Anneaux et modules

Matthieu Romagny

2013-2014

Table des matières

L'objectif principal de cette première partie du cours ALGB est de donner une introduction à la théorie des anneaux et à celle des modules. Un module est l'analogue, sur un anneau de base qui n'est pas nécessairement un corps, de la notion d'espace vectoriel. Étant donné qu'il y a une grande diversité d'anneaux, possédant des propriétés (arithmétiques, algébriques, géométriques) variées, l'étude des modules est plus riche en comportements de toutes sortes que l'algèbre linéaire classique. Dans ce cours, nous ne ferons d'étude plus avancée des modules que pour des modules *de type fini*. Nous développerons une telle étude en faisant une hypothèse simplificatrice :

- soit sur les anneaux : nous considérerons les anneaux *principaux* et les modules de type fini arbitraires,
- soit sur les modules : nous considérerons alors les anneaux arbitraires, et les modules *libres* de type fini.

On trouvera à la fin de ce polycopié une liste de livres dont la consultation peut être un bon support, ou complément, de lecture.

La préparation de ce texte a bénéficié de l'influence orale et écrite de Laurent Moret-Bailly et Dominique Bernardi, que je remercie chaleureusement tous les deux. Je remercie également les étudiants rennais pour leur lecture attentive, et notamment Salim Rostam qui m'a signalé de nombreuses erreurs et coquilles dans des versions précédentes du texte.

1 Rappels

1.1 Relations d'équivalence et quotients

Soit X un ensemble. Rappelons qu'une *relation* sur X est une partie $\mathscr{R}$ du produit cartésien $X \times X$. On note souvent $x\mathscr{R}y$, au lieu de $(x, y) \in \mathscr{R}$. Une relation $\mathscr{R}$ est dite :

(1) *réflexive* si $x\mathscr{R}x$ pour tout x,

(2) *transitive* si $x\mathscr{R}y$ et $y\mathscr{R}z$ impliquent $x\mathscr{R}z$ pour tous x, y, z,

(3) *symétrique* si $x\mathscr{R}y$ implique $y\mathscr{R}x$ pour tous x, y, et

(4) *antisymétrique* si $x\mathscr{R}y$ et $y\mathscr{R}x$ implique $x = y$.

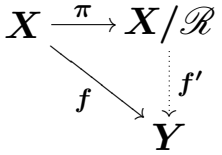
On appelle *relation d'équivalence* une relation réflexive, transitive et symétrique. Pour les relations d'équivalence, on utilise souvent la no-

tation $x \sim y$ au lieu de $x\mathscr{R}y$. On appelle *relation d'ordre* une relation réflexive, transitive et antisymétrique.

Soit $\mathscr{R}$ une relation d'équivalence sur X. On note $\overline{x}$ l'ensemble des $y \in X$ tels que $x \sim y$, et on l'appelle la *classe d'équivalence* de x. On note $X/\mathscr{R}$ ou $X/\sim$ l'ensemble des classes d'équivalence des éléments de X. L'ensemble des classes $\{\overline{x}\}_{\overline{x}\in X/\mathscr{R}}$ forme une partition de X ; réciproquement toute partition $\{X_i\}_{i\in I}$ de X donne naissance à une relation d'équivalence, définie par le fait que $x \sim y$ si et seulement si x, y appartiennent au même X_i.

Soit $f : X \to Y$ une application vers un ensemble Y. Alors, la relation $\mathscr{R}$ définie par « $x \sim x'$ si et seulement si $f(x) = f(x')$ » est une relation d'équivalence sur X que l'on appelle la *relation d'équivalence associée à f*, ou *relation d'équivalence définie par les fibres de f* (une *fibre* est une partie de X de la forme $f^{-1}(y)$, pour un $y \in Y$). Un résultat extrêmement important est que toutes les relations d'équivalence sur X sont de cette forme :

1.1.1 Théorème. *Soit $\mathscr{R}$ une relation d'équivalence sur X. Alors, l'application $\pi : X \to X/\mathscr{R}$ qui envoie x sur sa classe $\overline{x}$ est surjective, et la relation d'équivalence qui lui est associée est $\mathscr{R}$. De plus π vérifie la* propriété universelle *suivante : pour tout ensemble Y et toute application $f : X \to Y$ telle que $x \sim x'$ implique $f(x) = f(x')$ pour tous x, x' dans X, il existe une unique application $f' : X/\mathscr{R} \to Y$ telle que $f = f' \circ \pi$.*



L'application π est appelée *surjection canonique*.

1.1.2 Exercice. Avec les notations du théorème, vérifiez que l'image de f' est égale à l'image de f, et que les classes de la relation d'équivalence associée à f' sont les images dans $X/\mathscr{R}$ des classes de la relation d'équivalence associée à f.

1.1.3 Exemples. Voici des exemples de relations d'équivalence issus de l'algèbre, la géométrie, la topologie, l'analyse.

(1) X est l'ensemble $\mathbb{N}$ des entiers naturels ; $m \sim n$ ssi $|m - n|$ est pair ; $X/\sim = \{\overline{0}, \overline{1}\}$.

(2) $X = \mathbb{N} \times \mathbb{N}$; $(a, b) \sim (c, d)$ ssi $a + d = b + c$; $X/\sim = \mathbb{Z}$.

(3) $\boldsymbol{X = \mathbb{Z} \times \mathbb{N}^*}$; $\boldsymbol{(a,b) \sim (c,d)}$ ssi $\boldsymbol{ad = bc}$; $\boldsymbol{X/\sim = \mathbb{Q}}$.

(4) $\boldsymbol{X}$ est l'ensemble des paires de vecteurs unitaires d'un plan euclidien $\boldsymbol{E}$; $\boldsymbol{(u,v) \sim (u',v')}$ ssi il existe une rotation $\boldsymbol{f}$ de $\boldsymbol{E}$ qui envoie la paire $\boldsymbol{(u,v)}$ sur la paire $\boldsymbol{(u',v')}$; $\boldsymbol{X/\sim}$ est l'ensemble des angles orientés.

(5) $\boldsymbol{X}$ est l'ensemble des vecteurs non nuls dans le $\boldsymbol{k}$-espace vectoriel $\boldsymbol{k^{n+1}}$; $\boldsymbol{u \sim v}$ ssi $\boldsymbol{\exists \lambda \in k^*}$, $\boldsymbol{u = \lambda v}$; $\boldsymbol{X/\sim = \mathbb{P}^n(k)}$.

(6) $\boldsymbol{X}$ est l'espace $\boldsymbol{\mathscr{L}^p}$ des fonctions complexes mesurables de norme $\boldsymbol{p}$ finie ; $\boldsymbol{f \sim g}$ ssi $\boldsymbol{f - g}$ est nulle presque partout ; $\boldsymbol{X/\sim = L^p}$ (voir 2.2.9 pour plus de détails sur cet exemple).

(7) $\boldsymbol{X}$ est l'espace des suites rationnelles de Cauchy ; $\boldsymbol{(u_n) \sim (v_n)}$ ssi $\boldsymbol{(u_n - v_n)}$ converge vers $\boldsymbol{0}$; $\boldsymbol{X/\sim = \mathbb{R}}$.

(8) $\boldsymbol{X = \mathbb{R}[T]}$; $\boldsymbol{P \sim Q}$ ssi $\boldsymbol{P - Q}$ est divisible par $\boldsymbol{T^2 + 1}$; $\boldsymbol{X/\sim = \mathbb{C}}$.

(9) $\boldsymbol{X = \mathbf{GL}_n(k)}$; $\boldsymbol{A \sim B}$ ssi $\boldsymbol{\exists \lambda \in k^*}$, $\boldsymbol{A = \lambda B}$; $\boldsymbol{X/\sim = \mathbf{PGL}_n(k)}$

1.1.4 Remarque. Si $\boldsymbol{f : X \to Y}$ est une application d'ensembles, la relation d'équivalence $\boldsymbol{\mathscr{R}}$ associée à $\boldsymbol{f}$ sert à mesurer le défaut d'injectivité de $\boldsymbol{f}$ et l'image $\boldsymbol{f(X)}$ de $\boldsymbol{f}$ sert à mesurer son défaut de surjectivité. En quelque sorte, on « rend $\boldsymbol{f}$ injectif » en remplaçant $\boldsymbol{X}$ par $\boldsymbol{X/\mathscr{R}}$ et on « rend $\boldsymbol{f}$ surjectif » en remplaçant $\boldsymbol{Y}$ par $\boldsymbol{f(X)}$. Plus précisément, si l'on désigne par $\boldsymbol{\pi : X \to X/\mathscr{R}}$ la surjection canonique et par $\boldsymbol{i : f(X) \to Y}$ l'injection (inclusion) canonique, alors le théorème 1.1.1 implique qu'il existe une unique bijection $\boldsymbol{\overline{f} : X/\mathscr{R} \to f(X)}$ telle que $\boldsymbol{f = i \circ \overline{f} \circ \pi}$. Cette écriture est appelée la *décomposition canonique* de l'application $\boldsymbol{f}$. L'étude des quotients de groupes et d'anneaux, que nous ferons plus loin dans le cours, est motivée par le souhait d'obtenir des décompositions semblables pour les morphismes de groupes et d'anneaux.

1.2 Lois internes compatibles

Rappelons qu'une *loi de composition interne* (ou simplement *loi de composition*, ou *loi interne*, ou *loi*) sur un ensemble X est une application $X \times X \to X$, $(x,y) \mapsto x * y$. On appelle $x * y$ le *composé* de x et y pour la loi $*$.

1.2.1 Proposition. ***Soient $\mathscr{R}$ une relation d'équivalence sur un ensemble X et $\pi : X \to X/\mathscr{R}$ la surjection canonique. Soit $*$ une loi de composition sur X. Les conditions suivantes sont équivalentes :***

(1) ***pour tous*** x, x', y, y' ***dans*** X ***on a :*** $x \sim x'$ ***et*** $y \sim y'$ ***implique*** $x * y \sim x' * y'$ ***;***

(2) ***il existe une loi de composition*** $\overline{*}$ ***sur*** $X/\mathscr{R}$ ***telle que pour tous*** x, y ***dans*** X ***on a*** $\overline{x * y} = \overline{x} \,\overline{*}\, \overline{y}$.

Lorsque les conditions équivalentes de la proposition sont vérifiées, on dit que *la loi* $*$ *est compatible à la relation d'équivalence*, ou encore que *la loi* $*$ *passe au quotient en une loi* $\overline{*}$ *sur* $X/\mathscr{R}$.

1.3 Cas des groupes

Soit $*$ une loi de composition interne sur un ensemble G. On dit que la loi est *associative* si pour tous x, y, z dans G on a $(x * y) * z = x * (y * z)$. On dit que la loi est *commutative* si pour tous x, y dans G on a $x * y = y * x$. Un *élément neutre pour* $*$ est un élément $e \in G$ tel que $e * x = x * e = x$ pour tout $x \in G$; s'il existe un élément neutre, alors celui-ci est unique. Dans ce cas, pour $x \in G$, on appelle *symétrique de* x un élément $x' \in G$ tel que $x * x' = x' * x = e$.

1.3.1 Remarque. Soient $*$ une loi sur $\boldsymbol{G}$ et $\boldsymbol{R}$ une relation d'équivalence sur $\boldsymbol{G}$ qui sont compatibles. Soit $\overline{*}$ la loi induite sur $\boldsymbol{G/R}$. Si $*$ est associative (resp. commutative), alors $\overline{*}$ l'est aussi. Si $\boldsymbol{e}$ est neutre pour $*$, alors son image $\overline{\boldsymbol{e}}$ est neutre pour $\overline{*}$.

1.3.2 Définition. Un *groupe* est un ensemble $\boldsymbol{G}$ muni d'une loi $*$ telle que :

(1) la loi est associative,

(2) la loi possède un élément neutre $\boldsymbol{e}$,

(3) tout élément de $\boldsymbol{G}$ possède un symétrique.

On dit que le groupe est *commutatif* ou *abélien* lorsque la loi $*$ commutative.

1.3.3 Conventions. On utilise le plus souvent la notation et la terminologie *multiplicatives* pour désigner les objets précédents : ainsi on appelle *multiplication* la loi $*$ de $\boldsymbol{G}$, on note $\boldsymbol{xy}$ et on appelle *produit* le composé $\boldsymbol{x * y}$, on note $\mathbf{1}$ le neutre $\boldsymbol{e}$, on note $\boldsymbol{x^{-1}}$ et on appelle *inverse* le symétrique $\boldsymbol{x'}$. L'exception principale à cette convention a lieu lorsque le groupe est commutatif. Dans ce cas, on utilise le plus souvent la notation et la terminologie *additives* : on appelle alors *addition* la loi de $\boldsymbol{G}$, on note $\boldsymbol{x + y}$ et on appelle *somme* le composé $\boldsymbol{x * y}$, on note $\mathbf{0}$ le neutre $\boldsymbol{e}$, on note $\boldsymbol{-x}$ et on appelle *opposé* le symétrique $\boldsymbol{x'}$.

1.3.4 Définition. Soient G, H deux groupes. Un *morphisme de groupes* $f : G \to H$ est une application telle que pour tous x, y dans G on a $f(xy) = f(x)f(y)$. Le *noyau* de f noté $\ker(f)$ est l'ensemble $f^{-1}(1) = \{x \in G; f(x) = 1\}$, et l'*image* de f notée $\mathrm{im}(f)$ est l'ensemble $f(G) = \{y \in H; \exists x \in G, y = f(x)\}$.

On vérifie facilement que tout morphisme de groupes $f : G \to H$ envoie le neutre de G sur le neutre de H.

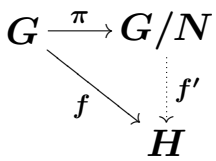
1.3.5 Définition. Un *sous-groupe* d'un groupe G est un sous-ensemble $H \subset G$ tel que $1 \in H$, pour tous $x, y \in H$ on a $xy \in H$, et pour tout $x \in H$ on a $x^{-1} \in H$.

Si $f : G \to H$ est un morphisme, son image est un sous-groupe de H.

1.3.6 Définition. Un sous-groupe $H \subset G$ est dit *distingué* (ou *normal*) si pour tous $x \in H$, $y \in G$ on a $yxy^{-1} \in H$. On note $H \lhd G$ pour indiquer que H est distingué. Le groupe G est dit *simple* s'il n'a pas de sous-groupe distingué autre que $\{1\}$ et G.

Si $f : G \to H$ est un morphisme, son noyau est un sous-groupe distingué. Noter que l'image n'est pas un sous-groupe distingué en général. L'importance des sous-groupes distingués provient du fait que réciproquement, tout sous-groupe distingué est noyau d'un morphisme de source G. Ceci est une conséquence du théorème suivant sur l'existence des quotients :

1.3.7 Théorème. ***Soient G un groupe et N un sous-groupe distingué. Alors il existe un groupe noté G/N et un morphisme de groupes $\pi : G \to G/N$ satisfaisant la propriété universelle : pour tout groupe H et tout morphisme $f : G \to H$ tel que $N \subset \ker(f)$, il existe un unique morphisme $f' : G/N \to H$ tel que $f = f' \circ \pi$. De plus, le morphisme $\pi : G \to G/N$ est surjectif, le sous-groupe N est distingué dans $\ker(f)$, le noyau de f' s'identifie à $\ker(f)/N$, et l'image de f' est égale à l'image de f.***



L'ensemble G/N est l'ensemble des classes d'équivalence des éléments de G pour la relation d'équivalence définie par les classes à gauche modulo N (ou les classes à droite : ce sont les mêmes lorsque N est distingué).

1.3.8 Remarque. Le groupe quotient $\boldsymbol{G/N}$ est un objet abstrait et la description qui en est donnée dans la preuve du théorème n'est pas toujours très maniable. Faute de mieux, on peut utiliser cette description, mais dans les situations concrètes on essaie d'identifier $\boldsymbol{G/N}$ à un groupe connu. Ainsi, il découle du théorème que si on dispose d'un morphisme surjectif $\boldsymbol{\rho : G \to Q}$ de noyau $\boldsymbol{N}$, alors le morphisme induit $\boldsymbol{\rho' : G/N \to Q}$ est un isomorphisme. Cette remarque s'applique :

(i) au quotient $\mathbf{GL}_n(\boldsymbol{k})/\mathbf{SL}_n(\boldsymbol{k})$ qui s'identifie à $\boldsymbol{k}^\times$ via le morphisme $\mathbf{det} : \mathbf{GL}_n(\boldsymbol{k}) \to \boldsymbol{k}^\times$,

(ii) au quotient d'un groupe $\boldsymbol{G}$ par son centre $\boldsymbol{Z = Z(G) = \{x \in G; \forall y \in G, xy = yx\}}$ qui s'identifie au groupe des automorphismes intérieurs de $\boldsymbol{G}$, à l'aide du morphisme $\boldsymbol{c : G \to \mathbf{Aut}(G)}$ qui envoie $\boldsymbol{x}$ sur la conjugaison $\boldsymbol{c_x : y \mapsto xyx^{-1}}$.

1.3.9 Exercice. Soit $\boldsymbol{G}$ un groupe et $\mathscr{R}$ une relation d'équivalence sur l'ensemble sous-jacent à $\boldsymbol{G}$. Montrez que $\mathscr{R}$ est compatible avec la multiplication de $\boldsymbol{G}$ si et seulement s'il existe un sous-groupe distingué $\boldsymbol{N \lhd G}$ tel que $\boldsymbol{x \mathscr{R} y}$ équivaut à $\boldsymbol{xy^{-1} \in N}$. (Indication : si $\mathscr{R}$ est compatible, montrez que la classe de $\mathbf{1}$ est un sous-groupe distingué).

1.3.10 Exercice. Soient $\boldsymbol{G}$ un groupe, $\boldsymbol{N}$ un sous-groupe distingué et $\boldsymbol{\pi : G \to G/N}$ le morphisme de quotient. Montrez que les applications $\boldsymbol{H \mapsto \pi(H)}$ et $\boldsymbol{K \mapsto \pi^{-1}(K)}$ sont des bijections inverses l'une de l'autre entre l'ensemble des sous-groupes $\boldsymbol{H \subset G}$ contenant $\boldsymbol{N}$ et l'ensemble des sous-groupes $\boldsymbol{K \subset G/N}$.

2 Théorie générale des anneaux et modules

2.1 Anneaux

Nous utilisons les conventions 1.3.3. Considérons un ensemble A muni de deux lois de composition $+ : (x, y) \mapsto x+y$ et $\times : (x, y) \mapsto xy$. On dit que $\times$ est *distributive à gauche (resp. à droite) sur* $+$ si pour tous x, y, z dans A on a $z(x+y) = zx+zy$ (resp. $(x+y)z = xz+yz$).

2.1.1 Définition. Un *anneau* est un triplet $(A, +, \times)$ tel que :

(1) $(A, +)$ est un groupe commutatif, dont on note 0 l'élément neutre,

(2) la loi $\times$ est associative et possède un neutre 1 distinct de 0,

(3) la loi $\times$ est distributive à droite et à gauche sur $+$.

On dit que l'anneau est *commutatif* si la loi $\times$ est commutative.

2.1.2 Remarques. (1) Il existe une notion d'anneau plus générale dans laquelle on ne requiert a priori ni l'associativité, ni l'existence d'un neutre multiplicatif 1, et des exemples extrêmement intéressants de tels anneaux généraux. Les anneaux de la définition 2.1.1 sont alors qualifiés d'anneaux *associatifs et unitaires*. Dans ce cours, nous ne considérerons que les anneaux associatifs et unitaires, et omettrons ces qualificatifs.

(2) Certaines définitions autorisent à avoir $1 = 0$; dans ce cas on a $A = \{0\}$.

(3) Les axiomes n'impliquent pas que $(A, \times)$ est un groupe. En fait $0.x = (1-1).x = 1.x - 1.x = 0$ pour tout $x \in A$ donc 0 n'a pas d'inverse si $A \neq \{0\}$.

2.1.3 Premiers exemples.

(a) l'anneau des entiers relatifs $\mathbb{Z}$, l'anneau des entiers de Gauss $\mathbb{Z}[i]$,

(b) les corps classiques $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (p premier),

(c) l'algèbre des quaternions $\mathbb{H} = \mathbb{R} \oplus i\mathbb{R} \oplus j\mathbb{R} \oplus k\mathbb{R}$ dont la multiplication est déterminée par $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $ik = -ki = -j$, $jk = -kj = i$.

(d) les anneaux de matrices,

(e) les anneaux de polynômes (voir 2.2.1) à coefficients dans un anneau, en une variable ou un nombre fini de variables,

(f) les anneaux de fonctions (voir 2.2.8) : sous-anneaux de l'anneau $\mathcal{F}(E, A)$ des fonctions sur un ensemble E à valeurs dans un anneau A, muni de la structure d'anneau naturelle induite par celle de A. Par exemple les anneaux de fonctions à valeurs réelles de classe C^k sur un intervalle de $\mathbb{R}$, ou l'anneau $\mathscr{H}(U)$ des fonctions holomorphes sur un ouvert U de $\mathbb{C}$,

(g) des sous-anneaux et quotients (voir 2.3.7) des exemples précédents.

2.1.4 Définition. Soient A, B deux anneaux. Un *morphisme d'anneaux* $f : A \to B$ est un morphisme de groupes de $(A, +)$ dans $(B, +)$ tel que $f(1) = 1$ et pour tous x, y dans A on a $f(xy) = f(x)f(y)$. Le *noyau* $\ker(f)$ et l'*image* $\mathrm{im}(f)$ sont par définition le noyau et l'image de f comme morphisme des groupes additifs sous-jacents.

Pour tout anneau A, il existe un unique morphisme $\mathbb{Z} \to A$, qui envoie n sur $n.1$.

2.1.5 Exercice. Pour tout anneau A, on appelle *anneau opposé à* A et on note A° l'anneau tel que $(A^\circ, +) = (A, +)$ muni de la multiplication renversée $x \times y := yx$. On appelle *anti-morphisme* (resp *anti-isomorphisme...*) de A vers B un morphisme d'anneaux $f : A \to B^\circ$, c'est-à-dire un morphisme de groupes de $(A, +)$ dans $(B, +)$ tel que $f(xy) = f(y)f(x)$ pour tous x, y. Montrez que l'anneau $\mathrm{M}_n(R)$ des matrices à coefficients dans un anneau commutatif R est anti-isomorphe à lui-même, c'est-à-dire que $\mathrm{M}_n(R)^\circ \simeq \mathrm{M}_n(R)$.

2.1.6 Définition. Un *sous-anneau* d'un anneau A est un sous-groupe A_0 de $(A, +)$ qui contient 1 et tel que pour tous $x, y \in A_0$ on a $xy \in A_0$.

Si $f : A \to B$ est un morphisme d'anneaux, alors son image $f(A)$ est un sous-anneau de B. Par ailleurs, il est facile de voir que si $\{A_i\}_{i \in I}$ est une famille de sous-anneaux de A, alors leur intersection $\cap A_i$ est un sous-anneau de A. Par exemple, si S est une partie de A, l'intersection de tous les sous-anneaux de A contenant S est un sous-anneau appelé le *sous-anneau engendré par S*. Il peut être décrit concrètement comme le sous-groupe engendré par les produits finis $s_1 \dots s_n$ d'éléments de S, i.e. l'ensemble des combinaisons linéaires à coefficients dans $\mathbb{Z}$ des tels produits. Un autre exemple important de sous-anneau est donné par le résultat suivant.

2.1.7 Lemme. ***Soit A un anneau et S une partie de A. Alors, l'ensemble des $x \in A$ tels que $xs = sx$ pour tout $s \in S$, appelé* commutant de *S, est un sous-anneau de A. En particulier, le commutant de A tout entier est un sous-anneau appelé le* centre de *A.***

Preuve : **C'est un exercice facile.** □

Si x est dans le commutant de S, on dit aussi parfois que x *centralise* S. Si x est dans le centre de A, on dit que x est *central*.

2.1.8 Définitions. Soient $\boldsymbol{A}$ un anneau et $\boldsymbol{x} \in \boldsymbol{A}$.

(1) $\boldsymbol{x}$ est *nilpotent* s'il existe un entier $\boldsymbol{n} \geqslant \mathbf{1}$ tel que $\boldsymbol{x^n} = \mathbf{0}$.

(2) $\boldsymbol{x}$ possède un *inverse à gauche* s'il existe $\boldsymbol{y} \in \boldsymbol{A}$ tel que $\boldsymbol{yx} = \mathbf{1}$.

(3) $\boldsymbol{x}$ est *régulier à gauche*, ou *non diviseur de zéro à gauche*, ou *simplifiable à gauche*, si $\boldsymbol{xy} = \mathbf{0}$ implique $\boldsymbol{y} = \mathbf{0}$, pour tout $\boldsymbol{y} \in \boldsymbol{A}$.

On définit de même les notions d'*inverse à droite* et d'*élément régulier à droite*.

(4) $\boldsymbol{x}$ est *inversible* s'il possède un inverse à gauche et à droite ; $\boldsymbol{x}$ est *régulier*, ou *non diviseur de zéro* s'il l'est à gauche et à droite.

(5) $\boldsymbol{A}$ est une *algèbre à division*, ou un *corps gauche*, si tout élément non nul est inversible.

Si $\boldsymbol{A}$ est commutatif, les notions « à gauche » et « à droite » coïncident et dans ce cas :

(6) $\boldsymbol{A}$ est un *intègre* si tout élément non nul est régulier.

(7) $\boldsymbol{A}$ est un *corps* si tout élément non nul est inversible.

Si x possède un inverse à gauche (resp. à droite), il est régulier à gauche (resp. à droite). Si x possède des inverses à gauche et à droite, ces inverses sont égaux à un même élément noté x^{-1}. L'ensemble des inversibles de A forme un groupe noté $A^\times$ ou parfois A^*.

Il est naturel de dire que x est *inversible à gauche* s'il possède un inverse à gauche, mais il faut noter que cela mène à une petite bizarrerie. En effet, notons $\gamma_x : A \to A$, $y \mapsto xy$ la multiplication à gauche par x et $\delta_x : A \to A$, $y \mapsto yx$ la multiplication à droite par x. Avec les définitions ci-dessus x est régulier à gauche si et seulement si la multiplication à gauche par x est injective, alors que x est inversible à gauche si et seulement si la multiplication à *droite* par x est surjective. En dépit de cet accident, la terminologie que nous avons introduite semble la meilleure et est largement partagée dans la littérature.

2.1.9 Exemples. Voici quelques exemples et contre-exemples d'anneaux intègres.

(1) Soit $\boldsymbol{n} \in \mathbb{N}$. L'anneau $\mathbb{Z}/\boldsymbol{n}\mathbb{Z}$ est intègre si et seulement si $\boldsymbol{n} = \mathbf{0}$ ou $\boldsymbol{n}$ est premier.

(2) L'anneau $\mathscr{C}(\mathbb{R},\mathbb{R})$ des fonctions continues de $\mathbb{R}$ dans $\mathbb{R}$ n'est pas intègre ; quels sont ses diviseurs de zéro ?

(3) L'anneau $\mathscr{H}(U)$ des fonctions holomorphes sur un ouvert connexe non vide $U \subset \mathbb{C}$ est intègre, à cause du principe des zéros isolés.

(4) Si A est intègre, l'anneau de polynômes $A[X]$ est intègre.

Voici quelques exemples de corps.

(5) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont des corps. L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.

(6) Si k est un corps, l'anneau des fractions rationnelles $k(X)$ est un corps. L'anneau $\mathscr{M}(U)$ des fonctions méromorphes sur un ouvert connexe non vide $U \subset \mathbb{C}$ est un corps.

(7) Le corps des fractions d'un anneau intègre. On notera que l'existence du corps des fractions montre qu'un anneau est intègre si et seulement si c'est un sous-anneau d'un corps.

2.1.10 Exercice. Soient E un espace vectoriel sur un corps k, $A = \mathbf{End}_k(E)$ son anneau d'endomorphismes, $f \in A$. Montrez que :

(1) $f \in A$ est inversible à gauche $\iff$ f est régulier à gauche $\iff$ f est injectif.

(2) $f \in A$ est inversible à droite $\iff$ f est régulier à droite $\iff$ f est surjectif.

Par exemple, prenons $k = \mathbb{Q}$ et $E = \mathbb{Q}[X]$. Soit $D : E \to E$ l'opérateur de dérivation, et $I : E \to E$ l'opérateur qui envoie un polynôme sur sa primitive nulle en 0. On a $D \circ I = \mathbf{Id}_E$ donc D possède un inverse à droite (et même une infinité) mais n'est pas régulier à gauche ; I possède un inverse à gauche (et même une infinité) mais n'est pas régulier à droite.

2.1.11 Exercice. Soit A un anneau et x un élément de A. Montrez que si x possède un inverse à gauche et est régulier à droite, alors il est inversible. Même énoncé si x possède un inverse à droite et est régulier à gauche. Soit $S \subset A$ une partie et C le commutant de S dans A. Montrez que si $x \in C$ est inversible dans A, alors $x^{-1} \in C$. Donnez un exemple dans lequel on suppose seulement que x possède un inverse à gauche x', mais $x' \notin C$.

2.2 Quelques exemples importants d'anneaux

2.2.1 Anneaux de polynômes. Soit $\boldsymbol{A}$ un anneau. On note $\boldsymbol{A[X]}$ l'anneau des polynômes à coefficients dans $\boldsymbol{A}$ en l'indéterminée (centrale) $\boldsymbol{X}$. On peut le construire, comme dans le cas classique où $\boldsymbol{A}$ est commutatif, comme ensemble des suites à support fini $\boldsymbol{(f_n)_{n\geqslant 0}}$ avec les lois $\boldsymbol{(f_n)+(g_n)=(f_n+g_n)}$ et $\boldsymbol{(f_n)(g_n)=(h_n)}$ avec $\boldsymbol{h_n=\sum_{i+j=n} f_i g_j}$. Par le morphisme qui envoie $\boldsymbol{a}$ sur la suite $\boldsymbol{(a,0,0,\dots)}$, l'anneau $\boldsymbol{A}$ s'identifie au sous-anneau de $\boldsymbol{A[X]}$ des polynômes *constants*. L'indéterminée $\boldsymbol{X}$ est la suite $\boldsymbol{(0,1,0,0,\dots)}$; elle commute avec tous les éléments de $\boldsymbol{A}$, donc est dans le centre de $\boldsymbol{A[X]}$. Tout élément $\boldsymbol{F=(f_n)}\in \boldsymbol{A[X]}$ s'écrit comme une somme finie $\boldsymbol{F=\sum_n f_n X^n=\sum_n X^n f_n}$. On définit le degré $\mathbf{deg}(\boldsymbol{F})$, et le coefficient dominant $\mathbf{cd}(\boldsymbol{F})$, de la manière habituelle ; rappelons que $\mathbf{deg}(\mathbf{0})=-\boldsymbol{\infty}$ et $\mathbf{cd}(\mathbf{0})=\mathbf{0}$. On a $\mathbf{deg}(\boldsymbol{FG})\leqslant \mathbf{deg}(\boldsymbol{F})+\mathbf{deg}(\boldsymbol{G})$ et en regardant les coefficients dominants, on voit qu'il y a égalité si $\mathbf{cd}(\boldsymbol{F})$ est régulier à gauche ou si $\mathbf{cd}(\boldsymbol{G})$ est régulier à droite. On peut faire des divisions euclidiennes à gauche et à droite ; ceci est énoncé précisément dans le lemme suivant.

2.2.2 Lemme. ***Soit A un anneau et $F,G\in A[X]$ des polynômes. On suppose que le coefficient dominant de G est inversible.***

(1) ***Division euclidienne à gauche : il existe un unique couple $(Q,R)\in A[X]^2$ tel que $F=GQ+R$ et $\deg(R)<\deg(G)$.***

(2) ***Division euclidienne à droite : il existe un unique couple $(Q',R')\in A[X]^2$ tel que $F=Q'G+R'$ et $\deg(R')<\deg(G)$.***

Preuve : Nous démontrons le point (1), la preuve de (2) est similaire. Notons aX^m et bX^n les monômes dominants de F et G.

Existence par récurrence sur m. Si $m<n$, on prend $Q=0$ et $R=F$. Sinon, on observe que le monôme dominant de $Gb^{-1}aX^{m-n}$ est $bX^n b^{-1}aX^{m-n}=aX^m$, de sorte que $F-Gb^{-1}aX^{m-n}$ est de degré strictement plus petit que m. Par l'hypothèse de récurrence, il existe (Q^*,R) tel que $F-Gb^{-1}aX^{m-n}=GQ^*+R$ avec $\deg(R)<n$. En posant $Q=Q^*+b^{-1}aX^{m-n}$, on obtient le couple (Q,R) souhaité.

Unicité. Supposons que (Q_1,R_1) et (Q_2,R_2) vérifient la conclusion de (1). Alors, on a $F=GQ_1+R_1=GQ_2+R_2$ donc $G(Q_1-Q_2)=R_2-R_1$. Comme b est régulier à gauche, on en déduit $\deg(G)+\deg(Q_1-Q_2)=$

$\deg(R_2-R_1) < \deg(G)$. Ceci n'est possible que si $\deg(Q_1-Q_2) = -\infty$, donc $Q_1 = Q_2$ puis $R_1 = R_2$. □

2.2.3 Remarque. Dans la preuve de (1), pour l'existence, on a besoin que b soit inversible à droite. Pour l'unicité, on a besoin que b soit régulier à gauche. Alors b est inversible (voir 2.1.11) donc on ne peut pas affaiblir l'hypothèse sur le coefficient dominant de G.

2.2.4 Exercice. Soit A un anneau.

(1) Soit Z le centre de A ; calculez le centre de $A[X]$.

(2) Pour $\alpha \in A$ et $F = \sum f_n X^n \in A[X]$, on note $F_g(\alpha) = \sum \alpha^n f_n$ la *valeur à gauche de* F *en* α. Considérons la division euclidienne à gauche $F = (X-\alpha)Q + r$ avec $\deg(r) \leqslant 0$. Montrez que $r = F_g(\alpha)$. Déduisez-en que $\{F \in A[X], F_g(\alpha) = 0\}$ est un idéal à droite. Mêmes questions de l'autre côté.

(3) Avec les notations de 2.2.2, supposons que tous les coefficients de F commutent avec tous les coefficients de G. Montrez qu'alors les deux divisions euclidiennes coïncident, i.e. $(Q, R) = (Q', R')$.

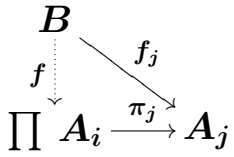
2.2.5 Anneaux de matrices. Soit R un anneau et $n \geqslant 1$ un entier. On note $S = \mathrm{M}_n(R)$ l'anneau des matrices carrées de taille n à coefficients dans R. Ses lois internes sont définies avec les formules habituelles ; on fera attention que dans la formule $c_{i,j} = \sum_{k=1}^{n} a_{i,k} b_{k,j}$ qui définit le produit $C = AB$ de deux matrices A et B, les coefficients de A et B ne sont pas permutables et sont bien écrits les uns à gauche, les autres à droite.

2.2.6 Exercice. Montrez que $\mathrm{M}_n(R)$ n'est pas commutatif, sauf si R est commutatif et $n = 1$. Soit Z le centre de R, montrez que le centre de $\mathrm{M}_n(R)$ est $Z.\mathrm{Id} = \{z\,\mathrm{Id}, z \in Z\}$.

2.2.7 Exercice. Donnez un isomorphisme canonique entre $\mathrm{M}_n(R[X])$ et $\mathrm{M}_n(R)[X]$.

2.2.8 Produits d'anneaux ; anneaux de fonctions. Soit $(A_i)_{i\in I}$ une famille d'anneaux. Le *produit direct* $A = \prod_{i\in I} A_i$ est l'ensemble produit cartésien des A_i, muni des lois d'addition et de multiplication définies coordonnée par coordonnée. Pour chaque $j \in I$,

on dispose d'une application de projection $\pi_j : \prod_{i\in I} A_i \to A_j$ qui est un morphisme d'anneaux. Le produit direct vérifie la propriété universelle suivante : pour tout anneau B et toute famille de morphismes d'anneaux $f_j : B \to A_j$, il existe un unique morphisme $f : B \to \prod A_i$ tel que $f_j = \pi_j \circ f$ pour tout j. La démonstration de cette propriété universelle est facile.



Si tous les A_i sont égaux à un même anneau A, alors $\prod_{i\in I} A_i$ s'identifie à l'anneau $\mathcal{F}(I, A)$ des fonctions de I à valeurs dans A, muni de l'addition et de la multiplication ponctuelles.

Un exemple classique est l'ensemble $\mathcal{P}(I)$ des parties de I. Pour A, B des parties de I, soit $A\Delta B = (A \setminus B) \cup (B \setminus A)$ la différence symétrique et $A \cap B$ l'intersection. Alors $(\mathcal{P}(I), \Delta, \cap)$ est un anneau commutatif, de neutre additif l'ensemble vide $\varnothing$ et de neutre multiplicatif l'ensemble I. L'application qui associe à une partie $A \subset I$ sa fonction indicatrice $\mathbf{1}_A$ établit un isomorphisme d'anneaux $\mathcal{P}(I) \to \mathcal{F}(I, \mathbb{Z}/2\mathbb{Z})$.

2.2.9 Espaces L^p (voir Rudin [R], chapitre 3). Soient a, b, p des réels avec $-\infty \leqslant a \leqslant b \leqslant +\infty$ et $1 \leqslant p \leqslant \infty$. Soit $\mathscr{L}^p$ l'ensemble des fonctions complexes définies et de puissance p-ième intégrable sur l'intervalle $[a, b]$. Muni de l'addition des fonctions, c'est un groupe abélien, d'après l'inégalité de Minkowski ; c'est même un $\mathbb{C}$-espace vectoriel. Soit L^p le quotient de $\mathscr{L}^p$ par le sous-espace des fonctions nulles presque partout.

(1) Si $p = 2$, les espaces $\mathscr{L}^2$ et L^2 sont stables par produit, d'après l'inégalité de Hölder. Ce sont donc des anneaux.

(2) Si $p \neq 2$, le produit ponctuel de deux fonctions $\mathscr{L}^p$ n'est pas dans $\mathscr{L}^p$ en général. Cependant, si $[a, b] = \mathbb{R}$ et si f et g sont dans $\mathscr{L}^1$, une application du théorème de Fubini montre que leur *produit de convolution* $f \star g : x \mapsto \int f(t)g(x - t)\, dt$ est encore dans $\mathscr{L}^1$. Le seul petit problème pour faire de $(\mathscr{L}^1, +, \star)$ un anneau est qu'il n'existe pas de neutre multiplicatif i.e. de fonction $e \in \mathscr{L}^1$ telle que $e \star f = f \star e = f$ pour tout f. Pour étudier $\mathscr{L}^1$ à l'aide de la théorie des anneaux, une solution est de se placer dans le cadre des anneaux non unitaires, voir remarque 2.1.2(1). Une autre solution est d'utiliser la construction suivante, qui plonge $\mathscr{L}^1$ de manière canonique dans un anneau unitaire. On étend le produit de $\mathscr{L}^1$ à l'espace vectoriel $A = \mathbb{C} \oplus \mathscr{L}^1$ par la formule :

$$(\lambda, f) \star (\mu, g) = (\lambda\mu, \lambda g + \mu f + f \star g).$$

Alors $(\boldsymbol{A}, +, \star)$ est un anneau de neutre multiplicatif $(\mathbf{1}, \mathbf{0})$, qui contient $\mathscr{L}^1$ comme idéal.

2.3 Idéaux

2.3.1 Définitions. Soit $\boldsymbol{A}$ un anneau.

(1) Un *idéal à gauche* de $\boldsymbol{A}$ est un sous-groupe $\boldsymbol{I}$ de $(\boldsymbol{A}, +)$ tel que pour tout $\boldsymbol{x} \in \boldsymbol{I}$ et tout $\boldsymbol{a} \in \boldsymbol{A}$, on a $\boldsymbol{ax} \in \boldsymbol{I}$. Un *idéal à droite...* $\boldsymbol{xa} \in \boldsymbol{I}$.

(2) Un *idéal bilatère* est un idéal à droite et à gauche.

L'anneau $\boldsymbol{A}$ est dit *simple* s'il n'a pas d'idéal bilatère autre que $\{\mathbf{0}\}$ et $\boldsymbol{A}$.

Si A est commutatif, les trois notions d'idéal coïncident.

Le seul idéal à gauche qui soit un sous-anneau est A tout entier : un sous-anneau contient toujours 1 alors qu'un idéal à gauche $I \neq A$ ne contient pas 1. Même chose avec les idéaux à droite.

Un idéal intéressant attaché à un anneau A est le noyau du morphisme $f : \mathbb{Z} \to A$, $i \mapsto i.1_A$. Pour le décrire, on utilise le résultat classique qui dit que tout idéal de $\mathbb{Z}$ est l'idéal $n\mathbb{Z}$ engendré par un entier $n \geqslant 0$. Rappelons la démonstration : soit $I \subset \mathbb{Z}$ un idéal. Si $I = \{0\}$ on prend $n = 0$. Si $I \neq \{0\}$, on pose $n = \min\{k \in I, k \geqslant 1\}$. On a $n \in I$ donc $n\mathbb{Z} \subset I$; réciproquement, pour $m \in I$ notons $m = nq + r$, $r < n$, la division euclidienne de m par n. D'après la définition de n, les deux propriétés $r < n$ et $r = m - nq \in I$ impliquent que $r = 0$, donc $m = nq \in n\mathbb{Z}$.

2.3.2 Définition. On appelle *caractéristique de* $\boldsymbol{A}$ l'unique générateur positif ou nul du noyau du morphisme $\mathbb{Z} \to \boldsymbol{A}$.

Ainsi $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ sont de caractéristique 0 ; l'anneau $\mathbb{Z}/n\mathbb{Z}$ est de caractéristique n ; un corps fini à $q = p^r$ éléments (avec p premier) est de caractéristique p ; l'anneau $(\mathcal{P}(I), \Delta, \cap)$ des parties d'un ensemble I est de caractéristique 2.

2.3.3 Idéaux engendrés, sommes d'idéaux, produits d'idéaux. Les notions d'idéaux engendrés et de sommes d'idéaux ont une version « à droite » et bilatère évidente ; nous nous limitons ci-dessous au cas des idéaux à gauche. L'intersection d'une famille d'idéaux à gauche est un idéal à gauche ; en particulier,

pour toute partie $S \subset A$ il existe un plus petit idéal à gauche de A contenant S, appelé l'*idéal à gauche engendré par* S. C'est l'ensemble des combinaisons linéaires à gauche à coefficients dans A d'éléments de S. Un *idéal principal à gauche* est un idéal à gauche engendré par un seul élément a ; on le note Aa. La *somme* d'une famille quelconque d'idéaux à gauche $\{I_\lambda\}_{\lambda \in L}$ est l'idéal à gauche engendré par la réunion des I_λ, noté $\sum_{\lambda \in L} I_\lambda$; c'est l'ensemble des sommes finies d'éléments des I_λ.

Pour les produits, nous ne considérons que des idéaux bilatères. Le *produit* d'une famille finie d'idéaux bilatères $I_1, \ldots, I_n$ est l'idéal bilatère noté $I_1 \ldots I_n$ engendré par les produits $i_1 \ldots i_n$ avec $i_\lambda \in I_\lambda$ pour tout λ.

2.3.4 Exemples. (1) Si I et J sont des idéaux à gauche de A, alors $\{a \in A, aI \subset J\}$ est un idéal à gauche.

(2) Soient X un ensemble et $x \in X$, alors l'ensemble $\{f \in \mathcal{F}(X, A),\ f(x) = 0\}$ est un idéal bilatère de l'anneau de fonctions $\mathcal{F}(X, A)$.

2.3.5 Exercice (voir [FGN1], exercices 6.24, 6.25, 6.26). Soient k un corps, E un k-espace vectoriel, $F \subset E$ un sous-espace, $A = \mathbf{End}_k(E)$.

(1) Montrez que $I_F = \{f \in A, f|_F = 0\}$ est un idéal à gauche et $J_F = \{f \in A, \mathbf{im}(f) \subset F\}$ un idéal à droite.

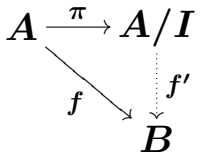
(2) Dans la suite, on suppose que E est de dimension finie. Montrez que les I_F et J_F sont les seuls idéaux de A.

(3) Déduisez de (2) que A est simple.

2.3.6 Exercice. Montrez que la préimage d'un idéal par un morphisme est un idéal, et que l'image d'un idéal par un morphisme surjectif est un idéal. Donnez un contre-exemple si l'on enlève l'hypothèse de surjectivité.

Si $f : A \to B$ est un morphisme, son noyau est un idéal bilatère. L'importance des idéaux bilatères provient du fait que réciproquement, tout idéal bilatère est noyau d'un morphisme de source A. La notion d'idéal bilatère est donc l'analogue, en théorie des anneaux, de la notion de sous-groupe distingué en théorie des groupes.

2.3.7 Théorème. ***Soient A un anneau et I un idéal bilatère distinct de A. Il existe un anneau noté A/I et un morphisme d'anneaux $\pi : A \to A/I$ satisfaisant la propriété universelle suivante : pour tout anneau B et tout morphisme $f : A \to B$ tel que $I \subset \ker(f)$, il existe un unique morphisme $f' : A/I \to B$ tel que $f = f' \circ \pi$. Le morphisme π est surjectif, le noyau de f' s'identifie à $\ker(f)/I$, et l'image de f'***
est égale à l'image de f.



Preuve : La preuve est semblable à la preuve du théorème de quotient pour les groupes : on considère la relation d'équivalence sur A définie par $x \sim y$ si et seulement si $x - y \in I$. Le fait que I soit un sous-groupe de $(A, +)$ implique que cette relation d'équivalence est compatible avec l'addition de A (on ne dit rien de nouveau ici que ce que l'on sait déjà pour le quotient d'un groupe par un sous-groupe distingué). Le fait que I soit stable par multiplication à droite et à gauche par des éléments de A implique que cette relation est compatible avec la multiplication de A : en effet, si $x \sim x'$ et $y \sim y'$, alors il existe i, j dans I tels que $x' = x + i$, $y' = y + j$ de sorte que

$$x'y' = xy + xj + iy + ij \text{ avec } xj + iy + ij \in I \ ;$$

ainsi $x'y' \sim xy$. Donc $+$ et $\times$ induisent des lois sur l'ensemble quotient $A/I := A/\sim$ qui le munissent d'une structure d'anneau. Le neutre additif de A/I est l'image de 0 et le neutre multiplicatif est l'image de 1 ; le fait que $I \neq A$ assure que ces deux éléments de A/I sont distincts. La démonstration de la propriété universelle et des autres propriétés énoncées dans le théorème ne pose pas de grande difficulté. □

2.3.8 Exercice. Soient A un groupe et $\mathscr{R}$ une relation d'équivalence sur l'ensemble sous-jacent à A. Montrez que $\mathscr{R}$ est compatible avec l'addition et la multiplication de A si et seulement s'il existe un idéal $I \subset A$ tel que $x \mathscr{R} y$ équivaut à $x - y \in I$.

2.3.9 Exercice. Soient A un anneau, I un idéal bilatère distinct de A et $\pi : A \to A/I$ le morphisme de quotient. Montrez que les applications $J \mapsto \pi(J)$ et $K \mapsto \pi^{-1}(K)$ sont des bijections inverses l'une de l'autre entre l'ensemble des idéaux à gauche $J \subset A$ contenant I et l'ensemble des idéaux à gauche K de A/I.

2.4 Idéaux des anneaux commutatifs

Dans cette sous-section, on considère un anneau *commutatif* A et on s'intéresse à certains idéaux importants.

2.4.1 Définition. Soit A un anneau commutatif.

(1) Un idéal *premier* est un idéal strict $p \subsetneq A$ tel que A/p est intègre, c'est-à-dire que pour tous $x, y \in A$ on a : $xy \in p$ implique ($x \in p$ ou $y \in p$).

(2) Un idéal *maximal* est un idéal strict $m \subsetneq A$ tel que A/m est un corps, c'est-à-dire que pour tout $x \notin m$, il existe $a \in A$ tel que $1 + ax \in m$.

On voit facilement que m est maximal si et seulement si c'est un idéal maximal pour l'inclusion.

Nous allons établir certains résultats d'existence d'idéaux premiers et maximaux, qui seront basés sur l'axiome du choix. L'axiome du choix possède des formes équivalentes qui sont parfois plus commodes d'utilisation ; le lemme de Zorn et le théorème d'existence de bons ordres dû à Zermelo en sont deux exemples. Nous allons donner tous ces énoncés. Ce n'est pas notre propos dans ce cours de nous attarder sur les démontrations ; contentons-nous de conseiller à la lectrice de s'accorder un instant de détente en dévorant les treize pages des chapitres 15, 16 et 17 de Halmos [Ha] (si ce n'est tout le livre, qui en vaut la peine) ou alors le chapitre 1 de Douady et Douady [DD].

Commençons par rappeler l'énoncé de l'axiome du choix.

2.4.2 Axiome du choix. ***Si I est un ensemble non vide et $\{E_i\}_{i \in I}$ est une famille d'ensembles non vides, alors le produit $\prod_{i \in I} E_i$ est non vide.***

Cet axiome porte ce nom car il affirme que si chaque E_i est non vide, on peut « choisir » un élément x_i dans chacun des E_i, donnant ainsi un élément $(x_i)_{i \in I}$ du produit des E_i. On appelle « fonction de choix » une fonction qui associe à i un élément $x_i \in E_i$.

Rappelons que dans un ensemble partiellement ordonné E, on appelle *chaîne* toute partie totalement ordonnée de E. On dit que E est *inductif* si chacune de ses chaînes possède une borne supérieure dans E.

2.4.3 Lemme de Zorn. *Tout ensemble non vide inductivement ordonné possède un élément maximal.*

Ce théorème est énoncé par Zorn dans un article de 1935, mais il semble qu'il avait été établi par d'autres auteurs auparavant ; au moins par Kuratowski en 1922.

Rappelons qu'on appelle *bon ordre* un ordre sur un ensemble E tel que toute partie non vide de E admet un plus petit élément. Par exemple, l'ordre habituel sur $\mathbb{N}$ est un bon ordre.

2.4.4 Théorème du bon ordre. *Tout ensemble peut être muni d'un bon ordre.*

Ce théorème est établi par Zermelo en 1904. On montre que l'axiome du choix, le lemme de Zorn et le théorème de bon ordre sont équivalents.

Nous pouvons revenir à l'étude des anneaux.

2.4.5 Théorème. *Soit A un anneau commutatif non nul. Alors, tout idéal distinct de A est inclus dans un idéal maximal.*

Ce résultat est dû à Krull en 1929.

Preuve : Soit I un idéal strict, i.e. distinct de A. Soit E l'ensemble des idéaux stricts contenant I. Cet ensemble n'est pas vide car il contient I. Il est inductivement ordonné, car si $\{J_\lambda\}_{\lambda\in L}$ est une famille totalement ordonnée d'idéaux de E, leur réunion est un idéal contenant I qui est strict, car sinon il contiendrait 1, et donc l'un des J_λ contiendrait 1, en contradiction avec le fait que les J_λ sont stricts. D'après le lemme de Zorn, l'ensemble E possède un élément maximal ; un tel élément est un idéal maximal contenant I. □

En fait, W. Hodges a démontré en 1975 que le théorème de Krull implique l'axiome du choix ; ainsi les énoncés 2.4.2, 2.4.3, 2.4.4, 2.4.5 sont équivalents.

2.4.6 Corollaire. *Tout anneau commutatif A possède un morphisme surjectif vers un corps.*

Preuve : L'idéal $\{0\}$ est strict et par le théorème ci-dessus, il est inclus dans idéal maximal m. Le morphisme $A \to A/m$ répond à la question. □

2.4.7 Définition. Soit $\boldsymbol{A}$ un anneau commutatif. On dit que $\boldsymbol{A}$ est *réduit* si son seul élément nilpotent est $\mathbf{0}$. On note $\mathbf{Nil}(\boldsymbol{A})$ l'ensemble des éléments nilpotents de $\boldsymbol{A}$, et on l'appelle le *nilradical* de $\boldsymbol{A}$

2.4.8 Lemme. *Le nilradical* $\mathrm{Nil}(A)$ *est un idéal de A.*

Preuve : Soient x, y deux éléments nilpotents de A, de sorte qu'il existe $m, n \geqslant 1$ tels que $x^m = y^n = 0$. On a :

$$(x+y)^{m+n-1} = \sum_{i=0}^{m+n-1} \binom{m+n-1}{i} x^i y^{m+n-1-i}.$$

Si $i \geqslant m$, on a $x^i = 0$; sinon, on a $m+n-1-i \geqslant n$, donc $y^{m+n-1-i} = 0$. Ainsi tous les termes de la somme de droite s'annulent et on voit que $(x+y)^{m+n-1} = 0$. Ainsi $\mathrm{Nil}(A)$ est un sous-groupe. Par ailleurs, si $a \in A$ et $x \in \mathrm{Nil}(A)$, alors il existe n tel que $x^n = 0$ donc $(ax)^n = a^n x^n = 0$ et $ax \in \mathrm{Nil}(A)$. Finalement $\mathrm{Nil}(A)$ est un idéal. □

Il est important de noter que la commutativité de A est tout à fait essentielle pour utiliser la formule du binôme de Newton. Il est d'ailleurs bien connu que l'ensemble des éléments nilpotents d'un anneau non commutatif n'est pas un idéal en général : on le voit dans les anneaux de matrices.

2.4.9 Exercice. Montrez que l'anneau quotient $\boldsymbol{A/\,\mathrm{Nil}(A)}$ est réduit.

2.4.10 Proposition. *Soit A un anneau commutatif. Alors, le nilradical est égal à l'intersection des idéaux premiers de A.*

Preuve : Soit x un élément nilpotent et n tel que $x^n = 0$. Alors, pour tout idéal premier p, le fait que $x^n = 0 \in p$ implique $x \in p$. Ceci

montre que $\mathrm{Nil}(A)$ est inclus dans l'intersection des idéaux premiers. Réciproquement, soit $x \in A$ un élément qui n'est pas nilpotent. Alors, la partie multiplicative $S = \{x^n\}_{n \geqslant 0}$ ne contient pas 0. Considérons l'ensemble E des idéaux de A qui ne rencontrent pas S. Cet ensemble est non vide, puisqu'il contient $\{0\}$. Par ailleurs, il est inductivement ordonné, car si $\{I_\lambda\}_{\lambda \in L}$ est une famille totalement ordonnée d'idéaux qui ne rencontrent pas S, alors leur réunion est un idéal qui ne rencontre pas S, donc c'est une borne supérieure pour la famille. D'après le lemme de Zorn, il y a dans E un idéal p qui est un élément maximal pour l'inclusion. Vérifions que p est premier. Si x, y n'appartiennent pas à p, alors les idéaux $p + (x)$ et $p + (y)$ contiennent p strictement, donc rencontrent S, par maximalité. Il s'ensuit qu'il existe $u, v \in p$, $a, b \in A$ et $m, n \geqslant 0$ tels que $u + ax = s^m$ et $v + by = s^n$. En faisant le produit, on trouve :

$$uv + uby + vax + abxy = s^{m+n}.$$

Dans le membre de gauche, les trois premiers termes sont dans p. Le fait que p ne rencontre pas S impose que $xy \notin p$, d'où notre assertion. On a trouvé un idéal premier qui ne contient pas x. □

2.4.11 Corollaire. *Un anneau commutatif A est réduit si et seulement s'il s'injecte dans un produit de corps.*

Cet énoncé est à mettre en rapport avec le fait qu'un anneau est intègre si et seulement s'il s'injecte dans un corps.

Preuve : Si A est inclus dans un produit de corps, il est clair qu'il est réduit. Réciproquement, si A est réduit, d'après 2.4.10 l'intersection de ses idéaux premiers est nulle. Notons $\mathscr{P}$ l'ensemble des idéaux premiers de A et pour chaque $p \in \mathscr{P}$, notons K_p le corps de fractions de l'anneau intègre A/p. Le noyau du morphisme naturel

$$A \longrightarrow \prod_{p \in \mathscr{P}} A/p \longrightarrow \prod_{p \in \mathscr{P}} K_p$$

est l'intersection des $p \in \mathscr{P}$, donc nul. On a plongé A dans un produit de corps. □

2.5 Modules et algèbres

Certains exemples d'anneaux, parmis les plus intéressants, sont construits à partir d'un anneau R qui joue un rôle d'anneau de « scalaires » : il en va ainsi des anneaux de polynômes $A = R[X]$, anneaux de matrices $A = \mathrm{M}_n(R)$ ou anneaux de fonctions $A = \mathcal{F}(E, R)$, voir sous-section 2.2. Pour ces anneaux, un grand nombre de choses se passent – en tout cas si R est supposé commutatif – comme dans le cas plus familier où $R = k$ est un corps et ces anneaux ont une structure de k-espace vectoriel. Pour ces raisons et pour bien d'autres, il est très souhaitable de formaliser la notion de *module* sur un anneau qui est l'analogue direct de la notion d'espace vectoriel sur un corps.

2.5.1 Définition. Soit $\boldsymbol{A}$ un anneau. Un $\boldsymbol{A}$-*module à gauche* est un groupe commutatif $\boldsymbol{M}$ muni d'une loi externe $\boldsymbol{A \times M \to M}$, pour laquelle l'image de $\boldsymbol{(a, x)}$ est notée $\boldsymbol{a.x}$ ou $\boldsymbol{ax}$, telle que pour tous $\boldsymbol{a, b \in A}$ et $\boldsymbol{x, y \in M}$ on a :

(1) $\boldsymbol{a.(x + y) = a.x + a.y}$,

(2) $\boldsymbol{(a + b)x = a.x + b.x}$,

(3) $\boldsymbol{(ab).x = a.(b.x)}$.

(4) $\boldsymbol{1.x = x}$.

Un $\boldsymbol{A}$-*module à droite* est muni d'une loi externe $\boldsymbol{M \times A \to M}$, l'image de $\boldsymbol{(x, a)}$ est notée $\boldsymbol{x.a}$ ou $\boldsymbol{xa}$, et ces données vérifient quatre axiomes évidents semblables aux quatre ci-dessus.

Un A-module à droite est la même chose qu'un module à gauche sur l'anneau A° opposé à A (voir exercice 2.1.5). Via ce dictionnaire, la théorie à droite et la théorie à gauche sont donc équivalentes. Si A est commutatif, on a $A = A^\circ$ et on ne distingue pas entre modules à gauche et à droite. Dans la suite, nous parlerons essentiellement de modules à gauche.

2.5.2 Exemples. (1) La multiplication de $\boldsymbol{A}$ le munit d'une structure de $\boldsymbol{A}$-module à gauche et d'une structure de $\boldsymbol{A}$-module à droite.

(2) Si $\boldsymbol{A}$ est un corps, un $\boldsymbol{A}$-module est juste un espace vectoriel.

(3) Un $\mathbb{Z}$-module est juste un groupe abélien car à cause des axiomes (2) et (4) il n'y a qu'une manière de définir une structure de $\mathbb{Z}$-module sur $\boldsymbol{M}$: pour $\boldsymbol{n \in \mathbb{Z}}$

et $x \in M$ on pose $nx = (1 + \cdots + 1)x = x + \cdots + x$ qui est la somme de n termes égaux à x dans M. Exemples : $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Z}_{(p)} = \{a/b \in \mathbb{Q}, p \nmid b\}$ (p premier), $\mathbb{Q}/\mathbb{Z}_{(p)}$, $\mathbb{R}$.

(4) Pour tout anneau A et tout ensemble I, le module *produit direct* $M = A^I$ est l'ensemble des collections $(a_i)_{i \in I}$ d'éléments de I, ou encore l'ensemble des fonctions de I dans A. Le module *somme directe* $M = A^{(I)}$ est le sous-ensemble de A^I formé des suites $(a_i)_{i \in I}$ dont tous les termes sont nuls sauf un nombre fini. Dans les deux cas, la structure de A-module est définie coordonnée par coordonnée.

(5) Soit $f : A \to B$ un morphisme d'anneaux. Alors B est muni d'une structure de A-module par $a.b := f(a)b$.

2.5.3 Remarque. Soit M un groupe abélien et considérons l'ensemble $\mathbf{End}(M)$ de ses endomorphismes. Muni de la loi $+$ d'addition des endomorphismes et de la composition $\circ$, c'est un anneau, non commutatif sauf cas exceptionnel, voir exercice 2.2.6. Le neutre additif $\mathbf{0}$ est l'endomorphisme nul, et le neutre multiplicatif $\mathbf{1} = \mathbf{Id}_M$ est l'endomorphisme identité. Ceci étant dit, considérons une structure de A-module à gauche sur M et pour chaque $a \in A$, soit $\gamma_a : M \to M$, $x \mapsto a.x$. L'axiome (1) de la définition 2.5.1 dit que l'application γ_a est un élément de $\mathbf{End}(M)$, et les axiomes (2)-(3)-(4) disent que l'application $\gamma : A \to \mathbf{End}(M)$ ainsi obtenue est un morphisme d'anneaux. Il est clair que ceci décrit une bijection entre structures de A-module à gauche sur M et morphismes d'anneaux $A \to \mathbf{End}(M)$. De même, une structure de A-module à droite sur M est équivalente à la donnée d'un *anti*-morphisme d'anneaux $A \to \mathbf{End}(M)$.

2.5.4 Définitions. Soient $M, M_1, \ldots, M_n, N$ des A-modules.

(1) Un *morphisme de A-modules*, ou *application A-linéaire* est un morphisme de groupes $f : M \to N$ tel que pour tous $a \in A$ et $x \in M$, on a $f(ax) = af(x)$.

(2) Le *noyau* $\mathbf{ker}(f)$ et l'*image* $\mathbf{im}(f)$ sont par définition le noyau et l'image de f comme morphisme des groupes additifs sous-jacents.

(3) Une application $f : M_1 \times \cdots \times M_n \to N$ est dite *n-linéaire* si pour tout $i \in \{1, \ldots, n\}$ et pour tout $(n-1)$-uplet $(x_j)_{j \neq i} \in \prod_{j \neq i} M_j$, l'application $f(x_1, \ldots, x_{i-1}, -, x_{i+1}, \ldots, x_n) : M_i \to P$ est A-linéaire.

(4) Une application n-linéaire $f : M_1 \times \cdots \times M_n \to N$ est dite *alternée* si elle s'annule dès que deux des variables sont égales.

2.5.5 Module $\mathbf{Hom}_A(M, N)$. On note $\mathbf{Hom}_A(M, N)$ l'ensemble des morphismes de A-modules de M dans N. C'est un groupe abélien. Pour tous $a \in A$ et $f \in \mathbf{Hom}_A(M, N)$, notons $a.f$ l'application $M \to N$, $x \mapsto a.f(x)$. Il est clair qu'elle est additive ; étudions sa linéarité par rapport aux scalaires de A. Pour $b \in A$ on a $(a.f)(bx) = a.f(bx) = ab.f(x)$ et $b.(a.f)(x) = ba.f(x)$. Si a et b commutent, ces deux quantités sont égales. Notons Z le centre de A. On en déduit que :

(i) $\mathbf{Hom}_A(M, N)$ est muni d'une structure de Z-module,

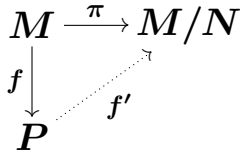
(ii) $\mathbf{Hom}_Z(M, N)$ est muni d'une structure de A-module,

et de manière plus mémorable, si A est commutatif, $\mathbf{Hom}_A(M, N)$ est canoniquement muni d'une structure de A-module.

2.5.6 Définition. Un *sous-A-module* d'un A-module M est un sous-groupe N tel que pour tous $a \in A$ et $x \in N$, on a $ax \in N$.

Le noyau, resp. l'image, d'un morphisme de A-modules $f : M \to N$ est un sous-A-module de M, resp. de N. Les idéaux de l'anneau A sont ses sous-A-modules. Une intersection de sous-modules est un sous-module. Dans un A-module M, étant donnée une partie $S \subset M$, il existe un plus petit sous-module contenant S, appelé le *sous-module engendré par S*. Par exemple, si M est un A-module et I est un idéal de A, les éléments de la forme ix avec $i \in I$ et $x \in M$ engendrent un sous-module noté IM. Si $I = (a)$ est engendré par un seul élément de A, on note simplement aM pour IM. Enfin, un dernier exemple est fourni par les *idéaux annulateurs* : étant donnés deux sous-modules N, P de M, on pose $(P : N) = \{a \in A, aN \subset P\}$; c'est un idéal de A. Un cas particulier est l'idéal $(0 : M) = \{a \in A, aM = 0\}$ appelé *annulateur de M* et noté $\mathrm{Ann}(M)$. Le morphisme $A \to \mathrm{End}(M)$ qui décrit la structure de A-module de M (voir 2.5.3) se factorise par l'anneau quotient $A/\mathrm{Ann}(M)$, induisant ainsi une structure de $A/\mathrm{Ann}(M)$-module sur M.

2.5.7 Théorème. ***Soient M un A-module et N un sous-A-module. Il existe un module noté M/N et un morphisme de A-modules $\pi : M \to M/N$ satisfaisant la propriété universelle suivante : pour tout module P et tout morphisme $f : M \to P$ tel que $N \subset \ker(f)$, il existe un unique morphisme $f' : M/N \to P$ tel que $f = f' \circ \pi$.***



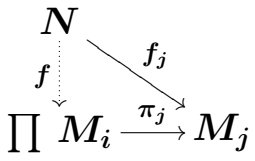
Preuve : Exercice. □

On a vu aussi que la somme directe $A^{(I)}$ est un sous-module du produit direct A^I. On peut généraliser les notions de produit et de somme au cas de familles quelconques $(M_i)_{i\in I}$ de modules : le produit direct $\prod_{i\in I} M_i$ est l'ensemble produit cartésien des M_i, et la somme directe $\oplus_{i\in I} M_i$ est le sous-module du produit direct composé des suites $(x_i)_{i\in I}$ dont tous les termes sont nuls sauf un nombre fini. Dans les deux cas, la structure de A-module est définie coordonnée par coordonnée.

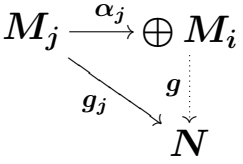
2.5.8 Remarque. L'inclusion $\oplus M_i \to \prod M_i$ est un isomorphisme si et seulement si seuls un nombre fini des M_i sont non nuls.

2.5.9 Théorème. ***Soit $(M_i)_{i\in I}$ une famille de A-modules.***

(1) ***Pour chaque $j \in I$, soit $\pi_j : \prod_{i\in I} M_i \to M_j$ la projection sur le j-ième facteur. Le produit direct vérifie la propriété universelle suivante : pour tout A-module N et toute famille de morphismes $f_j : N \to M_j$, il existe un unique morphisme $f : N \to \prod M_i$ tel que $f_j = \pi_j \circ f$ pour tout j.***



(2) ***Pour chaque $j \in I$, soit $\alpha_j : M_j \to \oplus_{i\in I} M_i$ le morphisme qui envoie x sur la suite dont le seul terme non nul est x sur la j-ième coordonnée. La somme directe vérifie la propriété universelle suivante : pour tout A-module N et toute famille de morphismes $g_j : M_j \to N$, il existe un unique morphisme $g : \oplus M_i \to N$ tel que $g_j = g \circ \alpha_j$ pour tout j.***



Preuve : La preuve n'est pas difficile ; nous indiquons juste comment sont définis les morphismes f et g. Dans (1), on pose $f(x) = (f_i(x))_{i\in I}$. Dans (2), on note que chaque élément $x = (x_i)_{i\in I}$ de la somme directe possède un nombre fini de composantes non nulles, disons $x_{i_1}, \ldots, x_{i_n}$. On pose alors $g(x) = g_{i_1}(x_{i_1}) + \cdots + g_{i_n}(x_{i_n})$. □

2.6 Algèbres

Les exemples d'anneaux $A = R[X]$, $A = \mathrm{M}_n(R)$ et $A = \mathcal{F}(E, R)$ possèdent une structure d'anneau et une structure de R-module. De plus, ces deux structures sont « compatibles » en un certain sens qui donne naissance à la notion de *R-algèbre*.

Nous nous limiterons au cas des algèbres sur un anneau de base commutatif.

2.6.1 Définition. Soit R un anneau commutatif. On appelle *R-algèbre* un anneau A muni d'une structure de R-module telle que la multiplication $m : A \times A \to A$ est R-bilinéaire.

Il se trouve que l'on peut décrire une structure d'algèbre de manière très simple, essentiellement grâce au fait que les anneaux possèdent des éléments neutres pour la multiplication. Précisément :

2.6.2 Proposition. *Soient R un anneau commutatif et A un anneau. La donnée d'une structure de R-algèbre sur A est équivalente à la donnée d'un morphisme d'anneaux $f : R \to A$ tel que $f(R)$ est inclus dans le centre de A. La loi extérieure est alors donnée par la formule $r.a = f(r) \times a$.*

Preuve : Soit A une R-algèbre au sens de la définition 2.6.1. On définit une application $f : R \to A$ par $f(r) = r.1$. Cette application est un morphisme de groupes additifs grâce à l'axiome (2) des modules. Elle est multiplicative grâce au fait que la multiplication de A est supposée bilinéaire ; en effet, $f(rs) = (rs).1 = (rs).(1 \times 1) = (r.1) \times (s.1) = f(r) \times f(s)$. Elle vérifie $f(1_R) = 1_R.1_A = 1_A$ grâce à l'axiome (4) des modules. C'est donc un morphisme d'anneaux. Enfin l'image de f est incluse dans le centre de A encore par bilinéarité : $f(r) \times a = (r.1) \times a = r.(1 \times a) = r.(a \times 1) = a \times (r.1) = a \times f(r)$.

Réciproquement soit $f : R \to A$ un morphisme dont l'image est centrale. Alors A est muni d'une structure de R-module par la formule $r.a = f(r) \times a$. Utilisant le fait que $f(R)$ est centrale, on vérifie immédiatement que pour cette structure, la multiplication de A est R-bilinéaire.

Il est clair que partant d'une R-algèbre A, sa structure est celle qui est définie par le morphisme associé $f(r) = r.1$. Il est clair aussi que partant d'un morphisme $f : R \to A$, ce morphisme est celui associé à la structure de R-algèbre $r.a = f(r) \times a$ sur A. Ces remarques fournissent l'équivalence entre les deux points de vue. □

2.6.3 Exercice. Remplacer tous les « il est clair que » de la preuve précédente par des vérifications en bonne et due forme, incluant la justification de chaque calcul avec les axiomes de modules et d'algèbres.

2.6.4 Morphismes d'algèbres, sous-algèbres, etc. De manière parallèle à ce que nous avons fait pour les anneaux, on peut exposer les notions de morphisme de R-algèbres, de sous-R-algèbre, sous-R-algèbre engendrée par une partie, etc. Nous épargnerons au lecteur le développement de toutes ces notions qu'il n'aura pas de mal à formuler lui-même.

2.6.5 Remarque. Tout anneau est une $\mathbb{Z}$-algèbre d'une unique manière : ceci se voit sur la définition 2.6.1 puisque la multiplication d'un anneau est $\mathbb{Z}$-bilinéaire par définition, ou alors via la description de la proposition 2.6.2 puisque tout anneau possède un unique morphisme $\mathbb{Z} \to A$, $n \mapsto n.1_A$ dont l'image est manifestement centrale. Ainsi, la théorie des anneaux est incluse dans la théorie des algèbres sur un anneau commutatif.

2.6.6 Exercice. Le classique théorème de Cayley dit que tout groupe G fini d'ordre n se plonge dans le groupe symétrique $\mathfrak{S}_G \simeq \mathfrak{S}_n$, via le morphisme qui associe à g la multiplication à gauche $\gamma_g : x \mapsto gx$. Ce théorème est précieux car il montre que les groupes symétriques contiennent tous les groupes finis. De la même manière, les algèbres de matrices contiennent toutes les algèbres de dimension finie sur un corps k : vérifiez en effet que pour toute k-algèbre de dimension finie A, l'application $A \to \mathbf{End}_k(A)$ qui associe à a la multiplication à gauche $\gamma_a : x \mapsto ax$ est un morphisme injectif de k-algèbres.

3 Modules libres de type fini

3.1 Modules libres

3.1.1 Définition. Soit $\boldsymbol{A}$ un anneau et $\boldsymbol{I}$ un ensemble. On appelle $\boldsymbol{A}$-*module libre standard de base* $\boldsymbol{I}$ le $\boldsymbol{A}$-module $\boldsymbol{A^{(I)}} := \oplus_{i\in I}\boldsymbol{A}$, somme directe indicée par $\boldsymbol{I}$ de copies de $\boldsymbol{A}$. C'est le $\boldsymbol{A}$-module des fonctions à support fini de $\boldsymbol{I}$ dans $\boldsymbol{A}$. Pour tout $\boldsymbol{i} \in \boldsymbol{I}$, on note $\boldsymbol{e_i} \in \boldsymbol{A^{(I)}}$ l'élément dont la seule composante non nulle est celle d'incide $\boldsymbol{i}$ qui vaut $\mathbf{1}$, c'est-à-dire, la fonction indicatrice de $\boldsymbol{i}$.

3.1.2 Proposition. ***Pour tout A-module M et toute famille $x = (x_i)_{i\in I}$ d'éléments de M, il existe un unique morphisme de A-modules $\varphi_x : A^{(I)} \to M$ tel que $\varphi(e_i) = x_i$ pour tout $i \in I$.***

Preuve : Chaque e_j définit un morphisme d'inclusion $\alpha_j : Ae_j \to A^{(I)}$. On voit alors que la propriété est un cas particulier de la propriété universelle d'une somme directe, voir théorème 2.5.9(2). On notera que l'image de φ_x est le sous-module de M engendré par les x_i. Le noyau de φ_x est appelé le *module des relations entre les x_i*. □

3.1.3 Définitions. Soit $\boldsymbol{M}$ un $\boldsymbol{A}$-module et $\boldsymbol{x} = (\boldsymbol{x_i})_{i\in I}$ une famille d'éléments de $\boldsymbol{M}$. Soit $\boldsymbol{\varphi_x} : \boldsymbol{A^{(I)}} \to \boldsymbol{M}$, $\boldsymbol{e_i} \mapsto \boldsymbol{x_i}$ l'application associée comme dans la proposition 3.1.2.

(1) On dit que la famille $\boldsymbol{x}$ est *génératrice* si le morphisme $\boldsymbol{\varphi_x}$ est surjectif.

(2) On dit que la famille $\boldsymbol{x}$ est *libre* si le morphisme $\boldsymbol{\varphi_x}$ est injectif.

(3) On dit que la famille $\boldsymbol{x}$ est *une base* si le morphisme $\boldsymbol{\varphi_x}$ est bijectif.

(4) On dit que $\boldsymbol{M}$ est *libre* s'il possède une base $\boldsymbol{(x_i)_{i\in I}}$.

3.1.4 Remarques. (1) $\boldsymbol{M}$ est libre si et seulement s'il est isomorphe à $\boldsymbol{A^{(I)}}$ pour un certain ensemble $\boldsymbol{I}$.

(2) Une famille est libre si et seulement si toute sous-famille finie est libre.

(3) Il existe des parties libres maximales, et des parties génératrices minimales, qui ne sont pas des bases : par exemple avec $\boldsymbol{A} = \mathbb{Z}$, $\boldsymbol{M} = \mathbb{Z}$, les parties $\boldsymbol{\{2\}}$ et $\boldsymbol{\{2, 3\}}$.

3.1.5 Exemples. (1) Si k est un corps, tout k-espace vectoriel est libre : d'après le lemme de Zorn, il existe une famille libre maximale, et il est élémentaire de voir que, puisque k est un corps, une telle famille est nécessairement génératrice.

(2) Le $\mathbb{Z}$-module $\mathbb{Z}/2\mathbb{Z}$ n'est pas libre ; le $\mathbb{Z}/2\mathbb{Z}$-module $\mathbb{Z}/2\mathbb{Z}$ est libre.

(3) Le $\mathbb{Z}$-module $\mathbb{Q}$ n'est pas libre (observer que deux éléments non nuls quelconques a/b et c/d sont multiples scalaires de $1/bd$).

(4) Pour tout anneau A, l'ensemble $\{X^i\}_{i\in\mathbb{N}}$ est une base de l'anneau de polynômes $A[X]$. En revanche, ce n'est pas une base de $A[[X]]$.

3.2 Modules libres de type fini

3.2.1 Définition. Soient A un anneau. On dit qu'un A-module M est *de type fini* s'il peut être engendré par un nombre fini d'éléments, c'est-à-dire s'il existe un entier n et des éléments $x_1, \ldots, x_r$ dans M qui engendrent un sous-module égal à M.

3.2.2 Exercice. Montrez que M est de type fini si et seulement s'il existe un morphisme surjectif de A-modules $A^n \to M$. Montrez que si $N \subset M$ est un sous-module tel que N et M/N sont de type fini, alors M est de type fini.

3.2.3 La notion de rang. Considérons maintenant un A-module M qui est *libre*. Ceci signifie qu'il possède une base $\mathscr{B} = (e_i)_{i\in I}$. Si $x_1, \ldots, x_r$ sont des éléments de M, chacun d'entre eux possède un nombre fini de composantes non nulles sur la base $\mathscr{B}$, si bien que l'ensemble des indices des composantes non nulles des x_j forme un sous-ensemble fini $J \subset I$. En particulier, si on suppose de plus que M est *de type fini*, il peut être engendré par un tel r-uplet $x_1, \ldots, x_r$ (avec r choisi minimal si on veut) et le raisonnement qui précède montre que M est inclus dans le sous-module engendré par les e_i avec $i \in J$. Alors chaque élément de $\mathscr{B}$ est combinaison linéaire de ceux des éléments de $\mathscr{B}$ dont l'indice est dans J, donc est égal à l'un d'entre eux (par les propriétés d'une base), et $J = I$. Ainsi I est fini i.e. il existe un entier $r \geqslant 0$ tel que $M \simeq A^r$.

Supposons de plus que A est commutatif. Montrons qu'alors l'entier r est uniquement déterminé, c'est-à-dire que $A^r \simeq A^s$ implique $r = s$. Pour cela, choisissons un idéal maximal $m \subset A$, ce qui est possible d'après le théorème 2.4.5, et notons $k = A/m$ le corps résiduel. Partant d'un isomorphisme de A-modules $A^r \simeq A^s$, en réduisant modulo m on obtient un isomorphisme de k-espaces

vectoriels $\boldsymbol{k^r \simeq k^s}$. La théorie de la dimension des espaces vectoriels nous apprend qu'alors $\boldsymbol{r = s}$.

Les remarques qui précèdent peuvent sembler évidentes, car les propriétés des familles libres et génératrices en algèbre linéaire classique (sur un corps) nous les rendent familières. Cependant, on a vu qu'il faut du soin pour les justifier, et ce soin n'est pas superflu : il existe des anneaux non commutatifs $\boldsymbol{A}$ tels que $\boldsymbol{A^m \simeq A^n}$ pour tous les entiers $\boldsymbol{m, n \geqslant 1}$. Pour tout corps $\boldsymbol{k}$, l'anneau des endomorphismes d'un $\boldsymbol{k}$-espace vectoriel de dimension infinie est un tel exemple (mais ce n'est pas évident de le voir !). Pour de tels anneaux, la notion de rang n'est pas définie.

3.2.4 Définition. Soient $\boldsymbol{A}$ un anneau commutatif et $\boldsymbol{M}$ un $\boldsymbol{A}$-module libre de type fini. L'unique entier $\boldsymbol{r}$ tel que $\boldsymbol{M \simeq A^r}$ est appelé le *rang* de $\boldsymbol{M}$.

3.2.5 Hypothèse. Dans toute la suite du cours, nous supposons que les anneaux considérés sont commutatifs ; cette règle sera répétée aussi souvent que possible (dans les limites du raisonnable) et restera en vigueur quoi qu'il arrive.

3.2.6 Représentation matricielle des morphismes. De nombreux concepts et résultats d'algèbre linéaire sur un corps de base restent valables pour les morphismes des modules libres de type fini sur un anneau commutatif quelconque. Ainsi en est-il du formalisme du calcul matriciel et de la théorie du déterminant. Nous terminerons cette sous-section en indiquant les rudiments du calcul matriciel pour les endomorphismes (il s'agit en fait plutôt de rappels, puisque tout se passe comme en algèbre linéaire habituelle). Dans la sous-section suivante, nous établirons les propriétés principales du déterminant et des concepts qui lui sont reliés avec un point de vue exclusivement matriciel ; la lectrice ou le lecteur peut en trouver une présentation plus intrinsèque par exemple dans la section 2.7 du polycopié [CL].

L'ensemble usuel de matrices $\mathrm{M}_{r,s}(\boldsymbol{A})$ est muni d'une structure de $\boldsymbol{A}$-module évidente, et le produit matriciel définit des applications $\boldsymbol{A}$-bilinéaires $\mathrm{M}_{r,s}(\boldsymbol{A}) \times \mathrm{M}_{s,t}(\boldsymbol{A}) \to \mathrm{M}_{r,t}(\boldsymbol{A})$. En particulier ceci fait de l'ensemble des matrices carrées $\mathrm{M}_r(\boldsymbol{A})$ une $\boldsymbol{A}$-algèbre.

Dans ce qui suit, nous considérerons des couples $(\boldsymbol{E}, \boldsymbol{e})$ formés d'un $\boldsymbol{A}$-module libre de type fini $\boldsymbol{E}$ et d'une base $\boldsymbol{e} = \{e_1, \ldots, e_r\}$ où $\boldsymbol{r} = \mathrm{rang}(\boldsymbol{E})$. Soit $\boldsymbol{u} : (\boldsymbol{E}, \boldsymbol{e}) \to (\boldsymbol{F}, \boldsymbol{f})$ une application $\boldsymbol{A}$-linéaire entre deux modules libres de type fini munis de bases. Pour chaque élément $\boldsymbol{e_j}$ de la base $\boldsymbol{e}$, soit $\boldsymbol{u(e_j) = \sum_i u_{i,j} f_i}$ l'écriture de son image sur la base $\boldsymbol{f}$.

3.2.7 Définition. La matrice de coefficients $u_{i,j}$ est appelée *matrice de* u *dans les bases* e *et* f et notée $\mathrm{Mat}_{e,f}(u)$. Si $E = F$ et $e = f$, on note $\mathrm{Mat}_e(u)$ au lieu de $\mathrm{Mat}_{e,f}(u)$.

Soient $r = \mathrm{rang}(E)$ et $s = \mathrm{rang}(F)$. Comme $u : E \to F$ est déterminée de manière unique par les valeurs $u(e_j)$, et chacune d'entre elles est déterminée de manière unique par les scalaires $u_{i,j} \in A$, l'application $u \mapsto \mathrm{Mat}_{e,f}(u)$ est un isomorphisme de A-modules :

$$\mathrm{Hom}_A(E, F) \simeq \mathrm{M}_{s,r}(A).$$

Si $E = F$ et $e = f$, on obtient un isomorphisme de A-algèbres :

$$\mathrm{End}_A(E) \simeq \mathrm{M}_r(A).$$

Le groupe des automorphismes de E correspond au groupe des matrices inversibles, qui comme on le verra en 3.3.10 n'est rien d'autre que le groupe des matrices de déterminant inversible noté $\mathrm{GL}_r(A)$.

3.2.8 Proposition. *La matrice de la composée de deux applications A-linéaires entre A-modules libres de type fini munis de bases :*

$$(E, e) \xrightarrow{u} (F, f) \xrightarrow{v} (G, g)$$

est donnée par la formule :

$$\mathrm{Mat}_{e,g}(vu) = \mathrm{Mat}_{f,g}(v)\,\mathrm{Mat}_{e,f}(u).$$

Plus généralement, la composée de n applications A-linéaires u_i : $(E^i, e^i) \to (E^{i+1}, e^{i+1})$ $(1 \leqslant i \leqslant n)$ a pour matrice $\mathrm{Mat}_{e^1,e^{n+1}}(u_n \cdots u_1) = \mathrm{Mat}_{e^n,e^{n+1}}(u_n) \cdots \mathrm{Mat}_{e^1,e^2}(u_1)$.

Preuve : Les coefficients u_{ij} et v_{ki} sont définis par les égalités $u(e_j) = \sum_i u_{ij} f_i$ et $v(f_i) = \sum_k v_{ki} g_k$. On a donc $(vu)(e_j) = \sum_i u_{ij} \sum_k v_{ki} g_k = \sum_k (\sum_i v_{ki} u_{ij}) g_k$. On voit que le coefficient d'indice (k, j) de la matrice de vu est $\sum_i v_{ki} u_{ij}$, qui est le coefficient d'indice (k, j) du produit matriciel annoncé. Le cas de la composée de n applications linéaires s'en déduit par une récurrence immédiate. □

On peut utiliser la formule précédente pour relier les matrices associées à un même endomorphisme dans des bases différentes.

3.2.9 Définition. Soit $\boldsymbol{E}$ un $\boldsymbol{A}$-module libre de type fini et $\boldsymbol{e}, \boldsymbol{e'}$ deux bases de $\boldsymbol{E}$. On appelle *matrice de changement de base (ou matrice de passage) de* $\boldsymbol{e}$ *à* $\boldsymbol{e'}$ la matrice :

$$\boldsymbol{P_e^{e'} = \mathrm{Mat}_{e',e}(\mathrm{Id}_E).}$$

C'est la matrice dont les colonnes sont les vecteurs de $\boldsymbol{e'}$ exprimés sur la base $\boldsymbol{e}$.

En appliquant la proposition 3.2.8 à la composée $(E,e) \xrightarrow{\mathrm{Id}} (E,e') \xrightarrow{\mathrm{Id}} (E,e)$ on voit que $P_e^{e'}P_{e'}^{e} = \mathrm{I}$. En particulier, ces matrices sont inversibles.

3.2.10 Proposition. ***Soit $u : E \to F$ une application A-linéaire entre deux A-modules libres de type fini. Soient e, e' deux bases de E et $P = P_e^{e'}$ la matrice de passage. Soient f, f' deux bases de F et $Q = P_f^{f'}$ la matrice de passage. Alors, on a :***

$$\boldsymbol{\mathrm{Mat}_{e',f'}(u) = Q^{-1}\ \mathrm{Mat}_{e,f}(u)\ P.}$$

En particulier si $E = F$, $e = f$ et $e' = f'$ on a :

$$\boldsymbol{\mathrm{Mat}_{e'}(u) = P^{-1}\ \mathrm{Mat}_{e}(u)\ P.}$$

Preuve : On applique la proposition 3.2.8 à la composée

$$(E,e') \xrightarrow{\mathrm{Id}} (E,e) \xrightarrow{u} (F,f) \xrightarrow{\mathrm{Id}} (F,f')$$

et cela donne directement le résultat. □

3.2.11 Remarque. Certaines notions d'algèbre linéaire usuelle (i.e. sur un corps) ne s'étendent cependant pas à des anneaux de scalaires commutatifs quelconques. Par exemple, pour une application linéaire $\boldsymbol{u : M \to N}$ entre deux modules libres de type fini, la notation de *rang* (au sens « dimension de l'image ») n'est pas bien définie car l'image de $\boldsymbol{u}$ n'est pas un module libre en général, donc n'a pas de rang (au sens de la définition 3.2.7). On fera donc attention de ne pas utiliser toute l'algèbre linéaire sans précaution !

3.3 Calcul matriciel

On fixe un anneau commutatif R et un entier $n \geqslant 1$. (Nous notons désormais R l'anneau de coefficients, pour disposer de la lettre A pour les matrices.) On note $\mathfrak{S}_n$ le groupe symétrique sur n lettres et $\epsilon : \mathfrak{S}_n \to \{\pm 1\}$ le morphisme signature. Soit $A = (a_{i,j})$ une matrice carrée de taille n à coefficients dans R. On définit :

$$\det(A) = \sum_{\sigma \in \mathfrak{S}_n} \epsilon(\sigma) a_{1,\sigma(1)} \dots a_{n,\sigma(n)}.$$

3.3.1 Proposition. *Soit ${}^{\mathrm{t}}A$ la transposée de la matrice A. On a :* $\det({}^{\mathrm{t}}A) = \det(A)$.

Preuve : En posant $\tau = \sigma^{-1}$ dans la somme et $j = \sigma(i)$ dans le produit, on a :

$$\det({}^{\mathrm{t}}A) \overset{\text{déf}}{=} \sum_{\sigma \in \mathfrak{S}_n} \epsilon(\sigma) \prod_{i=1}^{n} a_{\sigma(i),i} = \sum_{\tau \in \mathfrak{S}_n} \epsilon(\tau^{-1}) \prod_{j=1}^{n} a_{j,\tau(j)}.$$

Comme $\epsilon(\tau^{-1}) = \epsilon(\tau)$, c'est égal à $\det(A)$. □

3.3.2 Lemme. *Le déterminant est multilinéaire alterné en les lignes (ou colonnes) de A.*

Preuve : Compte tenu de 3.3.1, il suffit de considérer le cas des colonnes. La multilinéarité est évidente. Montrons que $\det(A) = 0$ si A possède deux colonnes égales, disons celles d'indices u et v. Soit τ la transposition (uv). On a une partition $\mathfrak{S}_n = \mathfrak{A}_n \cup \tau\mathfrak{A}_n$ d'où :

$$\det(A) = \sum_{\sigma \in \mathfrak{A}_n} \epsilon(\sigma) a_{1,\sigma(1)} \dots a_{n,\sigma(n)} + \sum_{\sigma \in \mathfrak{A}_n} \epsilon(\sigma\tau) a_{1,\sigma\tau(1)} \dots a_{n,\sigma\tau(n)}.$$

Or $a_{u,\sigma\tau(u)} a_{v,\sigma\tau(v)} = a_{u,\sigma(u)} a_{v,\sigma(v)}$ par égalité des colonnes u et v, et $a_{i,\sigma\tau(i)i} = a_{i,\sigma(i)}$ pour $i \notin \{u, v\}$, Ainsi :

$$\det(A) = \sum_{\sigma \in \mathfrak{A}_n} \epsilon(\sigma) a_{1,\sigma(1)} \dots a_{n,\sigma(n)} - \sum_{\sigma \in \mathfrak{A}_n} \epsilon(\sigma) a_{1,\sigma(1)} \dots a_{n,\sigma(n)} = 0,$$

comme souhaité. □

3.3.3 Théorème. *Soient A et B deux matrices carrées de taille n à coefficients dans un anneau commutatif R. On a :*

$$\det(AB) = \det(A)\det(B).$$

Preuve : Notons $\mathfrak{F}_n$ l'ensemble des fonctions de $\{1,\dots,n\}$ dans lui-même. La matrice B étant fixée, si $\tau \in \mathfrak{F}_n$, notons $M = B_\tau$ la matrice dont le terme d'indice (i,j) est $m_{i,j} = b_{\tau(i),j}$. Si τ n'est pas injectif, cette matrice possède deux lignes égales, donc son déterminant s'annule d'après le lemme. Nous utiliserons cette remarque simple dans le calcul ci-dessous. Le terme d'indice (i,j) de la matrice AB est $\sum_k a_{i,k}b_{k,j}$. On a :

$$\begin{aligned}
\det(AB) &= \sum_{\sigma\in\mathfrak{S}_n} \epsilon(\sigma) \prod_{i=1}^{n} \sum_{k=1}^{n} a_{i,k}b_{k,\sigma(i)} \\
&\text{par définition du déterminant,} \\
&= \sum_{\sigma\in\mathfrak{S}_n} \epsilon(\sigma) \sum_{\tau\in\mathfrak{F}_n} \prod_{i=1}^{n} a_{i,\tau(i)}b_{\tau(i),\sigma(i)} \\
&\text{en développant le produit de sommes,} \\
&= \sum_{\tau\in\mathfrak{F}_n} \sum_{\sigma\in\mathfrak{S}_n} \epsilon(\sigma) \prod_{i=1}^{n} a_{i,\tau(i)}b_{\tau(i),\sigma(i)} \\
&\text{en permutant } \textstyle\sum_\sigma \text{ et } \sum_\tau, \\
&= \sum_{\tau\in\mathfrak{F}_n} \prod_{i=1}^{n} a_{i,\tau(i)} \sum_{\sigma\in\mathfrak{S}_n} \epsilon(\sigma) \prod_{i=1}^{n} b_{\tau(i),\sigma(i)} \\
&\text{car } \textstyle\prod_i a_{i,\tau(i)} \text{ ne dépend pas de } \sigma, \\
&= \sum_{\tau\in\mathfrak{S}_n} \prod_{i=1}^{n} a_{i,\tau(i)} \sum_{\sigma\in\mathfrak{S}_n} \epsilon(\sigma) \prod_{i=1}^{n} b_{\tau(i),\sigma(i)} \\
&\text{car } \det(B_\tau) = 0 \text{ si } \tau \text{ n'est pas injectif,} \\
&= \sum_{\tau\in\mathfrak{S}_n} \epsilon(\tau) \prod_{i=1}^{n} a_{i,\tau(i)} \sum_{\rho\in\mathfrak{S}_n} \epsilon(\rho) \prod_{j=1}^{n} b_{j,\rho(j)} \\
&\text{en posant } \rho = \sigma\tau^{-1} \text{ et } j = \tau(i), \\
&= \det(A)\det(B),
\end{aligned}$$

comme souhaité. □

3.3.4 Définition. Soit $\boldsymbol{A}$ une matrice carrée de taille $\boldsymbol{n}$ à coefficients dans un anneau commutatif $\boldsymbol{R}$. Fixons un couple $\boldsymbol{(i,j)}$ d'entiers entre $\mathbf{1}$ et $\boldsymbol{n}$, et notons $\boldsymbol{M_{i,j}}$ la matrice obtenue à partir de $\boldsymbol{A}$ en effaçant la $\boldsymbol{i}$-ième ligne et la $\boldsymbol{j}$-ième colonne.

(1) le *mineur d'indice* $\boldsymbol{(i,j)}$ *de* $\boldsymbol{A}$ est le déterminant $\boldsymbol{\mu_{i,j} = \det(M_{i,j})}$,

(2) le *cofacteur d'indice* $\boldsymbol{(i,j)}$ *de* $\boldsymbol{A}$ est la quantité $\boldsymbol{(-1)^{i+j}\mu_{i,j}}$,

(3) la *comatrice* est la matrice $\mathbf{Com}(\boldsymbol{A})$ dont les coefficients sont les cofacteurs de $\boldsymbol{A}$.

3.3.5 Une convention sur la signature. Pour calculer avec des sous-matrices $\boldsymbol{M_{I,J} = (m_{i,j})_{i\in I, j\in J}}$ de $\boldsymbol{A}$ définies par des parties $\boldsymbol{I, J \subset \{1,\dots,n\}}$, il peut être nécessaire d'en écrire explicitement le numérotage des lignes et colonnes. Cependant, cela peut devenir très pénible et peut parfois être évité, en étant astucieux avec les notations. Par exemple, lorsque $\boldsymbol{I}$ et $\boldsymbol{J}$ sont de même cardinal $\boldsymbol{r}$ et qu'on veut manipuler le déterminant de $\boldsymbol{M_{I,J}}$, qui est un mineur de taille $\boldsymbol{r}$, il est utile d'étendre ainsi la notion de signature aux bijections entre ensembles finis ordonnés : si $\boldsymbol{I}$ et $\boldsymbol{J}$ sont des ensembles finis de même cardinal $\boldsymbol{r}$, les munir d'un ordre revient à les munir de bijections $\boldsymbol{\alpha : \{1,\dots,r\} \to I}$ et $\boldsymbol{\beta : \{1,\dots,r\} \to J}$, et on *définit* la signature d'une bijection $\boldsymbol{\sigma : I \to J}$ comme étant celle de la permutation $\boldsymbol{\beta^{-1}\sigma\alpha}$. (Dans la suite, nous noterons $\boldsymbol{\sigma : I \simeq J}$ une telle bijection.) Il est immédiat de constater que la signature ainsi définie est multiplicative lorsqu'on compose des bijections entre ensembles finis ordonnés. Revenons à une sous-matrice $\boldsymbol{M_{I,J}}$. Ici, les parties $\boldsymbol{I}$ et $\boldsymbol{J}$ sont munies de l'ordre induit par celui de $\boldsymbol{\{1,\dots,n\}}$. Avec ces conventions, le mineur $\boldsymbol{\mu_{I,J}}$ correspondant à $\boldsymbol{M_{I,J}}$ possède une expression simple :

$$\boldsymbol{\mu_{I,J} = \sum_{\sigma : I \simeq J} \epsilon(\sigma) \prod_{i\in I} a_{i,\sigma(i)}.}$$

Prenons l'exemple de la matrice $\boldsymbol{M_{i,j}}$. Observons que pour être en cohérence avec la notation générale $\boldsymbol{M_{I,J}}$, il vaut mieux la noter $\boldsymbol{M_{i^\star,j^\star} = (m_{i,j})_{i\in i^\star, j\in j^\star}}$ où l'on a posé

$$\boldsymbol{i^\star := \{1,\dots,n\} \smallsetminus \{i\}\ ;}$$

cependant, lorsqu'on ne manipule que des mineurs de taille $\boldsymbol{(n-1, n-1)}$ comme ici, c'est la notation $\boldsymbol{M_{i,j}}$ qui prévaut. La renumérotation explicite des lignes et

colonnes de $M_{i,j}$ se fait avec la permutation $\beta_i = (i, i+1, \ldots, n)$ et pour $1 \leqslant u, v \leqslant n-1$, le coefficient d'indice (u, v) s'écrit alors $m_{u,v} = a_{\beta_i(u),\beta_j(v)}$. La manipulation de cette permutation est pesante. Nos conventions précédentes nous mènent plutôt à l'expression du mineur :

$$\mu_{i,j} = \det(M_{i,j}) = \sum_{\sigma : i^\star \to j^\star} \epsilon(\sigma) \prod_{s \in i^\star} a_{s,\sigma(s)}.$$

Les conventions d'écriture que nous venons d'indiquer seront utiles ci-dessous, et encore plus dans le calcul de la remarque 5.1.7.

Le lemme suivant, qui utilise les mêmes notations, nous sera utile.

3.3.6 Lemme. *Soient $i, j \in \{1, \ldots, n\}$ et σ une bijection de $\{1, \ldots, n\}$ telle que $\sigma(j) = i$. Soit $\tau : j^\star \to i^\star$ la restriction de σ. Alors $\epsilon(\tau) = (-1)^{i+j}\epsilon(\sigma)$.*

Preuve : Partons de l'expression $\epsilon(\sigma) = \prod_{u<v} \frac{\sigma(v)-\sigma(u)}{v-u}$. En séparant le cas où $u = j$, le cas où $v = j$, et le cas où $u, v \neq j$ on trouve :

$$\epsilon(\sigma) = \prod_{j<v} \frac{\sigma(v) - i}{v - j} \times \prod_{u<j} \frac{i - \sigma(u)}{j - u} \times \epsilon(\tau) = \prod_{v \neq j} \frac{\sigma(v) - i}{v - j} \times \epsilon(\tau).$$

Le produit indicé par $v \neq j$ vaut ± 1, et pour le calculer il nous suffit de compter les signes négatifs. Le numérateur est négatif lorsque $\sigma(v) \in \{1, \ldots, i-1\}$ c'est-à-dire $i-1$ fois, et le dénominateur est négatif lorsque $v \in \{1, \ldots, j-1\}$ c'est-à-dire $j-1$ fois. Finalement $\epsilon(\tau) = (-1)^{i-1+j-1}\epsilon(\sigma) = (-1)^{i+j}\epsilon(\sigma)$. □

3.3.7 Proposition (Développement lignes-colonnes). *Notations de 3.3.4. On a :*

(1) *Développement par rapport à la i-ième ligne :*

$$\det(A) = \sum_{j=1}^{n} a_{i,j}(-1)^{i+j}\mu_{i,j}.$$

(2) *Développement par rapport à la j-ième colonne :*

$$\det(A) = \sum_{i=1}^{n} a_{i,j}(-1)^{i+j}\mu_{i,j}.$$

Preuve : (1) Découpons la somme qui exprime $\det(A)$ en n sommes, une pour chaque $j \in \{1, \ldots, n\}$, indicées par les permutations σ telles que $\sigma(j) = i$:

$$\det(A) = \sum_{j=1}^{n} \sum_{\substack{\sigma \in \mathfrak{S}_n \\ \sigma(j)=i}} \epsilon(\sigma) \prod_{s=1}^{n} a_{\sigma(s),s}.$$

En isolant le facteur $a_{\sigma(j),j} = a_{i,j}$ et en posant $\tau = \sigma|_{j^\star}$, on trouve, vu le lemme 3.3.6 :

$$\det(A) = \sum_{j=1}^{n} a_{i,j} \sum_{\tau : j^\star \to i^\star} (-1)^{i+j} \epsilon(\tau) \prod_{v \in j^\star} a_{\tau(v),v} = \sum_{j=1}^{n} a_{i,j} (-1)^{i+j} \mu_{i,j}.$$

(2) Découle de (1), compte tenu de la proposition 3.3.1. □

3.3.8 Théorème (Formule de la comatrice). *Soit A une matrice carrée à coefficients dans un anneau commutatif R. Alors on a les égalités :*

$$A\, {}^{\mathrm{t}}\mathrm{Com}(A) = {}^{\mathrm{t}}\mathrm{Com}(A) A = \det(A)\, \mathrm{Id}.$$

Preuve : Notons $\mu_{i,j}$ les mineurs de A et $c_{i,j}$ les coefficients de $A\, {}^{\mathrm{t}}\mathrm{Com}(A)$, c'est-à-dire $c_{i,j} = \sum_k a_{i,k}(-1)^{k+j}\mu_{j,k}$. La formule de développement par rapport à la i-ième ligne donne $c_{i,i} = \det(A)$. Supposons ensuite que $i \neq j$. Soit A' la matrice obtenue en remplaçant la j-ième ligne de A par la i-ième et affectons d'un « $'$ » les quantités correspondant à A'. Pour tout k, on a $a'_{j,k} = a_{i,k}$ et $\mu'_{j,k} = \mu_{j,k}$. La formule de développement par rapport à la j-ième ligne donne $\det(A') = \sum_k a'_{j,k}(-1)^{k+j}\mu'_{j,k} = \sum_k a_{i,k}(-1)^{k+j}\mu_{j,k} = c_{i,j}$. Mais comme A' possède deux lignes égales, finalement $c_{i,j} = \det(A') = 0$. Ces remarques assemblées montrent que $A\, {}^{\mathrm{t}}\mathrm{Com}(A) = \det(A)\, \mathrm{Id}$. Les formules de développement par rapport aux colonnes montrent de même que ${}^{\mathrm{t}}\mathrm{Com}(A) A = \det(A)\, \mathrm{Id}$. □

3.3.9 Remarque. Dans tous ces énoncés, il est crucial que l'anneau de coefficients R soit commutatif. En revanche, on n'a pas utilisé l'existence du neutre multiplicatif $\mathbf{1}$. De fait, les résultats 3.3.2 à 3.3.7 sont valables dans un anneau commutatif non unitaire, de même que 3.3.8 quitte à remplacer $\det(A)\,\mathrm{Id}$ par la matrice diagonale de coefficients diagonaux égaux à $\det(A)$.

3.3.10 Corollaire. *La matrice A est inversible si et seulement si* $\det(A)$ *est inversible.*

Preuve : Si A est inversible, on a $\det(A)\det(A^{-1}) = \det(AA^{-1}) = 1$ donc $\det(A)$ est inversible. Réciproquement, si $\det(A)$ est inversible la formule de la comatrice montre que $\det(A)^{-1}({}^{\mathrm{t}}\mathrm{Com}(A))$ est une inverse pour A. □

3.3.11 Théorème (Cayley-Hamilton). *Soit A une matrice carrée à coefficients dans un anneau commutatif R, et χ son polynôme caractéristique. Alors $\chi(A) = 0$.*

Preuve : Soit $S = R[A]$ la sous-R-algèbre de $\mathrm{M}_n(R)$ engendrée par la matrice A. C'est un anneau commutatif de neutre multiplicatif $1 = \mathrm{Id}$. Les polynômes $\chi(T) \in R[T]$ et $T\,\mathrm{Id} - A = T - A$ peuvent tous deux être vus dans $S[T]$. Écrivons la division euclidienne de $\chi(T)$ par $(T-A)$ dans $S[T]$:

$$(\star) \qquad \chi(T) = (T-A)Q + R, \quad Q, R \in S[T], \quad \deg(R) \leqslant 0.$$

Or la formule de la comatrice dit que $\chi(T) = (T-A)B$ où $B \in \mathrm{M}_n(R)[T]$ est la transposée de la comatrice de $T - A$. Par unicité de la division euclidienne à gauche dans $\mathrm{M}_n(R)[T]$ (voir lemme 2.2.2), on a donc $Q = B$ et $R = 0$. En particulier, la matrice B est dans le sous-anneau commutatif $S[T]$ de $\mathrm{M}_n(R)[T]$. En appliquant à l'égalité $(\star)$ le morphisme d'évaluation $\mathrm{ev}_A : S[T] \to S$, $P \mapsto P(A)$, on trouve $\chi(A) = 0$. □

Pour finir, nous allons raffiner le corollaire 3.3.10 en étudiant les liens entre injectivité, surjectivité et bijectivité des endomorphismes en termes du déterminant. En algèbre linéaire classique (sur un corps de base), les trois propriétés sont équivalentes ; considérons maintenant un anneau commutatif quelconque R. Concernant l'injectivité, on voit déjà en dimension 1 qu'elle n'est pas équivalente à la bijectivité : une matrice de dimension 1 est donnée par un seul coefficient $x \in R$, l'endomorphisme associé f est la multiplication par x de R dans lui-même, et f est injectif si et seulement si x est non diviseur de 0. Il se trouve que la réponse en général est semblable à cet exemple :

3.3.12 Proposition. *Soit A une matrice carrée de taille n à coefficients dans un anneau R. Soit $f : R^n \to R^n$ l'endomorphisme R-linéaire associé, et $\det(f) = \det(A)$. Alors :*

(1) *f est surjectif ssi f est bijectif ssi $\det(f)$ est inversible,*

(2) *f est injectif ssi $\det(f)$ est non diviseur de 0.*

Preuve : Soient $e_1, \ldots, e_n$ les vecteurs de la base canonique de R^n.
(1) Compte tenu de 3.3.10, il suffit de montrer que surjectif implique bijectif. Si f est surjectif, pour tout i il existe un vecteur $\epsilon_i \in R^n$ tel que $f(\epsilon_i) = e_i$. Soit le morphisme $g : R^n \to R^n$ défini par $g(e_i) = \epsilon_i$. On a $f \circ g = \mathrm{Id}$ car ceci est vrai pour tous les e_i, qui forment une partie génératrice. On en déduit que $\det(f)\det(g) = 1$ et donc $\det(f)$ est inversible. Alors, la formule de la comatrice montre que f est bijectif.
(2) Posons $d = \det(f)$. Si d est non diviseur de zéro, soit $v \in R^n$ un vecteur tel que $f(v) = 0$. Si V est le vecteur colonne correspondant à v, on a $AV = 0$ et en appliquant la transposée de la comatrice, on trouve $dV = 0$. En regardant coordonnée par coordonnée, le fait que d est non diviseur de 0 implique que $V = 0$, donc f est injectif.

Réciproquement, si d est diviseur de zéro, montrons que f n'est pas injectif. Soit $r \in R$ non nul tel que $rd = 0$. Rappelons qu'on appelle *mineur de A* le déterminant d'une matrice extraite de A ; ceci étend la définition 3.3.4(1). Si pour tout mineur μ de A on a $r\mu = 0$, alors en particulier ceci est vrai pour les mineurs de taille 1, i.e. les coefficients de la matrice A. On a donc $f(re_1) = 0$, or $re_1 \neq 0$, donc f n'est pas injectif. Sinon, il existe une matrice extraite B de A telle que $r\det(B) \neq 0$. Choisissons une telle matrice de taille m maximale ; on a $m < n$ puisque $rd = 0$. Quitte à réordonner les vecteurs de base à la source et au but, c'est-à-dire à multiplier A à gauche et à droite par des matrices de permutation (inversibles), on peut supposer que B est la matrice de taille m située en haut à gauche. Pour chaque $i \in \{1, \ldots, n\}$, bordons B avec la i-ème ligne et la $m+1$-ième colonne de A pour former la matrice de taille $m+1$ suivante :

$$C_i = \begin{pmatrix} a_{1,1} & \cdots & a_{1,m} & a_{1,m+1} \\ \vdots & & \vdots & \vdots \\ a_{m,1} & \cdots & a_{m,m} & a_{m,m+1} \\ a_{i,1} & \cdots & a_{i,m} & a_{i,m+1} \end{pmatrix} .$$

Pour $i \leqslant m$ la matrice C_i a deux lignes égales donc son déterminant est nul. Pour $i \geqslant m+1$ c'est une matrice extraite de A de taille $m+1$, donc son déterminant est annulé par r compte tenu de l'hypothèse sur m. Dans tous les cas, on a $r\det(C_i) = 0$. Développant par rapport à la dernière ligne, on trouve $r\sum_{j=1}^{m+1}(-1)^j a_{i,j}\mu_j = 0$ où μ_j est le mineur du coefficient de position $(m+1, j)$. Pour i variant, ces égalités disent exactement que $f(rv) = 0$ où v est le vecteur de coordonnées $(-\mu_1, \ldots, (-1)^{m+1}\mu_{m+1}, 0, \ldots, 0)$. Comme $r\mu_{m+1} = r\det(B) \neq 0$, on a $rv \neq 0$, donc f n'est pas injectif. □

4 Anneaux factoriels et principaux

Dans cette section, comme depuis 3.2.5, tous les anneaux considérés sont commutatifs. Nous commencerons par étudier brièvement les anneaux noethériens, qui forment une classe d'anneaux jouissant de propriétés de *finitude* remarquables, puis les anneaux factoriels et principaux, qui eux possèdent des propriétés *arithmétiques* intéressantes.

4.1 Anneaux noethériens

4.1.1 Définition. Soit $\boldsymbol{A}$ un anneau. On dit que $\boldsymbol{A}$ est *noethérien* si toute suite croissante d'idéaux de $\boldsymbol{A}$ est stationnaire.

4.1.2 Exemples. Un corps est noethérien ; un anneau principal est noethérien. Par exemple $\mathbb{Z}$ et l'anneau $\boldsymbol{k}[\boldsymbol{X}]$ de polynômes à coefficients dans un corps $\boldsymbol{k}$ sont noethériens (ce n'est pas évident, et nous ne l'avons pas encore prouvé à ce stade du cours). L'anneau $\boldsymbol{k}[\boldsymbol{X_1}, \ldots, \boldsymbol{X_n}, \ldots]$ de polynômes en une infinité dénombrable de variables n'est pas noethérien, car l'idéal $(\boldsymbol{X_1}, \ldots, \boldsymbol{X_n}, \ldots)$ n'est pas de type fini. L'anneau $\mathscr{H}(\mathbb{C})$ des fonctions holomorphes sur $\mathbb{C}$ n'est pas noethérien, voir la remarque 4.2.14.

On dit qu'un idéal est *de type fini* s'il peut être engendré par un nombre fini d'éléments, c'est-à-dire s'il est de type fini comme A-module (voir 3.2.1).

4.1.3 Lemme. ***Soit A un anneau. Les conditions suivantes sont équivalentes :***

(1) ***A est noethérien ;***

(2) ***tout idéal de A est de type fini.***

Preuve : Supposons qu'il existe un idéal $I \subset A$ qui n'est pas de type fini. Nous allons construire une suite d'idéaux non stationnaire, dont le n-ième terme I_n est engendré par n éléments $x_1, \ldots, x_n$ de I. On choisit $x_1 \in I$ et on pose $I_1 = (x_1)$. Supposons I_n construit ; comme I n'est pas de type fini, il existe $x_{n+1} \in I \smallsetminus I_n$. On pose $I_{n+1} = (x_1, \ldots, x_n, x_{n+1})$.

Réciproquement, si tout idéal est de type fini, considérons une suite croissante d'idéaux $I_1 \subset I_2 \subset \ldots ...$ La réunion $I = \cup_{n \geqslant 1} I_n$ est un idéal, de type fini par hypothèse, donc engendré par des éléments $x_1, \ldots, x_r$. Ces éléments appartiennent tous à un certain I_m, pour m assez grand. On en déduit que $I = I_m = I_{m+1} = \ldots$ et la suite stationne à I_m. □

4.1.4 Lemme. ***Tout quotient d'un anneau noethérien est noethérien.***

Preuve : On doit montrer que pour tout morphisme surjectif $A \to B$ avec A noethérien, l'anneau B est noethérien. Si J est un idéal de B, sa préimage dans A est un idéal qui est de type fini par hypothèse, donc engendré par un nombre fini d'éléments $x_1, \ldots, x_r$. Les images des x_i engendrent J, donc celui-ci est de type fini et B est noethérien. □

4.1.5 Théorème de la base de Hilbert. ***Soit A un anneau noethérien. Alors, l'anneau de polynômes $A[X]$ est noethérien.***

Ce résultat a été établi par Hilbert en 1888.

Preuve : S'il existe un idéal $I \subset A[X]$ qui n'est pas de type fini, on construit une suite $(f_k)_{k \geqslant 1}$ d'éléments de I de la manière suivante. On choisit dans I un polynôme f_1 de degré minimal puis, une fois construits $f_1, \ldots, f_k$, on choisit dans $I \smallsetminus (f_1, \ldots, f_k)$, qui n'est pas vide d'après l'hypothèse sur I, un polynôme f_{k+1} de degré minimal. Soit $a_k X^{d_k}$ le monôme dominant de f_k. Comme A est noethérien, l'idéal engendré par tous les a_k peut être engendré par un nombre fini d'entre eux,

disons $a_1, \ldots, a_m$. On a donc $a_{m+1} = u_1 a_1 + \cdots + u_m a_m$ pour certains $u_k \in A$. Considérons le polynôme

$$g = (u_1 f_1 X^{d_{m+1}-d_1} + \cdots + u_m f_m X^{d_{m+1}-d_m}) - f_{m+1}.$$

Par construction $\deg(g) < \deg(f_{m+1})$ et $g \in I \setminus (f_1, \ldots, f_m)$. Ceci est une contradiction avec le choix de f_{m+1}. □

On dit qu'une A-algèbre $A \to B$ est *de type fini* si elle peut être engendrée par un nombre fini d'éléments $x_1, \ldots, x_r$ i.e. si la sous-algèbre engendrée par les x_i est égale à B. C'est encore équivalent à dire que B est quotient de l'anneau de polynômes $A[X_1, \ldots, X_r]$.

4.1.6 Corollaire. *Soient A un anneau noethérien. Alors toute A-algèbre de type fini est un anneau noethérien.*

Preuve : D'après le théorème de la base de Hilbert et par récurrence sur r, l'anneau de polynômes $A[X_1, \ldots, X_r]$ est noethérien. Une A-algèbre de type fini $A \to B$ est un quotient d'un anneau $A[X_1, \ldots, X_r]$, donc est noethérien d'après 4.1.4. □

4.1.7 Remarque. Nous avons vu que la classe des anneaux noethériens possède de bonnes propriétés de stabilité par quotient et par passage à un anneau de polynômes en un nombre fini de variables, mais elle n'est pas stable par passage à un sous-anneau. Par exemple, nous verrons que l'anneau $\mathbb{Z}[X]$ est noethérien, mais son sous-anneau $A = \mathbb{Z}[2X, ZX^2, 2X^3, \ldots]$ engendré par les éléments $2X^n$ pour $n \geqslant 1$ ne l'est pas : il est facile de voir que la suite d'idéaux $I_n = (2X^2, 2X^3, \ldots, 2X^n)$ est croissante non stationnaire. Un autre exemple est fourni par l'anneau de polynômes en une infinité de variables $k[X_1, \ldots, X_n, \ldots]$, qui est sous-anneau de son corps de fractions qui est noethérien.

4.2 Divisibilité, anneaux factoriels

Pour tout anneau A, nous notons $A^\times$ le groupe multiplicatif de ses éléments inversibles.

4.2.1 Définitions. Soient A un anneau et a, b des éléments de A.

(1) On dit que $\boldsymbol{a}$ *divise* $\boldsymbol{b}$, et on écrit $\boldsymbol{a \mid b}$, s'il existe $\boldsymbol{c \in A}$ tel que $\boldsymbol{b = ac}$. On dit aussi que $\boldsymbol{a}$ *est un diviseur de* $\boldsymbol{b}$, ou que $\boldsymbol{b}$ *est un multiple de* $\boldsymbol{a}$.

(2) On dit que $\boldsymbol{a}$ et $\boldsymbol{b}$ sont *associés*, et on écrit $\boldsymbol{a \sim b}$, si $\boldsymbol{a \mid b}$ et $\boldsymbol{b \mid a}$.

Si A est intègre, il est équivalent de dire que $a \sim b$ ou qu'il existe $u \in A^\times$ tel que $a = ub$; mais ce n'est pas vrai en général. L'ensemble des éléments associés à 1 est $A^\times$. La relation de divisibilité est une relation réflexive et transitive (on parle de *préordre*) mais pas antisymétrique en général, qui est compatible à la multiplication. La relation d'association $\sim$ est une relation d'équivalence, et la divisibilité induit une relation antisymétrique sur l'ensemble quotient $A/\sim$; c'est donc une relation d'ordre sur $A/\sim$, également compatible à la multiplication (induite).

Notant (a) l'idéal engendré par a, il est clair que $a \mid b$ si et seulement si $(b) \subset (a)$, et que $a \sim b$ si et seulement si $(a) = (b)$. Ainsi $A/\sim$ s'identifie avec l'ensemble des idéaux principaux de A, ordonné par inclusion.

4.2.2 Remarque. Contrairement à ce que la notation habituelle $\leqslant$ laisse entendre, la notion de relation d'ordre n'est pas orientée i.e. ne donne pas de statut différent aux éléments « grands » et aux éléments « petits ». Ainsi, à toute relation d'ordre $\leqslant$ correspond une relation $\leqslant'$ définie par « $\boldsymbol{x \leqslant' y}$ si et seulement si $\boldsymbol{y \leqslant x}$ », et les éléments grands pour $\leqslant$ sont ceux qui sont petits pour $\leqslant'$. Si l'on utilise une notation neutre pour une relation d'ordre (comme $\boldsymbol{x * y}$ au lieu de $\boldsymbol{x \leqslant y}$) ce fait est d'ailleurs évident. En conséquence, lorsque dans un ensemble ordonné on définit les notions de majorant, minorant, maximum, minimum, borne supérieure, borne inférieure, il convient de préciser si les majorants sont les éléments qui se situent à gauche, ou à droite, du signe de relation. Concernant la divisibilité, pour respecter la terminologie de pgcd introduite ci-dessous, on doit convenir que lorsque $\boldsymbol{a \mid b}$, c'est $\boldsymbol{a}$ qui est petit et $\boldsymbol{b}$ qui est grand. Cette convention est un peu étonnante en termes d'idéaux, puisqu'elle veut dire que lorsque $\boldsymbol{(b) \subset (a)}$, c'est $\boldsymbol{(b)}$ le plus grand.

4.2.3 Définition. Soit $\boldsymbol{(a_i)_{i \in I}}$ une famille d'éléments non nuls de $\boldsymbol{A}$.

(1) On dit que *les* $\boldsymbol{a_i}$ *ont un pgcd* si l'ensemble de leurs diviseurs communs possède un plus grand élément dans $\boldsymbol{A/\sim}$. Lorsqu'il existe, le pgcd est bien défini à association près et on le note $\boldsymbol{\mathbf{pgcd}((a_i)_{i \in I})}$.

(2) On dit que *les* a_i *ont un ppcm* si l'ensemble de leurs multiples communs possède un plus petit élément. Lorsqu'il existe, le ppcm est bien défini à association près et on le note $\mathbf{ppcm}((a_i)_{i\in I})$.

Lorsqu'on raisonne dans A, il est commode d'appeler pgcd des a_i n'importe lequel des représentants (mod $\sim$) du pgcd ; le même abus de langage est valable avec les ppcm.

(3) On dit que *les* a_i *sont premiers entre eux* si leur pgcd existe et est égal à 1.

4.2.4 Définitions. Soient A un anneau et p, a, b des éléments de A.

(1) On dit que p est *irréductible* s'il est non nul, non inversible et si pour tous a, b, on a : $p = ab$ entraîne que a ou b est inversible.

(2) On dit que p est *premier* s'il ne divise pas 0 et si l'idéal (p) est premier.

Ces définitions sont en général données pour un anneau A *intègre* ; dans ce cas, bien sûr, p est *premier* s'il est non nul et si l'idéal (p) est premier.

Il est commode d'appeler *factorisation non triviale de* p une écriture $p = ab$ telle que ni a ni b n'est inversible. Ainsi, un élément irréductible est un élément non nul, non inversible qui n'a pas de factorisation non triviale. Si p est premier, il est irréductible mais la réciproque n'est pas vraie en général, voir 4.2.10 et 4.2.13.

4.2.5 Exercice. Montrez que si $a, p \in A$ avec p irréductible, alors $\mathbf{pgcd}(a, p)$ existe et vaut p ou 1, selon que p divise a ou non. En particulier, si p et q sont des irréductibles distincts, alors $\mathbf{pgcd}(p, q) = 1$.

4.2.6 Définition. Soit A un anneau. On dit que A est *factoriel* s'il vérifie les trois conditions suivantes :

(I) Intégrité : A est intègre,

(E) Existence : tout $a \in A$ non nul possède une écriture $a = up_1^{\alpha_1} \dots p_r^{\alpha_r}$ avec $u \in A^\times$, $p_1, \dots, p_r$ irréductibles distincts et $\alpha_i \geqslant 1$ pour tout i,

(U) Unicité : une écriture comme dans (E) est unique, à l'ordre près et à association près des facteurs.

4.2.7 Exemples. Un corps est factoriel. Dans la sous-section 4.3, nous montrerons à l'aide de la division euclidienne que les anneaux $\mathbb{Z}$ et $\boldsymbol{k}[\boldsymbol{X}]$ (pour un corps $\boldsymbol{k}$) sont principaux donc factoriels (voir 4.3.8 et 4.3.3). Cela n'est pas si facile !

La propriété d'unicité (U) est essentielle. Il n'est pas inutile de l'écrire en toutes lettres : elle signifie que si a possède deux décompositions $a = up_1^{\alpha_1} \dots p_r^{\alpha_r} = vq_1^{\beta_1} \dots q_r^{\beta_s}$ comme indiqué dans (E), alors $r = s$ et il existe une permutation $\sigma \in \mathfrak{S}_r$ telle que $p_i \sim q_{\sigma(i)}$ et $\alpha_i = \beta_{\sigma(i)}$, pour tout $i \in \{1, \dots, r\}$.

Soit Σ un ensemble de représentants des éléments irréductibles pour la relation d'association, i.e. un ensemble qui contient un élément de chaque classe. Si A est factoriel, tout élément non nul $a \in A$ possède une *unique* décomposition

$$a = u \prod_{p \in \Sigma} p^{\alpha_p}$$

avec $u \in A^\times$ et $\alpha_p = 0$ sauf pour un nombre fini de p. L'entier α_p est appelé la *multiplicité de p dans a*.

4.2.8 Remarque. Dans les anneaux $\mathbb{Z}$ et $\boldsymbol{k}[\boldsymbol{X}]$, il existe un choix privilégié de famille de représentants des irréductibles. Dans $\mathbb{Z}$, cela résulte de l'existence du *signe* qui permet de sélectionner les irréductibles positifs ; dans $\boldsymbol{k}[\boldsymbol{X}]$ cela résulte de l'existence du *coefficient dominant* qui permet de sélectionner les irréductibles unitaires. En général, il n'y a pas de choix privilégié.

Nous ferons une étude précise de la condition (U) ci-dessous, mais notons d'abord que la condition (E) d'existence de décompositions en irréductibles est, elle, relativement commune. Par exemple, on peut voir que tous les anneaux noethériens la vérifient.

4.2.9 Proposition. ***Tout anneau noethérien vérifie la condition*** (E).

Preuve : **Pour $a \in A$ non nul, notons $\mu(a)$ le supremum de l'ensemble des entiers n tels que a s'écrit comme produit de n éléments non inversibles de A (en particulier $n = 0$ si $a \in A^\times$). C'est un entier ou le symbole ∞. La fonction μ est une mesure de la « grandeur arithmétique » des éléments de $A \setminus \{0\}$. Elle vérifie $\mu(aa') \geqslant \mu(a) + \mu(a')$**

pour tous $a, a' \in A$; $\mu(a) = 0$ ssi $a \in A^\times$; $\mu(a) = 1$ ssi a est irréductible. Supposons qu'il existe $a \in A$ tel que $\mu(a) = \infty$, et construisons par récurrence des écritures comme produit d'éléments non inversibles $a = b_1 \dots b_n a_n$ avec $\mu(a_n) = \infty$. On pose $a_0 = a$. Par récurrence, si $a = b_1 \dots b_n a_n$ avec $\mu(a_n) = \infty$, il existe une factorisation non triviale $a_n = b_{n+1} a_{n+1}$ et l'un des deux facteurs doit être de mesure infinie ; quitte à les renommer, on peut supposer que c'est a_{n+1}. Posons :

$$I_n = (a : b_1 \dots b_n) := \{x \in A, x b_1 \dots b_n \in (a)\}.$$

Une vérification immédiate montre que la suite I_n est croissante, mais elle n'est pas stationnaire car $a_{n+1} \in I_{n+1} \setminus I_n$. Par contraposée, si A est noethérien on a $\mu(a) < \infty$ pour tout a. Soit $a = b_1 \dots b_n$ une écriture en produit d'éléments non inversibles avec $n = \mu(a)$ maximal ; alors les b_i sont nécessairement de mesure 1, c'est-à-dire irréductibles. □

4.2.10 Exemple. (1) Voir [P], contre-exemple dans II, § 3, c). L'anneau $\mathbb{Z}[i\sqrt{5}] = \{a + i\sqrt{5}, a, b \in \mathbb{Z}\}$ est intègre, comme sous-anneau de $\mathbb{C}$. Il est isomorphe à $\mathbb{Z}[T]/(T^2 + 5)$ donc noethérien d'après le théorème de la base de Hilbert 4.1.5. Il vérifie donc (I) et (E). Néanmoins il ne vérifie pas (U) car $9 = 3 \times 3 = (2 + i\sqrt{5})(2 - i\sqrt{5})$ où l'on vérifie que les quatre facteurs qui apparaissent sont irréductibles. On voit aussi dans cet exemple que l'élément 3 est irréductible, mais non premier : en effet

$$\mathbb{Z}[i\sqrt{5}]/(3) \simeq \mathbb{Z}[T]/(T^2+5, 3) \simeq \mathbb{F}_3[T]/(T^2+2) \simeq \mathbb{F}_3[T]/((T-1)(T-2))$$

est un anneau dans lequel la classe de $T - 1$ est un diviseur de 0.

(2) On peut montrer que pour tout corps k, l'anneau quotient $k[X, Y, Z, T]/(XY - ZT)$ vérifie lui aussi (I) et (E) mais pas (U). Ici, la classe de X dans A est un élément irréductible non premier.

Nous étudions maintenant le lien entre la factorialité et l'existence des pgcd.

4.2.11 Lemme. ***Soient A un anneau factoriel. Alors toute famille finie d'éléments non nuls de A possède un pgcd et un ppcm. Plus précisément, soit Σ un ensemble de représentants des éléments irréductibles.***

Soient $a_1, \dots, a_r$ des éléments non nuls de A et $\alpha_p(i)$ la multiplicité de p dans a_i. Alors, on a :

$$\operatorname{pgcd}(a_1, \dots, a_r) = \prod p^{\min_i \alpha_p(i)} \quad \textit{et} \quad \operatorname{ppcm}(a_1, \dots, a_r) = \prod p^{\max_i \alpha_p(i)}.$$

Preuve : Le produit de deux éléments non nuls $a = u \prod p^{\alpha_p}$ et $b = v \prod p^{\beta_p}$ est égal à $c = uv \prod p^{\alpha_p + \beta_p}$. On en déduit que $\prod p^{\alpha_p}$ divise $\prod p^{\beta_p}$ si et seulement si $\alpha_p \leqslant \beta_p$ pour tout p. Le résultat en découle. □

4.2.12 Lemme. *Soit A un anneau intègre et a, b, x non nuls dans A. Si xa et xb possèdent un pgcd, alors a et b possèdent un pgcd et on a la formule* $\operatorname{pgcd}(xa, xb) = x \operatorname{pgcd}(a, b)$.

Preuve : Notons $d_1 = \operatorname{pgcd}(xa, xb)$. Comme x est un diviseur commun de xa et xb, il divise le pgcd, donc il existe d tel que $d_1 = xd$. Comme xd divise xa et xb, on voit que d divise a et b i.e. est un de leurs diviseurs communs. Soit e un diviseur commun de a et b. Alors xe est un diviseur commun de xa et xb, donc il divise leur pgcd $d_1 = xd$. On en déduit que e divise d, donc d est le pgcd de a et b. □

4.2.13 Théorème. *Soit A un anneau vérifiant les conditions* (I) *et* (E)*, par exemple un anneau intègre noethérien. Dans ce qui suit, les lettres a, b, c, p, désignent des éléments quelconques de A. Les conditions suivantes sont équivalentes :*

(1) *A est factoriel ;*

(2) *Lemme d'Euclide : si p est irréductible et $p \mid ab$, alors $p \mid a$ ou $p \mid b$;*

(3) *si p est irréductible, alors (p) est premier ;*

(4) *Lemme de Gauss : si $a \mid bc$ et a est premier avec b, alors $a \mid c$;*

(5) *deux éléments non nuls quelconques de A ont un pgcd.*

Preuve : (2) ⇔ (3) est évident : il s'agit essentiellement d'une reformulation. Nous allons montrer que (1) ⇒ (5) ⇒ (4) ⇒ (2) ⇒ (1). Choisissons une famille Σ de représentants des éléments irréductibles

pour la relation d'assocation, i.e. un ensemble qui contient un élément de chaque classe. Comme A vérifie la propriété (E), tout $a \in A$ possède au moins une décomposition $a = u \prod p^{\alpha_p}$ où p décrit Σ, $u \in A^\times$ et les α_p sont nuls sauf un nombre fini d'entre eux.
(1) $\Rightarrow$ (5) est un cas particulier du lemme 4.2.11.
(5) $\Rightarrow$ (4). Soient a, b, c tels que $\operatorname{pgcd}(a, b) = 1$ et $a \mid bc$, c'est-à-dire qu'il existe $u \in A$ tel que $bc = au$. Utilisant le lemme 4.2.12, on trouve :

$$c = c \operatorname{pgcd}(a, b) = \operatorname{pgcd}(ac, bc) = \operatorname{pgcd}(ac, au) = a \operatorname{pgcd}(c, u),$$

donc a divise c.
(4) $\Rightarrow$ (2) est immédiat en appliquant l'hypothèse avec $(a, b, c) = (p, a, b)$.
(2) $\Rightarrow$ (1). Appelons *longueur* d'une décomposition $a = u \prod p^{\alpha_p}$ la somme des α_p, et notons $\nu(a)$ le minimum des longueurs des décompositions de a. Montrons par récurrence sur $\nu(a)$ que chaque a ne possède qu'une décomposition en irréductibles. Si $\nu(a) = 0$, alors a est inversible et le résultat est clair. Si $\nu(a) \geqslant 1$, choisissons une écriture $a = u \prod p^{\alpha_p}$ qui réalise le minimum des longueurs i.e. telle que $\nu(a) = \sum \alpha_p$. Soit $a = v \prod p^{\beta_p}$ une autre décomposition de a. Comme $\nu(a) \geqslant 1$, il existe q tel que $\alpha_q \geqslant 1$. Alors q divise $v \prod p^{\beta_p}$, donc d'après le lemme d'Euclide il divise l'un des facteurs. Comme les irréductibles distincts sont premiers entre eux (voir exercice 4.2.5), ceci signifie que $\beta_q \geqslant 1$. Ainsi $a = qa'$ avec

$$a' = uq^{\alpha_q - 1} \prod_{p \neq q} p^{\alpha_p} = vq^{\beta_q - 1} \prod_{p \neq q} p^{\beta_p}.$$

Comme $\nu(a') < \nu(a)$, on conclut grâce à l'hypothèse de récurrence. □

Notons que la fonction $\nu : A \to \mathbb{N}$ utilisée dans la preuve de (2) $\Rightarrow$ (1) est distincte de la fonction μ de la preuve de 4.2.9 ; en particulier sa définition comme minimum fait que $\nu(aa') \leqslant \nu(a) + \nu(a')$, contrairement à μ. Lorsque A est noethérien, la fonction μ fait aussi bien l'affaire que ν pour notre besoin, mais en général on ne sait pas si $\mu(a) < \infty$ pour tout a, or on a besoin d'une fonction à valeurs finies pour faire la récurrence.

4.2.14 Remarque. Il existe des anneaux intègres dans lesquels tout couple (et même, toute famille) d'éléments non nuls possède un pgcd mais qui ne sont pas factoriels. Bien sûr, ces anneaux ne sont pas noethériens, à cause du résultat qui précède. Un exemple est l'anneau $\mathscr{H}(\mathbb{C})$ des fonctions holomorphes sur $\mathbb{C}$; une discussion très intéressante de ses propriétés est donnée dans [B].

Nous allons maintenant établir le théorème de Gauss 4.2.17 sur la factorialité des anneaux de polynômes ; nous aurons besoin de la notion capitale suivante.

4.2.15 Définition. Soit A un anneau factoriel et $P \in A[X]$. On appelle *contenu* de P, noté $\mathbf{c}(P)$, le pgcd de ses coefficients. On dit que P est *primitif* si $c(P) = 1$.

4.2.16 Lemme. ***Soient A factoriel et $P, Q \in A$. On a : $\mathrm{c}(PQ) = \mathrm{c}(P)\,\mathrm{c}(Q)$. En particulier, le produit de deux polynômes primitifs est primitif.***

Preuve : Il est clair que pour $a \in A$, on a $\mathrm{c}(aP) = a\,\mathrm{c}(P)$. Notant $P = aP'$ et $Q = bQ'$ avec P', Q' primitifs, on est ramené à démontrer que $\mathrm{c}(P'Q') = \mathrm{c}(P')\,\mathrm{c}(Q')$ i.e. on est ramené au cas où P et Q sont primitifs. Mais dire que P est primitif signifie que pour tout irréductible $p \in A$, l'un au moins de ses coefficients n'est pas divisible par p, c'est-à-dire que la classe $\overline{P}$ dans l'anneau quotient $(A/p)[X] \simeq A[X]/(p)$ est non nulle. De même, la classe $\overline{Q}$ dans $(A/p)[X]$ est non nulle. Comme A/p est intègre, alors $(A/p)[X]$ l'est aussi et $\overline{P}\,\overline{Q}$ est non nulle. Comme c'est vrai pour tout p, alors PQ est primitif. □

Le lemme implique que tout polynôme non nul de $A[X]$ est produit d'une constante non nulle qui est (à association près) son contenu, par un polynôme primitif, notons : $P = \mathrm{c}(P)P'$. De plus, cette décomposition en produit « constant × primitif » est multiplicative au sens où $\mathrm{c}(PQ) = \mathrm{c}(P)\,\mathrm{c}(Q)$ et $(PQ)' = P'Q'$, aux constantes inversibles près bien sûr.

4.2.17 Théorème (Gauss). ***Soit A un anneau factoriel. Alors, l'anneau de polynômes en une variable $A[X]$ est factoriel. De plus, la famille $\mathscr{I}_{A[X]}$ des irréductibles de $A[X]$ est réunion de la famille $\mathscr{I}_A$ des polynômes***

constants irréductibles dans A et de la famille $\mathscr{I}'$ des polynômes primitifs qui sont irréductibles dans $K[X]$, où K est le corps de fractions de A.

Preuve : Il est facile de voir que les éléments de $\mathscr{I}_A$ sont irréductibles dans $A[X]$. Vérifions qu'un élément $P \in \mathscr{I}'$ l'est aussi. Si $P = QR$ dans $A[X]$, comme P est irréductible dans $K[X]$, l'un des deux polynômes Q, R est constant. Par ailleurs, comme $1 = \mathrm{c}(P) = \mathrm{c}(Q)\,\mathrm{c}(R)$, on voit que ce polynôme constant est inversible dans A. Donc P est irréductible. On obtient ainsi l'inclusion $\mathscr{I}_A \cup \mathscr{I}' \subset \mathscr{I}_{A[X]}$. Nous allons montrer que $A[X]$ vérifie les trois conditions (I)-(E)-(U) de 4.2.6, et la preuve montrera au passage que l'inclusion précédente est une égalité.
(I) L'anneau $A[X]$ est intègre, car si $P \neq 0$ et $Q \neq 0$, leurs coefficients dominants sont non nuls, donc le coefficient dominant de PQ est non nul, et $PQ \neq 0$.
(E) Si $P \in A[X]$, on peut écrire $P = aP'$ avec $a \in A$ et P' primitif. On peut décomposer a en produit d'éléments de $\mathscr{I}_A$. Pour terminer, il nous suffit de décomposer P', c'est-à-dire de montrer que : tout polynôme primitif $P \in A[X]$ est produit d'éléments de $\mathscr{I}'$. Observons d'abord que tout polynôme de $K[X]$ peut s'écrire sous la forme $\frac{r}{s}Q$ avec r, s dans A (premiers entre eux si on veut) et $Q \in A[X]$ primitif (il suffit de mettre en facteur le ppcm des coefficients du polynôme). Nous avons besoin d'utiliser ici le fait que l'anneau $K[X]$ est factoriel, ce qui sera établi dans la sous-section suivante, voir 4.3.8 et 4.3.3. On peut donc écrire une factorisation :

$$P = \frac{r}{s}\prod(\frac{r_i}{s_i}Q_i)^{\alpha_i}$$

en produit d'irréductibles *dans* $K[X]$. On en déduit

$$(s\prod s_i^{\alpha_i})P = r\prod r_i^{\alpha_i}\prod Q_i^{\alpha_i}$$

puis en prenant le contenu $s\prod s_i^{\alpha_i} = r\prod r_i^{\alpha_i}$. Il en découle que $P = \prod Q_i^{\alpha_i}$ comme on voulait le montrer. On a montré au passage que tout polynôme de $A[X]$ peut être écrit comme produit d'éléments de $\mathscr{I}_A$ et $\mathscr{I}'$, donc $\mathscr{I}_{A[X]} \subset \mathscr{I}_A \cup \mathscr{I}'$.
(U) Utilisant le fait que la décomposition $P = \mathrm{c}(P)P'$ est multiplicative, on voit que $P \mid Q$ si et seulement si $\mathrm{c}(P) \mid \mathrm{c}(Q)$ et $P' \mid Q'$. En

utilisant cela et le fait que A et $K[X]$ sont factoriels, on montre que le lemme d'Euclide est vrai dans $A[X]$. L'implication (2) $\Rightarrow$ (1) de 4.2.13 permet de conclure. □

Par une récurrence immédiate, on voit alors que pour tout n l'anneau $k[X_1, \ldots, X_n]$ est factoriel. Cela entraîne sans beaucoup d'effort que l'anneau $k[X_1, \ldots, X_n, \ldots]$ de polynômes en une infinité dénombrable de variables, qui est non noethérien, est factoriel : l'observation principale est qu'un polynôme de cet anneau ne fait intervenir qu'un nombre fini m de variables, et on peut alors le décomposer de manière unique en produit d'irréductibles dans $k[X_1, \ldots, X_m]$.

4.3 Anneaux principaux et euclidiens

On rappelle qu'un idéal d'un anneau commutatif est dit *principal* s'il peut être engendré par un seul élément.

4.3.1 Définition. Un anneau A est dit *principal* s'il est intègre et si tous ses idéaux sont principaux.

4.3.2 Exemples. (1) Tout corps est un anneau principal.

(2) Les anneaux $\mathbb{Z}$ et $\mathbb{Z}_{(p)} = \{a/b \in \mathbb{Q}, p \nmid b\}$ sont principaux.

(3) Si k est un corps, l'anneau des polynômes en une variable $k[X]$ et l'anneau des séries formelles en une variable $k[[X]]$ sont principaux.

(4) L'anneau $\mathbb{Z}[X]$ n'est pas principal, car l'idéal $(2, X)$ n'est pas principal. L'anneau $k[X, Y]$ n'est pas principal, car l'idéal (X, Y) n'est pas principal.

(5) Si $n \geqslant 2$ est un entier composé, l'anneau $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre donc n'est pas principal, alors que tous ses idéaux sont principaux.

4.3.3 Proposition. ***Tout anneau principal A est factoriel. Si a et b sont des éléments non nuls de A, leur pgcd est un générateur de l'idéal (a, b) et leur ppcm est un générateur de l'idéal $(a) \cap (b)$.***

Preuve : Soient $a, b \in A$ et d un générateur de l'idéal (a, b). Pour tout $e \in A$, on a :

$$(e \mid a \text{ et } e \mid b) \iff (a) \subset (e) \text{ et } (b) \subset (e) \iff (a, b) \subset (e) \iff (d) \subset (e).$$

Ceci montre que d est un pgcd pour a et b. Soit m un générateur de l'idéal $(a) \cap (b)$, qui est l'idéal des multiples communs de a et b ; la définition de m revient à dire que c'est un ppcm pour a et b. Pour conclure, l'anneau A est intègre, noethérien et admet des pgcd, donc il est factoriel d'après 4.2.13. □

4.3.4 Corollaire (Bézout). *Soient A un anneau principal et $a, b \in A$. Alors a et b sont premiers entre eux si et seulement s'il existe $u, v \in A$ tels que $ua + vb = 1$. Plus généralement, le pgcd de a et b est égal à d si et seulement s'il existe $u, v \in A$* premiers entre eux *tels que $ua + vb = d$.*

Un couple (u, v) satisfaisant les conditions du corollaire est appelé *couple de Bézout*. Notons qu'un énoncé similaire est valable avec un nombre fini d'éléments $a_1, \ldots, a_n$ dans A.

Preuve : D'après 4.3.3, a et b sont premiers entre eux si et seulement si $(a, b) = A$. En particulier $1 \in (a, b)$ donc il existe $u, v \in A$ tels que $ua + vb = 1$. Réciproquement, si d divise a et b alors il divise $ua + vb$ pour tous u, v. Il s'ensuit que si $ua + vb = 1$, alors a et b sont premiers entre eux. Le cas où le pgcd de a et b est un élément d quelconque n'est pas beaucoup plus difficile et est laissé à la lectrice. □

4.3.5 Définition. Soit $\boldsymbol{A}$ un anneau intègre. On appelle *stathme (euclidien)* ou *jauge (euclidienne)* sur $\boldsymbol{A}$ une application $\boldsymbol{\delta : A \to \mathbb{N}}$ satisfaisant les deux conditions :

(1) (croissance) si $\boldsymbol{a \mid b}$ et $\boldsymbol{b \neq 0}$, alors $\boldsymbol{\delta(a) \leqslant \delta(b)}$;

(2) (division euclidienne) pour tout couple $\boldsymbol{(a, b) \in A^2}$ avec $\boldsymbol{b \neq 0}$, il existe un couple $\boldsymbol{(q, r) \in A^2}$ tel que $\boldsymbol{a = bq + r}$ et $\boldsymbol{\delta(r) < \delta(b)}$.

On appelle *anneau euclidien* un anneau intègre muni d'un stathme euclidien.

4.3.6 Remarques. (1) L'élément $\mathbf{0}$ est l'unique élément de stathme minimal. En effet, si $\boldsymbol{a \neq 0}$, la condition (2) avec $\boldsymbol{b = a}$ fournit $\boldsymbol{\delta(0) < \delta(a)}$. Par ailleurs, quitte à changer $\boldsymbol{\delta}$ en $\boldsymbol{\delta - \delta(0)}$, on peut toujours supposer que $\boldsymbol{\delta(0) = 0}$.

(2) S'il existe une application $\delta : A \to \mathbb{N}$ satisfaisant la condition (2), alors il existe un stathme, défini par $\delta'(0) = \delta(0)$ et $\delta'(a) = \min\{\delta(ax), x \neq 0\}$ si $a \neq 0$. La condition de croissance (1) est utile pour les algorithmes.

(3) Cette définition est l'objet de petites variations dans la littérature, en général sans conséquence. Par exemple, pour certains le stathme est une fonction $\delta : A \setminus \{0\} \to \mathbb{N}$, et pour d'autres c'est une fonction $\delta : A \to \mathbb{N} \cup \{-\infty\}$ avec $\delta(0) = -\infty$.

(4) On ne demande pas a priori que le couple (q, r) soit unique. L'unicité, lorsqu'elle a lieu, peut cependant être utile.

4.3.7 Exemples. (1) $\mathbb{Z}$ est euclidien pour $\delta(a) = |a|$.

(2) Si k est un corps, $k[X]$ est euclidien avec $\delta(P) = 0$ si $P = 0$ et $\delta(P) = 1 + \deg(P)$ si $P \neq 0$. (Il peut sembler plus naturel de prendre $\delta : k[X] \to \mathbb{N} \cup \{-\infty\}$ égal au degré, *cf* la remarque (3) précédente.)

(3) $\mathbb{Z}[i]$ est euclidien pour $\delta(a) = |a|^2$.

4.3.8 Proposition. ***Tout anneau euclidien A est principal.***

Preuve : Soit I un idéal de A. Si $I = (0)$, il est principal. Sinon, soit b un élément non nul de I de stathme minimal. Pour tout $a \in I$, on peut écrire $a = bq + r$ avec $\delta(r) < \delta(b)$. Alors $r = a - bq \in I$ a un stathme inférieur à celui de b, ce qui n'est possible que si $r = 0$. Ceci montre que $I = (b)$. □

4.3.9 Définition. Soient A un anneau commutatif, I, J des idéaux, $a, b \in A$.

(1) On dit que I et J sont *étrangers* si $I + J = A$, c'est-à-dire s'il existe $i \in I$ et $j \in J$ tels que $i + j = 1$.

(2) On dit que $a, b \in A$ sont *étrangers* si (a) et (b) le sont, c'est-à-dire s'il existe $u, v \in A$ tels que $ua + vb = 1$.

4.3.10 Théorème des restes chinois. ***Soient A un anneau commutatif et I, J des idéaux étrangers. Alors le morphisme canonique $A/IJ \to A/I \times A/J$ est un isomorphisme. En particulier si A est principal et a, b sont premiers entre eux, le morphisme canonique $A/(ab) \to A/(a) \times A/(b)$ est un isomorphisme.***

On rappelle (voir 2.3.3) que le produit IJ est l'idéal engendré par les produits ij avec $i \in I$ et $j \in J$, ou encore l'ensemble des sommes finies de tels produits ij.

Preuve : Notons $a \mod K$ la classe de a modulo un idéal K. Le morphisme $f : A/IJ \to A/I \times A/J$ envoie $(a \mod IJ)$ sur $(a \mod I, a \mod J)$. Comme I et J sont étrangers, il existe $i \in I$ et $j \in J$ tel que $i + j = 1$. Montrons que $IJ = I \cap J$. L'inclusion directe est vraie sans hypothèse sur I et J, et la réciproque vient du fait que si $x \in I \cap J$, on a $x = xi + xj \in IJ$. Ceci montre que f est injectif. Par ailleurs, soient x, y dans A. Utilisant le fait que $i \equiv 1 \mod J$ et $j \equiv 1 \mod I$, on voit que $(x \mod I, y \mod J) \in A/I \times A/J$ est l'image de $xj + yi \in A/IJ$. Ceci montre que f est surjectif, ainsi f est un isomorphisme.

Dans le cas principal, la proposition 4.3.3 montre que a et b sont premiers entre eux si et seulement s'ils sont étrangers, donc le résultat découle de ce qui précède. □

4.3.11 Proposition. *Soient A un anneau principal qui n'est pas un corps, et $p \in A$ non nul. Les conditions suivantes sont équivalentes :*

(1) *p est irréductible,*

(2) *l'idéal (p) est premier,*

(3) *l'idéal (p) est maximal.*

Preuve : L'implication (3) ⇒ (2) est évidente et l'implication (2) ⇒ (1) est facile. Il ne reste qu'à montrer que (1) ⇒ (3). Soit $(p) \subsetneq (a) \subset A$ une chaîne d'idéaux. De $p \in (a)$ il découle qu'il existe $b \in A$ tel que $p = ab$. Comme $(p) \neq (a)$, on doit avoir $a \sim 1$ donc $(a) = A$. Ceci montre que (p) est maximal. □

5 Modules sur les anneaux principaux

5.1 Matrices à coefficients dans un anneau principal

Pour tout anneau commutatif A, nous notons $\mathrm{M}_{n,p}(A)$ le A-module des matrices de taille (n, p), qui s'identifie au A-module des mor-

phismes de A^p dans A^n. C'est un A-module libre de rang np, dont la base canonique est formée des matrices $E_{i,j}$ avec $1 \leqslant i \leqslant n$ et $1 \leqslant j \leqslant p$, dont le seul coefficient non nul est celui placé en position (i,j) qui vaut 1 :

$$E_{i,j} = \begin{array}{c} \\ i \to \end{array} \begin{array}{c} \begin{array}{c} j \\ \downarrow \end{array} \\ \begin{pmatrix} & & \\ & 1 & \\ & & \end{pmatrix} \end{array}.$$

Si $E_{i,j} \in \mathrm{M}_{n,p}(A)$ et $E_{k,l} \in \mathrm{M}_{p,q}(A)$, on a :

$$E_{i,j}E_{k,l} = \delta_{j,k}E_{i,l}$$

où $\delta_{j,k}$ désigne le symbole de Kronecker.

Le A-module $\mathrm{M}_n(A) = \mathrm{M}_{n,n}(A)$ des matrices carrées, qui s'identifie à $\mathrm{End}(A^n)$, est muni d'une structure d'anneau et même de A-algèbre. Le groupe de ses éléments inversibles est $\mathrm{GL}_n(A)$, le groupe des matrices de déterminant inversibles. Nous noterons aussi $\mathrm{SL}_n(A)$ le sous-groupe des matrices de déterminant 1. On appelle *matrices élémentaires* les matrices de $\mathrm{SL}_n(A)$ définies pour $i \neq j$ et $a \in A$ par :

$$E_{i,j}(a) = \mathrm{Id} + aE_{i,j} = \begin{array}{c} \\ i \to \end{array} \begin{array}{c} \begin{array}{c} j \\ \downarrow \end{array} \\ \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & a & \ddots & \\ & & & 1 \end{pmatrix} \end{array}.$$

On a clairement $E_{i,j}(a) \in \mathrm{SL}_n(A)$. Notons $\mathrm{E}_n(A)$ le sous-groupe de $\mathrm{SL}_n(A)$ engendré par les $E_{i,j}(a)$; ce groupe a une importance algorithmique dans les calculs que nous ferons ci-dessous.

5.1.1 Lemme. *Soient $M \in \mathrm{M}_{n,p}(A)$, L_i sa i-ième ligne et C_j sa j-ième colonne.*

(1) *Multiplier M à droite par une matrice élémentaire $E_{i,j}(a) \in \mathrm{M}_p(A)$ a pour seul effet de remplacer la j-ième colonne C_j par $C_j + aC_i$. En abrégé : $C_j \to C_j + aC_i$.*

(2) ***Multiplier M à gauche par une matrice élémentaire $E_{i,j}(a) \in \mathrm{M}_n(A)$ a pour seul effet de remplacer la i-ième ligne L_i par $L_i + aL_j$. En abrégé : $L_i \to L_i + aL_j$.***

Preuve : Ces faits sont immédiats en posant le calcul matriciel. On peut les démontrer de manière plus formelle, comme suit. Le coefficient de $E_{i,j}(a)$ en position (u, v) est $\delta_{u,v} + a\delta_{i,u}\delta_{j,v}$. On en déduit que le coefficient de $ME_{i,j}(a)$ de position u, v est :

$$\sum_w m_{u,w}(\delta_{w,v} + a\delta_{i,w}\delta_{j,v}) = m_{u,v} + am_{u,i}\delta_{j,v}.$$

On voit que les coefficients de la colonne C_v sont inchangés lorsque $v \neq j$, et se voient additionner $am_{u,i}$ lorsque $v = j$. C'est ce qu'affirme (1). Le point (2) se démontre de manière identique, ou en observant qu'il résulte de (1) par transposition. □

5.1.2 Définition. On dit que deux matrices M, M' de $\mathbf{M}_{n,p}(A)$ sont :

(1) *équivalentes* s'il existe $P \in \mathbf{GL}_n(A)$ et $Q \in \mathbf{GL}_p(A)$ telles que $M' = PMQ$; on note $M \overset{\mathrm{G}}{\sim} M'$ ou simplement $M \sim M'$.

(2) **S**-*équivalentes* si P et Q peuvent être choisies dans $\mathbf{SL}_n$ et $\mathbf{SL}_p$; on note $M \overset{\mathrm{S}}{\sim} M'$.

(3) **E**-*équivalentes* si P et Q peuvent être choisies dans $\mathbf{E}_n$ et $\mathbf{E}_p$; on note $M \overset{\mathrm{E}}{\sim} M'$.

Deux matrices sont équivalentes si elles sont dans la même orbite pour l'action à gauche du produit $\mathrm{GL}_n(A) \times \mathrm{GL}_p(A)$ sur $\mathrm{M}_{n,p}(A)$ donnée par :

$$(P, Q).M = PMQ^{-1}.$$

Elles sont S-équivalentes, resp. E-équivalentes, si elles sont dans la même orbite pour l'action du sous-groupe $\mathrm{SL}_n(A) \times \mathrm{SL}_p(A)$, resp. $\mathrm{E}_n(A) \times \mathrm{E}_p(A)$.

5.1.3 Théorème (Forme normale de Smith). ***Si A est principal, toute***

matrice $M \in \mathrm{M}_{n,p}(A)$ est S*-équivalente à une matrice de la forme :*

$$D = \mathrm{diag}(d_1, \ldots, d_r) = \begin{pmatrix} d_1 & & 0 & & 0 \\ & \ddots & & & \\ 0 & & d_r & & \\ 0 & \cdots & 0 & \cdots & 0 \end{pmatrix}$$

avec $d_i \in A \smallsetminus \{0\}$ et $d_1 \mid d_2 \mid \cdots \mid d_r$. Une telle matrice D est dite en forme normale de Smith*. Si A est euclidien, la matrice M est même* E*-équivalente à D. De plus, la forme normale de Smith de M est unique à association près des coefficients non nuls : si*

$$\mathrm{diag}(d_1, \ldots, d_r) \overset{\mathrm{G}}{\sim} \mathrm{diag}(d'_1, \ldots, d'_s),$$

sont deux formes normales de Smith équivalentes, on a $r = s$ et $d_i \sim d'_i$ pour tout i. Autrement dit, la suite d'idéaux $(d_1) \supset (d_2) \supset \cdots \supset (d_r)$ ne dépend que de M. Ces idéaux, ou les d_i, sont appelés les facteurs invariants *de M.*

La preuve consiste à décrire un algorithme qui met M en forme normale de Smith. Elle se présente comme une récurrence sur la « taille » et le « poids » de M, deux quantités que nous définissons tout de suite. On appelle *taille de M* la quantité $\tau(M) = \max(n, p)$. C'est un entier $\geqslant 1$. Pour $a \in A$ non nul, appelons *poids de a* la quantité :

$$\pi(a) = \begin{cases} \delta(a) \text{ si } A \text{ est euclidien, muni d'un stathme } \delta, \\ \text{nombre de facteurs irréductibles de } a, \text{ sinon.} \end{cases}$$

et pour $M = (m_{i,j})$ non nulle, définissons le *poids de M* par :

$$\pi(M) = \min_{i,j\,;\, m_{i,j} \neq 0} \pi(m_{i,j}).$$

C'est un entier $\geqslant 0$. La fonction π mesure la « grandeur arithmétique » tout comme les fonctions μ et ν que nous avons utilisées dans 4.2. Avant de commencer la preuve du théorème, nous allons décrire trois procédures qui permettent de réaliser certaines opérations simples sur les matrices.

Procédure P1. Soient $a, b \in A$. Par des multiplications à droite par des matrices élémentaires, on a les équivalences matricielles :

$$\begin{aligned}(\ a \ \ b \ ) &\overset{\mathrm{E}}{\sim} (\ a \ \ a+b \ ) \text{ en faisant } C_2 \to C_2 + C_1, \\ &\overset{\mathrm{E}}{\sim} (\ -b \ \ a+b \ ) \text{ en faisant } C_1 \to C_1 - C_2, \\ &\overset{\mathrm{E}}{\sim} (\ -b \ \ a \ ) \text{ en faisant } C_2 \to C_2 + C_1.\end{aligned}$$

Pour une matrice quelconque, la même suite de trois opérations permet d'échanger deux colonnes, à un signe près (mais le signe ne nous importe pas). La même suite de trois multiplications à gauche permet d'échanger deux lignes de M, à un signe près. En conséquence, par des opérations élémentaires, tout coefficient de M peut être placé en position en position $(1,1)$, avec des changements de signe éventuels, mais sans changer $\pi(M)$.

Procédure P2. Soient $a, q \in A$. Alors, on a :

$$(\ a \ \ qa \ ) \overset{\mathrm{E}}{\sim} (\ a \ \ 0 \ ) \text{ en faisant } C_2 \to C_2 - qC_1.$$

Ainsi, si un coefficient de M divise un coefficient de la même ligne, on peut remplacer ce dernier par 0, en ne changeant que les éléments de sa colonne.

Procédure P3. Soient $a, b \in A$ non nuls, avec $a \nmid b$.
(1) Dans le cas non euclidien, posons $d = \mathrm{pgcd}(a, b)$. D'après le théorème de Bézout (énoncé ici en corollaire 4.3.4) il existe $u, v \in A$ tels que $d = ua + vb$ et $a', b' \in A$ tels que $a = da'$, $b = db'$. On en déduit que $ua' + vb' = 1$ et $ab' = da'b' = ba'$. En conséquence :

$$(\ a \ \ b \ ) \begin{pmatrix} u & -b' \\ v & a' \end{pmatrix} = (\ d \ \ 0 \ )$$

où la matrice $(2,2)$ qui intervient est de déterminant 1 i.e. dans $\mathrm{SL}_2(A)$. On appelle *matrice de Bézout* une matrice de cette forme. Par ailleurs d divise a mais n'est pas associé à a, car $a \nmid b$. Ainsi $(\ a \ \ b \ ) \overset{\mathrm{S}}{\sim} (\ d \ \ 0 \ )$ avec $\pi(d) < \pi(a)$.
(2) Dans le cas euclidien, on écrit la division euclidienne $b = aq + r$ avec $\delta(r) < \delta(a)$, d'où

$$(\ a \ \ b \ ) \begin{pmatrix} 1 & -q \\ 0 & 1 \end{pmatrix} = (\ a \ \ r \ )$$

où la matrice $(2,2)$ qui intervient est un élément de $E_2(A)$. Ainsi $\begin{pmatrix} a & b \end{pmatrix} \overset{\mathrm{E}}{\sim} \begin{pmatrix} a & r \end{pmatrix}$ avec $\pi(r) < \pi(a)$. Ceci termine la description de la procédure 3.

5.1.4 Preuve de 5.1.3 : existence. Comme indiqué précédemment, on fait une récurrence sur l'entier $\tau(M) + \pi(M)$. Si $\tau(M) = 1$, la matrice M est sous forme normale de Smith ; en particulier ceci initialise la récurrence. Supposons $\tau(M) + \pi(M) \geqslant 2$ et supposons le théorème démontré pour les valeurs inférieures de $\tau + \pi$.

Par P1, on peut supposer que $m_{1,1} \neq 0$ et $\pi(m_{1,1}) = \pi(M)$.

S'il existe $\ell > 1$ tel que $m_{1,1} \nmid m_{1,\ell}$ (ou $m_{1,1} \nmid m_{\ell,1}$), d'après P3 on a $M \sim M'$ avec $\pi(M') < \pi(M)$. On conclut alors par l'hypothèse de récurrence. Noter qu'ici, comme à chaque fois qu'on utilise P3, l'équivalence est la $\mathbf{S}$-équivalence ou la $\mathbf{E}$-équivalence selon qu'on est dans le cas euclidien ou non.

Si $m_{1,1}$ divise tous les coefficients de L_1 et C_1, on applique P2 à $\begin{pmatrix} m_{1,1} & m_{1,\ell} \end{pmatrix}$ pour chaque ℓ. La ligne L1 devient $\begin{pmatrix} m_{1,1} & 0 & \cdots & 0 \end{pmatrix}$ et la colonne C1 est inchangée. On applique ensuite P2 à $\binom{m_{1,1}}{m_{\ell,1}}$ pour chaque ℓ. On a obtenu :

$$M \sim \begin{pmatrix} m_{1,1} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & M_1 & \\ 0 & & & \end{pmatrix}.$$

Comme $\tau(M_1) < \tau(M)$, par l'hypothèse de récurrence il existe des matrices P_1, Q_1 appartenant à $\mathbf{SL}_*(A)$ ou $\mathbf{E}_*(A)$ telles que $M_1 = P_1 D_1 Q_1$ où $D_1 = \mathbf{diag}(d_2, \ldots, d_r)$ avec $d_2 \mid \cdots \mid d_r$. En posant ;

$$P = \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & & & \\ \vdots & & P_1 & \\ 0 & & & \end{pmatrix}, \quad Q = \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & & & \\ \vdots & & Q_1 & \\ 0 & & & \end{pmatrix},$$

et $D = \mathbf{diag}(m_{1,1}, d_2, \ldots, d_r)$, on obtient $M = PDQ$. Si $m_{1,1} \mid d_2$ on a terminé. Sinon, on observe que :

$$\begin{pmatrix} m_{1,1} & 0 \\ 0 & d_2 \end{pmatrix} \overset{\mathrm{E}}{\sim} \begin{pmatrix} m_{1,1} & d_2 \\ 0 & d_2 \end{pmatrix}$$

en faisant $\boldsymbol{L_1 \leftarrow L_1 + L_2}$. Comme $\boldsymbol{m_{1,1} \nmid d_2}$, on peut alors appliquer P3 pour obtenir $\boldsymbol{M \sim M'}$ avec $\boldsymbol{\pi(M') < \pi(M)}$ et on conclut par l'hypothèse de récurrence. □

Pour démontrer l'assertion d'unicité dans le théorème 5.1.3, nous utiliserons une description des facteurs invariants d'une matrice M en termes des idéaux de A engendrés par ses mineurs.

5.1.5 Notation. Soient $\boldsymbol{A}$ un anneau, $\boldsymbol{M \in \mathrm{M}_{n,p}(A)}$ et $\boldsymbol{r \geqslant 0}$. On note $\boldsymbol{I_r(M)}$ l'idéal de $\boldsymbol{A}$ engendré par les mineurs de taille $\boldsymbol{r}$ de $\boldsymbol{M}$.

5.1.6 Proposition. ***Les idéaux $I_r(M)$ vérifient les propriétés suivantes :***

(1) $\boldsymbol{I_r({}^{\mathrm{t}}M) = I_r(M)}$,

(2) $\boldsymbol{I_{r+1}(M) \subset I_r(M)}$,

(3) $\boldsymbol{I_r(MN) \subset I_r(M) \cap I_r(N)}$ ***pour*** $\boldsymbol{M \in \mathrm{M}_{n,p}(A)}$ ***et*** $\boldsymbol{N \in \mathrm{M}_{p,q}(A)}$,

(4) $\boldsymbol{I_r(PMQ) = I_r(M)}$ ***pour*** $\boldsymbol{P \in \mathrm{GL}_n(A)}$ ***et*** $\boldsymbol{Q \in \mathrm{GL}_p(A)}$,

(5) ***Soit*** $\boldsymbol{D = \mathrm{diag}(d_1, \ldots, d_n)}$ ***avec*** $\boldsymbol{d_1 \mid \cdots \mid d_n}$. ***Alors*** $\boldsymbol{I_r(D) = (d_1 \ldots d_r)}$ ***si*** $\boldsymbol{0 \leqslant r \leqslant n}$, ***et*** $\boldsymbol{I_r(M) = (0)}$ ***si*** $\boldsymbol{r > n}$.

Preuve : (1) est clair car M et ${}^{\mathrm{t}}M$ ont les mêmes mineurs.

(2) provient du fait que par développement par rapport à une ligne, un mineur de taille $r+1$ est combinaison linéaire de mineurs de taille r.

(3) Les colonnes de MN sont des combinaisons linéaires de celles de M. Par multilinéarité des déterminants, les r-mineurs de MN sont des combinaisons linéaires des r-mineurs de M, donc $I_r(MN) \subset I_r(M)$. Par transposition, on a aussi $I_r(MN) \subset I_r(N)$.

(4) Les matrices P, Q étant inversibles vérifient $I_r(P) = I_r(Q) = A$. D'après (3) on a $I_r(PMQ) \subset I_r(P) \cap I_r(M) \cap I_r(Q) = I_r(M) = I_r(P^{-1}PMQQ^{-1}) \subset I_r(PMQ)$ donc toutes les inclusions sont des égalités.

(5) L'idéal $I_r(D)$ est engendré par les produits de r éléments parmi les d_i. Compte tenu de la condition de divisibilité, tous sont multiples de $d_1 \ldots d_r$. □

5.1.7 Remarque. On peut améliorer 5.1.6(3) en montrant que $\boldsymbol{I_r(MN)}$ est inclus dans le produit d'idéaux $\boldsymbol{I_r(M)I_r(N)}$. Pour cela, on va généraliser la formule de multiplicativité du déterminant 3.3.3 (qui est le mineur d'ordre maximal) au cas des mineurs d'ordre $\boldsymbol{r}$. Soient $\boldsymbol{M \in \mathbf{M}_{n,p}(A)}$ une matrice et $\boldsymbol{I \subset \{1,\ldots,n\}}$, $\boldsymbol{J \subset \{1,\ldots,p\}}$ des sous-ensembles de même cardinal $\boldsymbol{r \leqslant \min(n,p)}$. Soit $\boldsymbol{M_{I,J}}$ la sous-matrice de $\boldsymbol{M}$ dont les lignes sont dans $\boldsymbol{I}$ et les colonnes dans $\boldsymbol{J}$. Avec les conventions de 3.3.5, le mineur correspondant est :

$$\boldsymbol{m_{I,J} = \det(M_{I,J}) = \sum_{\sigma : I \simeq J} \epsilon(\sigma) \prod_{i \in I} m_{i,\sigma(i)}.}$$

Pour deux matrices multipliables $\boldsymbol{M \in \mathbf{M}_{n,p}(A)}$ et $\boldsymbol{N \in \mathbf{M}_{p,q}(A)}$, on a la formule suivante pour les mineurs du produit $\boldsymbol{P = MN}$:

$$\boldsymbol{p_{I,J} = \sum_{K} m_{I,K}\, n_{K,J}}$$

où la somme porte sur les parties $\boldsymbol{K \subset \{1,\ldots,p\}}$ de cardinal $\boldsymbol{r}$. En effet, en

reprenant la stratégie de la preuve du théorème 3.3.3 :

$$\begin{aligned}
\boldsymbol{p_{I,J}} &= \sum_{\boldsymbol{\sigma : I \simeq J}} \boldsymbol{\epsilon(\sigma)} \prod_{\boldsymbol{i \in I}} \sum_{\boldsymbol{k \in \{1..p\}}} \boldsymbol{m_{i,k} n_{k,\sigma(i)}} \\
&= \sum_{\boldsymbol{\sigma : I \simeq J}} \boldsymbol{\epsilon(\sigma)} \sum_{\boldsymbol{\tau : I \to \{1..p\}}} \prod_{\boldsymbol{i \in I}} \boldsymbol{m_{i,\tau(i)} n_{\tau(i),\sigma(i)}}
\end{aligned}$$

en développant le produit de sommes ;

ici $\boldsymbol{\tau}$ décrit toutes les applications de $\boldsymbol{I}$ dans $\boldsymbol{\{1, \ldots, p\}}$;

$$= \sum_{\boldsymbol{\tau : I \to \{1..p\}}} \sum_{\boldsymbol{\sigma : I \simeq J}} \boldsymbol{\epsilon(\sigma)} \prod_{\boldsymbol{i \in I}} \boldsymbol{m_{i,\tau(i)} n_{\tau(i),\sigma(i)}}$$

en permutant $\sum_{\boldsymbol{\sigma}}$ et $\sum_{\boldsymbol{\tau}}$;

$$= \sum_{\boldsymbol{\tau : I \to \{1..p\}}} \prod_{\boldsymbol{i \in I}} \boldsymbol{m_{i,\tau(i)}} \left(\sum_{\boldsymbol{\sigma : I \simeq J}} \boldsymbol{\epsilon(\sigma)} \prod_{\boldsymbol{i \in I}} \boldsymbol{n_{\tau(i),\sigma(i)}} \right)$$

car $\prod_{\boldsymbol{i}} \boldsymbol{m_{i,\tau(i)}}$ ne dépend pas de $\boldsymbol{\sigma}$,

$$= \sum_{\boldsymbol{\tau : I \hookrightarrow \{1..p\}}} \prod_{\boldsymbol{i \in I}} \boldsymbol{m_{i,\tau(i)}} \left(\sum_{\boldsymbol{\sigma : I \simeq J}} \boldsymbol{\epsilon(\sigma)} \prod_{\boldsymbol{i \in I}} \boldsymbol{n_{\tau(i),\sigma(i)}} \right)$$

car la parenthèse est un déterminant nul si $\boldsymbol{\tau}$ n'est pas injectif ;

ici $\boldsymbol{\tau}$ décrit les applications *injectives*,

$$= \sum_{\substack{\boldsymbol{K \subset \{1..p\}} \\ \boldsymbol{|K| = r}}} \sum_{\boldsymbol{\tau : I \simeq K}} \prod_{\boldsymbol{i \in I}} \boldsymbol{m_{i,\tau(i)}} \left(\sum_{\boldsymbol{\sigma : I \simeq J}} \boldsymbol{\epsilon(\sigma)} \prod_{\boldsymbol{i \in I}} \boldsymbol{n_{\tau(i),\sigma(i)}} \right)$$

en écrivant que $\boldsymbol{\tau}$ est une bijection sur son image,

$$= \sum_{\boldsymbol{K}} \sum_{\boldsymbol{\tau : I \simeq K}} \prod_{\boldsymbol{i \in I}} \boldsymbol{m_{i,\tau(i)}} \left(\sum_{\boldsymbol{\rho : K \simeq J}} \boldsymbol{\epsilon(\rho)\epsilon(\tau)} \prod_{\boldsymbol{k \in K}} \boldsymbol{n_{k,\rho(k)}} \right)$$

en posant $\boldsymbol{\rho = \sigma\tau^{-1} : K \simeq J}$ et $\boldsymbol{k = \tau(i)}$,

$$\begin{aligned}
&= \sum_{\boldsymbol{K}} \left(\sum_{\boldsymbol{\tau : I \simeq K}} \boldsymbol{\epsilon(\tau)} \prod_{\boldsymbol{i \in I}} \boldsymbol{m_{i,\tau(i)}} \right) \left(\sum_{\boldsymbol{\rho : K \simeq J}} \boldsymbol{\epsilon(\rho)} \prod_{\boldsymbol{k \in K}} \boldsymbol{n_{k,\rho(k)}} \right) \\
&= \sum_{\boldsymbol{K}} \boldsymbol{m_{I,K}\, n_{K,J}}.
\end{aligned}$$

Cette formule montre que le mineur $\boldsymbol{p_{I,J}}$ d'un produit est somme de produits de

mineurs, de sorte que $\boldsymbol{I_r(MN) \subset I_r(M)I_r(N)}$. Par ailleurs, on est immédiatement frappé par le fait qu'elle ressemble comme deux gouttes d'eau à la formule du produit matriciel. Cette remarque peut être exploitée en associant à $\boldsymbol{M}$ une matrice $\wedge^r \boldsymbol{M}$ dont les coefficients sont les mineurs $\boldsymbol{m_{I,J}}$, indicés par les paires $\boldsymbol{(I,J)}$ de parties de même cardinal $\boldsymbol{r}$, de telle manière que sous les conditions précédentes :

$$\wedge^r(\boldsymbol{MN}) = \wedge^r(\boldsymbol{M}) \wedge^r (\boldsymbol{N}).$$

Cette matrice est appelée *puissance extérieure $\boldsymbol{r}$-ième de $\boldsymbol{M}$*.

5.1.8 Corollaire : unicité dans 5.1.3. ***Soient $D = \mathrm{diag}(d_1, \ldots, d_s), D' = \mathrm{diag}(d'_1, \ldots, d'_t)$ deux matrices en forme de Smith dans $\mathrm{M}_{n,p}(A)$. Supposons que $D' = PDQ$ avec $P \in \mathrm{GL}_n(A)$ et $Q \in \mathrm{GL}_p(A)$. Alors $s = t$ et $d_i \sim d'_i$ pour tout i.***

Preuve : D'après les points (4) et (5) de 5.1.6, on a $(d_1 \ldots d_r) = I_r(D) = I_r(D') = (d'_1 \ldots d'_r)$ pour tout r. Ceci montre que $s = \inf\{r; I_r(D) = 0\} = \inf\{r; I_r(D') = 0\} = t$ puis, par récurrence sur i, que $d_i \sim d'_i$ pour tout i. □

5.1.9 Corollaire. ***Soient M, N des A-modules libres de type fini, de rangs respectifs p et n. Soit $u : M \to N$ un morphisme. Alors il existe des bases $\mathscr{B}$ et $\mathscr{C}$ pour M et N tels que $\mathrm{Mat}_{\mathscr{B},\mathscr{C}}(u)$ soit une matrice diagonale de Smith $\mathrm{diag}(d_1, \ldots, d_r)$. Les idéaux $(d_1), \ldots, (d_r)$ ne dépendent que de u. De plus :***

(1) ***u est injectif si et seulement si $r = p$,***

(2) ***u est surjectif si et seulement $r = n$ et $d_i \in A^\times$ pour tout i.***

Preuve : La preuve est laissée en exercice, utilisant 5.1.3. □

5.2 Structure des modules de type fini sur un anneau principal

5.2.1 Lemme. ***Soient A un anneau commutatif noethérien et $n \geqslant 1$ un entier. Alors tout sous-module de A^n est de type fini. Si A est principal, tout sous-module de A^n est engendré par au plus n éléments.***

Preuve : On fait une récurrence sur n. Si $n = 1$, un sous-module de A n'est rien d'autre qu'un idéal et le résultat découle de 4.1.3. En général, soit M un sous-module de A^n avec $n \geqslant 2$. Notons A^{n-1} le sous-module libre de rang $n-1$ engendré par les $n-1$ premiers vecteurs de la base canonique de A^n. Par l'hypothèse de récurrence, le module $N = M \cap A^{n-1}$ est de type fini. De plus, l'inclusion $M \subset A^n$ induit une application A-linéaire injective $M/N \to A^n/A^{n-1} \simeq A$ ce qui montre, encore par l'hypothèse de récurrence, que M/N est de type fini. Soient $x_1, \ldots, x_r$ des générateurs de N et $x_{r+1}, \ldots, x_s$ des éléments de M dont les images dans M/N sont des générateurs. Alors $x_1, \ldots, x_s$ sont des générateurs de M et on a fini. Dans le cas où A est principal, d'après l'hypothèse de récurrence on a $r \leqslant n-1$ et de plus M/N est engendré par un seul élément x_{r+1}. Donc $x_1, \ldots, x_{r+1}$ sont des générateurs de M en nombre $r+1 \leqslant n$ et on a fini. □

5.2.2 Théorème de la base adaptée. *Soit A un anneau principal, L un A-module de type fini, libre de rang l, et $K \subset L$ un sous-A-module. Alors K est un A-module de type fini, libre de rang $k \leqslant l$. De plus, il existe des éléments non nuls $d_1, \ldots, d_k$ de A et une base $\{f_1, \ldots, f_l\}$ de L tels que $d_1 \mid \cdots \mid d_k$ et que $\{d_1 f_1, \ldots, d_k f_k\}$ est une base de K. La suite d'idéaux (d_i) ne dépend que de L et K.*

Preuve : Comme $L \simeq A^l$, d'après le lemme précédent le module K est de type fini, engendré par un certain nombre $k \leqslant l$ d'éléments. Supposons k choisi minimal, et soit $s : A^k \to K$ un morphisme surjectif défini par un système minimal de générateurs. Notons $u : A^k \to K \hookrightarrow L$ la composée de s et de l'inclusion ; c'est un morphisme entre deux A-modules libres de rangs finis. Choisissons des bases pour A^k et L. D'après le théorème 5.1.3 appliqué à la matrice de u dans ces bases, il existe un entier $r \leqslant \min(k,l)$, des éléments non nuls $d_1, \ldots, d_r$ de A tels que $d_1 \mid \cdots \mid d_r$, une base $e_1, \ldots, e_k$ de A^k et une base $f_1, \ldots, f_l$ de L, telles que $u(e_i) = d_i f_i$ pour $1 \leqslant i \leqslant r$ et $u(e_i) = 0$ pour $i > r$. Comme on a choisi k minimal, nécessairement $r = k$. On voit alors que u est injectif donc $K \simeq A^k$ est libre de rang k. Il ne reste que l'unicité à montrer. Supposons que des éléments $d_1, \ldots, d_k$ et une base $(f_1, \ldots, f_l)$ satisfont à la conclusion du théorème, de même

que des éléments $d'_1, \ldots, d'_k$ et une base $(f'_1, \ldots, f'_l)$. Les matrices du morphisme d'inclusion $K \hookrightarrow L$ dans ces deux jeux de bases sont les matrices diagonales $D = \mathrm{diag}(d_1, \ldots, d_k)$ et $D' = \mathrm{diag}(d'_1, \ldots, d'_k)$. Ainsi D et D' sont équivalentes via les matrices de changement de base P, Q et le corollaire 5.1.8 donne l'unicité. □

5.2.3 Calcul pratique de bases adaptées. Supposons donnés des vecteurs $x_1, \ldots, x_k$ dans un A-module libre $L = A^n$, et supposons que l'on souhaite effectuer le calcul pratique de bases adaptées pour le sous-module K engendré par ces vecteurs. Ceci nous amène à préciser la démonstration de 5.2.2 pour la rendre plus effective : on veut trouver les facteurs invariants $d_1, \ldots, d_r$ et une base explicite $e = \{e_1, \ldots, e_n\}$ de A^n telle que les vecteurs $f_1 = d_1 e_1, \ldots, f_r = d_r e_r$ forment une base de K. On a $r \leqslant k$ et comme on ne sait pas a priori si les x_i forment une famille libre, il est possible que $r < k$.

Notons $\epsilon = \{\epsilon_1, \ldots, \epsilon_k\}$ la base canonique de A^k et $\delta = \{\delta_1, \ldots, \delta_n\}$ la base canonique de A^n. La clé du problème est d'étudier le morphisme $u : A^k \to A^n$ qui envoie ϵ_i sur x_i. Utilisons les notations de 3.2.6 pour les matrices d'applications A-linéaires. Notons $M = \mathbf{Mat}_{\epsilon,\delta}(u)$ la matrice de u dans les bases canoniques. Le théorème 5.1.3 de mise sous forme normale de Smith fournit une écriture $PMQ = D$ avec $D = \mathbf{diag}(d_1, \ldots, d_k)$ et $d_1 \mid \cdots \mid d_k$. On notera r l'indice du dernier d_i non nul, donc $d_{r+1} = \cdots = d_k = 0$. Notons $e = \{e_1, \ldots, e_n\}$ les vecteurs colonnes de la matrice P^{-1} et $\gamma = \{\gamma_1, \ldots, \gamma_k\}$ les vecteurs colonnes de la matrice Q. Par définition P et Q sont donc les matrices de passage $P = P_e^\delta = \mathbf{Mat}_{\delta,e}(\mathbf{Id})$ et $Q = P_\epsilon^\gamma = \mathbf{Mat}_{\gamma,\epsilon}(\mathbf{Id})$, voir définition 3.2.9. L'égalité $PMQ = D$ n'est rien d'autre que l'égalité matricielle de changement de bases pour la matrice de u :

$$D = PMQ = \mathbf{Mat}_{\delta,e}(\mathbf{Id})\,\mathbf{Mat}_{\epsilon,\delta}(u)\,\mathbf{Mat}_{\gamma,\epsilon}(\mathbf{Id}) = \mathbf{Mat}_{\gamma,e}(u)$$

associée à la composition $(A^k, \gamma) \xrightarrow{\mathrm{Id}} (A^k, \epsilon) \xrightarrow{u} (A^n, \delta) \xrightarrow{\mathrm{Id}} (A^n, e)$ dans les termes de la proposition 3.2.8. L'égalité $D = \mathbf{Mat}_{\gamma,e}(u)$ implique que $u(\gamma_i) = d_i e_i$ pour $1 \leqslant i \leqslant k$. Ainsi le sous-module K, image de u, est engendré par les vecteurs $f_1 = d_1 e_1, \ldots, f_r = d_r e_r$ qui en forment une base.

D'un point de vue pratique, on dispose les vecteurs donnés x_i en colonnes pour former une matrice M. On applique l'algorithme de mise sous forme normale de Smith qui fournit $PMQ = D$, et on veut connaître les colonnes de P^{-1} qui sont la base $\{e_1, \ldots, e_n\}$. Ici, il est utile d'être un peu astucieux et de ne pas se jeter

sans réfléchir dans le calcul de $\boldsymbol{P}$ et de son inverse. Supposons que $\boldsymbol{A}$ est euclidien, ce qui est toujours le cas dans la pratique. L'algorithme utilise deux procédures P1 et P3(2), puisque P2 est un cas particulier de P3(2). Pour la recherche de bases adaptées, il n'est pas utile de se limiter à des opérations élémentaires de déterminant $\mathbf{1}$; dans P1, on utilisera donc l'échange de colonnes (resp. lignes) *sans changement de signe*, qui est plus simple et qui se fait par la multiplication à droite (resp. à gauche) par une matrice de tranposition $\boldsymbol{T_{ij}} = \mathbf{I}_n - \boldsymbol{E_{ii}} - \boldsymbol{E_{jj}} + \boldsymbol{E_{ij}} + \boldsymbol{E_{ji}}$, pour $\boldsymbol{i \neq j}$. Lorsqu'on effectue l'algorithme, les opérations effectuées sur les lignes se traduisent par des multiplications à gauche par des matrices $\boldsymbol{E_1, \ldots, E_\ell}$ de la forme $\boldsymbol{E_{ij}(a)}$ ou $\boldsymbol{T_{ij}}$. On a alors $\boldsymbol{P = E_\ell \ldots E_1}$ mais puisque c'est $\boldsymbol{P^{-1}}$ qui nous intéresse le plus, on calculera $\boldsymbol{P^{-1} = (E_1)^{-1} \ldots (E_\ell)^{-1}}$ en notant que $\boldsymbol{E_{ij}(a)^{-1} = E_{ij}(-a)}$ et $\boldsymbol{T_{ij}^{-1} = T_{ij}}$. On obtient ainsi la base $\boldsymbol{\{e_1, \ldots, e_n\}}$ en lisant les colonnes de $\boldsymbol{P^{-1}}$.

La base correspondante pour $\boldsymbol{K}$ est $\boldsymbol{\{d_1 e_1, \ldots, d_r e_r\}}$. La vérification du fait que $\boldsymbol{d_j e_j}$ $\boldsymbol{(1 \leqslant j \leqslant r)}$ est dans $\boldsymbol{K}$ est apportée par la matrice $\boldsymbol{Q = (q_{ij})}$. En effet, comme $\boldsymbol{Q = \mathrm{Mat}_{\gamma,\epsilon}(\mathrm{Id})}$, on a $\boldsymbol{\gamma_j = \sum_i q_{ij} \epsilon_i}$. En prenant les images par $\boldsymbol{u}$ on trouve :

$$\boldsymbol{d_j e_j = u(\gamma_j) = \sum_i q_{ij} u(\epsilon_i) = \sum_i q_{ij} x_i}$$

ce qui exprime $\boldsymbol{d_j e_j}$ comme combinaison $\boldsymbol{A}$-linéaire des $\boldsymbol{x_i}$. Dans le cas où $\boldsymbol{x_1, \ldots, x_k}$ ne sont pas libres, en regardant de même les images par $\boldsymbol{u}$ des $\boldsymbol{k - r}$ dernières colonnes de $\boldsymbol{Q}$ on obtient une base du module des relations entre les $\boldsymbol{x_i}$.

5.2.4 Théorème de structure des modules. ***Soit A un anneau principal et M un A-module de type fini. Alors il existe un entier $n \geqslant 0$ et des éléments $d_1, \ldots, d_r$ de A, non inversibles et éventuellement nuls, tels que $d_1 \mid \cdots \mid d_r$ et :***

$$\boldsymbol{M \simeq A/(d_1) \oplus \cdots \oplus A/(d_n).}$$

L'entier n et la suite d'idéaux (d_i) ne dépendent que de M ; ces derniers sont appelés les **facteurs invariants** ***de M.***

En notant q le nombre de d_i qui sont nuls (ce sont les derniers de la liste) et $r = n - q$, on obtient une variante intéressante de cet énoncé : il existe des entiers $q, r \geqslant 0$ et des éléments $d_1, \ldots, d_r$ de A, non nuls et non inversibles, tels que $d_1 \mid \cdots \mid d_r$ et :

$$\boldsymbol{M \simeq A^q \oplus A/(d_1) \oplus \cdots \oplus A/(d_r).}$$

Les entiers q, r et la suite d'idéaux (d_i) ne dépendent que de M. L'entier q est le *rang* de M, défini comme nombre d'éléments d'une partie libre maximale de M. Préparons la preuve de 5.2.4 avec un lemme qui nous servira pour montrer la partie unicité.

5.2.5 Lemme. *Soient A un anneau principal, $d \in A$ et $E = A/(d)$. Pour tout irréductible $p \in A$ et tout entier $h \geqslant 1$, notons $E_h = p^{h-1}E/p^hE$. Soit $k = A/(p)$ l'anneau quotient, qui est un corps d'après 4.3.11. Alors E_h est un k-espace vectoriel de dimension 1 si $p^h \mid d$, et 0 sinon.*

Preuve : Par construction, le morphisme de A-modules $s : A \to E_h$ qui envoie a sur la classe de ap^{h-1} est surjectif. Son noyau est l'idéal des $a \in A$ tels que $ap^{h-1} \in (p^h, d)$. Si $p^h \mid d$, alors $(p^h, d) = (p^h)$ et $a \in \ker(s)$ si et seulement si $p \mid a$. Dans ce cas $\ker(s) = (p)$ et $E_h \simeq A/(p) = k$ est de dimension 1 sur k. Sinon, l'idéal (p^h, d) est engendré par p^k pour un certain $k \leqslant h-1$; il contient p^{h-1}, donc $\ker(s) = A$. Dans ce cas $E_h \simeq A/A = 0$ qui est de dimension 0 sur k. □

Preuve de 5.2.4 : Soit n le nombre minimal d'éléments d'un système de générateurs de M et $s : A^n \to M$ un morphisme surjectif. D'après le théorème de la base adaptée, le noyau $K = \ker(s)$ est libre de rang $r \leqslant n$ et il existe des éléments non nuls $d_1, \ldots, d_r$ de A et une base $\{f_1, \ldots, f_n\}$ de $L = A^n$ tels que $d_1 \mid \cdots \mid d_r$ et que $\{d_1 f_1, \ldots, d_r f_r\}$ est une base de K. Posons $q = n - r$ et $d_{r+1} = \cdots = d_n = 0$. Comme on a choisi n minimal, aucun des d_i n'est inversible, et on voit que

$$M \simeq A^n/K \simeq A^q \oplus A/(d_1) \oplus \cdots \oplus A/(d_r).$$

Ceci montre l'existence. Pour l'unicité, soit M un A-module. Nous allons montrer que si $M \simeq A/(d_1) \oplus \cdots \oplus A/(d_n)$, alors n et la suite des d_i à association près peuvent être reconstruits à partir de M. Posons $d_0 = 1$. Il nous suffit de montrer que la liste des quotients d_{i+1}/d_i peut être reconstruite, et pour cela, il suffit de retrouver la liste des multiplicités $\alpha_p(d_{i+1}/d_i)$ des irréductibles $p \in A$ dans d_{i+1}/d_i. Fixons un $p \in A$ de corps résiduel $k = A/(p)$. Pour tout entier $h \geqslant 1$, posons $\delta_p(h) = \dim_k(p^{h-1}M/p^hM)$. D'après le lemme 5.2.5, on a

$\delta_p(h) = \operatorname{card}\{i; p^h \mid d_i\}$. Utilisant le fait que les d_i se divisent, on voit que $\delta_p(h) = n - i$ si et seulement si $p^h \nmid d_i$ et $p^h \mid d_{i+1}$. Il s'ensuit que :

$$\operatorname{card} \delta_p^{-1}(n-i) = \operatorname{card}\{h; p^h \nmid d_i \text{ et } p^h \mid d_{i+1}\} = \alpha_p(d_{i+1}/d_i).$$

Les $\alpha_p(d_{i+1}/d_i)$ sont donc déterminés à partir des fonctions δ_p intrinsèquement attachées à M, ce qui montre qu'ils sont uniques. □

On a vu qu'un $\mathbb{Z}$-module n'est rien d'autre qu'un groupe abélien. Le cas particulier $A = \mathbb{Z}$ du théorème 5.2.4 est donc spécialement intéressant : il donne une classification des groupes abéliens de type fini et (en faisant $q = 0$ dans l'énoncé suivant) une classification des groupes abéliens finis :

5.2.6 Théorème. *Soit G un groupe abélien de type fini. Alors il existe un unique entier $q \geqslant 0$ et une unique suite $d_1, \ldots, d_r$ d'entiers $\geqslant 2$ tels que $d_1 \mid \cdots \mid d_r$ et :*

$$G \simeq \mathbb{Z}^q \oplus \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_r\mathbb{Z}.$$

5.3 Modules de torsion, composantes primaires

5.3.1 Définition. Soient A un anneau commutatif intègre et M un A-module. Soit $a \in A$ non nul.

(1) On dit qu'un élément $x \in M$ est *de a-torsion* si $ax = 0$. On note $M(a)$ l'ensemble des éléments de a-torsion.

(2) On dit que x est *de a^∞-torsion* s'il existe $n \geqslant 1$ tel que $a^n x = 0$. On note $M(a^\infty)$ l'ensemble des éléments de a^∞-torsion.

(3) On dit que x est *de torsion* s'il existe $a \neq 0$ tel que $ax = 0$. On note $T(M)$ l'ensemble des éléments de torsion.

(4) On dit que M est *de a-torsion* si $M(a) = M$ et *sans a-torsion* si $M(a) = 0$. On dit que M est *de a^∞-torsion* si $M(a^\infty) = M$ et *sans a^∞-torsion* si $M(a^\infty) = 0$. On dit que M est *de torsion* si $T(M) = M$ et *sans torsion* si $T(M) = 0$.

Les propriétés de base de ces notions liées à la torsion font l'objet de l'exercice suivant.

5.3.2 Exercice. Soient $\boldsymbol{A}$ un anneau commutatif intègre et $\boldsymbol{M}$ un $\boldsymbol{A}$-module. On suit les notations de la définition précédente.

(1) Montrez que $\boldsymbol{x} \in \boldsymbol{M}$ est de torsion si et seulement si le sous-$\boldsymbol{A}$-module $\boldsymbol{Ax} \subset \boldsymbol{M}$ qu'il engendre n'est pas libre.

(2) Montrez que $\boldsymbol{M(a)}$, $\boldsymbol{M(a^\infty)}$, $\boldsymbol{T(M)}$ sont des sous-$\boldsymbol{A}$-modules de $\boldsymbol{M}$.

(3) Donnez un exemple qui montre que $\boldsymbol{M/M(a)}$ n'est pas nécessairement sans $\boldsymbol{a}$-torsion.

(4) Montrez que $\boldsymbol{M/M(a^\infty)}$ est sans $\boldsymbol{a^\infty}$-torsion et que tout morphisme $\boldsymbol{f : M \to N}$ vers un module $\boldsymbol{N}$ sans $\boldsymbol{a^\infty}$-torsion se factorise de manière unique par $\boldsymbol{M/M(a^\infty)}$. Mêmes questions avec $\boldsymbol{M/T(M)}$.

(5) Montrez que si $\boldsymbol{M}$ est libre, il est sans torsion.

(6) On suppose $\boldsymbol{M}$ de type fini. Montrez que $\boldsymbol{M}$ est de torsion si et seulement si son annulateur $\mathbf{Ann}(\boldsymbol{M}) = \boldsymbol{(0 : M)}$ est non nul (la notation $\boldsymbol{(0 : M)}$ est introduite après 2.5.6).

5.3.3 Exercice. Soit $\boldsymbol{A}$ un anneau principal. Soit $\boldsymbol{M}$ un $\boldsymbol{A}$-module de type fini isomorphe à $\boldsymbol{A^q \oplus A/(d_1) \oplus \cdots \oplus A/(d_r)}$. Montrez que :

(1) $\boldsymbol{T(M) = A/(d_1) \oplus \cdots \oplus A/(d_r)}$,

(2) $\boldsymbol{M/T(M)}$ est libre de rang $\boldsymbol{q}$,

(3) $\mathbf{Ann}(\boldsymbol{M}) = \boldsymbol{(d_r)}$.

5.3.4 Corollaire. ***Si A est un anneau principal, alors tout A-module de type fini sans torsion est libre.***

Preuve : C'est une conséquence du point (2) de l'exercice. □

Le corollaire n'est pas vrai pour les modules qui ne sont pas de type fini ; par exemple, le $\mathbb{Z}$-module $\mathbb{Q}$ est sans torsion mais n'est pas libre. L'énoncé n'est pas vrai non plus, pour les modules de type fini, si A est un anneau quelconque, même intègre ; par exemple, si $A = \mathbb{Z}[X]$, le sous-A-module $I = (2, X)$ de A est sans torsion mais il n'est pas libre.

Dans l'énoncé du théorème qui suit, nous aurons besoin de la notion de somme directe de sous-modules. On dit que M est *somme directe* d'une famille de sous-modules $\{M_i\}_{i\in I}$, et on écrit $M = \oplus_{i\in I} M_i$, si M

est engendré par les M_i et si pour toute somme finie nulle $x_{i_1} + \cdots + x_{i_n} = 0$ avec $x_{i_j} \in M_{i_j}$, on a $x_{i_1} = \cdots = x_{i_n} = 0$. Ceci revient à dire que le morphisme $f : \oplus_{i\in I} M_i \to M$ donné par la famille d'inclusions $f_i : M_i \to M$ est un isomorphisme.

5.3.5 Théorème (Composantes primaires des modules de torsion). *Soient A un anneau principal et M un A-module de torsion. Pour chaque $a \in A$ non nul, soit $M(a^\infty)$ le sous-module des éléments de a^∞-torsion, voir définition 5.3.1 et exercice 5.3.2. Soit Σ un ensemble de représentants des éléments irréductibles de A pour la relation d'association. Alors, on a :*

$$M = \bigoplus_{p\in\Sigma} M(p^\infty).$$

Le sous-module $M(p^\infty)$ est appelé la composante p-primaire *de M. Si M est de type fini, toutes les composantes primaires sont nulles sauf un nombre fini d'entre elles, et pour tout $p \in \Sigma$ il existe $n \geqslant 0$ tel que $M(p^\infty) = M(p^n)$.*

Preuve : Montrons que les $M(p^\infty)$ engendrent M. Soit $x \in M$. Comme M est de torsion, il existe $a \in A$ non nul tel que $ax = 0$. Soit $a = up_1^{\alpha_1} \dots p_r^{\alpha_r}$ la décomposition en irréductibles de a (elle est unique si l'on choisit les p dans Σ). Pour tout $j \in \{1, \dots, r\}$ posons $q_j = \prod_{i\neq j} p_i^{\alpha_i}$. Les éléments $q_1, \dots, q_r$ sont premiers entre eux dans leur ensemble donc il existe $u_1, \dots, u_r$ dans A tels que $u_1q_1 + \cdots + u_rq_r = 1$. Posons $y_j = q_jx$. On a alors :

(i) $p_j^{\alpha_j} y_j = u^{-1}ax = 0$ donc $y_j \in M(p_j^\infty)$,

(ii) $x = (u_1q_1 + \cdots + u_rq_r)x = u_1y_1 + \cdots + u_ry_r$.

Il s'ensuit que $x \in M(p_1^\infty) \oplus \cdots \oplus M(p_r^\infty)$.

Montrons que les $M(p^\infty)$ sont en somme directe. Soit $\Sigma' \subset \Sigma$ un sous-ensemble fini, et $\sum_{p\in\Sigma'} x_p = 0$ une somme nulle avec $x_p \in M(p^\infty)$ pour tout $p \in \Sigma'$. Soit $n_p \geqslant 0$ tel que $p^{n_p}x_p = 0$, et notons $t_q = \prod_{p\neq q} p^{n_p}$. Alors t_q et q^{n_q} sont premiers entre eux donc il existe $u_q, v_q \in A$ tels que $u_qt_q + v_qq^{n_q} = 1$. Par ailleurs, on a $t_qx_p = 0$ si $p \neq q$. On en déduit que $x_q = (u_qt_q + v_qq^{n_q})x_q = u_qt_qx_q = u_qt_q(\sum_{p\in\Sigma'} x_p) = 0$. Ceci étant vrai pour tout $q \in \Sigma'$, il s'ensuit que les $M(p^\infty)$ sont en somme directe.

Enfin, supposons que M est de type fini, et soit $\{x_1, \ldots, x_t\}$ une famille génératrice finie. Pour chaque i, on a une décomposition $x_i = \sum_{p \in \Sigma} x_{i,p}$ où $x_{i,p} \in M(p^\infty)$ et les $x_{i,p}$ non nuls vivent dans un ensemble fini $\Sigma_i \subset \Sigma$. Soit Σ' la réunion des Σ_i avec $1 \leqslant i \leqslant r$. L'ensemble des $x_{i,p}$ avec $A \leqslant i \leqslant t$ et $p \in \Sigma'$ est une famille génératrice finie dont les éléments sont *primaires*, c'est-à-dire appartiennent à l'une des composantes primaires. On voit alors que $M(p^\infty) = 0$ si $p \notin \Sigma'$. Enfin pour p fixé, soit N un entier tel que $p^N x_{1,p} = \cdots = p^N x_{t,p} = 0$. On a alors $M(p^\infty) = M(p^N)$. □

5.3.6 Remarque. Soit A principal et M un A-module de type fini de torsion. La décomposition en composantes primaires est une décomposition en somme de sous-modules *canoniques*, alors que dans la décomposition donnée par le théorème de structure des modules 5.2.4, il n'existe pas de collection canonique de sous-modules isomorphes chacun à l'un des facteurs $A/(d_i)$. En revanche, la décomposition primaire est moins fine que celle du théorème de structure, et peut être obtenue facilement à partir de ce dernier. En effet, soient $d_1 \mid \cdots \mid d_r$ non nuls et non inversibles tels que $M \simeq A/(d_1) \oplus \cdots \oplus A/(d_r)$. Alors on peut choisir un ensemble fini d'irréductibles $p_1, \ldots, p_s$ et pour chaque i, une décomposition en irréductibles :

$$d_i = u_i p_1^{\alpha_{i,1}} \ldots p_s^{\alpha_{i,s}}.$$

D'après le théorème des restes chinois 4.3.10, on a un isomorphisme canonique de modules :

$$A/(d_i) \simeq A/(p_1^{\alpha_{i,1}}) \oplus \cdots \oplus A/(p_s^{\alpha_{i,s}}).$$

En regroupant les facteurs, on a finalement :

$$M \simeq \left(\bigoplus_{i=1}^{r} A/(p_1^{\alpha_{i,1}}) \right) \oplus \cdots \oplus \left(\bigoplus_{i=1}^{r} A/(p_s^{\alpha_{i,s}}) \right).$$

On reconnaît les composantes primaires $M(p_1^\infty), \ldots, M(p_s^\infty)$.

5.3.7 Exemple. Sur l'anneau $A = \mathbb{Z}$, considérons le module

$$M = \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z} \oplus \mathbb{Z}/45\mathbb{Z}.$$

Utilisant le théorème des restes chinois, on voit que :

$$M \simeq \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}.$$

Ainsi M est somme de trois composantes primaires :

$$M(2^\infty) = \mathbb{Z}/8\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z} \quad , \quad M(3^\infty) = \mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/9\mathbb{Z} \quad \text{et} \quad M(5^\infty) = \mathbb{Z}/5\mathbb{Z}.$$

En utilisant de nouveau le théorème chinois, on a :

$$M \simeq \mathbb{Z}/12\mathbb{Z} \oplus \mathbb{Z}/360\mathbb{Z}$$

donc les facteurs invariants de M sont $\{12, 360\}$.

5.4 Application à la réduction des endomorphismes

5.4.1 Prélude : l'action de X. Soit A un anneau commutatif et M un $A[X]$-module. Alors M est muni d'une structure de A-module obtenue par restriction de l'action des scalaires de $A[X]$ au sous-anneau A. Par ailleurs, l'action de X sur M définit un endomorphisme A-linéaire $u : M \to M$ tel que $u(m) = X.m$ pour tout $m \in M$.

Réciproquement, soit M un A-module et $u : M \to M$ un endomorphisme A-linéaire. Pour tout polynôme $P \in A[X]$, on sait définir l'endomorphisme $P(u)$; explicitement, si $P = a_nX^n + \cdots + a_1X + a_0$, alors $P(u) = a_nu^n + \cdots + a_1u + a_0\,\mathrm{Id}$. On définit une structure de $A[X]$-module sur M par la formule $P.m = P(u)(m)$, pour tous $P \in A[X]$ et $m \in M$.

La morale est que l'action de X s'identifie à un endomorphisme A-linéaire de M, et qu'il y a équivalence entre la donnée d'un $A[X]$-module M et celle d'une paire (M, u) composée d'un A-module et d'un endomorphisme.

5.4.2 Endomorphismes des espaces vectoriels. Soient k un corps et E est un k-espace vectoriel. Nous allons appliquer les remarques qui précèdent à l'étude des endomorphismes de E. Chaque $u \in \mathrm{End}_k(E)$ munit E une structure de $k[X]$-module ; nous noterons E_u le $k[X]$-module ainsi défini, d'ensemble sous-jacent E. Le théorème de structure des modules sur l'anneau principal $k[X]$ va permettre de décrire u et E_u. Dans la correspondance de 5.4.1, si (E, u) et (F, v) sont des espaces vectoriels munis d'endomorphismes, définissant des $k[X]$-modules E_u et F_v, alors un morphisme de $k[X]$-modules $\varphi : E_u \to F_v$ est un endomorphisme d'espaces vectoriels $\varphi : E \to F$ tel que $\varphi \circ u = v \circ \varphi$. On peut ainsi établir un dictionnaire entre l'algèbre linéaire de (E, u) et la structure de $k[X]$-module de E_u :

(E, u), $u \in \mathrm{End}_k(E)$	$k[X]$-module E_u
k-endomorphisme qui commute avec u	endomorphisme du $k[X]$-module
sous-espace vectoriel u-stable	sous-$k[X]$-module
vecteur $x \in E$	morphisme de $k[X]$-modules $k[X] \to E_u$, $P \mapsto P(u)(x)$
polynôme minimal de u	générateur unitaire de l'idéal annulateur de E_u

Soit $\lambda \in k$ et notons D_λ le $k[X]$-module quotient $k[X]/(X - \lambda)$. On voit facilement que si $\lambda \neq \mu$ dans k, alors D_λ n'est pas isomorphe à D_μ. Si $x \in E$ est un vecteur propre pour u pour la valeur propre λ, le morphisme de $k[X]$-modules associé $k[X] \to E_u$, $P \mapsto P(u)(x)$ a un noyau engendré par $(X - \lambda)$. Il se factorise donc en un morphisme injectif de modules $D_\lambda \hookrightarrow E_u$. Ainsi, les espaces propres pour u correspondent du côté $k[X]$-module à des sommes de sous-modules de la forme D_λ. L'endomorphisme u est diagonalisable si et seulement si E_u est isomorphe à une somme directe $D_{\lambda_1} \oplus \cdots \oplus D_{\lambda_n}$.

5.4.3 Définition. On dit qu'un $k[X]$-module M est *cyclique* s'il existe $P \in k[X]$ non nul tel que $M \simeq k[X]/(P)$.

On peut toujours choisir P unitaire. Si M est cyclique, le polynôme P est alors déterminé de manière unique : c'est le générateur unitaire de l'idéal annulateur de M, i.e. $\mathrm{Ann}(M) = (0 : M) = \{Q \in k[X], Q.M = 0\}$. Une autre façon de dire que M est cyclique est qu'il est de torsion, engendré par un seul élément.

5.4.4 Remarque. Soit $M \simeq k[X]/(P)$ un module cyclique. Notons x la classe de X dans M et $n = \deg(P)$. Alors M est un k-espace vectoriel de dimension n, avec pour base $\{1, x, \ldots, x^{n-1}\}$.

5.4.5 Lemme. ***Soient E un k-espace vectoriel et $u \in \mathrm{End}_k(E)$. Alors, les conditions suivantes sont équivalentes :***

(1) ***le $k[X]$-module E_u est cyclique ;***

(2) *il existe* $x \in E$ *et* $n \geqslant 0$ *tels que* $\{x, u(x), \ldots, u^{n-1}(x)\}$ *est une base de* E *sur* k *;*

(3) *il existe* $x \in E$ *et* $n \geqslant 0$ *tels que* $\{x, u(x), \ldots, u^{n-1}(x)\}$ *engendre* E *sur* k*.*

Preuve : (1) $\Rightarrow$ (2). Si $E \simeq k[X]/(P)$, notons $x \in E$ la classe de X dans E et $n = \deg(P)$. Par division euclidienne par P, on voit que $1, x, \ldots, x^{n-1}$ engendre E.
(2) $\Rightarrow$ (3) est évident.
(3) $\Rightarrow$ (1). On définit un morphisme de $k[X]$-modules $\varphi : k[X] \to E_u$ en envoyant $Q \in k[X]$ sur $Q(u)(x)$. L'hypothèse implique que ce morphisme est surjectif. Il n'est pas injectif, car $\dim_k(E) < \infty$. Soit P un générateur du noyau, alors φ se factorise en un isomorphisme $k[X]/(P) \simeq E_u$. □

5.4.6 Remarque. Si E_u est cyclique, alors il est isomorphe à $k[X]/(P)$ où P est le polynôme minimal (unitaire) de u. Si l'on écrit $P = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$, la matrice de u dans la base $\{x, u(x), \ldots, u^{n-1}(x)\}$ est :

$$C_P := \begin{pmatrix} 0 & \ldots & 0 & -a_0 \\ 1 & \ddots & \vdots & -a_1 \\ & \ddots & 0 & \vdots \\ 0 & & 1 & -a_{n-1} \end{pmatrix}.$$

Cette matrice est appelée la *matrice compagnon* du polynôme P. Comme $\deg(P) = n = \dim(E_u)$, on voit que P est à la fois le polynôme minimal et le polynôme caractéristique de u.

5.4.7 Lemme. *Soient* E *un* k*-espace vectoriel et* $u \in \mathrm{End}_k(E)$*. Alors, les conditions suivantes sont équivalentes :*

(1) $\dim_k(E) < \infty$ *:*

(2) E_u *est un* $k[X]$*-module de type fini et de torsion.*

Preuve : (1) $\Rightarrow$ (2). Soit $\mathscr{B} = \{e_1, \ldots, e_n\}$ une base de E sur k. Alors $\mathscr{B}$ engendre E comme k-espace vectoriel, donc a fortiori E_u comme $k[X]$-module. Ainsi E_u est de type fini. Puisque $\dim_k(E) < \infty$, pour i

fixé la famille $\{u^n(e_i)\}_{n\geqslant 0}$ ne peut être libre, donc il existe un polynôme $P_i \in k[X]$ non nul tel que $P_i.e_i = P_i(u)(e_i) = 0$. Alors le polynôme P produit des P_i annule E_u, ce qui montre que M est de torsion.

(2) $\Rightarrow$ (1). Soit $e_1, \ldots, e_n$ un système fini de générateurs de E_u et $\varphi : k[X]^n \to E_u$ le morphisme surjectif de $k[X]$-modules qui envoie $(Q_1, \ldots, Q_n)$ sur $(Q_1(u)(e_1), \ldots, Q_n(u)(e_n))$. Comme chaque e_i est de torsion, il existe un polynôme $P_i \in k[X]$ non nul tel que $P_i.e_i = 0$. Le morphisme φ se factorise en un morphisme surjectif $k[X]/(P_1) \times \cdots \times k[X]/(P_n) \to E_u$. Comme le membre de gauche est de k-dimension finie $\sum \deg(P_i)$, alors $\dim_k(E) < \infty$. □

5.4.8 Théorème (Décomposition de Frobenius). *Soient k un corps, E un k-espace vectoriel de dimension finie et $u \in \mathrm{End}_k(E)$ un endomorphisme de E. Alors il existe une unique famille de polynômes unitaires non constants $P_1, \ldots, P_r \in k[X]$ tels que $P_1 \mid \cdots \mid P_r$ et que la matrice de u dans une base convenable de E soit la matrice diagonale par blocs :*

$$\begin{pmatrix} \boxed{C_{P_1}} & 0 & \ldots & 0 \\ 0 & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ 0 & \ldots & 0 & \boxed{C_{P_r}} \end{pmatrix}.$$

Les polynômes $P_1, \ldots, P_r$ sont appelés les facteurs invariants, *ou* invariants de similitude, *de u. Le polynôme minimal de u est P_r et le polynôme caractéristique de u est $P_1 \ldots P_r$.*

Preuve : D'après le théorème 5.2.4, il existe une suite de polynômes $P_1 \mid \cdots \mid P_r$ tels que $E_u \simeq k[X]/(P_1) \oplus \cdots \oplus k[X]/(P_r)$. Ces polynômes sont non nuls car $\dim_k(E) < \infty$ et non inversibles, donc non constants. Chaque facteur $k[X]/(P_i)$ correspond à un sous-espace $E_i \subset E$ qui est stable par u, i.e. un module cyclique, et il admet une base $\mathscr{B}_i$ dans laquelle la matrice de u est C_{P_i}. La base $\mathscr{B}$ réunion des $\mathscr{B}_i$ est une base de E dans laquelle la matrice de u est diagonale par blocs comme indiqué. L'unicité des P_i provient du fait que la structure de $k[X]$-module définie par la matrice de l'énoncé est isomorphe à $k[X]/(P_1) \oplus \cdots \oplus k[X]/(P_r)$, qui détermine la suite $(P_1, \ldots, P_r)$. □

Le nom d'*invariants de similitude* pour les P_i se justifie par le résultat suivant :

5.4.9 Corollaire. *Soient A et A' deux matrices de $\mathrm{M}_n(k)$. Alors A et A' sont semblables (c'est-à-dire qu'il existe $Q \in \mathrm{GL}_n(k)$ telle que $A' = Q^{-1}AQ$) si et seulement si A et A' ont les mêmes facteurs invariants.*

Preuve : Soient $E = k^n$ et u, u' les endomorphismes de E correspondant à A, A'. On a les conditions équivalentes : A et A' sont semblables ; il existe $Q \in \mathrm{GL}_n(k)$ telle que $A' = Q^{-1}AQ$; il existe un isomorphisme $v : E_{u'} \to E_u$ (c'est l'automorphisme de E défini par la matrice Q) ; les matrices A et A' ont les mêmes facteurs invariants. □

5.4.10 Corollaire. *Soient $k \subset K$ une extension de corps, $A \in \mathrm{M}_n(k)$ et $P_1, \ldots, P_r$ ses facteurs invariants. Alors les facteurs invariants de A dans $\mathrm{M}_n(K)$ sont $P_1, \ldots, P_r$.*

Preuve : On a une description de la matrice A, semblable à une matrice diagonale par blocs compagnon, comme dans le théorème 5.4.8. Cette description reste valable dans $\mathrm{M}_n(K)$. Les polynômes P_i vérifient la même condition de divisibilité dans $K[X]$. La propriété d'unicité montre qu'ils sont les facteurs invariants de A dans $\mathrm{M}_n(K)$. □

5.4.11 Corollaire. *Soient $k \subset K$ une extension de corps et $A, B \in \mathrm{M}_n(k)$. Si A et B sont semblables dans $\mathrm{M}_n(K)$, alors elles sont semblables dans $\mathrm{M}_n(k)$.*

Preuve : Soient $P_1, \ldots, P_r$ les invariants de similitude de A et $Q_1, \ldots, Q_s$ ceux de B. D'après le corollaire précédent et l'hypothèse que A et B sont semblables, les suites d'invariants sont les mêmes dans $K[X]$, donc les mêmes dans $k[X]$. Il découle de 5.4.9 que A et B sont semblables dans $\mathrm{M}_n(k)$. □

5.4.12 Remarques. La décomposition de Frobenius possède certains avantages sur d'autres méthodes de réduction classique en algèbre linéaire comme la décomposition de Dunford-Chevalley, la réduction de Jordan... Par exemple, elle ne

nécessite aucune hypothèse ni sur le corps $\boldsymbol{k}$, ni sur $\boldsymbol{E}$ et $\boldsymbol{u}$. Ceci est précieux pour démontrer un résultat comme 5.4.11, ou comme dans l'exercice 5.4.13 ci-dessous.

En revanche, elle présente l'inconvénient que les matrices compagnon $\boldsymbol{C_P}$ ne sont pas très agréables du point de vue du calcul. Songeons seulement que si $\boldsymbol{\lambda \neq \mu}$, la réduction de Frobenius de la matrice diagonale $\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$ est la matrice compagnon $\begin{pmatrix} 0 & -\lambda\mu \\ 1 & \lambda+\mu \end{pmatrix}$. On voit qu'on y perd au change !

5.4.13 Exercice. Soient $\boldsymbol{k}$ un corps et $\boldsymbol{A \in \mathrm{M}_n(k)}$. Montrez que $\boldsymbol{A}$ est semblable à sa transposée. (Indication : utilisez la décomposition de Frobenius.)

5.4.14 Notation (blocs de Jordan). Soient $\boldsymbol{\lambda \in k}$ et $\boldsymbol{n \geqslant 1}$. On pose :

$$\boldsymbol{J_n(\lambda)} = \begin{pmatrix} \lambda & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & \lambda \end{pmatrix}.$$

Cette matrice est appelée *bloc de Jordan de taille* $\boldsymbol{n}$ *et de valeur propre* $\boldsymbol{\lambda}$. On note que $\boldsymbol{J_n(\lambda) = \lambda \mathrm{I}_n + J_n(0)}$.

5.4.15 Remarque. Dans le $\boldsymbol{k[X]}$-module $\boldsymbol{k[X]/(X-\lambda)^n}$, l'endomorphisme de multiplication par $\boldsymbol{X}$ a pour matrice $\boldsymbol{J_n(\lambda)}$ dans la base $\boldsymbol{\{1, (X-\lambda), \ldots, (X-\lambda)^{n-1}\}}$, puisque

$$\boldsymbol{X.(X-\lambda)^i = (X-\lambda)(X-\lambda)^i + \lambda(X-\lambda)^i.}$$

Dit autrement on a un isomorphisme de $\boldsymbol{k[X]}$-modules entre $\boldsymbol{k[X]/(X-\lambda)^n}$ et le $\boldsymbol{k[X]}$-module $\boldsymbol{(k^n)_{J_n(\lambda)}}$ défini par l'espace vectoriel $\boldsymbol{E = k^n}$ et l'endomorphisme $\boldsymbol{u}$ déterminé par la matrice $\boldsymbol{J_n(\lambda)}$.

5.4.16 Théorème (Décomposition de Jordan). ***Soient k un corps algébriquement clos, E un k-espace vectoriel de dimension finie et $u \in \mathrm{End}_k(E)$ un endomorphisme de E. Alors il existe une base de E dans laquelle la matrice de u est de la forme diagonale par blocs :***

$$\boldsymbol{J} = \begin{pmatrix} \boxed{J_{n_1}(\lambda_1)} & 0 & \ldots & 0 \\ 0 & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ 0 & \ldots & 0 & \boxed{J_{n_r}(\lambda_r)} \end{pmatrix}.$$

De plus, pour chaque i les tailles des différents blocs de Jordan correspondant à λ_i sont indépendantes du choix de la base ; en d'autres termes J ne dépend que de u, à permutation près des blocs. Pour que u et u' soient semblables, il faut et il suffit qu'elles aient la même liste (non ordonnée) de blocs de Jordan.

Preuve : La décomposition en composantes primaires (proposition 5.3.5) fournit une écriture $E_u \simeq \oplus_{i=1}^{r} k[X]/(P_i^{n_i})$ où les P_i sont des polynômes unitaires *irréductibles*, pas nécessairement tous distincts. Comme k est algébriquement clos, on a $P_i = X - \lambda_i$ pour un certain $\lambda_i \in k$. Compte tenu de la remarque 5.4.15, ceci fournit l'existence de la forme diagonale par blocs annoncée. L'unicité résulte de l'assertion analogue d'unicité dans le théorème de structure 5.2.4 appliquée pour chacune des composantes primaires. □

5.4.17 Remarque. On peut affaiblir l'hypothèse que k est algébriquement clos en demandant simplement que le polynôme minimal (ou le polynôme caractéristique) de u soit scindé dans k.

Références

[B] D. Bourqui, *Arithmétique des anneaux de fonctions holomorphes*, **note disponible en ligne à l'adresse** `http://agreg-maths.univ-rennes1.fr/documentation/docs/holomorphe.pdf`.

[CL] A. Chambert-Loir, *Algèbre commutative*, **cours disponible en ligne à l'adresse** `http://perso.univ-rennes1.fr/antoine.chambert-loir/2006-07/g1/coursg1.pdf`.

[DD] R. Douady, A. Douady, *Algèbre et théories galoisiennes*, **Cassini, 2005.**

[FGN1] S. Francinou, H. Gianella, S. Nicolas, *Exercices de Mathématiques, Oraux X-ENS, Algèbre 1*, **Cassini, 2001.**

[Ha] P. Halmos, *Introduction à la théorie des ensembles*, **Gauthier-Villars, 1967.**

[L] S. Lang, *Algèbre*, **Dunod, 2004.**

[P] D. Perrin, *Cours d'algèbre*, **Ellipses, 1996.**

[RB] J.-J. Risler, P. Boyer, *Algèbre pour la Licence 3*, **Dunod, 2006.**

[R] W. Rudin, *Analyse réelle et complexe*, **Dunod, 1998.**

[T] P. Tauvel, *Algèbre*, **Dunod, 2005.**