Algèbre 1-ANNEAUX ET MODULES

David Harari

1. Généralités sur les anneaux

1.1. Définitions, premières propriétés

Définition 1.1 Un *anneau* $(A, +, .)$ est la donnée d'un ensemble A et de deux lois internes $+, .$ vérifiant :

1. $(A, +)$ est un groupe abélien.
2. La multiplication . est associative et possède un élément neutre (noté 1).
3. . est distributive par rapport à + : pour tous x, y, z dans A, on a $x(y+z) = xy + xz$ et $(y+z)x = yx + zx$.

Si la multiplication est commutative, on dit que l'anneau A est *commutatif*.

Exemples :

1. L'anneau nul $\{0\}$.
2. $(\mathbf{Z}, +, .)$, $(\mathbf{Z}/n\mathbf{Z}, +, .)$ sont des anneaux commutatifs.
3. Un corps K est par définition un anneau *commutatif* [1], distinct de $\{0\}$, tel que tout élément non nul ait un inverse pour la multiplication.
4. Le produit direct $\prod_{i \in I} A_i$ d'une famille d'anneaux $(A_i)_{i \in I}$ est un anneau (pour les lois évidentes).
5. Si A est un anneau *commutatif* [2], on dispose de l'*anneau des polynômes en n variables* $A[X_1, ..., X_n]$ qui est commutatif.

[1] D'après la convention déjà adoptée dans les autres parties du cours.

[2] On peut définir cet anneau de polynômes pour A non-commutatif, mais aucune des bonnes propriétés habituelles ne se conserve, donc on se limitera dans ce cours au cas commutatif.

6. Pour tout corps K, $(M_n(K), +, .)$ est un anneau, non commutatif si $n \geq 2$.

Définition 1.2 On appelle ensemble des éléments *inversibles* d'un anneau A l'ensemble des $x \in A$ tels qu'il existe $y \in A$ avec $xy = yx = 1$. C'est un groupe pour la multiplication, noté en général A^*.

Exemples :

1. $(\mathbf{Z}/n\mathbf{Z})^*$ est l'ensemble des classes $\bar{m}$, avec m premier à n.
2. Dans un corps K, on a par définition $K^* = K \setminus \{0\}$.
3. Si K est un corps, $K[X_1, ..., X_n]^*$ est l'ensemble des polynômes constant non nul (qui est isomorphe au groupe multiplicatif K^*). On n'a pas l'analogue en remplaçant K par un anneau commutatif A quelconque : si A contient un élément non nul ε tel que $\varepsilon^2 = 0$ (ex. $A = \mathbf{Z}/4\mathbf{Z}$), alors le polynôme $1 + \varepsilon X$ n'est pas constant et admet $1 - \varepsilon X$ pour inverse dans $A[X]$.
4. Si K est un corps, on a $M_n(K)^* = \mathrm{GL}_n(K)$.

Définition 1.3 Un *homomorphisme* (ou morphisme) d'anneaux $f : A \to B$ est une application entre deux anneaux vérifiant :

1. $f(x + y) = f(x) + f(y)$.
2. $f(xy) = f(x)f(y)$.
3. $f(1) = 1$.

On notera que l'application nulle n'est pas un morphisme d'anneaux car elle ne vérifie pas 3.

Définition 1.4 Une partie A de B est un *sous-anneau* si $(B, +, .)$ est un anneau *possédant le même élément unité que* A. Il est équivalent de dire que $1 \in B$, et que $(B, +)$ est un sous-groupe de $(A, +)$ qui est stable par multiplication interne.

On fera bien attention à la condition $1 \in B$, par exemple l'ensemble des $(x, 0)$ avec $x \in \mathbf{Z}$ n'est pas un sous-anneau de $\mathbf{Z} \times \mathbf{Z}$. Comme on va le voir, la notion de sous-anneau n'est souvent pas la plus intéressante, c'est celle d'idéal qui est la plus utile.

[Exercice : Soit A un anneau commutatif; la donnée d'un homomorphisme d'anneaux de $A[X_1, ..., X_n]$ vers un anneau B est équivalente à la donnée d'un homomorphisme d'anneaux de A vers B et de n éléments $b_1, ..., b_n$ de B (les images des X_i); c'est ce qu'on appelle la *propriété universelle* des anneaux de polynômes.]

1.2. Idéaux, anneaux quotient

On supposera désormais tous les anneaux commutatifs, sauf mention expresse du contraire (la théorie des anneaux non commutatifs est intéressante, mais très différente, et elle n'a pas les mêmes applications).

Définition 1.5 Une partie I d'un anneau commutatif A est un *idéal* de A si elle vérifie :

1. I est un sous-groupe de A pour $+$.
2. Pour tout x de I et tout a de A, on a $ax \in I$.

On prendra garde de ne pas confondre cette notion avec celle de sous-anneau. En particulier un idéal de A contient 1 (ou encore un élément inversible de A) si et seulement s'il est égal à A.

Exemples :

1. $\{0\}$ et A sont des idéaux de A. Ce sont les seuls si A est un corps.
2. Les idéaux de $\mathbf{Z}$ sont les $n\mathbf{Z}$ avec $n \in \mathbf{N}$.
3. Si $f : A \to B$ est un morphisme entre deux anneaux commutatifs, l'image réciproque d'un idéal de B par f est un idéal de A. En particulier le *noyau* $\ker f = f^{-1}(0)$ est un idéal de A. Ceci implique qu'un morphisme de corps (=morphisme entre les anneaux sous-jacents) est toujours injectif. Notons que si f n'est pas surjective, l'image directe d'un idéal de A par f n'est pas forcément un idéal de B (prendre pour f l'injection canonique de $\mathbf{Z}$ dans $\mathbf{Q}$). Par contre l'image $\mathrm{Im}\, f$ de f est un sous-anneau de B.
4. Si E est une partie d'un anneau commutatif A, alors l'ensemble des éléments de A de la forme $a_1x_1 + ... + a_nx_n$ avec $x_i \in E$ et $a_i \in A$ est un idéal, appelé *idéal engendré* par E; c'est le plus petit idéal de A contenant E. On notera (a) ou aA l'idéal engendré par un élément a de A.

Attention, contrairement à ce qui se passe pour les espaces vectoriels, un idéal J inclus dans un idéal I engendré par n éléments ne peut pas forcément être engendré par n éléments, par exemple l'idéal A est toujours engendré par 1 alors que certains idéaux peuvent ne pas être principaux (i.e. engendrés par un seul élément). En fait, il se peut même que J ne soit pas engendré par un nombre fini d'éléments. On verra toutefois que pour certains types d'anneaux particuliers (principaux, noethériens), ces problèmes disparaissent.

Proposition 1.6 *Soient A un anneau commutatif et I un idéal de A. Alors le groupe quotient A/I muni de la multiplication $\bar{a}\bar{b} := \overline{ab}$ est un anneau, appelé anneau quotient de A par I. La surjection canonique $p : A \to A/I$ est un morphisme d'anneaux, et l'élément unité de A/I est $\bar{1}$.*

Démonstration : Le seul point non trivial est que l'élément $\overline{ab}$ de A/I ne dépend pas du choix des représentants a, b. Or si $\bar{a} = \bar{a}'$ et $\bar{b} = \bar{b}'$, alors il existe i, j dans I avec $a' = a + i$, $b' = b + j$ d'où $a'b' = ab + (aj + ib + ij)$ avec $(aj + ib + ij) \in I$.

□

On a alors immédiatement le théorème de factorisation habituel :

Theorème 1.7 *Soit $f : A \to B$ un morphisme d'anneaux. Alors il existe un unique morphisme d'anneaux $\tilde{f} : A/\ker f \to B$ tel que $f = \tilde{f} \circ p$, où $p : A \to A/\ker f$ est la surjection canonique. De plus $\tilde{f}$ est injectif d'image $\operatorname{Im} f$, i.e. on a un isomorphisme d'anneaux $A/\ker f \simeq \operatorname{Im} f$.*

Exemples :

1. $\mathbf{Z}/n\mathbf{Z}$ est le quotient de $\mathbf{Z}$ par l'idéal $n\mathbf{Z}$.
2. L'application $P \mapsto P(i)$ est un morphisme d'anneaux surjectif de $\mathbf{R}[X]$ dans $\mathbf{C}$ dont le noyau est l'idéal $(X^2 + 1)$ engendré par le polynôme $X^2 + 1$ (pour le voir effectuer la division euclidienne par $X^2 + 1$). On a donc un isomorphisme d'anneaux $\mathbf{R}[X]/(X^2+1) \simeq \mathbf{C}$ et $\mathbf{R}[X]/(X^2+1)$ est un corps (on peut prendre cela pour définition de $\mathbf{C}$!).
3. Si K est un corps l'anneau $K[X]/(X^2)$ possède un élément ε non nul (la classe de X) tel que $\varepsilon^2 = 0$.

[Exercice : les idéaux de A/I sont les $\pi(J)$, où π est la surjection canonique $A \to A/I$ et J un idéal de A contenant J. Le quotient de A/I par l'idéal $\pi(J)$ est isomorphe à l'anneau A/J.]

Définition 1.8 Un anneau commutatif A est dit *intègre* s'il est non nul, et si pour tous a, b de A, la condition $ab = 0$ implique $a = 0$ ou $b = 0$.

Exemples :

1. Pour $n \in \mathbf{N}^*$, $\mathbf{Z}/n\mathbf{Z}$ est intègre si et seulement si n est premier.
2. Tout corps est un anneau intègre.
3. Tout sous-anneau d'un anneau intègre est intègre.
4. Si A est intègre, les anneaux $A[X]$, $A[X_1, ..., X_n]$ sont intègres.

On rappelle le résultat classique suivant :

Proposition 1.9 *Soit A un anneau intègre; alors il existe un corps K et un homomorphisme injectif $i : A \to K$ tel que pour tout morphisme injectif d'anneaux de A vers un corps K', il existe un unique morphisme de corps $j : K \to K'$ tel que $f = j \circ i$. K est unique à isomorphisme près, et s'appelle le corps des fractions de A. On le note* $\operatorname{Frac} A$.

Cela signifie que K est le "plus petit corps" contenant A; ainsi un anneau est intègre si et seulement s'il est sous-anneau d'un corps. Par exemple $\operatorname{Frac} \mathbf{Z} = \mathbf{Q}$, et $\operatorname{Frac}(K[X]) = K(X)$ (le corps des fractions rationnelles en une indéterminée). Noter que l'anneau nul n'a pas de corps des fractions (ce qui justifie qu'il ne soit pas intègre par convention).

Définition 1.10 Un anneau commutatif A est dit *principal* s'il est intègre et si tous ses idéaux sont de la forme $(a) = aA$ avec $a \in A$.

Par exemple $\mathbf{Z}$ et $K[X]$ (quand K est un corps) sont principaux.

Définition 1.11 Un idéal I de A est dit *premier* si A/I est intègre. De manière équivalente cela signifie : $A \neq I$, et la condition $ab \in I$ implique $a \in I$ ou $b \in I$.

Exemples :

1. Les idéaux premiers de $\mathbf{Z}$ sont $\{0\}$ et les $n\mathbf{Z}$ pour n premier.
2. Un anneau A est intègre si et seulement si $\{0\}$ est premier.
3. L'image réciproque d'un idéal premier par un morphisme d'anneaux est un idéal premier.
4. Les idéaux (X_1) et (X_1, X_2) sont tous deux premiers dans $K[X_1, X_2]$.

Définition 1.12 Un idéal I de A est dit *maximal* si $I \neq A$ et si tout idéal J contenant I est égal à A où à I.

Proposition 1.13 *Un idéal I est maximal si et seulement si A/I est un corps.*

Démonstration : Si I est maximal et $\bar{x}$ est non nul dans A/I, alors $x \notin I$ donc l'idéal $I + xA$ contient strictement I; par maximalité de I, on a $A = I + xA$ et 1 s'écrit $1 = i + xa$ avec $i \in I$ et $a \in A$ ce qui se traduit par $\bar{1} = \bar{x}\bar{a}$, d'où $\bar{x}$ inversible dans A/I. Comme $I \neq A$, l'anneau A/I n'est pas nul et ses éléments non nuls sont inversibles, i.e. A/I est un corps.

En sens inverse si A/I est un corps, alors $I \neq A$, et tout idéal J de A contenant strictement I contient un élément $x \notin I$. Alors $\bar{x}$ est inversible dans A/I, soit $\bar{1} = \bar{x}\bar{a}$ avec $a \in A$, ou encore $1 = xa + i$ avec $i \in I \subset J$ et $x \in J$. Ainsi $1 \in J$ et $J = A$.

□

Le théorème suivant est utile pour les questions théoriques générales. [3]

Theorème 1.14 (Krull) *Dans un anneau commutatif* [4] *A, tout idéal $I \neq A$ est inclus dans un idéal maximal.*

Démonstration : L'ensemble des idéaux de A contenant I et distincts de A est inductif car si $(I_i)_{i\in I}$ est une famille totalement ordonnée d'idéaux de A distincts de A, la réunion est encore un idéal (parce que la famille est totalement ordonnée) distinct de A (parce qu'elle ne contient pas 1). On applique alors le lemme de Zorn.

□

2. Divisibilité dans les anneaux intègres

2.1. Éléments irréductibles, anneaux factoriels

Dans tout ce paragraphe, A désigne un anneau commutatif intègre.

Définition 2.1 Soient a, b dans A. On dit que a *divise* b et on écrit $a \mid b$ s'il existe $c \in A$ tel que $b = ac$. En termes d'idéaux, c'est équivalent à $(a) \supset (b)$.

En particulier 0 ne divise que lui-même, et un élément de A^* divise tous les éléments de A.

Proposition 2.2 *Soient a, b dans A. Alors ($a \mid b$ et $b \mid a$) si et seulement s'il existe $u \in A^*$ tel que $a = ub$. On dit alors que a et b sont associés.*

[3] En particulier quand on travaille avec des anneaux non noethériens, ce qui est souvent le cas en analyse.

[4] On notera que l'existence d'un élément unité dans A est cruciale pour ce théorème. On a l'analogue dans un anneau non commutatif en remplaçant "idéal" par "idéal à gauche", "idéal à droite", ou "idéal bilatère".

Démonstration : Si $a = ub$ avec $u \in A^*$, alors $b \mid a$ et $b = u^{-1}a$ donc $a \mid b$. En sens inverse si $a = bc$ et $b = ad$ avec c, d dans A, alors $a = adc$ donc $dc = 1$ par intégrité de A, soit $c \in A^*$.

□

La relation "être associé" est d'équivalence sur A ou $A \setminus \{0\}$.

Définition 2.3 On dit qu'un élément p de A est *irréductible* s'il vérifie les deux propriétés suivantes :

1. p n'est *pas* inversible dans A.
2. La condition $p = ab$ avec a, b dans A implique que a ou b soit inversible.

La deuxième condition signifie que les seuls diviseurs de p sont ses associés et les inversibles de A. On fera bien attention au fait que par convention, les éléments de A^* ne sont pas irréductibles.

Par exemple, les irréductibles de $\mathbf{Z}$ sont les $\pm p$ avec p nombre premier; ceux de $\mathbf{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 sans racine réelle.

Définition 2.4 On dit que deux éléments a et b de A sont *premiers entre eux* si leurs seuls diviseurs communs sont les éléments de A^*.

On a l'analogue du théorème de Bezout quand A est *principal* :

Proposition 2.5 *Soit A un anneau principal. Deux éléments a et b de A sont premiers entre eux si et seulement s'il existe u, v dans A tels que $ua + vb = 1$ (i.e. si $A = (a, b)$, idéal engendré par a et b).*

Démonstration : Si $1 = ua + bv$, alors tout diviseur commun de a et b divise 1, donc est inversible (cette implication est vraie dans tout anneau commutatif). En sens inverse, si a et b sont premiers entre eux, alors l'idéal (a, b) s'écrit (d) avec $d \in A$ car A est principal. En particulier d divise a et b, donc est inversible donc $(d) = A$.

□

Notons que dans l'anneau $A = K[X, Y]$, les polynômes X et Y sont premiers entre eux mais ne satisfont pas $A = (X, Y)$ (par exemple parce que tout polynôme de (X, Y) s'annule en $(0, 0)$). Ainsi $K[X, Y]$ n'est pas principal.

[Exercice : Si A est un anneau commutatif, alors $A[X]$ est principal si et seulement si A est un corps.]

On aimerait quand même avoir une théorie de la divisibilité raisonnable pour des anneaux plus généraux que les anneaux principaux. C'est ce qui motive l'introduction de la notion d'anneau factoriel.

Définition 2.6 Un anneau commutatif A est dit *factoriel* s'il vérifie les trois propriétés suivantes :

1. A est intègre.
2. Tout élément non nul a de A s'écrit comme produit

$$a = up_1...p_r$$

avec $u \in A^*$ et les p_i irréductibles [5].

3. Il y a unicité de cette décomposition au sens suivant : si $a = vq_1...q_s$ en est une autre, alors $r = s$ et il existe une permutation σ de $\{1, ..., r\}$ telle que pour tout i de $\{1, ..., r\}$, les éléments p_i et $q_{\sigma(i)}$ soient associés.

Remarques : a) Comme pour principal, on n'oubliera pas la condition d'intégrité de A.

b) Une autre formulation, souvent plus commode, de l'unicité, est la suivante : fixons un *système de représentants irréductibles* $\mathcal{P}$ de A, i.e. un ensemble d'éléments irréductibles tels que tout irréductible de A soit associé à un et un seul élément de $\mathcal{P}$. Alors tout élément non nul a de A s'écrit d'une manière unique $a = u \prod_{p \in \mathcal{P}} p^{n_p}$ avec $u \in A^*$, et $(n_p)_{p \in \mathcal{P}}$ famille presque nulle d'entiers naturels. On note alors $n_p = v_p(a)$.

c) Comme on le verra au paragraphe suivant, la plupart des anneaux intègres que l'on rencontre en algèbre ont la propriété d'existence de la décomposition, la propriété forte est l'unicité.

Exemples :

1. $\mathbf{Z}$ est factoriel (prendre pour $\mathcal{P}$ l'ensemble des nombres premiers).
2. $K[X]$ est factoriel (on peut prendre pour $\mathcal{P}$ l'ensemble des polynômes irréductibles unitaires).
3. On verra que plus généralement tout anneau principal est factoriel, mais que la réciproque est fausse par exemple pour $K[X_1, ..., X_n]$.

[5] Si a n'est pas inversible, le produit des p_i qui apparaît n'est pas un produit vide, et on peut remplacer up_1 par p_1, donc se passer de l'unité u dans la décomposition.

4. L'anneau $A = \mathbf{Z}[i\sqrt{5}] = \mathbf{Z}[T]/(T^2+5)$, qui est aussi le sous-anneau de $\mathbf{C}$ constitué des $a + bi\sqrt{5}$ avec $a, b \in \mathbf{Z}$, est intègre mais n'est pas factoriel. En effet on voit facilement que A^* est constitué des $a + bi\sqrt{5}$ avec $a^2 + 5b^2 = \pm 1$; puis que 3 est irréductible, mais n'est associé à aucun des irréductibles $2 - i\sqrt{5}$, $2 + i\sqrt{5}$. Pourtant $9 = 3 \times 3 = (2 - i\sqrt{5})(2 + i\sqrt{5})$ dans A.

5. L'anneau $A = \mathbf{Z}[\sqrt{3}]$ n'est pas non plus factoriel car l'élément $a = \frac{-1+i\sqrt{3}}{2}$ de $\operatorname{Frac} A$ annule le polynôme unitaire $X^2 + X + 1$ de $A[X]$ et il est facile de voir que dans un anneau factoriel, seul les éléments de A ont cette propriété (on dit qu'un anneau factoriel est *intégralement clos*, ou *normal*). On peut démontrer sans trop de mal que $\mathbf{Z}[i\sqrt{5}]$ est intégralement clos.

La proposition suivante donne un critère pour qu'un anneau soit factoriel quand on connaît déjà l'existence de la décomposition en irréductibles.

Proposition 2.7 *Soit A un anneau intègre tel que tout élément non nul de A soit produit d'irréductibles. Alors les propriétés suivantes sont équivalentes :*

1. *A est factoriel*
2. *Si $p \in A$ est irréductible, alors l'idéal (p) est premier.*
3. *Soient a, b, c dans $A \setminus \{0\}$. Si a divise bc et est premier avec b, alors a divise c ("lemme de Gauss").*

Démonstration : 3. implique 2. : déjà $(p) \neq A$ car p n'est pas inversible puisqu'irréductible. Si maintenant p divise ab et ne divise pas a, alors p est premier avec a puisque p est irréductible (donc un diviseur commun non inversible de a et p serait associé à p, et p diviserait a), d'où p divise b d'après 3. Ainsi (p) est premier.

2. implique 1. : Soit $\mathcal{P}$ un système de représentants irréductibles. Si $u \prod_{p\in\mathcal{P}} p^{m_p} = v \prod_{p\in\mathcal{P}} p^{n_p}$ sont deux décompositions, alors la condition $m_q > n_q$ pour un certain q de $\mathcal{P}$ impliquerait que q divise $\prod_{p\in\mathcal{P}, p\neq q} p^{n_p}$, donc l'un des facteurs d'après 2. Mais q ne peut diviser p pour $p \in \mathcal{P}$ distinct de q car $\mathcal{P}$ est un système de représentants irréductibles. Ainsi $m_p = n_p$ pour tout $p \in \mathcal{P}$, puis $u = v$ par intégrité de A.

1. implique 3. : on décompose a, b, c comme ci-dessus. Alors pour tout p de $\mathcal{P}$, $v_p(a) \leq v_p(b) + v_p(c)$ (car a divise bc) et $v_p(b) > 0$ implique $v_p(a) = 0$ (car a est premier avec b) donc $v_p(a) \leq v_p(c)$. Ainsi a divise c.

□

Proposition 2.8 *Si A est un anneau factoriel, alors deux éléments non nuls a et b de A ont un pgcd, bien défini à association près.*

Rappelons qu'un pgcd (plus grand commun diviseur) de a et b est un diviseur commun d de a et b, tel que tout autre diviseur commun divise d; "grand" fait réference à la relation d'ordre partiel "divise" sur l'ensemble quotient de $A\backslash\{0\}$ par la relation d'association. La proposition est immédiate en décomposant a et b suivant un système de représentants $\mathcal{P}$, un pgcd étant $\prod_{p\in\mathcal{P}} p^{\min(v_p(a),v_p(b))}$. On a de même un ppcm (plus petit commun multiple) en prenant $\prod_{p\in\mathcal{P}} p^{\max(v_p(a),v_p(b))}$. Notons que deux éléments de A sont premiers entre eux si et seulement si leur pgcd est 1.

Pour ce qui est de l'existence de la décomposition, on a besoin d'une propriété de finitude qui est à l'origine de la notion d'anneau noethérien.

2.2. Anneaux noethériens

Dans tout ce paragraphe, A est un anneau commutatif, mais ici on ne le suppose pas forcément intègre.

Proposition 2.9 *Soit A un anneau commutatif. Alors les trois propriétés suivantes sont équivalentes :*

1. *Tout idéal de A est engendré par un nombre fini d'éléments.*
2. *Toute suite croissante (pour l'inclusion) $(I_n)_{n\in\mathbf{N}^*}$ d'idéaux est stationnaire.*
3. *Toute famille non vide d'idéaux de A a un élément maximal pour l'inclusion.*

On dira que A est noethérien s'il vérifie ces propriétés.

Démonstration : 1. implique 2. : soit (I_n) une telle suite, alors la réunion I des I_n est encore un idéal car la famille (I_n) est totalement ordonnée pour l'inclusion. Soient $x_1, ..., x_r$ des éléments de I qui l'engendrent, alors chaque x_i est dans l'un des I_n, donc il existe n_0 (le plus grand des indices correspondants) tel que I_{n_0} les contienne tous. Alors $I = I_{n_0}$ et la suite (I_n) stationne à I_{n_0}.

2. implique 3. : si une famille non vide d'idéaux de A n'a pas d'élément maximal, on construit par récurrence une suite infinie strictement croissante d'idéaux de A, ce qui contredit 2.

3. implique 1. : soit I un idéal de A, alors la famille E des idéaux $J \subset I$ qui sont engendrés par un nombre fini d'éléments est non vide (elle contient $\{0\}$). Soit J_0 un élément maximal de E, alors pour tout x de I, l'idéal $J_0 + xA$ est aussi dans E, donc $J_0 + xA = J_0$ par maximalité. Ceci signifie que $x \in J_0$. Finalement $I = J_0$ et I est engendré par un nombre fini d'éléments.

□

Par exemple, tout anneau principal est noethérien, et si A est noethérien tout quotient de A l'est encore (immédiat à partir de la caractérisation 1., vu que les idéaux de A/I sont les J/I). L'anneau $K[(X_n)_{n\in\mathbf{N}^*}]$ n'est pas noethérien car $(X_1) \subset (X_1, X_2) \subset ...(X_1, ..., X_n) \subset ...$ forme une suite infinie strictement croissante d'idéaux. [6]
La plupart des anneaux avec lesquels on travaille en algèbre sont noethériens, via le théorème suivant :

Theorème 2.10 (Hilbert) *Soit A un anneau noethérien. Alors $A[X]$ est noethérien.*

Démonstration : Soient I un idéal de $A[X]$ et $n \in \mathbf{N}$; on note $d_n(I)$ le sous-ensemble de A constitué de 0 et des coefficients dominants des éléments de degré n de I. Il est immédiat que I est un idéal de A, et que l'inclusion $I \subset J$ implique $d_n(I) \subset d_n(J)$. On a d'autre part les deux propriétés suivantes :

i) Si $n \in \mathbf{N}$, alors $d_n(I) \subset d_{n+1}(I)$: en effet il suffit de remarquer que si $P \in I$, alors $XP \in I$.

ii) Si $I \subset J$, alors le fait que $d_n(I) = d_n(J)$ pour tout $n \in \mathbf{N}$ implique que $I = J$: en effet si J contient strictement I, on choisit un polynôme P dans $J \setminus I$ de degré r minimal; comme $d_r(I) = d_r(J)$, I contient un polynôme Q de degré r qui a même coefficient dominant que P, mais alors $P - Q$ est dans $J \setminus I$ et est de degré $< r$, contradiction.

Ceci dit, soit $(I_n)_{n\in\mathbf{N}^*}$ une suite croissante d'idéaux de $A[X]$. Comme A est noethérien, la famille des $d_k(I_n)$ pour $k \in \mathbf{N}$ et $n \in \mathbf{N}^*$ admet un élément maximal, mettons $d_l(I_m)$. D'autre part pour chaque $k \leq l$, la suite d'idéaux $(d_k(I_n))_{n\in\mathbf{N}^*}$ est croissante, donc elle est stationnaire, c'est-à-dire qu'il existe n_k tel que pour $n \geq n_k$, on ait $d_k(I_n) = d_k(I_{n_k})$. Soit alors N le plus grand des entiers $m, n_0, n_1, ..., n_l$, nous allons montrer que pour tout $n \geq N$, on a $d_k(I_n) = d_k(I_N)$, ce qui suffira à conclure via la propriété ii) ci-dessus. On distingue deux cas :

[6] Cet anneau est factoriel; ceci se déduit aisément du fait, que l'on prouvera plus tard, que $K[X_1, ..., X_n]$ est factoriel, car un élément *fixé* de $K[(X_n)_{n\in\mathbf{N}^*}]$ est dans $K[X_1, ..., X_n]$ pour un certain n.

a) Si $k \leq l$, alors $d_k(I_N) = d_k(I_{n_k}) = d_k(I_n)$ par définition de n_k puisque n et N sont tous deux $\geq n_k$.

b) Si $k \geq l$, alors $d_k(I_N)$ et $d_k(I_n)$ contiennent tous deux $d_l(I_m)$ d'après la propriété i) ci-dessus, donc par maximalité de $d_l(I_m)$ ils lui sont égaux, et en particulier $d_k(I_N) = d_k(I_n)$.

□

Corollaire 2.11 *1. Si A est noethérien, alors l'anneau $A[X_1, ..., X_n]$ est noethérien.*

2. Si A est noethérien, tout anneau B qui est une A-algèbre de type fini est nothérien.

Démonstration : 1. résulte du théorème précédent par récurrence sur n.

2. Rappelons qu'une *A-algèbre* B est un anneau équipé d'un homomorphisme $f : A \to B$. Elle est dite *de type fini comme A-algèbre* s'il existe $x_1, ...x_n$ dans B tels que le morphisme d'anneaux $A[X_1, .., X_n] \to B$ qui envoie X_i sur x_i et coïncide avec f sur les constantes soit surjectif (il revient au même de dire que B est la plus petite sous-A-algèbre de B qui contient les x_i); ainsi B est une A-algèbre de type fini si et seulement si c'est un quotient d'un anneau de polynômes $A[X_1, ..., X_n]$. Le corollaire précédent donne alors le résultat, en utilisant le fait qu'un quotient d'anneau noethérien est noethérien.

□

On s'intéresse maintenant à l'existence de la décomposition en produit d'irréductibles dans un anneau intègre noethérien.

Proposition 2.12 *Soit A un anneau intègre noethérien. Alors tout élément x non nul de A s'écrit : $x = up_1...p_r$ avec $u \in A^*$ et les p_i irréductibles.*

Démonstration : Soit $\mathcal{F}$ l'ensemble des idéaux de A de la forme xA avec x non inversible ne s'écrivant pas comme produit d'irréductibles. Si $\mathcal{F}$ n'était pas vide, il admettrait un élément maximal $(a) = aA$. En particulier a n'est alors pas irréductible, donc comme il n'est pas inversible il s'écrit $a = bc$ avec b, c dans A non associés à a. Mais alors les idéaux (b) et (c) contiennent strictement (a), donc par maximalité b et c se décomposent en produit d'irréductibles, ce qui contredit le fait que a ne s'écrit pas comme produit d'irréductibles.

□

Remarque : Il n'y a pas d'implication entre noethérien et factoriel. Si K est un corps, $K[X_n]_{n\in\mathbf{N}^*}$ est factoriel mais pas noethérien. D'autre part $\mathbf{Z}[X]/(X^2+5)$ est noethérien via le théorème 2.10, et on a déjà vu qu'il n'était pas factoriel.

Corollaire 2.13 *Si A est principal, A est factoriel.*

Démonstration : On vient de voir l'existence de la décomposition en irréductibles. D'autre part si $p \in A$ est irréductible, alors l'idéal (p) est maximal car si $I = (a)$ contient (p), alors a divise p, ce qui implique que a est inversible ou associé à p, i.e. $(a) = (p)$ ou $(a) = A$. En particulier (p) est premier et on conclut avec la proposition 2.7. [7]

□

2.3. Critères de principalité et de factorialité

Dans ce paragraphe, A est de nouveau un anneau commutatif intègre.

Définition 2.14 A est dit *euclidien* s'il existe une application $v : A-\{0\} \to \mathbf{N}$ ("stathme euclidien") tel que si a, b sont non nuls dans A, alors il existe q, r dans A avec $a = bq + r$ et r vérifiant : $r = 0$ ou $v(r) < v(b)$.

Noter qu'on ne demande pas d'unicité dans cette "division euclidienne". Par exemple $\mathbf{Z}$ est euclidien avec $v(x) =\mid x \mid$, $K[X]$ (K corps) est euclidien avec $v(P) = \deg P$.

[Exercice : $\mathbf{Z}[i]$ est euclidien avec $v(x) =\mid x \mid^2$, sans qu'on ait unicité dans la division euclidienne.]

Theorème 2.15 *Si A est euclidien, A est principal.*

Démonstration : Soit I un idéal non nul de A, on choisit b non nul dans I avec $v(b$ minimal. Alors tout a de I s'écrit $a = bq + r$ avec $r = 0$ ou $v(r) < v(b)$. Mais le deuxième cas est impossible car $r \in I$ d'où $a \in (b)$. Finalement $I = (b)$.

□

La réciproque est fausse mais les contre-exemples classiques ne sont pas évidents ($\mathbf{Z}[\frac{1+i\sqrt{19}}{2}]$, $\mathbf{R}[X,Y]/X^2+Y^2+1$).

[7] On dit qu'un anneau intègre est *de dimension 1* si tout idéal premier non nul est maximal. On vient de voir qu'un anneau principal est de dimension 1. Par contre $\mathbf{Z}[i\sqrt{5}]$ est de dimension 1 sans être principal (ni même factoriel), et $K[X_1, X_2]$ est factoriel sans être de dimension 1.

On a vu que A principal n'impliquait pas du tout $A[X]$ principal (ceci n'est vrai que si A est un corps). On va voir par contre que la propriété analogue est vraie pour factoriel. On commence par une définition :

Définition 2.16 Soit A un anneau factoriel. Le *contenu* (noté $c(P)$) d'un polynôme P est le p.g.c.d. de ses coefficients. P est dit primitif si $c(P) = 1$.

On notera que le contenu est défini à multiplication par un inversible de A près, par contre l'idéal qu'il engendre est bien défini.

Lemme 2.17 (Gauss) *Pour tous P, Q de $A[X]$, on a $c(PQ) = c(P)c(Q)$ (toujours modulo A^*).*

Démonstration : Supposons d'abord P et Q primitifs et montrons que PQ est primitif. Sinon il existe un irréductible p de A qui divise tous les coefficients de PQ. Comme P et Q sont primitifs, chacun a au moins un coefficient non divisible par p. Soit a_{i_0} (resp. b_{j_0}) le coefficient de P (resp. Q) d'indice minimal non divisible par p. Alors le coefficient d'indice $i_0 + j_0$ de PQ est somme de termes divisibles par p et de $a_{i_0}b_{j_0}$ donc il n'est pas divisible par p car (p) est premier vu que A est factoriel. Ceci contredit le fait que tous les coefficients de PQ soient divisibles par p.

On se ramène à P, Q primitifs en appliquant le résultat précédent à $P/c(P)$, $Q/c(Q)$.

□

On en déduit l'important résultat suivant :

Theorème 2.18 *Soit A un anneau factoriel de corps des fractions K. Alors les irréductibles de $A[X]$ sont de deux types :*

i) Les polynômes $P = p$ constants avec p irréductible dans A.

ii) Les polynômes primitifs de degré ≥ 1 qui sont irréductibles dans $K[X]$.

En particulier, pour un polynôme primitif de $A[X]$, il revient au même d'être irréductible dans $A[X]$ et dans l'anneau principal $K[X]$ (ce qui n'est pas du tout évident vu qu'il y a a priori plus de décompositions possibles dans $K[X]$). On fera attention avec les polynômes non primitifs : 2 est irréductible dans $\mathbf{Z}[X]$ mais pas dans $\mathbf{Q}[X]$ (il y est inversible) tandis que $2X$ est irréductible dans $\mathbf{Q}[X]$ mais pas dans $\mathbf{Z}[X]$.

Démonstration : Comme $A[X]^* = A^*$, il est clair qu'un polynôme constant $P = p$ est irréductible si et seulement si p est irréductible dans A. Si d'autre part P est un polynôme primitif de degré ≥ 1 de $A[X]$ qui est irréductible dans $K[X]$, alors une écriture $P = QR$ avec Q, R dans $A[X]$ implique avec le lemme précédent que $c(Q)$ et $c(R)$ soient inversibles. Comme d'autre part l'un des polynômes Q, R est constant (parce que P est irréductible dans $K[X]$), c'est une constante inversible dans A. Finalement P est bien irréductible dans $A[X]$ (il n'est pas inversible car de degré au moins 1).

Il reste à montrer qu'un polynôme P de degré ≥ 1 qui est irréductible dans $A[X]$ est primitif, et irréductible dans $K[X]$. Le fait que P soit primitif résulte de ce que $c(P)$ divise P dans $A[X]$ et ne lui est pas associé pour raison de degré. Il reste à montrer que P (qui n'est pas inversible dans $K[X]$) est irréductible dans $K[X]$. Or si $P = QR$ dans $K[X]$, on peut écrire $Q = Q_1/q$ et $R = R_1/r$ avec q, r dans A et Q_1, R_1 dans $A[X]$. Alors en posant $a = qr$, on obtient $aP = Q_1R_1$, et en passant aux contenus : $a = c(Q_1)c(R_1)$ (modulo A^*). Ainsi $P = u\frac{P_1}{C(P_1)}\frac{Q_1}{C(Q_1)}$ avec $u \in A^*$. Comme P est irréductible dans $A[X]$, l'un des polynômes $\frac{P_1}{C(P_1)}$, $\frac{Q_1}{C(Q_1)}$ de $A[X]$ est inversible, donc constant, et l'un des polynômes Q, R est constant ce qui achève la preuve.

□

On en déduit enfin

Theorème 2.19 *Si A est factoriel, $A[X]$ est factoriel.*

Démonstration : On doit d'abord démontrer qu'on a l'existence de la décomposition (qui est claire via le théorème 2.10 et la proposition 2.12 si A est de plus supposé noethérien). Quitte à écrire $P = c(P)P_1$ et à décomposer $c(P)$ en produit d'irréductibles dans A, on se ramène à P primitif. On décompose alors P (qu'on peut supposer non constant) dans l'anneau principal $K[X]$, soit $P = P_1...P_r$, ou encore $aP = Q_1...Q_r$ avec $Q_i \in A[X]$, $a \in A$, et Q_i irréductible dans $K[X]$. En passant aux contenus, on obtient $a = c(Q_1)...c(Q_r)$ (mod. A^*) et d'après le théorème précédent $P = \prod_{i=1}^{r} \frac{P_i}{c(P_i)}$ est une décomposition de P en produits d'irréductibles de $A[X]$, puisque chaque $\frac{P_i}{c(P_i)}$ est un polynôme primitif de $A[X]$ qui est irréductible dans $K[X]$ (il est le produit de Q_i par une constante de K^*).

Il suffit donc d'après la proposition 2.7 de montrer que si $P \in A[X]$ est irréductible, alors (P) est premier. Si $P = p$ est une constante irréductible de $A[X]$, ceci est clair (vérification directe, ou encore en remarquant que $A[X]/(p)$ est isomorphe à $(A/(p))[X]$, qui est intègre vu que (p) est premier dans A). Supposons donc P primitif de degré au moins 1, et donc irréductible

dans $K[X]$ d'après le théorème précédent. Alors si P divise le produit QR de deux polynômes de $A[X]$, il divise Q ou R dans $K[X]$ vu que $K[X]$ est principal, par exemple Q. Il existe donc a dans A tel que $aQ = SP$ avec $S \in A[X]$. Alors $ac(Q) = c(S)$ car P est primitif, et a divise $c(S)$. En particulier $Q = (S/a)P$ avec S/a dans $A[X]$, i.e. P divise Q dans $A[X]$. C'est ce qu'on voulait montrer.

□

Corollaire 2.20 *Si A est factoriel, $A[X_1, ..., X_n]$ est factoriel.* [8]

Il est commode d'avoir un critère pratique d'irréductibilité dans les anneaux factoriels. Le résultat suivant est souvent utile :

Theorème 2.21 (Critère d'Eisenstein) *Soient A un anneau factoriel, P un polynôme non constant de $A[X]$, p irréductible dans A. On pose $P = \sum_{k=0}^{n} a_k X^k$ et on suppose :*

1. *p ne divise pas a_n.*
2. *p divise a_k pour $0 \leq k \leq n-1$.*
3. *p^2 ne divise pas a_0.*

Alors P est irréductible dans $K[X]$ (donc aussi dans $A[X]$ s'il est primitif).

Démonstration : Notons que $P/c(P)$ vérifie les mêmes hypothèse que P vu que $c(P)$ n'est pas divisible par p via 1. On peut donc supposer P primitif et $\deg P \geq 2$. Si P n'était pas irréductible, il s'écrirait (d'après le théorème 2.18) $P = QR$ avec Q, R non constants dans $A[X]$. Posons $Q = b_r X^r + ... + b_0$, $R = c_s X^s + ... + c_0$. L'anneau $B = A/(p)$ est intègre, et $A[X]/pA[X]$ est isomorphe à $B[X]$. Dans $A[X]/pA[X]$, on a $\overline{P} = \overline{QR}$, soit $\bar{a}_n X^n = \overline{Q}.\overline{R}$ dans $B[X]$. On a $\bar{a}_n \neq 0$ dans B, donc $\bar{b}_r$ et $\bar{c}_s$ sont aussi non nuls. Ainsi $\overline{Q}$ et $\overline{R}$ ne sont pas constants et l'égalité $\bar{a}_n X^n = \overline{Q}.\overline{R}$ dans l'anneau principal (donc factoriel) $(\mathrm{Frac}\, B)[X]$ implique alors (comme X est irréductible dans cet anneau) que $\overline{Q}$ et $\overline{R}$ sont divisibles par X dans $(\mathrm{Frac}\, B)[X]$. Cela signifie que p divise b_0 et c_0, ce qui contredit le fait que a_0 n'est pas divisible par p^2.

□

Par exemple $X^{18} - 4X^7 - 2$ est irréductible dans $\mathbf{Q}[X]$, et $X^5 - XY^3 - Y$ est irréductible dans $\mathbf{C}[X, Y]$ (prendre $A = \mathbf{C}[Y]$ et $p = Y$).

[Exercice : si p est un nombre premier, alors $1 + X + ... + X^{p-1} = \frac{X^p - 1}{X - 1}$ est irréductible dans $\mathbf{Q}[X]$.]

[8] On a l'analogue avec une infinité d'indéterminées, c'est immédiat à partir du cas fini.

3. Modules sur un anneau commutatif

La notion de module est la généralisation naturelle de celle d'espace vectoriel. Elle est absolument fondamentale, par exemple en géométrie algébrique et en théorie des nombres. Dans toute la suite, A désigne un anneau commutatif, que l'on sera parfois amené à supposer *non nul*.

3.1. Généralités

Définition 3.1 Un *A-module* $(M, +, .)$ est un ensemble équipé d'une loi interne $+$ et d'une loi externe $A \times M \to M$, $(\alpha, m) \mapsto \alpha m$ vérifiant :

- $(M, +)$ est un groupe abélien.
- On a en plus les quatre propriétés suivantes :

  1. $\alpha(m + m') = \alpha m + \alpha m'$
  2. $(\alpha + \beta)m = \alpha m + \beta m$
  3. $(\alpha\beta)m = \alpha(\beta m)$
  4. $1.m = m$

  pour tous $\alpha, \beta \in A$ et tous $m, m' \in M$.

Remarque : Comme A est supposé commutatif, il n'y a pas lieu de distinguer entre modules à gauche et à droite (pour A non commutatif, le troisième axiome serait différent pour un module à droite).

Définition 3.2 Soit M un A-module. Un *sous-module* N de M est un sous-groupe de $(M, +)$ qui est en plus stable pour la multiplication externe par tout élément de A.

Autrement dit une partie N de M est un sous-module si et seulement s'il contient 0, et si pour tous x, y de N et tout α de A on a : $x + y \in N$ et $\alpha x \in N$.

Exemples :

1. A est un A-module, l'opération externe étant la multiplication dans A.
2. Tout groupe abélien M peut être considéré comme un $\mathbf{Z}$-module pour la loi externe : $\alpha m = m+m+...+m$ (α termes) si $\alpha > 0$, $\alpha m = (-\alpha)(-m)$ si $\alpha < 0$ et $0.m = 0$.

3. Soient $n > 0$ et M un groupe abélien *de n-torsion*, c'est-à-dire tel que $nx = 0$ pour tout x de M. Alors M est un $\mathbf{Z}/n\mathbf{Z}$-module pour la loi $\bar{\alpha}.x = \alpha x$, où $\alpha \in \mathbf{Z}$ a pour classe $\bar{\alpha}$ dans $\mathbf{Z}/n\mathbf{Z}$.

4. Soit I une partie de A. Alors I est un sous A-module de A si et seulement si c'est un idéal de A.

5. Soit $(M_i)_{i\in I}$ une famille (finie ou non) de A-modules. Alors l'ensemble produit $\prod_{i\in I} M_i$ est un A-module pour les lois évidentes; on l'appelle le *A-module produit* des M_i.

6. Soit S une partie d'un A-module M. Alors le *sous-module engendré* par S est l'ensemble des combinaisons linéaires $\sum_{s\in S} \alpha_s s$, où $(\alpha_s)_{s\in S}$ est une famille presque nulle d'éléments de S. C'est le plus petit sous-module de M qui contient S. Cette notion est surtout utile quand S est fini.

Définition 3.3 Un *homomorphisme* (ou morphisme) de A-modules est une application $f : M \to M'$ entre deux A-modules qui vérifie : $f(x + y) = f(x) + f(y)$ et $f(\alpha.x) = \alpha.f(x)$ pour tous x, y de M et tout α de A. On note $\ker f := f^{-1}(\{0\})$ le *noyau* de f et $\operatorname{Im} f := f(M)$ son image. Ce sont des sous-modules de M, M' respectivement.

Au lieu de morphisme de A-modules, on dit parfois application A-linéaire. On a bien sûr les notions d'isomorphisme et d'automorphisme de A-modules.

On a le théorème de factorisation habituel (preuve immédiate) :

Proposition 3.4 *Soient M un A-module et N un sous-module de M. Alors le groupe quotient M/N, équipé de la loi externe $\alpha.\bar{m} = \overline{\alpha.m}$ est un A-module, appelé module quotient de M par N. Si $f : M \to M'$ est un morphisme de A-modules, il existe un unique morphisme $\tilde{f} : M/\ker f \to M'$ tel que $f = \tilde{f} \circ \pi$, où $\pi : M \to M/\ker f$ est la surjection canonique. De plus $\tilde{f}$ est injective d'image* $\operatorname{Im} f$.

La définition suivante est analogue à celle qu'on a dans les espaces vectoriels :

Définition 3.5 • Soit $(M_i)_{i\in I}$ une famille de A-modules. La *somme directe* ("externe") des M_i est le sous module $\bigoplus_{i\in I} M_i$ du produit $\prod_{i\in I} M_i$ constitué des familles $(m_i)_{i\in I}$ presque nulles. Si I est fini, la somme directe coïncide avec le produit direct.

- Soit $(M_i)_{i\in I}$ une famille de sous-modules du A-module M. Alors le sous-module *somme* $\sum_{i\in I} M_i$ est le module engendré par la réunion des M_i. Si la condition $\sum_{i\in I} m_i = 0$ implique $m_i = 0$ pour tout i (où $(m_i)_{i\in I}$ est une famille presque nulle avec $m_i \in M_i$ pour chaque i), on dit que la somme des M_i est *directe*; dans ce cas $\sum_{i\in I} M_i$ est isomorphe à la somme directe $\bigoplus_{i\in I} M_i$, et on notera $\bigoplus_{i\in I} M_i$ pour $\sum_{i\in I} M_i$ ("somme directe interne").

On notera que deux sous-modules M_1, M_2 d'un A-module M sont en somme directe si et seulement si $M_1 \cap M_2 = \{0\}$, mais ceci ne se généralise pas à plus de deux sous-modules. D'autre part si $M = M_1 \oplus M_2$, alors M/M_1 est isomorphe à M_2 mais contrairement au cas des espaces vectoriels, il n'y a pas de réciproque [9] (par exemple $\mathbf{Z}$ n'est pas isomorphe à la somme directe externe de $n\mathbf{Z}$ et $\mathbf{Z}/n\mathbf{Z}$ puisque $\mathbf{Z}$ n'a pas délément non nul annulé par n).

3.2. Modules libres, modules de type fini

Définition 3.6 Un A-module M est dit *de type fini* s'il existe une partie finie S de M tel que M soit engendré par S. Il est dit *libre* s'il admet une base, i.e. une famille $(x_i)_{i\in I}$ telle que tout élément x de M s'écrive de manière unique $x = \sum_{i\in I} \alpha_i x_i$, avec $(\alpha_i)_{i\in I}$ famille presque nulle d'éléments de A.

Remarques :

1. On verra que si M est libre et de type fini, alors il admet une base finie mais pour l'instant cela n'a rien d'évident !

2. Dire que $(x_i)_{i\in I}$ est une base équivaut au fait que la famille (x_i) soit à la fois génératrice et *libre*, ce dernier point signifiant que la condition $\sum_{i\in I} \alpha_i x_i = 0$ implique que la famille presque nulle (α_i) est nulle.

3. Un A-module M admet une base de cardinal n si et seulement s'il est isomorphe à A^n. Plus généralement il admet une base de cardinal I si et seulement s'il est isomorphe à $A^{(I)}$ (ensemble des familles $(\alpha_i)_{i\in I}$ presque nulles dans A^I). [10]

4. Un A-module M est de type fini si et seulement s'il s'écrit comme quotient de A^n pour un certain $n > 0$. On ne confondra pas cette notion avec celle de A-algèbre de type fini (qui correspond à être un quotient

[9] Autrement dit : une suite exacte d'espaces vectoriels est toujours scindée, mais pas une suite exacte de A-modules.

[10] Attention, si I est infini, il n'y a aucune raison que A^I soit libre.

de l'anneau de polynômes $A[X_1, ..., X_n]$). Quand une A-algèbre est de type fini en tant que A-module, on parle parfois de A-algèbre *finie*.

Exemples :

1. $\mathbf{Z}/n\mathbf{Z}$ est un $\mathbf{Z}$-module de type fini (il est engendré par $\bar{1}$), mais il n'est pas libre car dans un $\mathbf{Z}$-module libre, la condition $\alpha x = 0$ implique $\alpha = 0$ ou $x = 0$ si $\alpha \in Z$, $x \in M$ (on dit qu'un tel module est *sans torsion*. C'est plus généralement le cas dans tout module libre sur un anneau intègre).

2. Bien que le $\mathbf{Z}$-module $\mathbf{Q}$ soit sans torsion, il n'est pas libre car il est *divisible* : si $n > 0$, tout élément x de $\mathbf{Q}$ s'écrit ny avec $y \in \mathbf{Q}$, ce qui n'est pas possible dans un $\mathbf{Z}$-module libre (prendre un élément dont l'une des composantes sur la base est 1 et $n \geq 2$). On verra que sur un anneau *principal*, un module de type fini et sans torsion est libre.

3. De manière immédiate, un quotient d'un module de type fini est encore de type fini.

4. Si A est un anneau non noethérien, un idéal de A qui n'est pas engendré par un nombre fini d'éléments n'est pas de type fini comme A-module, bien que ce soit un sous-module de A (qui est engendré par 1). On verra que si A est noethérien, un sous-module d'un module de type fini sur A est encore de type fini.

Ainsi, la situation est beaucoup moins bonne pour les modules que pour les espaces vectoriels. Il y a quand même un énoncé qui est vrai en toute généralité, c'est que les bases de M sont finies et de même cardinal si M est libre et de type fini. C'est l'objet du théorème suivant :

Theorème 3.7 *Soit A un anneau commutatif* **non nul**. *Supposons qu'il existe un morphisme surjectif de A-modules $f : A^r \to A^s$. Alors $r \geq s$.*

Démonstration : Nous allons donner deux preuves. La première consiste à se ramener au résultat connu pour les espaces vectoriels, la seconde à effectuer un calcul matriciel utilisant les propriétés du déterminant.

Preuve 1 : Comme $A \neq \{0\}$, A possède au moins un idéal maximal I (ce résultat utilise le théorème de Zorn en général, mais il est immédiat si A est noethérien). Pour tout A-module M, on définit le sous A-module IM comme le module engendré par les im pour $i \in I$ et $m \in M$. Alors M/IM est un espace vectoriel sur le corps $K := A/I$ via $\bar{a}\bar{m} := \overline{am}$, $a \in A$, $m \in M$.

On applique cela à $M = A^r$, $N = A^s$. Le morphisme surjectif de A-modules $f : M \to N$ induit un morphisme $\bar{f}$ de K-espaces vectoriels $M/IM \to N/IN$ défini par $\bar{f}(\bar{m}) = \overline{f(m)}$ et il est clair que $\bar{f}$ est encore surjectif. Comme M/IM est isomorphe à K^r (on envoie la classe de $(a_1, ..., a_r)$ sur $(\bar{a}_1, ..., \bar{a}_r)$), on obtient un morphisme surjectif de K-espaces vectoriels de K^r sur K^s, donc $r \geq s$ par la théorie de la dimension. [11]

Preuve 2 : Soit $B \in M_{s,r}(A)$ la matrice de l'application A-linéaire $f : A^r \to A^s$. Comme f est surjectif, les éléments $\varepsilon_1, ..., \varepsilon_s$ de la base canonique de A^s ont chacun un antécédent par f, d'où des vecteurs colonnes $X_1, ..., X_s$ de A^r tels que $BX_i = \varepsilon_i$. La matrice C de $M_{r,s}(A)$ dont les vecteurs colonnes sont les X_i vérifie alors $BC = I_s$. Si on avait $s > r$, on pourrait considérer la matrice B_1 obtenue en ajoutant $s - r$ colonnes nulles à B, et la matrice C_1 obtenue en ajoutant $s - r$ lignes nulles à C, et on aurait encore $B_1C_1 = I_s$, avec B_1 et C_1 dans $M_s(A)$. Mais alors $\det B_1 \det C_1 = 1$ (qui est non nul car A n'est pas nul !), ce qui est impossible vu les propriétés du déterminant.

□

Corollaire 3.8 *Soit M un module sur un anneau non nul A. Si M est de type fini et admet une base, alors cette base est finie. On dit dans ce cas que M est libre de type fini, et toutes les bases de M ont le même cardinal, qu'on appelle le rang de M.*

Démonstration : Soit r un entier. Notons d'abord que si M possède une base (finie ou non) de cardinal $> r$, alors il existe un sous-module N de M tel que M/N soit isomorphe à A^{r+1} (il suffit de prendre $r+1$ éléments $e_1, ..., e_{r+1}$ dans la base, et de choisir pour N le sous-module consitué des m de M dont la composante sur e_i est nulle pour tout i de $[1, r+1]$). Ceci dit, supposons que M soit engendré par une famille finie $(f_1, ..., f_r)$. Alors on a un morphisme surjectif de A-modules $u : A^r \to M$ défini par $u(a_1, ..., a_r) = \sum_{i=1}^r a_i f_i$. Si M possédait une base infinie (en particulier de cardinal $> r$), on aurait un quotient M/N tel que M/N soit isomorphe à A^{r+1}. En composant u avec la surjection canonique $M \to M/N$, on obtiendrait alors une application A-linéaire surjective de A^r dans A^{r+1}, ce qui contredit le théorème. Ainsi, si M admet une base, cette base est finie. Le fait que les bases aient toutes le même cardinal résulte alors immédiatement du théorème.

□

[11] On a tensorisé M et N par le A-module $K = A/I$; cette opération préserve le caractère surjectif des morphismes, et transforme A^r en K^r. Noter que si A n'est pas intègre, on ne peut pas faire la même chose en utilisant un corps de fractions.

Notons que $2\mathbf{Z}$ est un sous $\mathbf{Z}$-module strict de $\mathbf{Z}$, bien qu'ils aient tous deux pour rang 1. Ainsi $2\mathbf{Z}$ n'a pas de supplémentaire dans $\mathbf{Z}$, et la famille libre (2) ne peut pas être complétée en une base de $\mathbf{Z}$.

[Exercice : soit A un anneau commutatif non nul. a) Soit P une matrice de $M_r(A)$, et f l'application A-linéaire $A^r \to A^r$ qu'elle induit. Montrer que f est injective si et seulement si $\det A$ est régulier [12] dans A, et que f est surjective si et seulement si $\det A \in A^*$.

b) En déduire que si $f : A^r \to A^s$ est linéaire injective, alors $r \leq s$.

c) Soit M un sous-module de A^r. Alors si M est libre, son rang est au plus r. En particulier un idéal I d'un anneau A ne peut pas être un A-module libre s'il n'est pas principal (=engendré par un seul élément). On ne peut donc espérer un énoncé positif que pour les anneaux principaux; on verra que c'est effectivement le cas.]

Theorème 3.9 *Soient A un anneau noethérien et M un A-module de type fini. Alors tout sous-module de M est de type fini.*

Démonstration : Comme M est de type fini, on peut l'écrire comme un quotient A^r/M' avec M' sous-module de A^r; un sous-module de A^r/M' est de la forme N'/M', avec N' sous-module de A^r contenant M'. Ainsi il suffit de prouver le résultat pour $M = A^r$ car un quotient d'un module de type fini est encore de type fini.

On montre cela par récurrence sur r. Pour $r = 1$, c'est la définition d'un anneau noethérien. Supposons le résultat vrai pour tout entier $< r$, et soit N un sous-module de A^r. Appelons M_1 le sous-module de A^r constitué des $(a, 0, 0, .., 0)$ avec $a \in A$, alors M_1 est isomorphe à A. D'après le cas $r = 1$, $N_1 := N \cap M_1$ est de type fini. D'autre part l'application linéaire $\pi : N \to A^r/M_1$ qui à x associe $\bar{x}$ a pour noyau N_1; le module A^r/M_1 est isomorphe à A^{r-1}, donc $\operatorname{Im}\pi$ est de type fini par hypothèse de récurrence. Soit $(\bar{x}_1, ..., \bar{x}_n)$ une famille finie engendrant $\operatorname{Im}\pi$ ($x_i \in A^r$) et $(y_1, ..., y_m)$ une famille finie engendrant N_1, alors il est immédiat que $(x_1, ..., x_n, y_1, ..., y_m)$ engendre N.[13]

□

Remarque : Noter qu'on peut avoir besoin de plus de générateurs pour un sous-module de M que pour N, prendre par exemple un idéal de A qui

[12] Un élément a de A est *régulier* si $ab = 0$ avec $b \in A$ implique $b = 0$; pour cette question, supposer que $a := \det A$ n'est pas régulier, et considérer un mineur m de P de taille maximale tel que $am \neq 0$.

[13] Plus généralement si $0 \to M_1 \to M \to M_2 \to 0$ est une suite exacte de A-modules, il est clair que le fait que M_1 et M_2 soient de type fini implique que M est de type fini.

n'est pas principal. On va voir que précisément, cette difficulté disparaît quand A est principal.

3.3. Modules sur un anneau principal : les grands théorèmes

Dans tout ce paragraphe, A désigne un anneau principal. Le premier résultat raffine considérablement le théorème 3.9 dans ce cadre.

Theorème 3.10 *Soit A un anneau principal. Alors tout sous-module N de A^n est libre et de rang fini $m \leq n$.*

Remarque : Comme A est noethérien, on sait déjà que N est de type fini. Si on savait déjà que N était libre, le fait que son rang soit au plus n résulterait de l'exercice vu plus haut, mais c'est bien la liberté de N qui est le point difficile, et qui ne marche pas dès que A n'est pas principal.

Démonstration : On procède par récurrence sur n. Pour $n = 1$, c'est la définition d'un anneau principal. Supposons donc le résultat vrai pour tous les entiers $< n$. Soit N un sous-module de A^n, posons $M_1 = Ae_2 \oplus ... \oplus Ae_n$, où $(e_1, ..., e_n)$ est la base canonique de A^n. Si $N \subset M_1$, c'est fini par hypothèse de récurrence car M_1 est isomorphe à A^{n-1}. On suppose donc désormais $N \not\subset M_1$. Par hypothèse de récurrence, $(N \cap M_1)$ possède une base $(f_2, ..., f_m)$ avec $m \leq n$. La difficulté est maintenant de trouver un élément de N pour compléter cette base en une base de N.

Considérons le sous-ensemble I de A constitué des $b \in A$ tels qu'il existe $y \in M_1$ avec $be_1 + y \in N$. Il est immédiat que I est un idéal de A, et cet idéal n'est pas nul car N contient un élément qui n'est pas dans M_1, donc s'écrit (en le décomposant sur la base canonique de A^n) $be_1 + y$ avec $y \in M_1$ et $b \neq 0$. Comme A est principal, on peut écrire $I = (d)$ avec $d \neq 0$ dans A. Par définition de I, on a alors un élément $f_1 = de_1 + y_1$ dans N avec $y_1 \in M_1$. Notons que $f_1 \neq 0$, sinon d serait nul vu que $A^n = Ae_1 \oplus M_1$. Nous allons montrer que $(f_1, ..., f_m)$ est une base de N.

Montrons d'abord que $(f_1, ..., f_m)$ engendre N. Si $x \in N$, on a $x = be_1 + y$ avec $b \in A$ et $y \in M_1$. Mais alors $b \in I$ d'où $b = ad$ avec $a \in A$. Ceci donne $x = af_1 + (y - ay_1)$, donc $(x - af_1)$ est dans $N \cap M_1$, ce qui permet de le décomposer sur la base $(f_2, ..., f_m)$ de $N \cap M_1$. Ainsi $x = af_1 + x'$ avec $x' \in Af_2 + ... + Af_m$, ce qui montre que $(f_1, ..., f_m)$ engendre N.

Montrons enfin que $(f_1, ..., f_m)$ est libre. Pour cela il suffit de montrer que (f_1) est libre et qu'on a $Af_1 \cap (N \cap M_1) = \{0\}$, car $(f_2, ..., f_m)$ est déjà

libre par hypothèse. Le premier point est évident en décomposant f_1 (qui est non nul) sur la base canonique de A^n. D'autre part si λf_1 est dans M_1 avec $\lambda \in A$, alors $\lambda d e_1 + \lambda y_1 \in M_1$, d'où $(\lambda d)e_1 \in M_1$ mais par définition de M_1 et de la base canonique de A^n, ceci implique $\lambda d = 0$ donc $\lambda = 0$ par intégrité de A.

□

Pour aller plus loin dans la classification des modules sur un anneau principal, il faut connaître le résultat plus précis suivant. C'est sans doute le théorème le plus important de toute la théorie.

Theorème 3.11 ("de la base adaptée") *Soient A un anneau principal, M un A-module libre de rang n, et N un sous-module de M. Alors il existe une base $(e_1, ..., e_n)$ de M et des éléments $(d_1, ..., d_r)$ de A (avec $r \leq n$) tels que :*

1. *$(d_1 e_1, ..., d_r e_r)$ soit une base de N.*
2. *on ait les divisibilités : $d_1 \mid d_2 \mid ... \mid d_r$.*

En particulier les d_i sont non nuls, et on peut remplacer chaque d_i par n'importe quel élément de A qui lui est associé. Notons qu'on savait déjà que N était libre de rang $\leq n$ via le théorème 3.10.

La preuve du théorème de la base adaptée est longue et assez compliquée. On commence par un lemme qui initialise un raisonnement par récurrence sur n.

Lemme 3.12 *On suppose $N \neq \{0\}$. Alors il existe une application linéaire $f_1 : M \to A$ telle que*

1. *$f_1(N)$ soit maximal (pour l'inclusion) parmi les $f(N)$ avec $f : N \to A$ linéaire.*
2. *Si on pose $f_1(N) = (d_1)$, alors il existe $e_1 \in M$ tel que $f_1(e_1) = 1$ et $u_1 := d_1 e_1$ soit dans N.*

Démonstration : Pour toute forme linéaire $f : M \to A$, $f(N)$ est un idéal de A. Le premier point résulte alors de ce que A est principal, donc noethérien. Notons que d_1 est non nul car N est non nul (prendre par exemple une forme linéaire "coordonnée" associée à une base de M).

Soit alors $u_1 \in N$ tel que $f_1(u_1) = d_1$. Si $f : M \to A$ est une forme linéaire quelconque, posons $d = f(u_1)$ et $e = (d, d_1)$ (attention on ne sait pas

encore que d_1 divise d car $f_1(N)$ est a priori juste maximal, pas forcément un plus grand élément). Alors par Bezout il existe α, β dans A tels que $(\alpha f + \beta f_1)(u_1) = e$. Ceci implique que $(\alpha f + \beta f_1)(N) \supset eA \supset d_1 A$, et par maximalité e et d_1 sont associés, soit $d_1 \mid d$. Finalement $f(u_1) \in d_1 A$ pour toute forme linéaire $f : M \to A$. En prenant les formes linéaires "coordonnées" associées à une base de M, on voit que $u_1 = d_1 e_1$ avec $e_1 \in M$, puis $f_1(e_1) = 1$ vu que $f_1(u_1) = d_1 \neq 0$.

□

On a ensuite

Lemme 3.13 *Avec les hypothèses et notations du lemme précédent, on a :*

1. $M = Ae_1 \oplus \ker f_1$ *et* $N = Au_1 \oplus (\ker f_1 \cap N)$.
2. *Pour toute forme linéaire* $f : M \to A$, *on a* $f(N) \subset d_1 A$.

Démonstration : 1. Comme $f_1(e_1) = 1$, $Ae_1 \cap \ker f_1 = \{0\}$ est clair. Tout x de M s'écrit $x = f_1(x)e_1 + (x - f_1(x)e_1)$ avec $(x - f_1(x)e_1) \in \ker f_1$ donc $M = Ae_1 \oplus \ker f_1$. De même tout x de N vérifie $f_1(x) = ad_1$ avec $a \in A$, d'où $x = au_1 + (x - au_1)$ avec $(x - au_1) \in (\ker f_1 \cap N)$. Enfin $Au_1 \cap \ker f_1 = \{0\}$ résulte de $f_1(u_1) = d_1 \neq 0$, et A intègre.

2. Soit $f : M \to A$ linéaire. Via 1., on définit $g : M \to A$ linéaire par : $g(x) = f(x)$ si $x \in \ker f_1$, et $g(e_1) = 1$. Alors comme $g(u_1) = d_1$, on a $g(N) = d_1 A$ par maximalité. En particulier la restriction de f à $(\ker f_1 \cap N)$ a son image incluse dans $d_1 A$, donc celle de f à N aussi puisque N est la somme de $(\ker f_1 \cap N)$ et de Au_1, tandis que $f(u_1) = d_1 f(e_1)$ est divisible par d_1.

□

Fin de la preuve du théorème de la base adaptée : Pour $n = 1$, on peut supposer $M = A$ et le résultat vient de la définition d'un anneau principal. Supposons le résultat vrai pour les entiers $< n$. On applique alors le lemme 3.13, et l'hypothèse de récurrence au A-module $\ker f_1$ (qui est libre par le théorème 3.10, puis de rang $n - 1$ par le corollaire 3.8 et l'égalité $M = Ae_1 \oplus \ker f_1$) et à son sous-module $(\ker f_1 \cap N)$. On obtient une base $(e_2, ..., e_n)$ de $\ker f_1$, et des éléments $d_2, ..., d_r$ de A avec $r \leq n$ et $d_2 \mid ... \mid d_r$ tels que $M = Ae_1 \oplus ... \oplus Ae_n$ et $N = A(d_1 e_1) \oplus ... \oplus A(d_r e_r)$. Enfin d_1 divise d_2 en appliquant le lemme 3.13 à la forme linéaire "deuxième coordonnée" (dans la base $(e_1, ..., e_n)$) sur M.

□

Attention aux erreurs habituelles : le théorème de la base adaptée ne dit pas que N admet un supplémentaire, ni qu'on peut compléter une base de N en une base de M (prendre simplement $A = \mathbf{Z}$, $M = \mathbf{Z}$, $N = 2\mathbf{Z}$).

Corollaire 3.14 *Soit M un module de type fini sur A principal. Alors il existe $d_1, ..., d_s$ dans A, non nuls et non inversibles, tels que M soit isomorphe à*

$$A^m \oplus \bigoplus_{i=1}^{s} (A/d_i A)$$

avec $m \in \mathbf{N}$ et $d_1 \mid d_2 \mid ... \mid d_s$.

Démonstration : Comme M est de type fini, il est engendré par n éléments, d'où une suite exacte de A-modules

$$0 \to N \to A^n \xrightarrow{p} M \to 0$$

(cela signifie simplement que M est isomorphe à un quotient de A^n).

On applique alors le théorème de la base adaptée au sous-module N du A-module libre A^n. On obtient

$$A^n = \bigoplus_{i=1}^{n} Aei$$

$$N = \bigoplus_{i=1}^{r} A(d_i e_i)$$

Soit alors z_i l'image de e_i dans M (par p). Alors $M = \bigoplus_{i=1}^{r} Az_i$ car les z_i engendrent M (par surjectivité de p), et si $\sum_{i=1}^{r} \lambda_i z_i = 0$ avec $\lambda_i \in A$, alors $\sum_{i=1}^{r} \lambda_i e_i \in N$ donc chaque λ_i est multiple de d_i (parce que $(d_i e_i)_{1 \leq i \leq r}$ est une base de N) et chaque $\lambda_i e_i$ est donc dans N, i.e. $\lambda_i z_i = 0$. Finalement $M = \bigoplus_{i=1}^{r} A.z_i$. Chaque $A.z_i$ est isomorphe à $(A/d_i A)$ car le noyau de la surjection $\lambda \mapsto \lambda z_i$ de A dans $A.z_i$ est $d_i A$ (toujours parce que $(d_i e_i)_{1 \leq i \leq r}$ est une base du noyau N de p). On obtient $M \simeq A^{n-r} \oplus \bigoplus_{i=1}^{r} (A/d_i A)$, mais pour d_i inversible on a $A/d_i A = 0$, donc on peut ne garder que les d_i non inversibles.

□

Définition 3.15 Soit M un module sur un anneau commutatif A. On rappelle que M est dit *sans torsion* si la condition $ax = 0$ (avec $a \in A$, $x \in M$) implique $a = 0$ ou $x = 0$. On dit que M est *de torsion* si pour tout x de M, il existe a non nul dans A tel que $ax = 0$.

Attention, "sans torsion" n'est pas le contraire de "de torsion". De manière évidente un module libre sur un anneau intègre est sans torsion. On peut maintenant démontrer la réciproque pour un anneau principal :

Corollaire 3.16 *Soit M un module de type fini sur A principal. Alors M est libre si et seulement s'il est sans torsion.*

Démonstration : Cela résulte immédiatement du corollaire 3.14, car la condition que M est sans torsion implique que $s = 0$ (pour d non inversible, A/dA est non nul, et tout élément de A/dA est annulé par d).

□

Ce dernier corollaire est très spécifique aux anneaux principaux. Si A est intègre noethérien, tout idéal I de A est un A-module de type fini et sans torsion, mais d'après l'exercice après le corollaire 3.8, I n'est pas libre dès qu'il n'est pas principal.

Remarque : Si A est un anneau intègre, un A-module (de type fini) M est dit *projectif* s'il est *facteur direct* d'un module libre, i.e. s'il existe un A-module N tel que $M \oplus N$ soit libre. On a donc en particulier qu'un module projectif (de type fini) sur un anneau principal est toujours libre. [14] Ce n'est pas vrai pour un anneau intègre en général, par exemple pour $A = \mathbf{Z}[i\sqrt{5}]$, un idéal non principal ne peut pas être libre comme on l'a déjà vu, mais c'est quand même un A-module projectif (difficile). [15]

Pour finir la classification des modules de type fini sur un anneau principal A, on a besoin d'assertions d'unicité. De manière un peu surprenante, il est difficile de prouver un tel résultat directement à partir du corollaire 3.14; il est nettement plus commode d'introduire la notion de *composantes p-primaires*.

Définition 3.17 Soit p un irréductible de A. On dit qu'un A-module est *p-primaire* s'il est isomorphe à un module du type $\bigoplus_{i=1}^{s}(A/p^{v_i}A)$ avec $v_i \in \mathbf{N}^*$.

En particulier un A-module p-primaire est de type fini et de torsion.

Pour tout d non nul dans l'anneau principal A, on note comme d'habitude $v_p(d)$ la plus grande puissance de l'irréductible p qui divise d.

[14] L'hypothèse de finitude n'est pas indispensable, mais la preuve est nettement plus compliquée sans; voir l'article de Kaplansky dans *Ann. Math.* **68** (1958).

[15] La condition que A soit factoriel n'est ni nécessaire ni suffisante pour que tout A-module projectif soit libre, en particulier cette propriété est vraie pour tout anneau *local*, c'est-à-dire qui n'a qu'un idéal maximal, et il y a des anneaux locaux non factoriels. Cela marche aussi pour certains anneaux qui ne sont pas de dimension 1, par exemple pour $K[X_1, ...X_n]$ quand K est un corps (théorème de Quillen-Suslin, 1976, *quondam* conjecture de Serre).

Proposition 3.18 *1. Soit $d = u\prod_{p\in S} p^{\alpha_p}$ une décomposition de d en produits d'irréductibles (où S est un ensemble fini d'irréductibles deux à deux non associés). Alors*

$$A/dA \simeq \bigoplus_{p\in S}(A/p^{\alpha_p}A)$$

2. Soit $M = \bigoplus_{i=1}^{s}(A/d_iA)$ avec $d_1 \mid d_2 \mid ... \mid d_s$. Alors pour tout irréductible p de A et tout entier $k \geq v_p(d_s)$, on a

$$M/p^kM \simeq \bigoplus_{i=1}^{s}(A/p^{v_p(d_i)}A)$$

3. Soient M un A-module de torsion et $\mathcal{P}$ un système d'irréductibles de A. Alors

$$M = \bigoplus_{p\in\mathcal{P}} M_p$$

où M_p est un module p-primaire tel que $M_p = M/p^kM$ pour k assez grand, et presque tous les M_p sont nuls. On dit que les M_p sont les composantes p-primaires de M.

Démonstration : 1. C'est le classique lemme chinois quand $A = \mathbf{Z}$. En raisonnant par récurrence sur le cardinal de S, il suffit de démontrer que $A/(d_1d_2)A \simeq A/d_1A \times A/d_2A$ quand d_1, d_2 sont deux éléments de A premiers entre eux. Or l'application qui à $a \in A$ associe $(\bar{a}, \bar{a})$ a clairement pour noyau $(d_1d_2)A$ car $(d_1, d_2) = 1$. Elle est surjective via Bezout.

2. p étant fixé, on remarque que si q est un irréductible de A non associé à p, alors la multiplication par p est surjective dans A/q^mA pour tout $m \in \mathbf{N}$ (utiliser une identité de Bezout pour q^m et p). On en déduit que si Q est un module q-primaire, la multiplication par p^n est surjective dans Q pour tout $n \in \mathbf{N}$, i.e. $Q/p^nQ = 0$.

D'après 1., M est isomorphe à $\bigoplus_{q\in S} M_q$ avec M_q module q-primaire (S étant un ensemble fini d'irréductibles deux à deux non associés, obtenu en décomposant tous les d_i). Ainsi $M/p^kM = M_p/p^kM$ puisque pour $q \neq p$ dans S, on a $M_q/p^kM_q = 0$. Comme d'après 1. on a $M_p = \sum_{i=1}^{s}(A/p^{v_p(d_i)}A)$, on obtient $M/p^kM = M_p$ dès que k est plus grand que tous les $v_p(d_i)$, i.e. pour $k \geq v_p(d_s)$.

3. est maintenant évident.

□

On va en déduire le résultat d'unicité annoncé :

Theorème 3.19 *Soit M un module de type fini sur A principal. Écrivons*

$$M \simeq A^m \oplus \bigoplus_{i=1}^{s} (A/d_i A)$$

avec $d_1, ..., d_s$ non nuls et non inversibles tels que $d_1 \mid ... \mid d_s$. Alors m, s, et les d_i à association près ne dépendent que de M.

En d'autres termes si on a une autre décomposition

$$M \simeq A^{m'} \oplus \bigoplus_{i=1}^{s'} (A/d'_i A)$$

alors $m = m'$, $s = s'$, et d'_i est associé à d_i pour tout i.

Démonstration : Soit M_{tors} le *sous-module de torsion* de M, c'est-à-dire l'ensemble des x de M tels qu'il existe $a \neq 0$ dans A avec $ax = 0$. Alors $M_{\text{tors}} \simeq \bigoplus_{i=1}^{s} (A/d_i A)$ et $M/M_{\text{tors}} \simeq A^m$. Par invariance du rang d'un module libre de type fini, m ne dépend que de M et on se ramène à M de torsion.

Il suffit alors de montrer que pour tout irréductible p, la suite des $v_p(d_i)$ est bien déterminée. Comme un A-module de torsion M est la somme directe de ses composantes p-primaires $M_p = \bigoplus_{i=1}^{s} (A/p^{v_p(d_i)} A)$, qui sont caractérisées par $M_p = M/p^k M$ pour k assez grand, on est ramené au cas où M est p-primaire.

Supposons donc $M = \bigoplus_{i=1}^{s} (A/p^{\alpha_i} A)$, où (α_i) est une suite croissante d'entiers. Comme A est principal et p irréductible, A/pA est un corps et d'autre part pour tout $k \in \mathbf{N}$, le A-module de p-torsion $p^k M/p^{k+1} M$ est muni canoniquement d'une structure de A/p-espace vectoriel via $(\bar{\lambda}, \bar{x}) \mapsto \lambda \bar{x}$ ($\lambda \in A$, $\bar{x} \in p^k M/p^{k+1} M$). On remarque que si $M_i := (A/p^{\alpha_i} A)$, on a pour tout entier k : $p^k M_i/p^{k+1} M_i = 0$ si $k \geq \alpha_i$, mais $p^k M_i/p^{k+1} M_i = A/pA$ si $k < \alpha_i$. En particulier pour tout $k \in \mathbf{N}$, le nombre de $\alpha_i > k$ n'est autre que la *dimension du A/pA-espace vectoriel $p^k M/p^{k+1} M$*. Ainsi ce nombre ne dépend que de M, et donc la suite finie croissante d'entiers (α_i) aussi.

□

3.4. Applications

Nous présentons trois exemples importants d'application des théorèmes du paragraphe précédent.

Groupes abéliens de type fini.

Dans le cas $A = \mathbf{Z}$, le théorème de structure général (corollaire 3.14 et théorème 3.19) donne :

Theorème 3.20 *Soit M un groupe abélien de type fini (i.e. engendré par un nombre fini d'éléments). Alors M est isomorphe à*

$$\mathbf{Z}^r \oplus \bigoplus_{i=1}^{s} \mathbf{Z}/d_i\mathbf{Z}$$

où $r \in \mathbf{N}$, et les d_i sont des entiers ≥ 2 vérifiant $d_1 \mid ... \mid d_s$. De plus, r et les d_i sont entièrement déterminés par M.

Bien entendu, M est fini si et seulement si $r = 0$. Dans ce cas, on obtient le p-Sylow M_p de M via la décomposition p-primaire.

Équivalence de matrices à coefficients dans un anneau principal.

Soit A un anneau commutatif. On note $\mathrm{GL}_n(A)$ le groupe des inversibles de l'anneau non commutatif $M_n(A)$. D'après l'identité de la comatrice, il s'agit simplement des matrices de $M_n(A)$ dont le déterminant est inversible dans A.

Définition 3.21 Soient p et q deux entiers > 0. On dit que deux matrices B, C de $M_{p,q}(A)$ sont *équivalentes* s'il existe $U \in \mathrm{GL}_p(A)$ et $V \in \mathrm{GL}_q(A)$ telles que $C = UBV$. Il revient au même de dire qu'il existe des bases respectives $\mathcal{B}$, $\mathcal{B}'$ de A^p, A^n telles que si u désigne l'application linéaire représentée par B dans les bases canoniques de A^p, A^n, on ait : $\mathrm{Mat}_{\mathcal{B},\mathcal{B}'}(u) = C$.

Quand A est un corps, on retrouve la définition classique (qu'on prendra garde de ne pas confondre avec la relation plus fine de similitude si $p = q$). Le théorème suivant décrit les classes d'équivalence pour la relation définie ci-dessus quand A est principal.

Theorème 3.22 *Soit A un anneau principal. Alors :*

1. *Toute matrice B de $M_{p,q}(A)$ est équivalente à une matrice-bloc de la forme*

$$\begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}$$

où $D = \mathrm{Diag}(d_1, ..., d_r)$, $r \leq n$, et $d_1, ..., d_r$ sont des éléments non nuls de A vérifiant $d_1 \mid ... \mid d_r$.

2. *Deux matrices* $\begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}$ *et* $\begin{pmatrix} D' & 0 \\ 0 & 0 \end{pmatrix}$ *avec* $D = \mathrm{Diag}(d_1, ..., d_r)$, $D' = \mathrm{Diag}(d'_1, ..., d'_{r'})$ *de la forme ci-dessus sont équivalentes si et seulement si :* $r = r'$ *et pour tout* i, d_i *et* d'_i *sont associés. En d'autres termes, la suite* $(d_1, ..., d_r)$ *du 1. ne dépend (à association près) que de la classe d'équivalence de* B.

On dit que $d_1, ..., d_r$ sont les *facteurs invariants* de B, et on appelle parfois les quotients d_2/d_1,..., d_r/d_{r-1} ses *diviseurs élémentaires*. Notons que r n'est autre que le *rang* de B vue comme matrice de $M_{p,q}(K)$, où $K := \mathrm{Frac}\, A$.

Démonstration : On montre d'abord 1. Soit $u : A^p \to A^q$ l'application définie par B dans les bases canoniques. Il s'agit de trouver des base respectives $\mathcal{B}$, $\mathcal{B}'$ de A^p, A^q telles que la matrice de u dans ces bases ait la forme voulue. On applique le théorème de la base adaptée au sous-module $\mathrm{Im}\, u$ du module libre de type fini A^q. On obtient une base $(e_1, ..., e_n)$ de A^q et une suite $(d_1, ..., d_r)$ d'éléments de $A \setminus \{0\}$, avec $d_1 \mid ... \mid d_r$, telle que $(d_1 e_1, ...d_r e_r)$ soit une base de $\mathrm{Im}\, u$. On choisit alors $\varepsilon_1, ..., \varepsilon_r$ dans A^p tels que $u(\varepsilon_i) = d_i e_i$ pour $i = 1, ..., r$. Alors $(u(\varepsilon_1), ..., u(\varepsilon_r))$ est libre, donc a fortiori $(\varepsilon_1, ..., \varepsilon_r)$ est libre. D'autre part on a

$$A^p = \ker u \oplus \bigoplus_{i=1}^{r} A\varepsilon_i$$

car $(u(\varepsilon_1), ..., u(\varepsilon_r))$ est libre, et tout élément x de A^p vérifie : $u(x)$ est combinaison linéaire des $d_i e_i = u(\varepsilon_i)$, donc x s'écrit comme somme d'un élément de $\ker u$ et d'une combinaison linéaire des ε_i. On peut alors prendre une base $(\varepsilon_{r+1}, ..., \varepsilon_p)$ de $\ker u$, et on obtient une base $\mathcal{B} = (\varepsilon_1, ..., \varepsilon_p)$ de A^p. Il suffit alors de prendre $\mathcal{B}' = (e_1, ..., e_n)$ pour obtenir la forme voulue. Notons que si B est la matrice d'une injection de A^p dans A^q, les d_i qui lui sont associés apparaissent comme ceux donnés par le thórème de la base adaptée pour le sous-module $\mathrm{Im}\, u \simeq A^p$ de A^q.

Pour prouver 2., il suffit clairement de démontrer le lemme suivant :

Lemme 3.23 *Pour toute matrice* B *de* $M_{p.q}(A)$ *et tout entier* s *(inférieur ou égal à* $\min(p, q)$*, ou encore au rang* r *de* B*), on note* $m_s(B)$ *le pgcd des mineurs d'ordre* s *de* B*. Alors*

1. *Si* B *et* C *sont équivalentes,* $m_s(B)$ *et* $m_s(C)$ *sont associés.*
2. *Si* $B = \begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}$ *avec* $D = \mathrm{Diag}(d_1, ..., d_r)$ *et* $d_1 \mid ... \mid d_r$*, alors :*

$$m_s(B) = d_1 ... d_s$$

pour tout $s \in \{1, ..., r\}$.

Démonstration : 1. Il suffit de remarquer que si $U \in M_p(A)$, alors les lignes de UB sont combinaisons linéaires des lignes de B et si $V \in M_q(A)$, les colonnes de BV sont combinaisons linéaires des colonnes de B. On en déduit que $m_s(B)$ divise $m_s(UBV)$ donc par symétrie, $m_s(B)$ et $m_s(C)$ sont associés si B et C sont équivalentes.

2. Quand B a cette forme particulière, tout mineur m d'ordre s est somme de produits $e_1...e_s$, où les e_i sont dans l'ensemble $\{d_1, ..., d_r\}$. D'après la propriété de divisibilité des d_i, $e_1...e_s$ est divisible par $d_1...d_s$. Comme d'autre part le mineur principal d'ordre s de B est $d_1...d_s$, on obtient le résultat voulu.

□

Remarque : Il est beaucoup plus difficile de déterminer les classes de *similitude* des matrices de $M_n(A)$. En fait on ne sait le faire que quand A est un corps, car comme on va maintenant le voir, ceci est lié à la classification des modules sur l'anneau $A[X]$, qui n'est pas principal si A n'est pas un corps.

Réduction des endomorphismes d'un K-espace vectoriel de dimension finie.

Soient K un corps, E un K-espace vectoriel de dimension finie n, et u un endomorphisme de E. On cherche à trouver une base dans laquelle la matrice de u a une forme agréable, et plus précisément à déterminer les classes de similitude dans $M_n(K)$. C'est l'objet du théorème principal de cet alinéa. On commence par rappeler une notation :

Définition 3.24 Soit $P = X^d + \sum_{i=0}^{d-1} a_i X^i$ un polynôme unitaire à coefficients dans K. On note $C(P)$ la matrice

$$\begin{pmatrix} 0 & ... & ... & ... & -a_0 \\ 1 & 0 & ... & ... & -a_1 \\ 0 & 1 & 0 & ... & -a_2 \\ ... & ... & ... & ... & ... \\ 0 & ... & ... & 1 & -a_{d-1} \end{pmatrix}$$

qu'on appelle *matrice compagnon* associée à P.

Theorème 3.25 • *Pour tout endomorphisme u d'un K-espace vectoriel de dimension finie E, il existe une base de E dans laquelle la matrice de u est diagonale par blocs, de la forme*

$$\begin{pmatrix} C(P_1) & & & \\ & C(P_2) & & \\ ... & & & \\ & & & C(P_s) \end{pmatrix}$$

où les P_i sont des polynômes unitaires de $K[X]$ de degré au moins 1, vérifiant : $P_1 \mid P_2 \mid ... \mid P_s$.

- *Les P_i sont entièrement déterminés par u; on les appelle les invariants de similitude de u. Deux matrices de $M_n(K)$ sont semblables si et seulement si elles ont les mêmes invariants de similitude.* [16]

- *Soient $B \in M_n(K)$ et $C := XI_n - B$ la matrice caractéristique de B (c'est une matrice de rang n de $M_n(K[X])$). Alors la suite des facteurs invariants de C est $(1, ..., 1, P_1, ..., P_s)$, où $P_1, ..., P_s$ sont les invariants de similitude de B. En particulier ces invariants sont donnés par la formule :*

$$P_1...P_h = m_{h+n-s}(C)$$

pour $h = 1, ..., s$, où $m_i(C)$ désigne le pgcd des mineurs d'ordre i de C dans $K[X]$.[17]

Notons que le polynôme minimal de u est P_s (attention, c'est le "plus grand" P_i, pas le plus petit !) et le polynôme caractéristique de u est $P_1...P_s$. On peut calculer les P_i successivement en commençant par P_s, avec les formules $P_s = m_n(C)/m_{n-1}(C)$, $P_{s-1} = m_{n-1}(C)/m_{n-2}(C)$ etc.

La preuve de ce théorème repose sur la théorie des modules sur l'anneau principal $A := K[X]$. Plus précisément on définit une structure de A-module M sur le K-espace vectoriel E via : $P.v := P(u)(v)$ pour $P \in K[X]$ et $v \in E$. Notons tout de suite que ce A-module est de torsion car si π est un polynôme annulateur [18] de u, on a $\pi.v = 0$ pour tout v de M. Il est d'autre part engendré par toute base du K-espace vectoriel E puisque A contient toutes les constantes de K. Pour identifier les invariants liés à M à ceux de la matrice caractéristique C, on a besoin du lemme suivant :

[16] Bien entendu, les invariants de similitude d'une matrice sont par définition les invariants de l'endomorphisme qu'elle représente dans la base canonique.

[17] Attention au décalage d'indices, dû aux facteurs invariants inversibles de C.

[18] Le théorème de Cayley-Hamilton dit que le polynôme caractéristique de u est annulateur; plus simplement la famille des u^i pour $0 \leq i \leq n^2$ est liée dans $M_n(K)$, d'où l'existence d'un polynôme annulateur non nul.

Lemme 3.26 *Soient $(\varepsilon_1, ..., \varepsilon_n)$ une base fixée de E, $B = (a_{ij})$ la matrice de u dans cette base, et $(e_1, ..., e_n)$ la base canonique du A-module $K[X]^n$. Soit φ l'application A-linéaire (surjective) de $K[X]^n$ dans M qui envoie e_i sur ε_i pour tout $i = 1, ..., n$. Posons $f_j = Xe_j - \sum_{i=1}^n a_{ij}e_i$ pour $j = 1, ..., n$. Alors $(f_1, ..., f_n)$ est une base du A-module* $\ker\varphi$

Démonstration : Déjà $f_j \in \ker\varphi$ vu que $\varphi(f_j) = X.\varepsilon_j - \sum_{i=1}^n a_{ij}\varepsilon_i = u(\varepsilon_j) - \sum_{i=1}^n a_{ij}\varepsilon_i = 0$ par définition de la matrice B.

Montrons que $(f_1, ..., f_n)$ engendre le A-module $\ker\varphi$. Tout élément $\mathbf{Y}$ de $K[X]^n$ s'écrit $\mathbf{Y} = \sum_{j=1}^n \lambda_j e_j$ avec $\lambda_j \in K[X]$. Mais en utilisant l'égalité $f_j = Xe_j - \sum_{i=1}^n a_{ij}e_i$, on peut récrire $\mathbf{Y}$ sous la forme $\mathbf{Y} = \sum_{j=1}^n \mu_j f_j + \sum_{j=1}^n b_j e_j$ avec $\mu_j \in K[X]$ et b_j constante de K. Si $\mathbf{Y}$ est dans $\ker f$, alors $\sum_{j=1}^n b_j e_j$ aussi, d'où $\sum_{j=1}^n b_j\varepsilon_j = 0$ et finalement tous les b_j sont nuls parce que $(\varepsilon_1, ..., \varepsilon_n)$ est une base du K-espace vectoriel E.

Montrons enfin que la famille $(f_1, ..., f_n)$ est libre dans le A-module $\ker\varphi$. Si $\sum_{j=1}^n \lambda_j f_j = 0$ avec $\lambda_j \in A$, alors

$$\sum_{j=1}^n (\lambda_j X)e_j = \sum_{1\leq i,j\leq n} \lambda_j a_{ij} e_i = \sum_{j=1}^n (\sum_{i=1}^n a_{ji}\lambda_i)e_j$$

et comme $(e_1, ..., e_n)$ est une base du A-module $K[X]^n$, on obtient pour tout $j = 1, ..., n$: $X\lambda_j = \sum_{i=1}^n a_{ji}\lambda_i$, ce qui implique que tous les λ_j sont nuls, sinon on obtient une contradiction en prenant j tel que λ_j soit de degré maximal parmi $\lambda_1, ..., \lambda_n$.

□

Preuve du théorème 3.25 : Avec les notations du lemme précédent, soit ψ l'injection canonique de $\ker\varphi$ dans $K[X]^n$. Sa matrice dans les bases $(f_1, ..., f_n)$ et $(e_1, ..., e_n)$ est par définition $C = XI_n - B$, dont le déterminant est non nul (c'est le polynôme caractéristique de u). La suite de ses facteurs invariants est donc de la forme $(1, ..., 1, P_1, ..., P_s)$ avec $P_1 \mid ... \mid P_s$, et on peut prendre les P_i unitaires de degré au moins 1. Comme on l'a vu dans la preuve du théorème 3.22, le A-module $M \simeq (K[X]^n/\ker\varphi)$ est alors isomorphe à $\bigoplus_{i=1}^s (A/P_i.A)$, ou encore $M = \bigoplus_{i=1}^s A.z_i$, où z_i est l'image dans M (via φ) du i-ième vecteur d'une base adaptée à l'inclusion ψ. L'idéal engendré par P_i apparaît alors comme l'annulateur de z_i dans le A-module M.

Soit alors E_i le sous-module $A.z_i$ de M, alors E_i est en particulier un sous-espace vectoriel de E, et il est stable par u; plus précisément c'est le sous-espace vectoriel engendré par les $P(u)(z_i)$ avec $P \in A$. Comme le noyau de l'application K-linéaire $P \mapsto P(u)(z_i)$ est $P_i.A$, ce sous-espace vectoriel

est de dimension $d_i := \deg P_i$, vu que $A/P_i.A$ est un K-espace vectoriel de dimension d_i. Maintenant la famille $\mathcal{B}_i := (z_i, u(z_i), ...u^{d_i-1}(z_i))$, est une base du K-espace vectoriel E_i (elle est de cardinal d_i et libre, toujours parce que l'annulateur de z_i est $P_i.A$). La matrice de la restriction de u à E_i dans $\mathcal{B}_i$ est $C(P_i)$ par définition de $C(P_i)$ et parce que $(P_i(u))(z_i) = 0$, Comme $E = \bigoplus_{i=1}^{s} E_i$ (comme A-module ou comme K-espace vectoriel), on en déduit le premier point en recollant les bases $\mathcal{B}_i$.

Si maintenant u a une matrice de la forme ci-dessus avec des polynômes $(Q_1, ..., Q_{s'})$ dans une autre base, alors il est immédiat que le A-module M est isomorphe à la somme directe des $(A/Q_i.A)$. Le fait que les P_i soient entièrement déterminés par u vient alors du théorème d'unicité 3.19. D'où le deuxième point.

Enfin, on a vu que $(1, ..., 1, P_1, ..., P_s)$ était la suite des facteurs invariants de C. La fin du troisième point résulte alors du lemme 3.23.

□

Remarques : -Dans le cas particulier où le polynôme caractéristique de u est scindé, on retrouve la réduction de Jordan comme la décomposition en composantes p-primaires de M, vu que les facteurs irréductibles de chaque P_i sont de la forme $(X - \lambda)$ avec $\lambda \in K$.

-Le théorème 3.25 permet par exemple de voir immédiatement que si deux matrices de $M_n(K)$ sont semblables sur un surcorps de K, elles sont déjà semblables sur K, résultat qui n'est pas du tout évident (en particulier si K est fini).