposons que tout polynôme de I de degré $< n$ appartient à J et soit $P \in I$ de degré n.

Soit a son coefficient dominant. Posons $m = \min(n, \nu)$, de sorte que $a \in I_m$. Ainsi, il existe des éléments $c_{m,j} \in A$ tels que $a = \sum_j c_{m,j} a_{m,j}$. Le polynôme $Q = P - X^{n-m} \sum_j c_{m,j} P_{m,j}$ est alors de degré $\leqslant n$ mais le coefficient du terme en X^n est nul. Donc $\deg Q < n$. De plus, $Q \in I$. Par récurrence, $Q \in J$. Finalement, $P \in I$.

Par récurrence, $I = J$ est un idéal de type fini de $A[X]$. Comme I était arbitraire, $A[X]$ est un anneau noethérien. □

COROLLAIRE 2.12.10. — *Si A est un anneau (commutatif) noethérien et si n est un entier, $A[X_1, \ldots, X_n]$ est un anneau noethérien.*

En particulier, si k est un corps, $k[X_1, \ldots, X_n]$ est un anneau noethérien.

COROLLAIRE 2.12.11. — *Soit A et B des anneaux commutatifs. On suppose que A est un anneau noethérien et que B est une A-algèbre de type fini. Alors B est un anneau noethérien.*

Démonstration. — Par hypothèse, il existe des éléments $b_1, \ldots, b_n \in B$ qui engendrent B comme A-algèbre. L'homomorphisme canonique $A[X_1, \ldots, X_n] \to B$ qui applique X_i sur b_i est alors surjectif, de sorte que B est un quotient de l'anneau noethérien $A[X_1, \ldots, X_n]$. Par suite, B est un anneau noethérien. □

THÉORÈME 2.12.12 (Hilbert, 1893). — *Soit k un corps et soit A une k-algèbre (commutative) de type fini et G un groupe fini d'automorphismes de A. Alors, l'ensemble A^G des $a \in A$ tels que pour tout $g \in G$, $g(a) = a$, est une sous-k-algèbre de type fini de A.*

Dans le cas où $A = k[X_1, \dots, X_n]$, A^G est l'ensemble des polynômes « invariants » par le groupe G. Le théorème de Hilbert affirme que ces invariants peuvent s'exprimer comme des polynômes en un nombre fini d'entre eux. Supposons par exemple que G soit le groupe symétrique $\mathfrak{S}_n$, agissant sur $k[X_1, \dots, X_n]$ par permutation des indéterminées (pour $\sigma \in \mathfrak{S}_n$, u_σ est l'automorphisme de $k[X_1, \dots, X_n]$ tel que $u_\sigma(X_i) = X_{\sigma(i)}$). Alors, A^G est l'algèbre des polynômes symétriques ; elle est engendrée par les polynômes symétriques élémentaires $S_1, \dots, S_n$, donnés par

$$S_k = \sum_{i_1 < \cdots < i_k} X_{i_1} \dots X_{i_k}, \quad \text{pour } 1 \leqslant k \leqslant n.$$

(Par exemple, $S_1 = X_1 + \cdots + X_n$ et $S_n = X_1 \dots X_n$.) C'est pour démontrer ce théorème que Hilbert a introduit la notion d'anneau noethérien et démontré que les anneaux de polynômes sur un corps sont noethériens !

La démonstration du théorème 2.12.12 se fait en trois étapes.

LEMME 2.12.13. — *A^G est une sous-k-algèbre de A.*

Démonstration. — Il faut démontrer que

- si a et b sont dans A^G, $a + b$, et ab aussi ;
- si a appartient à A^G et $\lambda \in k$, λa aussi.

Or, si $g \in G$, g est un automorphisme de k-algèbres de A, donc $g(a + b) = g(a) + g(b) = a + b$, et $g(ab) = g(a)g(b) = ab$, si bien que $a + b$ et ab appartiennent à A^G. De plus, $g(\lambda a) = \lambda g(a) = \lambda a$, si bien que $\lambda a \in A^G$. □

LEMME 2.12.14. — *Sous les hypothèses du théorème 2.12.12, A est un A^G-module de type fini.*

Démonstration. — Comme A est une k-algèbre de type fini, on peut choisir des éléments $a_1, \dots, a_r \in A$ tels que $A = k[a_1, \dots, a_r]$.

Fixons $i \in \{1; \dots; r\}$ et considérons le polynôme de $A[X]$,

$$P_i(X) = \prod_{g \in G} (X - g(a_i)).$$

Par suite, si $h \in G$,

$$h(P_i(X)) = \prod_{g \in G} (X - h(g(a_i))) = \prod_{g \in G} (X - g(a_i)) = P_i(X)$$

et les coefficients de P_i sont invariants par h. Ainsi, P_i est à coefficients dans A^G. Écrivons ainsi

$$P_i(X) = X^n + b_1 X^{n-1} + \cdots + b_n$$

où les b_j appartiennent à A^G. Comme $P_i(a_i) = 0$, il en résulte que, notant N le cardinal de G, a_i^N appartient au sous-A^G-module de A engendré par $1, \ldots, a_i^{N-1}$.

Montrons maintenant que A est engendré comme A^G-module par les N^r produits $\prod_{i=1}^r a_i^{n_i}$, où pour tout i, $0 \leqslant n_i \leqslant N-1$. Notons A' le sous-module engendré par ces éléments. Comme A est engendré comme k-module (donc *a fortiori* comme A^G-module) par tous les produits $\prod_{i=1}^r a_i^{n_i}$ avec $n_i \geqslant 0$, il suffit de montrer qu'un tel produit appartient à A'. Soit ainsi $X^{n_i} = Q_i(X)P_i(X) + R_i(X)$ la division euclidienne dans $A^G[X]$ de X^{n_i} par P_i, de sorte que R_i est un polynôme à coefficients dans A^G de degré $< N$. On a donc, en évaluant en $X = a_i$, $a_i^{n_i} = R_i(a_i)$, puis

$$\prod_{i=1}^r a_i^{n_i} = \prod_{i=1}^r R_i(a_i).$$

Si l'on développe cette dernière expression, on constate qu'elle appartient à A'. □

LEMME 2.12.15 (Artin–Tate). — *Soit $k \subset B \subset A$ trois anneaux. On suppose que k est un anneau noethérien, que A est une k-algèbre de type fini et un A-module de type fini. Alors, B est une k-algèbre de type fini.*

Démonstration. — Soit $(x_1, \ldots, x_r)$ une famille finie de générateurs de A comme k-algèbre et $(a_1, \ldots, a_n)$ une famille finie de générateurs de A comme B-module. Ainsi, tout élément de A s'écrit comme un polynôme en les x_i et comme combinaison linéaire des a_j. Appliquant cette remarque aux x_i et aux produits $x_i x_j$, il existe en particulier des éléments $\lambda_{i\ell}$ et $\mu_{ij\ell}$ dans B tels que pour tout $1 \leqslant i \leqslant r$, que $x_i = \sum_{\ell=1}^n \lambda_{i\ell} a_\ell$, et pour tous $1 \leqslant i, j \leqslant r$, $a_i a_j = \sum_{\ell=1}^n \mu_{ij\ell} a_\ell$.

Soit B_0 la sous-k-algèbre de B engendrée par les $\lambda_{i\ell}$ et les $\mu_{ij\ell}$. C'est une k-algèbre de type fini, donc un anneau noethérien.

Soit alors A_0 le sous-B_0-module de A engendré par les a_ℓ. Remarquons que A_0 est une k-algèbre. En effet, puisque les produits $a_i a_j$ sont par construction dans A_0, A_0 est stable par multiplication. Toujours par construction, les x_i appartiennent à A_0. Ainsi, $A_0 = A$ et A est un B_0-module de type fini. Comme B_0 est un anneau noethérien, A est un B_0-module noethérien.

Par suite, tout sous-B_0-module de A est de type fini. En particulier, B est un B_0-module de type fini, et donc *a fortiori*, une B_0-algèbre de type fini.

Comme B_0 est une k-algèbre de type fini, B est aussi une k-algèbre de type fini. Le lemme est démontré. □

Exercices. — 65) [*Lemme de Nakayama*] Soit M un A-module (à gauche) de type fini et soit I un idéal à gauche de A.

a) On suppose que $M = IM$. Montrer par récurrence sur le nombre de générateurs de M qu'il existe $a \in I$ tel que $(1+a)M = 0$.

b) On suppose que I est contenu dans tout idéal maximal de A. Soit N un sous-module de M tel que $M = N + IM$. Montrer que $M = N$.

c) [Autre démonstration lorsque A est commutatif.] Soit $(m_1, \ldots, m_r)$ une famille de r éléments qui engendre M. Soit a_{ij} pour $1 \leqslant i, j \leqslant r$ des éléments de I tels que $m_i = \sum_{j=1}^{r} a_{ij} m_j$ pour tout i et soit A la matrice (a_{ij}). Si B est la matrice des cofacteurs de $I_r - A$, montrer que $\det(B)$ est un élément de $1 + I$ qui annule M.

66) Soit A un anneau commutatif, soit M un A-module de type fini et soit u un endomorphisme surjectif de M.

a) Soit M_u le $A[X]$-module défini par M et l'endomorphisme u, de sorte que $P \cdot m = P(u)(m)$ pour $P \in A[X]$ et $m \in M$. Montrer que $M_u = (X) \cdot M_u$.

b) Utiliser le lemme de Nakayama pour démontrer que u est un isomorphisme.

67) Soit A un anneau, M un A-module de type fini et $\varphi : M \longrightarrow A^n$ un morphisme surjectif de A-modules.

a) Montrer que φ admet un inverse à droite.

b) Montrer que $M \simeq \ker\varphi \oplus \operatorname{im}\psi$.

c) Montrer que $\ker\varphi$ est de type fini.

68) Soit A un anneau, M un A-module, N un A-module de type fini et $u : M \longrightarrow N$ un homomorphisme de A-modules. Soit $\mathfrak{R}$ le radical de Jacobson de A (intersection de tous les idéaux maximaux).

a) Montrer que u induit un homomorphisme $v : M/\mathfrak{R} \cdot M \longrightarrow N/\mathfrak{R} \cdot N$.

b) Remarquer que si I est un idéal de A et si $N' \subset M'$ sont deux A-modules alors $I \cdot (M'/N') = (I \cdot M' + N')/N'$.

c) On suppose que v est surjectif. Calculer $\operatorname{im}(u) + \mathfrak{R}N$ et en déduire que u est surjectif.

69) Soit A un anneau et I un idéal de type fini de A tel que $I = I^2$. Montrer qu'il existe $e \in A$ tel que $e^2 = e$ et $I = (e)$. (*Utiliser le lemme de Nakayama pour trouver $a \in I$ tel que* $(1+a)I = 0$.)

70) Soit A un anneau. Si $A[X]$ est noethérien, A est-il nécessairement noethérien ?

71) Soit $\mathscr{E}$ une partie de $\mathbf{C}[X_1, \ldots, X_n]$ et $\mathscr{V}$ l'ensemble des n-uplets $(x_1, \ldots, x_n) \in \mathbf{C}^n$ tels que pour tout $P \in \mathscr{E}$, $P(x_1, \ldots, x_n) = 0$. Montrer qu'il existe une partie finie $\{P_1, \ldots, P_r\} \subset \mathscr{E}$ telle que $\mathscr{V}$ soit défini par les équations $P_i(x_1, \ldots, x_n) = 0$ (pour $1 \leqslant i \leqslant r$).

72) Soit A un anneau et $I_1 \subset I_2 \subset \ldots$ une suite croissante d'idéaux de type fini. Soit $I = \bigcup I_n$. Montrer que I est de type fini si et seulement si la suite (I_n) est stationnaire.

73) Soit A un anneau et I, J deux idéaux de A tels que $I \cap J = (0)$. Montrer que A est noethérien si et seulement si A/I et A/J sont noethériens.

74) [*Exemples d'anneaux non noethériens*] Montrer que les anneaux suivants ne sont pas noethériens.

a) $k[X_1, X_2, \ldots, X_n, \ldots]$;

b) $\mathscr{C}^0(\mathbf{R}, \mathbf{R})$;

c) $\mathscr{C}^\infty(\mathbf{R}, \mathbf{R})$. Montrer néanmoins que l'idéal des fonctions nulles en l'origine est principal.

d) le sous-module de $\mathbf{C}[X, Y]$ engendré par $\mathbf{C}$ et l'idéal (X) est un sous-anneau de $\mathbf{C}[X, Y]$. Il n'est pas noethérien.

75) Soit $\mathscr{F}$ l'ensemble des polynômes $P \in \mathbf{Q}[X]$ tel que pour tout $n \in \mathbf{Z}$, $P(n) \in \mathbf{Z}$.

a) Montrer que $\mathscr{F}$ est une sous $\mathbf{Z}$-algèbre de $\mathbf{Q}[X]$.

b) Montrer qu'une fonction $P : \mathbf{Z} \to \mathbf{Z}$ appartient à $\mathscr{F}$ si et seulement si $P(0) \in \mathbf{Z}$ et la fonction $n \mapsto P(n+1) - P(n) \in \mathscr{F}$.

c) Montrer que les polynômes 1, X, $X(X-1)/2$, …, $X(X-1)\ldots(X-p+1)/p!$, … forment une base de $\mathscr{F}$ comme $\mathbf{Z}$-module.

d) Montrer que $\mathscr{F}$ n'est pas noethérien.

76) Soit M un A-module noethérien et $I = (0 : M)$ l'annulateur de M dans A.

Montrer que A/I est un anneau noethérien.

77) Soit M un A-module noethérien et $\varphi : M \to M$ un endomorphisme de M. Montrer qu'il existe un entier $n \geqslant 1$ tel que

$$\ker \varphi^n \cap \operatorname{im} \varphi^n = (0).$$

78) Soit A un anneau et M un A-module de type fini. On définit pour tout idéal maximal $\mathfrak{m}$ de A,

$$d(\mathfrak{m}) = \dim_{A/\mathfrak{m}} M/\mathfrak{m}M.$$

a) Soit $\mathfrak{m}$ un idéal maximal de M, $d = d(\mathfrak{m})$. Montrer qu'il existe $a \in A \setminus \mathfrak{m}$ tel que si $S = \{1, a, a^2, \ldots\}$, $S^{-1}M$ soit engendré par d éléments.

b) Si $\mathfrak{m}'$ est un idéal maximal de A ne contenant pas a, montrer que $d(\mathfrak{m}') \leqslant d$.

APPENDICE

§A.1. Le théorème de Cantor-Bernstein

Il s'agit du résultat de théorie des ensembles suivant, évident lorsque les ensembles concernés sont finis.

THÉORÈME A.1.1. — *Soit A et B des ensembles. S'il existe une injection de A dans B, ainsi qu'une injection de B dans A, les ensembles A et B sont équipotents.*

Démonstration. — Notons $f^{-1}\colon f(A) \to A$ et $g^{-1}\colon g(B) \to B$ les applications réciproques de f et g, là où elles sont définies. L'idée de la démonstration consiste à itérer f^{-1} et g^{-1} aux éléments de B et de A, aussi longtemps que possible. Pour tout entier n, notons ainsi A_p l'ensemble des éléments de A de la forme $gfgf\dots f(b)$, où $b \notin f(A)$, A_i l'ensemble des éléments de A de la forme $gfgfgf\dots g(a)$, où $a \notin g(B)$; l'ensemble A_p est donc constitué des éléments de A où l'on peut itérer un nombre pair de fois f^{-1} et g^{-1}, l'ensemble A_i de ceux où l'on peut itérer un nombre impair de fois. Notons A_∞ le complémentaire de la réunion des A_n. Définissons de manière analogue des ensembles B_p, B_i et B_∞.

Par construction, l'application f induit une bijection de A_p sur B_i, ainsi qu'une bijection de A_∞ sur B_∞. L'application g induit une bijection de B_p sur A_i.

L'application $h\colon A \to B$ qui coïncide avec f sur $A_p \cup A_\infty$ et avec g^{-1} sur A_i est une bijection. Cela conclut la démonstration du théorème. □

§A.2. Le lemme de Zorn

Rappelons qu'un ordre $\prec$ sur un ensemble S est une relation vérifiant les axiomes suivants :

- les assertions $x \prec y$ et $y \prec x$ sont incompatibles ;
- si $x \prec y$ et $y \prec z$, alors $x \prec z$.

Un ensemble ordonné est un ensemble muni d'un ordre. Si pour tout couple (x, y) d'éléments de S, on a $x \prec y$, ou $y \prec x$, ou $x = y$, on dit que S est totalement ordonné.

Une *section commençante* d'un ensemble ordonné S est une partie C telle que pour tout $x \in C$ et tout $y \in S$ tel que $y \prec x$, on a $y \in S$.

Si A est une partie d'un ensemble ordonné S, un *majorant* de A est un élément $s \in S$ tel que $a \prec s$ pour tout $a \in A$; une partie qui possède un majorant est dite *majorée*. On dit qu'un élément $a \in A$ est un *élément maximal* de A si la relation $a \prec x$ n'est vérifiée pour aucun élément x de A. Une partie peut être majorant sans posséder un élément maximal, et un élément maximal n'est pas forcément un majorant, à moins que la partie ne soit totalement ordonnée.

On dit qu'un ordre sur S est un *bon ordre*, ou que S est *bien ordonné* si toute partie non vide admet un plus petit élément. Un ensemble bien ordonné possède un plus petit élément, donc est en particulier minoré. De plus, un ensemble bien ordonné S est totalement ordonné (si x et y sont des éléments de S, le plus petit élément de $\{x, y\}$ est plus petit que l'autre).

L'ensemble des entiers naturels, muni tant de l'ordre habituel, que de l'ordre donné par la divisibilité, est bien ordonné. Par contre, l'ensemble des nombres réels positifs ou nuls ne l'est pas, pas plus que l'ensemble des nombres relatifs positifs ou nuls : dans les deux cas, l'ensemble des éléments x tels que $x > 1$ n'a pas de plus petit élément.

Supposons que S soit bien ordonné et soit A une section commençante de S. Si $A \neq S$, soit a le plus petit élément de $\complement A$; alors, $A = \{x \in S\,;\, x \prec a\}$.

Nous supposons l'axiome du choix, à savoir que pour toute famille $(S_i)_{i\in I}$ d'ensembles non vides, le produit $\prod S_i$ n'est pas vide.

THÉORÈME A.2.1 (Lemme de Zorn). — *Soit S un ensemble ordonné. On suppose que toute partie bien ordonnée de S possède un majorant. Alors S admet un élément maximal.*

Démonstration. — Supposons par l'absurde que S n'a pas d'élément maximal.

Montrons que toute partie bien ordonnée A de S possède un majorant a tel que $a \notin A$. Sinon, A possèderait un unique majorant a dans A, qui en serait un élément maximal. Si $x \notin A$, la relation $a \prec x$ est fausse, sinon x serait un majorant de A ; par suite, a est un élément maximal de S, ce qui est absurde.

Soit $\mathscr{I}$ l'ensemble des parties bien ordonnées de S ; pour $A \in \mathscr{I}$, soit M_A l'ensemble (non vide) des majorants a de A tels que $a \notin A$. D'après l'axiome du choix, le produit $\prod_{A\in\mathscr{I}} M_A$ n'est pas vide ; il existe donc, une application γ qui associe, à toute partie bien ordonnée A de S, un majorant $\gamma(A)$ de A qui n'appartienne pas à A.

On dira qu'une partie bien ordonnée A de S est adaptée à γ si $a = \gamma(\{x \in A\,;\, x \prec a\})$ pour tout $a \in A$.

LEMME. — *Soit A' et A'' des parties bien ordonnées de S adaptées à γ. Alors, A' est une section commençante de A'', ou A'' est une section commençante de A'.*

Démonstration. — La réunion W des parties B de S qui sont des sections commençantes de A' et de A'' est une section commençante de chacune de ces deux parties ; c'est la plus grande partie de S qui vérifie cette propriété. Si $W = A'$, A' est une section commençante de A'' ; si $W = A''$, A'' est une section commençante de A'. Sinon, il existe $a' \in A'$ et $a'' \in A''$ tels que

$$W = \{x \in A' ; x \prec a'\} = \{x \in A'' ; x \prec a''\}.$$

Comme A' est adaptée à γ, $a' = \gamma(W)$; de même, $a'' = \gamma(W)$. Alors, $W' = W \cup \{\gamma(W)\}$ est une section commençante de A' et de A'', ce qui contredit le fait que W est la plus grande. □

Soit $\mathscr{B}$ l'ensemble des parties bien ordonnées de S qui sont adaptées à γ et soit A leur réunion. Montrons que A est une partie bien ordonnée de S, adaptée à γ.

Soit P une partie non vide de A. Si B et B' sont des éléments de $\mathscr{B}$ tels que $P \cap B$ et $P \cap B'$ sont non vides, les plus petits éléments de $P \cap B$ et $P \cap B'$ coïncident car B est une section commençante de B', ou le contraire. Par suite, le plus petit élément de $P \cap B$, pour $B \in \mathscr{B}$ tel que $P \cap B \neq \varnothing$, est le plus petit élément de P. Cela montre que A est bien ordonné.

Soit a un élément de A et soit B un élément de $\mathscr{B}$ tel que $a \in B$. Alors, $\{x \in A ; x \prec a\}$ et $\{x \in B ; x \prec a\}$ coïncident, par définition des sections commençantes. Comme B est adapté à γ, on a $\gamma(\{x \in A ; x \prec a\} = a$. Par conséquent, A est adapté à γ.

Cela démontre que A est la plus grande partie bien ordonnée de S qui soit adaptée à γ. Mais alors, $A \cup \{\gamma(A)\}$ est une partie bien ordonnée de S, adaptée à γ, et contenant strictement A, contradiction. □

On dit qu'un ensemble ordonné est *inductif* si toute partie totalement ordonnée est majorée. En appliquant la définition à la partie vide, on voit qu'un ensemble inductif n'est pas vide. Il résulte du théorème de Zorn le corollaire : Si S est inductif, l'ensemble des éléments x de S tels que $a \preceq x$ est inductif, pour tout $a \in S$.

COROLLAIRE. — *Tout ensemble inductif possède un élément maximal. Plus précisément, si S est un ensemble inductif et a un élément de S, il existe un élément maximal $b \in S$ tel que $a \prec b$.*

§A.3. Le langage des catégories

Il s'agit d'un vocabulaire très utile, et très utilisé, pour décrire aisément un certain nombre de structures (les catégories) et la façon dont on passe de l'une à l'autre (les foncteurs).

INDEX