Cours d'algèbre à la maîtrise

UQàM MAT7600

Christophe Reutenauer et Franco Saliola
Laboratoire de combinatoire et d'informatique mathématique,
Université du Québec à Montréal

22 septembre 2023

Table des matières

1 Contenu du cours selon l'UQàM **3**

2 Introduction **3**

I Axiome du choix, lemme de Zorn, théorème de Zermelo **3**

3 Axiome du choix **4**
3.1 Motivation : section d'une surjection 4
3.2 Axiome du choix 5
3.3 Application : existence d'une section 5
3.4 Application : existence d'un sous-ensemble non mesurable de $\mathbb{R}$ 5

4 Lemme de Zorn **6**
4.1 Notions sur les ensembles ordonnés 6
4.2 Ensembles inductifs et lemme de Zorn 7
4.3 Application : existence d'une base 7
4.4 Application : existence d'un idéal bilatère maximal 8
4.5 Application : existence d'une injection $X \to Y$ ou $Y \to X$ . . 8

5 Théorème de Zermelo **9**
5.1 Le théorème 9
5.2 Ce théorème implique l'axiome du choix 10

II Catégories **11**

6 Objets et morphismes **11**
6.1 Définition d'une catégorie 11
6.2 Exemples 12
6.3 Isomorphismes et autres 12
6.4 Objets initiaux et finaux 13
6.5 Produits et coproduits 14

7 Foncteurs **15**
7.1 Foncteurs covariants et foncteurs contravariants 15
7.2 Transformation naturelle et isomorphisme naturel 17
7.3 Equivalence de catégories 18

III Modules sur un anneau **20**

8 Modules : généralités **20**
8.1 C'est quoi, un module ? 20
8.2 Exemples 22
8.3 Sous-modules 22
8.4 Homomorphismes 22
8.5 Quotients 23
8.6 Combinaisons linéaires, bases et modules libres 23
8.7 Modules cycliques 25
8.8 Produits et somme directes 25
8.9 Théorèmes d'isomorphisme et de correspondance 25

9 Théorie des modules **26**
9.1 Modules indécomposables 26
9.2 Les conditions de chaînes : modules noetheriens, artiniens . . 27
9.3 Anneaux noetheriens, artiniens 29
9.4 Idempotents de End(M) 30
9.5 Anneaux locaux 30
9.6 Suites de composition 32
9.7 Théorème de Krull-Remak-Schmidt 35

10 Modules semisimples **36**
10.1 Modules semi-simples 36
10.2 Théorème de Wedderburn-Artin 39
10.3 Radical de Jacobson 41
10.4 Radical, artiniaté et semi-simplicité 43

10.5 Théorème de Hopkins-Levitzki 45

11 Modules sur un anneau commutatif principal intègre 45
11.1 Torsion 46
11.2 Mise sous forme diagonale des matrices sur $\mathbb{A}$ 46
11.3 Unicité de la forme diagonale 48
11.4 Sous-modules de $\mathbb{A}^p$ 50
11.5 Structure des $\mathbb{A}$-modules finiment engendrés 52
11.6 Unicité de cette structure 53
11.7 Application 1 : groupes abéliens finiment engendrés 53
11.8 Application 2 : réduction d'un endomorphisme d'un espace vectoriel 54

IV Solution de certains exercices 57

1 Contenu du cours selon l'UQàM

Lemme de Zorn. Catégories et foncteurs : notions et exemples de base : catégories de structures mathématiques, monoïde, catégorie des ensembles ; section, rétraction, exemples géométriques et algébriques. Foncteurs et transformations naturelles : exemples de base, catégories de foncteurs. Équivalence de catégories : exemples de base. Modules. Théorèmes d'homomorphisme et d'isomorphisme. Sommes et produits directs, modules libres. Modules de type fini sur un anneau principal et applications aux formes canoniques des matrices. Modules noethériens et artiniens : exemples et propriétés de base. Modules indécomposables, théorème de Krull-Schmidt. Anneaux et polynômes : nilradical et localisation ; élimination classique, ensembles algébriques, théorème des zéros de Hilbert. Théorie des corps : groupe de Galois, résolution par radicaux ; indépendance algébrique, degré de transcendance, dimension des ensembles algébriques irréductibles ; corps ordonnables, 17ème problème de Hilbert.

2 Introduction

Remerciements : Luc Bélair pour ses notes de cours [1] ; Charles Sénécal pour sa transcription du cours de Franco Saliola à l'automne 2021.

Première partie

Axiome du choix, lemme de Zorn, théorème de Zermelo

Nous allons étudier ces trois résultats fondamentaux, et voir qu'ils sont équivalents. Nous prouverons que le lemme de Zorn implique le théorème de Zermelo 5.1, et que celui-ci implique l'axiome du choix 5.2 ; celui-ci implique le lemme de Zorn, mais nous ne le prouverons pas.

3 Axiome du choix

3.1 Motivation : section d'une surjection

Le résultat suivant de la théorie des ensembles est bien connu (l'exercice 3.1 met ce résultat dans un cadre plus général).

Théorème 3.1. *Si $f : A \to B$ est une fonction surjective, alors il existe une fonction $g : B \to A$ telle que $f \circ g = \mathrm{id}_B$.*

La fonction g s'appelle une *section* de f ; autrement dit, c'est un inverse à droite de f.

Démonstration. Pour tout $b \in B$, il existe a dans A tel que $f(a) = b$. On choisit un tel a, et on pose $g(b) = a$. Ceci définit une fonction $g : B \to A$ et on a $f \circ g(b) = f(a) = b$, donc $f \circ g = \mathrm{id}_B$. □

Dans la démonstration précédente, on a utilisé sans le dire l'axiome du choix : pour tout $b \in B$, on a choisi un élément a dans le sous-ensemble $g^{-1}(b)$ de A (ce sous-ensemble, rappelons-le, est l'ensemble des antécédents de b dans A par la fonction g ; attention à la notation g^{-1}, qui ne signifie pas que g est inversible). Quand B est infini, il y a une infinité de choix à faire, et il n'est pas évident que c'est possible.

Exercice 3.1. *Soit une fonction $f : A \to B$. Démontrer les assertions suivantes.*

(a) f est injective si et seulement s'il existe un fonction $h : B \to A$ telle que $h \circ f = id_A$.

(b) f est surjective si et seulement s'il existe un fonction $g : B \to A$ telle que $f \circ g = id_B$.

(c) Si f est bijective, alors g et h ci-dessus sont uniques, et égales.

(d) Pour (a) et (b), montrer que si f est n'est pas bijective, alors h et g ne sont pas uniques.

Exercice 3.2. *Montrer que dans la preuve du théorème 3.1, on n'a pas besoin de l'axiome du choix lorsque A est fini.*

3.2 Axiome du choix

C'est l'axiome suivant : *soit A un ensemble et $\mathbb{P}^*(A)$ l'ensemble des parties non vides de A. Il existe une fonction $F : \mathbb{P}^*(A) \to A$ telle que pour tout $X \in \mathbb{P}^*(A)$, on a $f(X) \in X$.*

La fonction F s'appelle une *fonction de choix*.

3.3 Application : existence d'une section

Revoyons la preuve du théorème 3.1 en utilisant l'axiome du choix. Nous avons donc une surjection $f : A \to B$. Considérons une fonction de choix $F : \mathbb{P}^*(A) \to A$. Nous définissons alors la fonction $g : B \to A$ par $\forall b \in B, g(b) = F(f^{-1}(b))$. Ceci est bien défini car $f^{-1}(b)$ est non vide et $F(f^{-1}(b)) \in f^{-1}(b) \subset A$. Et on a $f \circ g(b) = f(F(f^{-1}(b)) = b$, car $F(f^{-1}(b)) \in f^{-1}(b)$, par définition d'une fonction de choix.

Donc g est une section de f.

3.4 Application : existence d'un sous-ensemble non mesurable de $\mathbb{R}$

Dans un cours d'intégration, on apprend ce qu'est un sous-ensemble mesurable de $\mathbb{R}$, ainsi que la notion de mesure d'un tel sous-ensemble. Tout ce que nous avons besoin de savoir là-dessus est comme suit :

- La *mesure de Lebesgue* sur $\mathbb{R}$ est une fonction μ qui associe une valeur numérique réelle ≥ 0, à certains sous-ensembles de $\mathbb{R}$, appelés *ensembles mesurables*, et la valeur est appelée leur *mesure*. On note $\mu(X)$ la mesure du sous-ensemble mesurable X.
- Les intervalles $[a, b]$ sont mesurables, de mesure $b - a$.
- On a $\mu(X + a) = \mu(X)$ (invariance de μ sous la translation).
- Si $X \subset Y$ et X, Y mesurables, alors $\mu(X) \leq \mu(Y)$.
- Si les X_n, $n \in \mathbb{N}$, sont mesurables, alors $\bigcup_n X_n$ est mesurable, et on a $\mu(\bigcup_n X_n) = \sum_n (X_n)$ si, de plus, les X_n sont deux à deux disjoints.

Nous construisons maintenant un sous-ensemble V de $[0, 1]$ et montrons qu'il n'est pas mesurable (construction due à Vitali). On considère le sous-groupe additif $\mathbb{Q}$ de $\mathbb{R}$; toute classe C de $\mathbb{R}$ modulo $\mathbb{Q}$ rencontre $[0, 1]$:

en effet, C contient un élément x, donc aussi l'élément ϵ, où l'on a posé $x = \lfloor x \rfloor + \epsilon$ (on dit que ϵ est la *partie fractionnaire* de x). Par l'axiome du choix, on choisit un élément $v \in C \cap [0,1]$, et on note V l'ensemble de ces v quand on considère toutes les classes de $\mathbb{R}$ modulo $\mathbb{Q}$. On a donc

$$\mathbb{R}/\mathbb{Q} = \{v + \mathbb{Q} \mid v \in V\}, V \subset [0,1],$$

et les v dans V son deux à deux non congrus modulo $\mathbb{Q}$.

Supposons par l'absurde que V est mesurable. Posons $A = \bigcup(q+V)$, où la réunion est sur tous les $q \in \mathbb{Q}$ tels que $-1 \leq q \leq 1$. La réunion est disjointe : en effet, si $q+V$ rencontre $q'+V$, alors il existe v, v' dans V tels que $q+v = q'+v'$, donc $v' = v+q-q'$, donc $v+\mathbb{Q} = v'+\mathbb{Q}$ et on en déduit $v = v'$ et $q = q'$, donc enfin $q+V = q'+V$.

Nous avons $[0,1] \subset A \subset [-1,2]$. En effet, si $r \in [0,1]$, alors il existe $v \in V$ tel que $r+\mathbb{Q} = v+\mathbb{Q}$. Donc $r-v \in \mathbb{Q}$ et $r-v \in [-1,1]$ car $v \in [0,1]$. Donc $r \in (r-v)+V \in A$. Ceci prouve la première inclusion. Pour la deuxième, on a $V \subset [0,1]$ et $q \in [-1,1]$, d'où l'on tire $q+V \in [-1,2]$.

Des inclusions ci-dessus, on déduit les inégalités de mesures $\mu([0,1] \leq \mu(\bigcup_q (q+V)) \leq \mu([-1,2])$, d'où $1 \leq \sum_q \mu(V) \leq 3$. Si $\mu(V) = 0$, la somme vaut 0, une contradiction ; si $\mu(V) > 0$, la somme est infinie (tous ses termes valent $\mu(V)$), ce qui est absurde aussi.

4 Lemme de Zorn

4.1 Notions sur les ensembles ordonnés

Définition 4.1. *Soit X un ensemble muni d'un ordre $\leq$.*

- Deux éléments x, y de X sont dits comparables *si $x \leq y$ ou $y \leq x$.*

- Un sous-ensemble Y de X est dit majoré *s'il existe $x \in X$ tel que $\forall y \in Y, y \leq x$.*

- Une chaine *dans X est une partie de X qui est totalement ordonnée par l'ordre induit.*

- Un élément maximal *dans X est un élément x tel que pour tout $y \in X$, si $x \leq y$, alors $y = x$.*

Exercice 4.1. *Dans l'ensemble des parties X d'un ensemble à n éléments, ordonné par inclusion, qulle est la cardinalité maximum des chaines ?*

Exercice 4.2. *Soit X l'ensemble des parties $\neq E$ d'un ensemble E, ordonné par inclusion ; quels sont les éléments maximaux de X ? Même question pour*

l'ensemble des sous-espaces vectoriels propres d'un espace vectoriel V, l'ordre étant l'inclusion ; on peut commencer par le cas où la dimension de V est finie.

4.2 Ensembles inductifs et lemme de Zorn

Définition 4.2. *Un ensemble ordonné est dit* inductif *si toute chaine y est majorée.*

Théorème 4.1. *(Lemme de Zorn) Tout ensemble ordonné inductif non vide possède un élément maximal.*

Le lemme de Zorn se déduit de l'axiome du choix en utilisant la théorie des ordinaux. Nous ne ferons pas ici cette démonstration.

4.3 Application : existence d'une base

Théorème 4.2. *Tout espace vectoriel sur un corps admet une base.*

Prouvons d'abord le joli résultat suivant, mettant en lumière la symétrie entre "linéairement indépendant" et "générateur".

Proposition 4.1. *Soit H une partie d'un espace vectoriel E. Les conditions suivantes sont équivalentes.*

(i) H est une base de E.

(ii) H est maximal dans l'ensemble $\mathcal{L}$ des parties linéairement indépendantes de E, ordonné par inclusion.

(iii) H est minimal dans l'ensemble $\mathcal{G}$ des parties génératrices de E, ordonné par inclusion.

Démonstration. Nous ne prouvons que (ii) $\Rightarrow$ (i), qui est la seule implication utilisée pour prouver le théorème. Soit donc H un élément maximal dans l'ensemble $\mathcal{L}$ des parties linéairement indépendantes de E, ordonné par inclusion. Si $e \in E$, et si e n'était pas combinaison linéaire de H, alors $H \cup e$ serait libre, ce qui contredirait la maximalité de H ; donc H engendre E. Donc H est une base de E. □

Preuve du théorème 4.2. Il suffit de montrer que l'ensemble $\mathcal{L}$ des parties linéairement indépendantes de l'espace vectoriel E, avec l'ordre d'inclusion, est inductif.

Soit donc une partie $\mathcal{J}$ totalement ordonnée de $\mathcal{L}$. Faisons la réunion L de toutes les éléments de $\mathcal{J}$ (ces éléments sont des parties de E !). Montrons que L est une partie linéairement indépendante. Sinon, il existe des vecteurs

distincts $v_1, \ldots, v_n$ dans L et des scalaires non tous nuls tels que $\sum_i a_i v_i = 0$. Chaque v_i est dans L, donc dans un élément L_i de $\mathcal{J}$. Les éléments $L_1, \ldots, L_n$ sont dans $\mathcal{J}$ qui est totalement ordonné ; donc l'un des L_i est plus que tous les autres, c'est-à-dire, les contient. Alors $v_1, \ldots, v_n \in L_i$, ce qui contredit que L_i doit être une partie linéairement indépendante. □

On peut plus généralement démontrer le théorème suivant, qui contient aussi le théorème de la base incomplète.

Théorème 4.3. *Si dans un espace vectoriel, on a une partie linéairement indépendante L et une partie génératrice G telles que $L \subset G$, alors il existe une base B telle que $L \subset B \subset G$.*

La preuve est très similaire, et elle est laissée en exercice 4.4.

Exercice 4.3. *Compléter la preuve de la proposition 4.1.*

Exercice 4.4. *Faire la preuve du théorème 4.3.*

4.4 Application : existence d'un idéal bilatère maximal

Un idéal bilatère *maximal* d'un anneau est un idéal bilatère propre qui n'est contenu strictement dans aucun idéal bilatère propre.

Théorème 4.4. *Tout anneau unitaire possède un idéal bilatère maximal.*

Démonstration. Soit A cet anneau. On considère l'ensemble des idéaux propres de A, ordonné par inclusion. C'est un ensemble inductif : toute chaine est majorée par la réunion de ses éléments ; cette réunion, notée J, est en effet un idéal ; J est propre, car sinon 1 est dans J, donc dans un des élément de la chaine, lequel ne serait pas propre. □

Exercice 4.5. *Montrer que tout idéal (à gauche, à droite, bilatère) propre est contenu dans un idéal (idem) maximal (adapter la preuve du théorème).*

4.5 Application : existence d'une injection $X \to Y$ ou $Y \to X$

Théorème 4.5. *Etant donnés deux ensembles X, Y, il existe une injection de X dans Y, ou une injection de Y dans X.*

Démonstration. Appelons *bijection partielle* $X \to Y$ une bijection f d'une partie de X, $Dom(f)$ (le domaine de f), vers Y. Si f, g sont deux bijections partielles $X \to Y$, nous écrivons $f \leq g$ si $f = g \mid Dom(f)$. On obtient ainsi une relation d'ordre sur l'ensemble F des bijections partielles $X \to Y$. Si $f \in F$, on note f^{-1} la bijection partielle $Y \to X$ définie de manière évidente.

Montrons d'abord que si f est un élément maximal pour cet ordre, alors f est une injection $X \to Y$ ou bien f^{-1} est une injection $Y \to X$. En effet, sinon, $Dom(f) \neq X$ et $Dom(f^{-1}) \neq Y$. Il existe donc $x \in X \setminus Dom(f)$ et $y \in Y \setminus Dom(f^{-1}) = \mathrm{Im}(f)$; alors la fonction partielle $g : X \to Y$, qui étend f par la condition $g(x) = y$, satisfait $f < g$: f ne serait pas maximale.

Montrons que F est un ensemble ordonné inductif. En effet, soit C une chaine C dans F. On définit une fonction partielle h de X vers Y, dont le domaine est la réunion $D = Dom(h)$ des domaines des $f \in C$; h est définie par la condition : si $x \in D$, soit $f \in C$ tel que $x \in Dom(f)$, alors $h(a) = f(a)$. Ceci définit correctement h, à cause de la condition de chaine. Il est clair que h est une bijection partielle, et qu'elle majore C.

On peut alors appliquer le lemme de Zorn et obtenir un élément maximal, ce qui conclut la preuve. □

Le résultat précédent est intéressant pour la théorie de la cardinalité. Il assure que deux ensembles ont toujours des cardinalités comparables : on dit en effet que la cardinalité d'un ensemble X est $\leq$ à la cardinalité d'un ensemble Y s'il existe une injection de X vers Y. On démontre de plus que cette relation sur les cardinalités est anti-symétrique : s'il existe une injection dans chaque sens, il existe aussi une bijection ; les cardinalités sont *égales*. De plus, on montre que l'existence d'une injection $X \to Y$ est équivalente à celle d'une surjection $Y \to X$ (c'est essentiellement dans l'exercice 3.1).

5 Théorème de Zermelo

5.1 Le théorème

Un ordre sur un ensemble X est appelé un *bon ordre* si toute partie non vide de X a un minimum (plus petit élément). L'exemple classique est $\mathbb{N}$ avec l'ordre naturel, alors que $\mathbb{Z}$ n'est pas bien ordonné par l'ordre naturel.

Théorème 5.1. *Tout ensemble admet un bon ordre.*

Appelons *idéal inférieur* d'un ensemble ordonné E tout sous-ensemble I de E tel que

$$\forall x, y \in E, y \in F, x \leq y \Rightarrow x \in F.$$

Lemme 5.1. *Si $I \subset J$ sont des idéaux inférieurs de l'ensemble ordonné E, si Z est une partie de E tels que* $\min(Z \cap I), \min(Z \cap J)$ *existent, alors* $\min(Z \cap I) = \min(Z \cap J)$.

Démonstration. Comme $I \subset J$, on a $I \cap Z \subset J \cap Z$, donc

$$\min(Z \cap I) \geq \min(Z \cap J).$$

Dans cette inégalité, l'élément de gauche est dans I, qui est un idéal inférieur ; donc l'élément de droite est aussi dans I, et il est aussi dans Z, donc il est dans $Z \cap I$, et l'inégalité ne peut être stricte. □

Lemme 5.2. *Soit $F = E \cup a$ avec $a \notin E$. On suppose que E est ordonné. Alors on peut étendre l'ordre de E à F en décidant que a est le plus grand élément de F.*

Preuve du théorème 5.1. Soit X un ensemble non vide et considérons $F = \{(Y, \leq) : Y \subset X, (Y, \leq) \text{ est un bon ordre}\}$. On vérifie que la relation suivante définit un ordre partiel sur F : $(Y_1, \leq_{Y_1}) \leq (Y_2, \leq_{Y_2})$ si $(Y_1, \leq_{Y_1})$ est un idéal inférieur de $(Y_2, \leq_{Y_2})$.

Alors F est non vide, puisqu'il contient $\emptyset$. De plus F est un ensemble inductif. En effet, soit C une chaîne dans F. On définit Z comme la réunion des Y, pour $(Y, \leq_Y) \in C$. On définit un ordre sur Z, qui coïncide avec celui de Y, pour tout $(Y, \leq_Y) \in C$; ceci est bien défini, car pour $(Y_1 \leq_{Y_1})$, $(Y_2, \leq_{Y_2}) \in C$, l'un des Y_i est contenu dans l'autre, et l'ordre du plus petit est la restriction de l'ordre du plus grand.

Montrons que Z est bien ordonné. On considère un sous-ensemble T non vide de Z. Alors, si pour $(Y, \leq_Y) \in C$, $T \cap Y$ est non vide, on définit $a_Y = \min(T \cap Y)$, qui existe car Y est bien ordonné. Le lemme 5.1 implique que a_Y ne dépend pas de Y. C'est donc le minimum de T.

Ainsi on peut appliquer le lemme de Zorn et obtenir un élément maximal de F, disons $(Y_0, \leq_0)$. Alors on doit avoir $Y_0 = X$, sinon soit $a \in X \setminus Y_0$, et alors on obtient un bon ordre sur $Y_0 \cup a$, en prenant a comme maximum de cet ensemble (lemme 5.2 ; alors Y_0 en est un idéal inférieur, ce qui contredit la maximalité. Ainsi $Y_0 = X$ et $\leq_0$ est le bon ordre cherché. □

5.2 Ce théorème implique l'axiome du choix

On peut déduire l'axiome du choix du théorème de Zermelo. En effet, si on a un ensemble non vide X, et un bon ordre $\leq$ sur X (dont l'existence nous est assurée par le théorème de Zermelo), on peut définir la fonction

$f : \mathbb{P}^*(X) \to X, f(Y) = \min(Y)$, qui est une fonction de choix, puisque $f(Y) \in Y$.

Deuxième partie
Catégories

Dans ce qui suit, on utilise le mot *classe* pour désigner une "collection d'objets". On parle par exemple de la classe de tous les ensembles ; on ne peut pas parler de "l'ensemble de tous les ensembles", car cela conduit à des contradictions.

6 Objets et morphismes

6.1 Définition d'une catégorie

Une *catégorie* $\mathcal{C}$ est définie par la donnée

- d'une classe $Obj(\mathcal{C})$, appelée classe des *objets* de $\mathcal{C}$;

- pour chaque paire d'objets (A, B) dans $\mathcal{C}$, d'une classe $Hom_{\mathcal{C}}(A, B)$, appelée classe des *morphismes de A vers B* ;

- d'une opération sur les morphismes appelée *composition*, qui pour chaque triplet d'objets (A, B, C) de $\mathcal{C}$, et tous morphismes $f \in Hom_{\mathcal{C}}(A, B)$ et $g \in Hom_{\mathcal{C}}(B, C)$ associe un morphisme noté $g \circ f$ dans $Hom_{\mathcal{C}}(A, C)$.

On a de plus les propriété suivantes :

(a) si $(A, B) \neq (A', B')$, alors $Hom_{\mathcal{C}}(A, B) \cap Hom_{\mathcal{C}}(A', B')$ est vide ;

(b) pour chaque objet A, il existe id_A, appelé le *morphisme identité*, dans $Hom_{\mathcal{C}}(A, A)$ tel que : pour tous objets B, C et pour tous $f \in Hom_{\mathcal{C}}(A, B)$ et $g \in Hom_{\mathcal{C}}(C, A)$, $f \circ \mathrm{id}_A = f$ et $\mathrm{id}_A \circ g = g$;

(c) $h \circ (g \circ f) = (h \circ g) \circ f$.

Pour signifier que $f \in Hom_{\mathcal{C}}(A, B)$, on écrit $f : A \to B$ ou $A \xrightarrow{f} B$. On abrège souvent aussi $g \circ f$ en gf.

Exercice 6.1. *Montrer que* id_A *est unique.*

Exercice 6.2. *La catégorie duale $\mathcal{C}^*$, avec les mêmes objets que $\mathcal{C}$, est obtenue en inversant les flèches : $f^* : A \to B$ est un morphisme dans $\mathcal{C}$ si et seulement si $f : B \to A$ est un morphisme dans $\mathcal{C}$. Montrer que c'est une catégorie.*

6.2 Exemples

Dans tous les exemples de catégories qui suivent, les morphismes sont des fonctions, et la composition des morphismes est la composition des fonctions.

- La catégorie Ens, dont les objets sont les ensembles, et les morphismes sont les applications.

- La catégorie Mon, dont les objets sont les monoïdes, et les morphismes les homomorphismes de monoïdes.

- La catégorie Gr, dont les objets sont les groupes, et les morphismes les homomorphismes de groupes.

- La catégorie Ab, dont les objets sont les groupes abéliens, et les morphismes les homomorphismes de groupe.

- La catégorie Ann_1, dont les objets sont les anneaux unitaires, et les morphismes les homomorphismes d'anneaux unitaires.

- La catégorie $Ev_{\mathbb{K}}$, dont les objets sont les K-espaces vectoriels, et les morphismes les applications $\mathbb{K}$-linéaires.

- La catégorie Top, dont les objets sont les espaces topologiques, et les morphismes les fonctions continues.

Dans tous ces exemples de catégories, les objets sont des ensembles. Voyons un exemple où ça n'est pas le cas. C'est la catégorie, notée $Mat_{\mathbb{K}}$, dont les objets sont les entiers naturels (donc $Obj(Mat_{\mathbb{K}}) = \mathbb{N}$), et telle que $Hom_{Mat_{\mathbb{K}}}(i, j)$ est l'ensemble des matrices de taille $j \times i$ sur $\mathbb{K}$. La composition est le produit des matrices, et le morphisme identité $i \to i$ est la matrice identité d'ordre i.

Dans tous ces exemples de catégories, $Hom_{\mathcal{C}}(A, B)$ est un ensemble. Une telle catégorie est dite *localement petite*.

Exercice 6.3. *Montrer que si A un objet dans une catégorie localement petite, alors $Hom_{\mathcal{C}}(A, A)$ est un monoïde.*

6.3 Isomorphismes et autres

Définition 6.1. *Soit $f \in Hom_{\mathcal{C}}(A, B)$. On dit que f est un isomorphisme s'il existe $g \in Hom_{\mathcal{C}}(B, A)$ tel que $g \circ f = \mathrm{id}_A$ et $f \circ g = \mathrm{id}_B$.*

Définition 6.2. *Un morphisme f dans une catégorie est dit* simplifiable à gauche *(resp.* à droite*) si pour tous morphismes g, h tels que $f \circ g = f \circ h$ (resp. $g \circ f = h \circ f$), on $g = h$.*

Un morphisme simplifiable à droite est appelé un épimorphisme*, et un morphisme simplifiable à gauche est appelé un* monomorphisme*.*

Un isomorphisme est simplifiable à gauche et à droite. La réciproque n'est pas vraie en générale (exercice 6.9).

Exercice 6.4. *Montrer que si A un objet dans une catégorie localement petite, alors l'ensemble des isomorphismes dans $Hom_{\mathcal{C}}(A, A)$ est un groupe.*

Exercice 6.5. *Montrer que dans les catégories Ens, Mon, Gr, Ab, Ann_1, $Ev_{\mathbb{K}}$, un morphisme est un isomorphisme si et seulement si c'est une application bijective. Montrer par un exemple que ce n'est pas le cas pour la catégorie Top.*

Exercice 6.6. *Montrer que dans la catégorie $Mat_{\mathbb{K}}$, les isomorphismes sont les matrices inversibles.*

Exercice 6.7. *Montrer que dans les catégories Ens et $Ev_{\mathbb{K}}$, un morphisme est un épimorphisme (resp. monomorphisme) si et seulement si c'est une application surjective (resp. injective).*

Exercice 6.8. *Montrer que dans la catégorie Ann_1, l'homomorphisme d'anneaux $\mathbb{Z} \to \mathbb{Q}$ qui envoie 1 sur 1, est un épimorphisme, mais n'est pas une application surjective.*

Exercice 6.9. *Dans la catégorie Top, montrer qu'un morphisme $f : X \to Y$ est un épimorphisme (resp. un monomorphisme) si et seulement si $f(X)$ est dense dans Y (resp. f est injective). Donner un exemple de morphisme qui est un épimorphisme et un monomorphisme sans être un isomorphisme.*

6.4 Objets initiaux et finaux

Définition 6.3. *Dans une catégorie, un objet A est dit* final *(resp.* initial*), si pour tout objet X, il existe un unique morphisme $X \to A$ (resp. $A \to X$).*

Proposition 6.1. *Un objet final (resp. initial) est unique à isomorphisme près.*

Qu'un objet final est "unique à isomorphisme près" signifie que si deux objets sont finaux, alors il existe un isomorphisme de l'un vers l'autre.

Démonstration. Soit A un objet final. Par hypothèse, il existe un unique morphisme $A \to A$, qui est donc forcément id_A. Si B est un autre objet final, il existe par hypothèse un morphisme $f : B \to A$ and un morphisme $g : A \to B$. Alors $f \circ g$ est un morphisme $A \to A$, et on a donc $f \circ g = \mathrm{id}_A$; symétriquement, $g \circ f = \mathrm{id}_B$. Donc f, g sont des isomorphismes. □

Application : propriété universelle

Les "propriétés universelles" apparaissent souvent en algèbre. Nous en donnons un exemple. La propriété universelle du quotient d'un groupe abélien se formule comme suit : *si H est un sous-groupe d'un groupe abélien G, et si on note $\pi : G \to G/H$ l'homomorphisme canonique, alors pour tout homomorphisme $f : G \to G'$ tel que $H \subset \mathrm{Ker}(f)$, il existe un unique homomorphisme $\bar{f} : G/H \to G'$ tel que $f = \bar{f} \circ \pi$.*

Voyons que cette propriété s'exprime de manière équivalente en disant qu'un certain objet est initial dans une certaine catégorie. La catégorie en question est la classe des paires (G', f) où G' est un groupe abélien et $f : G \to G'$ un homomorphisme dont le noyau contient H. Si (G', f') et (G'', f'') sont deux objets dans cette catégorie, un morphisme $(G', f') \to (G'', f'')$ est un homomorphisme $g : G' \to G''$ tel que $f'' = g \circ f'$. Ainsi, dire que (X, φ) est un objet initial dans cette catégorie (et en particulier $\varphi : G \to X$), c'est dire que pour tout groupe abélien G' et tout homomorphisme $f : G \to G'$ dont le noyau contient H, il existe un unique homomorphisme $g : X \to G'$ tel que $f = g \circ \varphi$; c'est bien la propriété universelle ci-dessus, avec $X = G/H$, $\varphi = \pi$.

Exercice 6.10. *Montrer qu'un objet est final dans la catégorie $\mathcal{C}$ si et seulement si c'est un objet initial dans la catégorie duale $\mathcal{C}^*$. Voir l'exercice 6.2.*

Exercice 6.11. *Enoncer la propriété universelle des quotients dans les catégories Ens, Mon, Gr, $Ev_{\mathbb{K}}$, Ann_1.*

6.5 Produits et coproduits

Définition 6.4. *Le* produit *de deux objets A et B dans une catégorie est la donnée d'un objet noté $C = A \sqcap B$ et de morphismes $p : C \to A$ et $q : C \to B$, tels que pour tout objet X et tous morphismes $f : X \to A$ et $g : X \to B$, il existe un unique morphisme $\theta : X \to C$ tel que $f = p\theta$ et $g = q\theta$.*

Le produit existe dans les catégories usuelles (voir exercice 6.12), mais n'existe pas dans n'importe quelle catégorie. S'il existe, c'est un objet final dans une certaine catégorie, voir exercice 6.13. On peut en déduire que le produit est unique à isomorphisme près.

Définition 6.5. *Le* coproduit *de deux objets A et B dans une catégorie est la donnée d'un objet noté $C = A \sqcup B$ et de morphismes $\alpha : A \to C$ et $\beta : B \to C$, tels que pour tout objet X et tous morphismes $f : A \to X$ et*

$g : B \to X$, il existe un unique morphisme $\theta : C \to X$ tel que $f = \theta\alpha$ et $g = \theta\beta$.

Exercice 6.12. *Montrer que dans les catégories Ens, Mon, Gr, Ab, Ann_1, $Ev_{\mathbb{K}}$, Top, le produit de deux objets A et B est le produit cartésien $A \times B$.*

Exercice 6.13. *Soit $\mathcal{C}$ une catégorie, et deux objets A, B dans $\mathcal{C}$. On construit la catégorie $\mathcal{C}_{A,B}$ dont les objets sont les triplets (Z, f, g), où Z est un objet dans $\mathcal{C}$ et $f : Z \to A$ et $g : Z :\to B$; un morphisme $(Z_1, f_1, g_1,) \to (Z_2, f_2, g_2)$ est un morphisme σ dans $\mathcal{C}$ tel que $f_1 = f_2\sigma$ et $g_1 = g_2\sigma$; vérifier que c'est bien une catégorie. Montrer que le produit de A et B dans $\mathcal{C}$ existe si et seulement si $\mathcal{C}_{A,B}$ a un objet final, auquel s'identifie alors ce produit.*

Exercice 6.14. *Montrer que le coproduit de A et B dans Ens est la réunion disjointe de A et B. Montrer que le coproduit de A et B, dans Ab et $Ev_{\mathbb{K}}$, est $A \times B$.*

Exercice 6.15. *Montrer que le coproduit s'interprète comme un objet initial dans la catégorie appropriée. Indication : inverser les flèches dans l'exercice 6.13.*

7 Foncteurs

7.1 Foncteurs covariants et foncteurs contravariants

De manière informelle, un foncteur est un "morphisme " entre deux catégories.

Définition 7.1. *Soient $\mathcal{C}$ et $\mathcal{D}$ deux catégories. Un* foncteur *$F : \mathcal{C} \to \mathcal{D}$ est une association d'un objet de $\mathcal{D}$ noté $F(A)$ à tout objet A de $\mathcal{C}$, et d'un morphisme $F(f) : F(A) \to F(B)$ dans $\mathcal{D}$ à tout morphisme $f : A \to B$ dans $\mathcal{C}$, de telle manière que F respecte la composition ($F(gf) = F(g)F(f)$) et préserve les identités ($F(\mathrm{id}_A) = \mathrm{id}_{F(A)}$).*

Un exemple général : le *foncteur oubli* de n'importe laquelle des catégories *Mon*, *Gr*, *Ab*, Ann_1, $Ev_{\mathbb{K}}$, *Top*, vers *Ens* ; il envoie tout objet sur l'ensemble sous-jacent, et tout morphisme sur l'application ensembliste correspondante.

Un foncteur est souvent appelé *foncteur covariant*, par opposition aux foncteurs contravariants que nous définissons ci-dessous.

Définition 7.2. *Soient $\mathcal{C}$ et $\mathcal{D}$ deux catégories. Un* foncteur contravariant *$T : \mathcal{C} \to \mathcal{D}$ est une association d'un objet de $\mathcal{D}$ noté $T(A)$ à tout objet A de $\mathcal{C}$, et d'un morphisme $T(f) : T(B) \to T(A)$ dans $\mathcal{D}$ à tout morphisme $f : A \to B$ dans $\mathbb{C}$, de telle manière que F renverse la composition ($T(gf) = T(f)T(g)$) et préserve les identités ($T(\mathrm{id}_A) = \mathrm{id}_{T(A)}$).*

Un exemple est le foncteur $V \to V^*$ (dual de V) ; c'est un foncteur contravariant de $Vect_{\mathbb{K}}$ dans elle-même, qui envoie le morphisme (application linéaire) $f : V \to W$ sur le morphisme transposé $f^* : W^* \to V^*$. En effet, si l'on a une autre application linéaire $g : W \to X$, alors $(gf)^* = f^*g^*$.

Exercice 7.1. *Définir des foncteurs oublis $Gr \to Mon$, $Ann_1 \to Ab$, $Ann_1 \to Mon$, $Ev_{\mathbb{K}} \to Ab$. Définir un foncteur $Ab \to Gr$.*

Exercice 7.2. *Montrer que $A \to \mathcal{P}(A)$ définit deux foncteurs de la catégorie Ens dans elle-même ; l'un est covariant (un morphisme f agit sur l'enseble des parties par image directe), l'autre est contravariant (un morphisme f agit sur l'enseble des parties par image réciproque).*

Exercice 7.3. *Le* sous-groupe dérivé *G' d'un groupe G est le sous-groupe engendré par les* commutateurs*, c'est-à-dire par les éléments de la forme $aba^{-1}b^{-1}$. Montrer que G' est un sous-groupe normal, et que G/G' est un groupe abélien. Montrer que $G \to G/G'$ définit un foncteur $Ab \to Gr$.*

Exercice 7.4. *Soit $\mathcal{C}$ une catégorie localement petite et A un objet fixé dans cette catégorie. On pose $F(X) = Hom(X, A)$. De plus, pour tout morphisme $f : X \to Y$ dans $\mathcal{C}$, on note $F(f)$ l'application $Hom(X, A) \to Hom(Y, A), h \mapsto f \circ h$. Montrer qu'on obtient ainsi on obtient un foncteur de $\mathcal{C}$ vers la catégorie Ens.*

Exercice 7.5. *Soit $\mathcal{C}$ une catégorie localement petite et A un objet fixé dans cette catégorie. On pose $T(X) = Hom(A, X)$. De plus, pour tout morphisme $f : X \to Y$ dans $\mathcal{C}$, on note $T(f)$ l'application $Hom(A, Y) \to Hom(A, X), h \mapsto h \circ f$. Montrer qu'on obtient ainsi on obtient un foncteur contravariant de $\mathcal{C}$ vers la catégorie Ens. Revisiter ainsi l'exemple du foncteur $V \to V^*$ de $Vect_{\mathbb{K}}$.*

Exercice 7.6. *Montrer l'application $V \to V^{**}$, $f \to f^{**}$ définit un foncteur de $Vect_{\mathbb{K}}$ dans elle-même. Indications : composer le foncteur contravariant de l'exemple ci-dessus avec lui-même.*

7.2 Transformation naturelle et isomorphisme naturel

De manière informelle, une transformation naturelle est un "morphisme" entre deux foncteurs.

Définition 7.3. *Soient $\mathcal{C}, \mathcal{D}$ deux catégories et $F, G : \mathcal{C} \to D$ deux foncteurs covariants (resp. contravariants). Une* transformation naturelle *τ de F vers G associe à tout objet X de $\mathcal{C}$ un morphisme $\tau_X : F(X) \to G(X)$ dans la catégorie $\mathcal{D}$, tel que pour tout morphisme $f : X \to Y$ dans $\mathcal{C}$, on a $\tau_Y \circ F(f) = G(f) \circ \tau_X$ (resp. $\tau_X \circ F(f) = G(f) \circ \tau_Y$).*

Une transformation naturelle est un isomorphisme naturel si chaque τ_X est un isomorphisme dans la catégorie $\mathcal{D}$.

Un exemple : considérons $\mathcal{C} = \mathcal{D} = Vect_K$, $F = \mathrm{id}$ (le foncteur identité) et $G(V) = V^{**}$ le foncteur "bidual". Nous montrons qu'il y a une transformation naturelle τ de F vers G. La fonction τ_X (où X est donc un espace vectoriel) $F(X) = X \to X^{**} = G(X)$ est la fonction définie par $\tau_X(x)(\varphi) = \varphi(x)$ pour tout $x \in X$ et tout $\varphi \in X^*$; on a donc bien $\tau_X(x) \in X^{**}$, et τ_X est linéaire, donc τ_X est un morphisme de $Vect_{\mathbb{K}}$. Si $f : X \to Y$ est un morphisme dans $Vect_{\mathbb{K}}$, alors $\tau_Y F(f) = G(f)\tau_X$; en effet, ceci s'écrit $\tau_Y f = f^{**}\tau_X$, ce qu'on vérifie en appliquant les deux côtés à $x \in X$: à gauche, ça donne la fonction $\tau_Y(f(x))$ et à droite la fonction $f^{**}\tau_X(x) = f^{**}(\tau_X(x)) = \tau_X(x) \circ f^*$; pour vérifier que $\tau_Y(f(x)) = \tau_X(x) \circ f^*$, on applique les deux côtés à $\varphi \in Y^*$; à gauche on obtient $\tau_Y(f(x))(\varphi) = \varphi(f(x))$, et à droite $\tau_X(x)(f^*(\varphi)) = \tau_X(x)(\varphi \circ f)) = \varphi \circ f(x)$, ce qui est bien la même chose.

La construction précédente s'applique aussi à la catégorie des espaces vectoriels de dimension finie ; alors τ est un isomorphisme naturel, car τ_X est un isomorphisme, puisque V et V^{**} ont la même dimension et que τ_X est injectif.

Exercice 7.7. *Soit le foncteur F de Ens dans elle-même considéré dans l'exercice 7.2 (version contravariante). Soit G le foncteur de Ens dans elle même qui envoie tout ensemble A sur l'ensemble des fonctions $A \to \{0, 1\}$, et tel que pour tout morphisme $f : A \to B$, $G(f)(G(B)) = \{u \circ f, u \in G(A)\}$; vérifier que G est un foncteur contravariant. Montrer que F et G sont naturellement isomorphes. Indication : τ_X envoie toute partie de X sur sa fonction caractéristique.*

7.3 Equivalence de catégories

Définition 7.4. *Un foncteur $F : \mathcal{C} \to \mathcal{D}$ est une* équivalence de catégories *s'il existe un foncteur $G : \mathcal{D} \to \mathcal{C}$ tel que $G \circ F$ est naturellement isomorphe à $\mathrm{id}_{\mathcal{C}}$ et que $F \circ G$ est naturellement isomorphe à $\mathrm{id}_{\mathcal{D}}$.*

Proposition 7.1. *Un foncteur $F : \mathcal{C} \to \mathcal{D}$ est une* équivalence de catégories *si et seulement si on a les deux conditions suivantes :*

(i) Pour tout objet X de $\mathcal{D}$, il existe un objet A de $\mathcal{C}$ tel que $F(A)$ soit isomorphe à X dans la catégorie $\mathcal{D}$ (F est essentiellement surjectif*).*

(ii) Pour tous objets A, B dans $\mathcal{C}$, le foncteur F induit une bijection de $Hom_{\mathcal{C}}(A, B)$ vers $Hom_{\mathcal{D}}(F(A), F(B))$ (F est pleinement fidèle*).*

Démonstration. ($\Rightarrow$) Supposons que $F : \mathcal{C} \to \mathcal{D}$ soit une équivalence de catégories. Par la définition 7.4, il existe un foncteur $G : \mathcal{D} \to \mathcal{C}$ tel que $G \circ F$ et $F \circ G$ sont naturellement isomorphes à $\mathrm{id}_{\mathcal{C}}$ et $\mathrm{id}_{\mathcal{D}}$, respectivement.

Comme $F \circ G$ est naturellement isomorphe à $\mathrm{id}_{\mathcal{D}}$, pour tout objet X dans $\mathcal{D}$ il existe un isomorphisme $\kappa_X : FG(X) \to \mathrm{id}_{\mathcal{D}}(X)$ dans $\mathcal{D}$ de sorte que pour tout morphisme $g : X \to Y$ dans $\mathcal{D}$ on a

$$\kappa_Y \circ FG(g) = \mathrm{id}_{\mathcal{D}}(g) \circ \kappa_X = g \circ \kappa_X. \tag{1}$$

De même, pour tout $A \in Obj(\mathcal{C})$ il existe un isomorphisme $\tau_A : GF(A) \to A$ dans $\mathcal{C}$ de sorte que pour tout morphisme $f : A \to B$ dans $\mathcal{C}$ on a

$$\tau_B \circ GF(f) = \mathrm{id}_{\mathcal{C}}(f) \circ \tau_A = f \circ \tau_A. \tag{2}$$

(i) Soit X un objet de $\mathcal{D}$. Posons $A = G(X)$. Alors, A est un object de $\mathcal{C}$ et κ_X est un isomorphisme entre $F(A) = F(G(X))$ et $\mathrm{id}_{\mathcal{D}}(X) = X$.

(ii) Injectivité. Montrons d'abord que $f \mapsto F(f)$ est une injection de $\mathrm{Hom}_{\mathcal{C}}(A, B)$ dans $\mathrm{Hom}_{\mathcal{D}}(F(A), F(B))$. Soient $f_1, f_2 \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ tels que $F(f_1) = F(f_2)$. Par (2), on a $\tau_B \circ (GF)(f_1) = f_1 \circ \tau_A$ et $\tau_B \circ (GF)(f_2) = f_2 \circ \tau_A$. On en déduit que $f_1 \circ \tau_A = f_2 \circ \tau_A$, et donc $f_1 = f_2$ puisque τ_A est un isomorphisme. D'où, la fonction $f \mapsto F(f)$ est injective.

De la même façon, on en déduit que la fonction $g \mapsto G(g)$ est une injection de $\mathrm{Hom}_{\mathcal{D}}(X, Y)$ dans $\mathrm{Hom}_{\mathcal{C}}(G(X), G(Y))$.

Surjectivité. Montrons maintenant que la fonction $f \mapsto F(f)$ est surjective. Soit $h \in \mathrm{Hom}_{\mathcal{D}}(F(A), F(B))$. Alors, $G(h) \in \mathrm{Hom}_{\mathcal{C}}(GF(A), GF(B))$, d'où $\tau_B \circ G(h) \circ \tau_A^{-1} \in \mathrm{Hom}_{\mathcal{C}}(A, B)$. Nous montrons que $GF(\tau_B \circ G(h) \circ \tau_A^{-1}) = G(h)$, ce qui implique $F(\tau_B \circ G(h) \circ \tau_A^{-1}) = h$ par l'injectivité de $g \mapsto G(g)$.

En prenant $f = G(h) : GF(A) \to GF(B)$ dans (2), on obtient $\tau_{GF(B)} \circ GFG(h) = G(h) \circ \tau_{GF(A)}$. En prenant $f = \tau_A : GF(A) \to A$ dans (2), on

obtient $\tau_A \circ GF(\tau_A) = \tau_A \circ \tau_{GF(A)}$, ce qui implique que $GF(\tau_A) = \tau_{GF(A)}$ pour tout objet A dans $\mathcal{C}$. D'où,

$$\begin{aligned} GF(\tau_B \circ G(h) \circ \tau_A^{-1}) &= GF(\tau_B) \circ GFG(h) \circ GF(\tau_A)^{-1} \\ &= \tau_{GF(B)} \circ GFG(h) \circ (\tau_{GF(A)})^{-1} \\ &= G(h) \circ \tau_{GF(A)} \circ (\tau_{GF(A)})^{-1} = G(h). \end{aligned}$$

($\Leftarrow$) Réciproquement, supposons que $F : \mathcal{C} \to \mathcal{D}$ satisfasse les hypothèses de l'énoncé ; on a donc :

(H1) Pour tout objet $X \in \mathcal{D}$, il existe un objet A_X dans $\mathcal{C}$ et un isomorphisme $\xi_X : X \to F(A_X)$ dans $\mathcal{D}$.

(H2) Pour toute paire d'objets A, B dans $\mathcal{C}$, la fonction $f \mapsto F(f)$ est une bijection de $\mathrm{Hom}_{\mathcal{C}}(A, B)$ dans $\mathrm{Hom}_{\mathcal{D}}(F(A), F(B))$.

Nous construisons un foncteur inverse $G : \mathcal{D} \to \mathcal{C}$ de F.

Définition du foncteur inverse. Par (H1) et l'axiome du choix, on fixe pour chaque objet X dans $\mathcal{D}$, un objet A_X dans $\mathcal{C}$ ainsi qu'un isomorphisme

$$\xi_X : X \to F(A_X).$$

On définit G sur les objets X et les morphismes $g : X \to Y$ dans $\mathcal{D}$ par

$$G(X) = A_X \qquad \text{et} \qquad G(g) = F^{-1}\Big(\xi_{X_2} \circ g \circ \xi_{X_1}^{-1}\Big), \tag{3}$$

où F^{-1} est une abréviation pour l'inverse de la fonction $f \mapsto F(f)$. Notons que $G(g)$ est un morphisme dans $\mathcal{C}$ de $G(X) = A_X$ vers $G(Y) = A_Y$, car

$$F(A_X) \xrightarrow{\xi_X^{-1}} X \xrightarrow{g} Y \xrightarrow{\xi_Y} F(A_Y) \ \in \ \mathrm{Hom}_{\mathcal{D}}(F(A_X), F(A_Y)),$$

et tout morphisme dans $\mathrm{Hom}_{\mathcal{D}}(F(A_X), F(A_Y))$ correspond par la fonction $f \mapsto F(f)$ à un unique morphisme dans $\mathrm{Hom}_{\mathcal{C}}(A_X, A_Y)$.

$*$ *La vérification que G est bien un foncteur est Exercice 7.10.*

Isomorphisme naturel de $\mathrm{id}_{\mathcal{D}}$ *vers* $F \circ G$. Nous montrons que la famille d'isomorphismes $\xi_X : X \to F(G(X))$ est un isomorphisme naturel de $\mathrm{id}_{\mathcal{D}}$ vers $F \circ G$. Soit $g : X \to Y$ est un morphisme dans $\mathcal{D}$. Alors,

$$(F \circ G)(g) \circ \xi_X = F\big(F^{-1}(\xi_Y \circ g \circ \xi_X^{-1})\big) \circ \xi_X = \xi_Y \circ g.$$

Isomorphisme naturel τ *de* $\mathrm{id}_{\mathcal{C}}$ *vers* $G \circ F$. Pour tout objet A dans $\mathcal{C}$, on a l'isomorphisme $\xi_{F(A)} : F(A) \to F(G(F(A)))$, ce qui correspond à un unique isomorphisme de A dans $G(F(A))$ par (H2). On définit alors

$$\tau_A = F^{-1}\big(\xi_{F(A)}\big) : A \to G(F(A)).$$

Nous montrons que τ est un isomorphisme naturel de $\mathrm{id}_{\mathcal{C}}$ vers $G \circ F$. Soit $f : A \to B$ un morphisme dans $\mathcal{C}$. Comme F^{-1} respecte la composition,

$$\begin{aligned}(G \circ F)(f) \circ \tau_A &= F^{-1}(\xi_{F(B)} \circ F(f) \circ \xi_{F(A)}^{-1}) \circ F^{-1}(\xi_{F(A)}) \\ &= F^{-1}(\xi_{F(B)}) \circ f = \tau_B \circ f.\end{aligned}$$

□

Considérons un exemple : $\mathcal{C}$ est la catégorie dont les objets sont les $[n] = \{1, 2, \ldots, n\}$ pour $n \in \mathbb{N}$ et les morphismes sont les fonctions $[n] \to [m]$, $n, m \in \mathbb{N}$, et $\mathcal{D} = FinEns$, la catégorie des ensembles finis. Soit F le foncteur $\mathcal{C} \to \mathcal{D}$ défini par $F([n]) = [n]$, tel que si $f : [n] \to [m]$ est un morphisme, $F(f) = f$. La condition (1) de la proposition est satisfaite, car tout ensemble fini est en bijection avec un certain $[n]$. De plus la condition (2) est satisfaite aussi : la bijection est l'identité.

Exercice 7.8. *Généraliser le dernier exemple pour montrer que la catégorie des groupes cycliques finis est équivalente à la catégories des groupes $\mathbb{Z}/n\mathbb{Z}$, $n \geq 1$; et que la catégorie des espaces vectoriels de dimension finie sur $\mathbb{K}$ est équivalente à la catégorie des espaces vectoriels $\mathbb{K}^n$, $n \geq 0$.*

Exercice 7.9 (Pour les amateurs de posets)**.** *Étendre le théorème de Birkhoff sur les treillis distributifs à une équivalence de catégories.*

Exercice 7.10. *Vérifier que G défini en (3) est bien un foncteur. (Indication : montrer que F^{-1} respecte la composition.)*

Troisième partie
Modules sur un anneau

8 Modules : généralités

8.1 C'est quoi, un module ?

Soit $\mathbb{A}$ un anneau (non nécessairement commutatif). Un $\mathbb{A}$-*module à gauche* est un groupe abélien M avec une opération externe $\mathbb{A} \times M \to M$, $(a, m) \mapsto am$, avec les propriétés suivantes :

(i) $(ab)m = a(bm)$;
(ii) $1_{\mathbb{A}} m = m$;
(iii) $(a + b)m = am + bm$;
(iv) $a(m + m') = am + am'$;

pour tous les $m, m' \in M$ et $a, b \in \mathbb{A}$.

Les *modules à droite* sont définis de manière analogues. Lorsque l'anneau est commutatif, un module à gauche est aussi un module à droite (voir les exercices 8.1 et 8.2).

Proposition 8.1. *Soit M un groupe abélien, noté additivement.*

(i) L'ensemble $\mathrm{End}_{\mathbb{Z}}(M)$ des endomorphismes du groupe abélien M est un anneau, avec l'addition des fonctions et la composition.

(ii) On suppose que M un module à gauche sur $\mathbb{A}$. Soit $a \in \mathbb{A}$; la fonction $f_a : m \mapsto am$ est dans $\mathrm{End}_{\mathbb{Z}}(M)$. La fonction qui à $a \in \mathbb{A}$ associe f_a est un homomorphisme d'anneaux de $\mathbb{A}$ dans l'anneau $\mathrm{End}_{\mathbb{Z}}(M)$.

(iii) On obtient ainsi, pour tout groupe abélien M, une correspondance bijective entre les structures de $\mathbb{A}$-modules sur M et les homomorphismes d'anneaux $\mathbb{A} \to \mathrm{End}_{\mathbb{Z}}(M)$.

Démonstration. (i) L'addition de deux fonctions f et g est $(f+g)(m) = f(m) + g(m)$. Si $f, g \in \mathrm{End}(M)$, alors $f+g, f \circ g \in \mathrm{End}(M)$ (vérification standard). Il faut vérifier maintenant que $\mathrm{End}(M)$ devient ainsi un anneau. C'est direct. Le 0 est la fonction nulle, et le 1 est la fonction id_M. La seule chose qui sort de l'ordinaire, et qui utilise la propriété que les fonctions considérées sont des endomorphismes, est la distributivité à gauche : $f \circ (g+h) = f \circ g + f \circ h$; cette égalité se vérifie en l'appliquant à $m \in M$, et on obtient $f((g+h)(m)) = f(g(m) + h(m)) = f(g(m)) + f(h(m)) = f \circ g(m) + f \circ h(m) = (f \circ g + f \circ h)(m)$, cqfd, et on a bien utilisé la propriété mentionnée.

(ii) Le fait que f_a est un homomorphisme de modules, c'est-à-dire $f_a(m+n) = f_a(m) + f_a(n)$, est équivalent à $a(m+n) = am + an$, un des axiomes des modules. Le fait que $a \mapsto f_a$ est un homomorphisme d'anneaux découle des trois autres axiomes : $f_{a+b} = f_a + f_b$ découle de $(a+b)m = am + bm$, $f_1 = \mathrm{id}_M$ découle de $1m = m$, et $f_a \circ f_b = f_{ab}$ découle de $a(bm) = (ab)m$.

(iii) On a déjà vu que toute structure de A-module sur le groupe abélien M donne un homomorphisme d'anneaux de $\mathbb{A}$ vers $\mathrm{End}(M)$. Réciproquement, si on a un homomorphisme d'anneaux $\mu : \mathbb{A} \to \mathrm{End}(M)$, alors M devient un $\mathbb{A}$-module avec l'opération externe $am = \mu(a)(m)$; les quatre propriétés de la définition de module sont aisément vérifiées.

Il reste à vérifier que les deux correspondances décrites sont inverses l'une de l'autre. On remarque entre autres que $\mu(a) = f_a$, et le reste est laissé au lecteur. □

Exercice 8.1. *Montrer que si M est un module à droite sur l'anneau commutatif $\mathbb{A}$, alors la loi externe $\mathbb{A}\times M \to M, (a,m) \mapsto ma$ en fait un $\mathbb{A}$-module à gauche.*

Exercice 8.2. *Montrer que si M est un $\mathbb{A}$-module à droite, alors M est aussi un $\mathbb{A}^{op}$-module à gauche sur l'*anneau opposé *$\mathbb{A}^{op}$, dont la multiplication est $(a,b) \mapsto ba$.*

8.2 Exemples

Lorsque $\mathbb{A}$ est un corps, les $\mathbb{A}$-modules à gauche sont les espaces vectoriels à gauche sur $\mathbb{A}$.

Un exemple de module à gauche est le suivant : soit M l'ensemble des vecteurs-colonnes de longueur n sur $\mathbb{A}$. C'est un module à gauche sur l'anneau des matrices carrées d'ordre n, noté $\mathbb{A}^{n\times n}$; la loi externe est le produit matriciel d'une telle matrice par un vecteur colonne.

De même, l'ensemble des vecteurs-lignes sur $\mathbb{A}$ est un module à droite sur cet anneau.

L'anneau $\mathbb{A}$ est un module à gauche, et aussi un module à droite, sur lui-même.

Un groupe abélien est un $\mathbb{Z}$-module, et réciproquement.

8.3 Sous-modules

Les *sous-modules* sont définis de manière évidente. Pour la structure de $\mathbb{A}$-module à gauche de $\mathbb{A}$, les sous-modules sont les idéaux à gauche. Les sous-modules des $\mathbb{Z}$-modules (= groupes abéliens) sont les sous-groupes.

8.4 Homomorphismes

Les *homomorphismes de modules*, appelés aussi *applications linéaires*, sont des fonctions qui préservent l'addition et la produit externe. Pour un tel homomorphisme, on doit avoir, dans le cas des modules à gauche

$$f(am) = af(m).$$

Le *noyau* se définit comme on pense par $\mathrm{Ker}(f) = f^{-1}(0)$. Sa propriété de base est que

$$f \text{ injective} \Leftrightarrow \mathrm{Ker}(f) = 0.$$

Exercice 8.3. *Soit M un module à droite. Montrer que l'ensemble des homomorphismes $M \to \mathbb{A}$ est naturellement un module à gauche sur $\mathbb{A}$, son dual. Avec $M = \mathbb{Z}/2\mathbb{Z}$ et $\mathbb{A} = \mathbb{Z}$, montrer que son dual est nul.*

8.5 Quotients

Le quotient d'un module par un sous-module se définit d'abord comme groupe abélien, puis la loi externe y est définie. Il n'y a pas vraiment de différence dans les preuves, par rapport aux espaces vectoriels.

Propriété universelle du quotient : Soient M, N des modules et $f : M \to N$ un homomorphisme de modules. Il existe une unique application linéaire $\bar{f} : M/\operatorname{Ker}(f) \to N$ telle que $f = \bar{f} \circ p$, où p est la projection canonique $M \to M/\operatorname{Ker}(f)$. L'homomorphisme $\bar{f}$ est injectif. Si f est surjectif, $\bar{f}$ est un isomorphisme.

Exercice 8.4. *Montrer que tout homomorphisme de module se décompose en le produit d'un homomorphisme surjectif, suivi d'un isomorphisme, suivi d'un homomorphisme injectif. Indication : utiliser la propriété universelle du quotient.*

8.6 Combinaisons linéaires, bases et modules libres

Une *combinaison linéaire* dans un $\mathbb{A}$-module à gauche M est définie de manière tout-à-fait analogue au cas des espaces vectoriels : $a_1 m_1 + \cdots + a_k m_k$. On pourra donc parler de *vecteurs linéairement indépendants*, etc...

Notons ce qui ne marche pas dans les modules, comparés aux espaces vectoriels : si des vecteurs sont linéairement dépendants $a_1 m_1 + \cdots + a_k m_k = 0$, alors il n'est pas vrai en général que l'un d'eux soit linéairement dépendants des autres ; car on peut bien écrire $a_1 m_1 = -\sum_{2 \leq i \leq k} a_i m_i$ en supposant par exemple que a_1 est non nul, mais on ne pourra pas multiplier à gauche par a_1^{-1}, car dans un anneau, un élément non nul n'est pas forcément inversible. De cette impossibilité, découle l'inexistence des bases dans un module en général.

Un module est dit *finiment engendré*, ou *de type fini*, s'il existe un nombre fini de vecteurs qui l'engendrent, c'est-à-dire que tout vecteur dans le module en est une combinaison linéaire.

Un module est dit *libre* s'il a une base. Une *base* est un ensemble de vecteurs tel que tout vecteur dans le module est combinaison linéaire de manière unique des vecteurs de la base. On appelle *rang* du module la cardinalité d'une base (on ne dit pas dimension, pour des raisons mystérieuses, cet adjectif étant réservé aux espaces vectoriels). Notez que le rang peut ne pas être unique : il existe des exemples où un module libre peut avoir des bases de cardinalités distinctes. Cependant, quand $\mathbb{A}$ est commutatif, le rang est unique, ce qu'on démontre en utilisant le déterminant : on montre que si

on a une base avec n éléments, alors il existe une forme n-linéaire alternée non nulle (déterminée par le déterminant), et que toute forme p-linéaire avec $p > n$ est nulle (voir exercice 8.5).

Propriété universelle des bases : toute fonction de la base vers un module se prolonge de manière unique en une application linéaire.

Conséquence : tout module finiment engendré est quotient d'un module libre de rang fini.

Ce qui ne marche pas non plus, c'est qu'on peut avoir un module libre de rang n, et un sous-module propre, qui est un module libre, et aussi de rang n. Un exemple simple est $\mathbb{Z}$, $2\mathbb{Z}$, avec $\mathbb{A} = \mathbb{Z}$.

Pour une application linéaire $f : M \to V$ entre modules à droite libres, avec bases respectives $m_1, \ldots, m_p$ et $v_1, \ldots, v_n$, on définit sa matrice $A = (a_{ij})_{1 \leq i \leq n, 1 \leq j \leq p}$ par la formule usuelle

$$f(m_j) = \sum_{1 \leq i \leq n} v_i a_{ij}.$$

Si on représente les vecteurs dans ces bases par des vecteurs colonnes, on a la formule usuelle

$$Y = MX, \tag{4}$$

X et Y étant les vecteurs colonnes associés à $x \in M$, $y = f(x) \in V$, avec donc $X = {}^t(x_1, \ldots x_p)$, $Y = (y_1, \ldots, y_n)$ et

$$X = \sum_i v_i x_i, Y = \sum_i v_i y_i.$$

Remarquez qu'on a choisi ici des modules à droite pour obtenir les formules usuelles. Pour des modules à gauche, ce sont des vecteurs-lignes qu'il faut employer, et il faut modifier aussi la définition de la matrice d'une application linéaire, en échangeant lignes et colonnes.

Exercice 8.5. *Montrer que si $\mathbb{A}$ est commutatif, alors le déterminant d'une matrice, vu comme une fonction $(\mathbb{A}^n)^n$ dans $\mathbb{A}$, est une forme n-linéaire alternée, où les lignes de la matrice sont vues comme des éléments de $\mathbb{A}^n$; montrer que cette forme est non nulle. Montrer que si $p > n$, alors toute forme p-linéaire alternée sur $\mathbb{A}^n$ est nulle. En déduire que les cardinalités des bases d'un $\mathbb{A}$-module libre finiment engendré sont égales.*

Exercice 8.6. *Montrer que les deux conditions suivantes sont équivalentes, pour anneau (non nécessairement commutatif $\mathbb{A}$) :*

(i) Pour chaque module libre, toutes ses bases ont même cardinalité.

(ii) Toute matrice inversible sur $\mathbb{A}$ est carrée (précisément : si $M \in M_{np}(\mathbb{A})$ et $N \in M_{pn}(\mathbb{A})$ et si $MN = I_n$, $NM = I_p$, alors $p = n$).

Exercice 8.7. *Donner les définitions adéquates de matrices d'une application linéaire entre modules à gauche libres, ainsi que pour celles des vecteurs-lignes associés aux vecteurs, et donner la formule remplaçant l'équation (4) et sa preuve.*

Exercice 8.8. *Montrer que si l'anneau est infini, alors tout module libre non trivial est infini. En déduire l'existence de $\mathbb{Z}$-modules qui ne sont pas libres.*

Exercice 8.9. *Montrer que si B est un ensemble, il existe un module libre de base B.*

8.7 Modules cycliques

Un module est dit *cyclique*, ou *monogène*, s'il existe un élément qui l'engendre. Tout anneau, vu comme un module sur lui-même, est cyclique : il est engendré par 1.

8.8 Produits et somme directes

Le *produit cartésien* d'une famille de modules $(M_i)_{i\in I}$ est, en tant qu'ensemble, leur produit cartésien $\prod_{i\in I} M_i$, avec somme et produit externe définis composante par composante.

La *somme directe (externe)* de cette famille est le sous-module du produit cartésien des I-uplets dont le *support* est fini. Il est noté $\bigoplus_{i\in I} M_i$.

Si I est fini, on a

$$\prod_{i\in I} M_i \cong \bigoplus_{i\in I} M_i$$

Si $(M_i)_{i\in I}$ est une famille finie de sous-modules d'un module M, et V un sous-module de M, on dit que V *est somme directe (interne)* de cette famille, si tout élément de V est somme d'éléments de M_i, et ce de manière unique. De manière équivalente, l'homomorphisme canonique $\bigoplus_{i\in I} M_i \to M$ est injectif, et d'image V. Cette dernière condition permet d'étendre la notion de somme directe interne à une famille infinie de sous-modules.

8.9 Théorèmes d'isomorphisme et de correspondance

Théorème 8.1. *Soient $S, T \subset M$ des sous-modules de M.*

(i) On a

$$S/S\cap T \cong S+T/T.$$

(ii) On suppose que $T \subset S \subset M$. Alors S/T s'identifie canoniquement à un sous-module de M/T, et

$$(M/T)/(S/T) \cong M/S.$$

Démonstration. (i) On compose l'injection canonique $S \to S+T$, suivie de la projection canonique $S+T \to S+T/T$. La composition est un homomorphisme surjectif, car tout élément $s+t \in S+T$ est congru à $s \in S$ modulo T. Le noyau est clairement $S \cap T$. On applique la propriété universelle du quotient.

(ii) On considère la restriction à S de la projection canonique $p : M \to M/T$. Son noyau est T, donc S/T s'injecte dans M/T, et la première assertion est prouvée. Comme $T \subset S$, p induit un homomorphisme surjectif $q : M/T \to M/S$, par $m+T \mapsto m+S$ (car $m \equiv m+t \mod S$). Le noyau de q est l'ensemble des $m+T$ tels que $m+T = S$, c'est-à-dire $m \in S$, donc ce noyau s'identifie à S/T. On applique la propriété universelle du quotient. □

Théorème 8.2. *Il y a bijection canonique entre les sous-modules de M contenant T et les sous-modules de M/T.*

Démonstration. La bijection associe à tout sous-module de M contenant T le sous-module $p(M)$ de M/T, où $p : M \to M/T$ est la projection canonique. □

9 Théorie des modules

9.1 Modules indécomposables

Un module M est dit *indécomposable* s'il est non nul et si pour tous sous-modules P, Q tels que $M = P \oplus Q$ (somme directe interne), on a $P = 0$ ou $Q = 0$.

Comme exemples et contre-exemples, on peut considérer les $\mathbb{Z}$-modules $\mathbb{Z}/n\mathbb{Z}$. Si n n'est pas la puissance d'un nombre premier, alors $n = ab$, $a, b \in \mathbb{N}, n \geq 2$, a, b premiers entre eux, et le théorème chinois nous assure que $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/a\mathbb{Z} \oplus \mathbb{Z}/b\mathbb{Z}$. Si par contre $n = p^k$ est la puissance d'un nombre premier, alors si nous supposons par l'absurde que $M = P \oplus Q$, alors la cardinalité de P, Q sont de la forme p^i, p^j avec $i, j < k$, et donc tout élément m de M satisfait $p^{\max(i,j)}m = 0$, ce qui n'est pas vrai avec $m = 1$.

Lorsqu'un module est décomposable, on peut l'écrire $M = P \oplus Q$ de manière non triviale ; si on recommence avec P, Q, on peut écrire M comme somme directe de sous-modules ; on aimerait que cette construction s'arrête,

c'est-à-dire que les sous-modules obtenus soient indécomposables, et que M soit leur somme directe. Ceci est fait dans la section suivante.

Exercice 9.1. *Lorsque $\mathbb{A}$ est un corps, montrer que les modules indécomposables sont les espaces vectoriels de dimension 1.*

9.2 Les conditions de chaînes : modules noetheriens, artiniens

Définition 9.1. *Un module M est dit*

(i) artinien *si tout ensemble non vide de sous-modules de M contient un élément minimal (pour l'inclusion) ;*

(ii) noetherien *si tout ensemble non vide de sous-modules de M contient un élément maximal (pour l'inclusion).*

Proposition 9.1. *Un module est artinien si et seulement si tout suite décroissante (au sens large) de sous-modules est stationnaire. Un module est noetherien si et seulement si tout suite croissante (au sens large) de sous-modules est stationnaire.*

Démonstration. Soit M un module artinien et considérons une suite décroissante de sous-modules :

$$M_0 \supseteq M_1 \supseteq M_2 \supseteq M_3 \supseteq \dots .$$

L'ensemble des M_i a par hypothèse un élément minimal, soit M_n. Alors pour tout $p \leq n$, on doit avoir $M_p = M_n$.

Réciproquement, démontrons la contraposée. Supposons qu'il existe un ensemble non vide E de sous-modules qui n'ait pas d'élément minimal. Soit $M_0 \in E$. Il existe alors un $M_1 \in E$ tel que $M_0 \supset M_1$ et $M_o \neq M_1$; de même un $M_1 \supset M_2$ et $M_o \neq M_1$. On construit ainsi une suite strictement décroissante de sous-modules, forcément non stationnaire.

La preuve de l'autre assertion est analogue. □

Proposition 9.2. *Tout sous-module, et tout quotient, d'un module artinien (resp. noetherien) est artinien (resp. noetherien).*

Proposition 9.3. *Soit M un module artinien ou noetherien. Alors M est somme directe finie de modules indécomposables.*

Démonstration. 1. Nous montrons d'abord que si M est décomposable, alors il existe une décomposition de M en somme directe $M = N_1 \oplus M_1$ de modules propres non nuls, avec N_1 indécomposable.

En effet, considérons l'ensemble E ses sous-modules N propres non nuls tels qu'il existe un sous-module N' propre non nul avec $M = N \oplus N'$. Comme M est décomposable, E est non vide.

Si M est artinien, il existe N_1 qui est un élément minimal de E. Alors $M = N_1 \oplus N_1'$; supposons par l'absurde que N_1 est décomposable : $N_1 = P \oplus Q$, P, Q sous-modules de N_1 propres et non nuls ; alors $M = P \oplus Q \oplus N_1'$, et N_1 n'est pas minimal dans E, contradiction.

Si M est noetherien, il existe un élément N_1 maximal de E, et $M = N_1 \oplus N_1'$; de plus N_1 est indécomposables, sinon $N_1 = P \oplus Q$, donc $M = P \oplus Q \oplus \oplus N_1'$, ce qui contredit la maximalité de N_1'.

2. Nous pouvons supposer M décomposable. Il existe donc $i \geq 1$ tel que $M = N_1 \oplus N_2 \oplus \cdots \oplus N_i \oplus M_i$, où les sous-modules N_j sont propres et non nuls (c'est vrai pour $i = 1$). Si M_i est indécomposable ou nul, c'est fini. Sinon, M_i est non nul, décomposable et artinien ou noetherien, et par 1, $M_i = N_{i+1} \oplus M_{i+1}$. On obtient alors $M = N_1 \oplus N_2 \oplus \cdots \oplus N_{i+1} \oplus M_{i+1}$.

Ce processus doit s'arrêter, sinon on obtient une suite infinie strictement décroissante de sous-modules

$$M_1 \supset M_2 \supset M_3 \supset \cdots ,$$

ainsi qu'une suite infinie strictement croissante de sous-modules

$$N_1 \subset N_1 \oplus N_2 \subset N_1 \oplus N_2 \oplus N_3 \subset \cdots ,$$

ce qui contredit que M est artinien ou noetherien. □

Théorème 9.1. *Un module est noetherien si et seulement si tout sous-module est de type fini.*

Démonstration. 1. Supposons M noetherien, et P un sous-module. Soit E l'ensemble des sous-modules de type fini de N. Il contient le module nul. Il a donc un élément maximal Q. On doit avoir $Q = P$ (et alors P est de type fini), sinon $\exists x \in P \setminus Q$, et alors $Q + \mathbb{A}x$ est dans E ; comme il contient strictement Q, on obtient une contradiction avec la maximalité de Q.

2. Supposons que tout sous-module de M soit de type fini. Considérons une suite croissante, au sens large, de sous-modules. La réunion de tous ces sous-modules est un sous-module, qui est de type fini. Il existe donc un ensemble fini de générateurs ; ceux-ci sont tous dans un certain sous-module de la suite. Alors la suite devient stationnaire à partir de ce sous-module. □

Théorème 9.2. *Soit M un module et N un sous-module. Si deux des trois modules $M, N, M/N$ sont noetheriens (resp. artiniens), alors le troisième l'est aussi.*

Démonstration. Si M est noetherien (resp. artinien), N et M/N le sont aussi.

Il reste donc à montrer que si N et M/N sont noetherien, alors M aussi (le cas artinien est analogue). Soit $P_i, i \geq 1$ une suite croissante de sous-modules de M. Alors la suite croissante de sous-modules $N \cap P_i$ de N est stationnaire, de même que la suite $(N + P_i)/N$ de sous-modules de M/N. Il existe donc $n \geq 1$ tel que pour tout $m \geq n$, on a $N \cap P_n = N \cap P_m$ et $(N + P_n)/N = (N + P_m)/N$. Nous montrons maintenant $P_m \subset P_n$ (ce qui implique $P_n = P_m$ et achève la preuve). En effet, soit $x \in P_m$; alors $x + N \in (N + P_m/N) = (N + P_n)/n$; il existe donc $y \in P_n, z' \in N$ tels que $x + N = y + z' + N$, et il s'ensuit qu'il y a un $z \in N$ tel que $x = y + z$. Or $x - y = z \in N$, $x - y \in P_m$; donc $x - y \in N \cap P_m = N \cap P_n$, donc $x - y \in P_n$, et $x = (x - y) + y \in P_n$. □

Corollaire 9.1. *Soient N, P des sous-modules de M. Si N, P sont noetheriens (resp. artiniens), alors $N + P$ l'est aussi.*

Démonstration. $(N+P)/N \cong P/(N \cap P)$ est noetherien, comme quotient de P. Comme N est noetherien, le théorème implique que $N+P$ l'est aussi. □

Exercice 9.2. *Dans la preuve de la réciproque de la proposition 9.1, utiliser formellement l'axiome du choix.*

Exercice 9.3. *Si $\mathbb{A}$ est un corps, à quelle condition um module sur $\mathbb{A}$ est-il artinien (resp. noetherien) ?*

Exercice 9.4. *On définit le sous-groupe additif de $\mathbb{Q}$: $P = \{m/p^k, m \in \mathbb{Z}, k \in \mathbb{N}\}$, qui est donc un $\mathbb{Z}$-module. Montrer qu'il n'est ni artinien, ni noetherien. Montrer que $P/\mathbb{Z}$ est noetherien, mais pas artinien. Indications : P contient le sous-module $\mathbb{Z}$, qui n'est pas artinien. Considérer la suite des sous-modules cycliques engendrés par $1/p^k$.*

9.3 Anneaux noetheriens, artiniens

Définition 9.2. *Un anneau $\mathbb{A}$ est dit* noetherien *(resp.* artinien*)* à gauche *si, en tant que $\mathbb{A}$-module à gauche sur lui-même, c'est un module noetherien (resp. artinien).*

Théorème 9.3. *Si $\mathbb{A}$ est un anneau noetherien (resp. artinien) à gauche, alors tout $\mathbb{A}$-module à gauche de type fini est noetherien (resp. artinien).*

Démonstration. Supposons $\mathbb{A}$ noetherien, et soit $M = \mathbb{A}x_1 + \cdots + \mathbb{A}x_n$ un $\mathbb{A}$-module à gauche de type fini. Grâce au corollaire 9.1, il suffit de montrer que $\mathbb{A}x_i$ est noetherien. Mais ce dernier module est l'image de l'homomorphisme de modules $\mathbb{A} \to \mathbb{A}x_i, a \mapsto ax_i$. Il est donc quotient du $\mathbb{A}$-module $\mathbb{A}$, donc il est noetherien (proposition 9.2). □

Un résultat important à mentionner ici est le *théorème de Hilbert* : *si $\mathbb{K}$ est un corps commutatif, alors l'algèbre des polynômes en n variables $\mathbb{K}[x_1, \ldots, x_n]$ est un anneau noetherien.*

9.4 Idempotents de $\mathrm{End}(M)$

Définition 9.3. *Deux idempotents e, f d'un anneau sont dits* orthogonaux *si $ef = fe = 0$.*

Soient $e_1, \ldots, e_n$ sont des idempotents d'un anneau, non nuls et deux à deux orthogonaux. Ils sont dits complets *si leur somme est 1 ; dans ce cas, on appelle cette somme une* décomposition de l'identité *de l'anneau.*

Théorème 9.4. *Soit M un module. Les décompositions de l'unité dans l'anneau $End(M)$ correspondent bijectivement aux décompositions de M en somme directe. Précisément : $1 = e_1 + \cdots + e_n$ correspond à $M = \mathrm{Im}(e_1) \oplus \cdots \oplus \mathrm{Im}(e_n)$.*

Ce théorème est déjà intéressant pour les espaces vectoriels. On le démontre en général pour un endomorphisme idempotent p ; alors $1 - p$ est aussi idempotent, et l'espace est somme directe des images de p et $1 - p$. La preuve du théorème est presque la même que celle de ce cas particulier et nous l'omettons.

Corollaire 9.2. *Un module M est indécomposable si et seulement si 1 et 0 sont les seuls idempotents de $\mathrm{End}(M)$.*

9.5 Anneaux locaux

Définition 9.4. *Un anneau est dit* local *si et seulement s'il n'a qu'un seul idéal à droite maximal.*

Proposition 9.4. *Un anneau est local si et seulement s'il a la propriété suivante : (*) pour tout élément a, au moins un des deux éléments a et $1 - a$ est inversible.*

La proposition implique que dans la définition d'un anneau local, on peut remplacer droite par gauche.

Lemme 9.1. *Soit $\mathbb{A}$ un anneau local, ou qui a la propriété (*). Alors les seuls idempotents de $\mathbb{A}$ sont 0 et 1, et pour tout $a \in \mathbb{A}$, on a : a inversible à gauche $\Leftrightarrow$ a inversible à droite.*

Démonstration. 1. Soit I l'unique idéal à droite maximal de l'anneau local $\mathbb{A}$. Soit e un idempotent. Si $e\mathbb{A} = \mathbb{A}$, alors il existe $a \in \mathbb{A}$ tel que $ea = 1$, d'où $e = e1 = eea = ea = 1$. Si $(1-e)a = 1$, de même $1 - e = 1, e = 0$. Si $e \neq 0, 1$, alors d'après ce qui précède, $e\mathbb{A}, (1-e)\mathbb{A} \neq \mathbb{A}$, donc ces deux idéaux à droite sont inclus dans I (lemme de Zorn), donc $1 = e + (1-e) \in I$, ce qui est impossible.

2. Soit $\mathbb{A}$ un anneau ayant la propriété (*). Soit e un idempotent. SI e est inversible, alors $e^2 = e$ implique $e = 1$. Sinon, $1 - e$ est un idempotent inversible, et similairement $1 - e = 1, e = 0$.

3. Soit $\mathbb{A}$ local, ou ayant la propriété (*). Nous montrons que pour $a \in \mathbb{A}$: a inversible à gauche $\Leftrightarrow$ a inversible à droite. Soit donc a inversible à droite. Il existe b tel que $ab = 1$. Alors $e = ba$ est idempotent, car $ee = b(ab)a = ba = e$. Si $e = 0$, alors $1 = a(ba)b = 0$, ce qui n'est pas. Donc $e = 1$ par ce qui précède, $ba = 1$ et a est inversible à gauche.

On démontre de manière analogue l'implication inverse. □

Preuve de la proposition 9.4. 1. Supposons que $\mathbb{A}$ soit local, et soit I son unique idéal à droite maximal. Soit $a \in \mathbb{A}$. Si a n'est pas inversible, alors il n'est pas inversible à droite par le lemme ; alors l'idéal à droite $a\mathbb{A}$ est contenu dans I. L'idéal à droite $(1-a)\mathbb{A}$ n'est pas contenu sans I, sinon $a, 1 - a \in I$, donc $1 \in I$, contradiction. Donc $(1-a)\mathbb{A} = \mathbb{A}$ et $1 - a$ est inversible à droite. Donc $1 - a$ est inversible par le lemme.

2. Réciproquement, supposons que pour tout élément a, au moins un des deux éléments a et $1-a$ est inversible.$\mathbb{A}$ ait la propriété (*). Soit I l'ensemble des éléments non inversibles de A. Si $a \in A$ et $x \in I$, alors $ax \in I$, sinon ax est inversible et x aussi par le lemme, contradiction. De même, $xa \in I$. Si x, y est dans I, alors $x+y$ aussi, sinon $a(x+y) = 1$, donc $1-ay = ax \in I$, et $1 - ay$ n'est pas inversible, donc ay est inversible, et y aussi, contradiction. Donc I est un idéal bilatère, et il est maximal comme idéal à droite. Tout idéal à droite propre est constitué d'éléments non inversibles, donc il est contenu dans I ; celui-ci est donc l'unique idéal à droite maximal. □

La preuve démontre aussi le

Corollaire 9.3. *Si $\mathbb{A}$ est un anneau local, l'ensemble des éléments non inversibles est l'unique idéal (gauche, droite, bilatère) maximal.*

Théorème 9.5. *(lemme de Fitting) Soit M un module artinien et noetherien. Si $f \in \mathrm{End}(M)$, alors il existe un exposant $n > 0$ tel que $M = \mathrm{Ker}(f^n) \oplus \mathrm{Im}(f^n)$.*

Démonstration. La suite des images des f^n est décroissante, et celle de leurs noyaux est croissante. Comme M est noetherien et artinien, il existe $n > 0$ tel que $\forall m \geq n$, $\mathrm{Im}(f^m) = \mathrm{Im}(f^n), \mathrm{Ker}(f^m) = \mathrm{Ker}(f^n)$. Comme $\mathrm{Im}(f^{2n} = \mathrm{Im}(f^n)$, il existe pour tout $x \in M$ un $y \in M$ tel que $f^n(x) = f^{2n}(y)$. On a alors $x = f^n(y) + (x - f^n(y)$ et le second terme est dans $\ker(f^n)$. Donc $M = \mathrm{Ker}(f^n) + \mathrm{Im}(f^n)$. Considérons un élément dans l'intersection de ces deux modules ; il s'écrit $f^n(z)$. Alors $f^n(z) \in \ker(f^n)$, donc $f^{2n}(z) = 0$, donc $z \in \ker(f^{2n} = \ker(f^n)$, donc $f^n(z) = 0$ et cet élément est nul. Donc $\mathrm{Ker}(f^n) \cap \mathrm{Im}(f^n) = 0$. □

Corollaire 9.4. *Soit M un module indécomposable, artinien et noetherien. Si $f \in \mathrm{End}(M)$, alors f est nilpotent ou un automorphisme de M.*

Démonstration. Par le théorème, $M = \mathrm{Ker}(f^n) \oplus \mathrm{Im}(f^n)$, $n > 0$. L'un de ces deux modules doit être nul, et l'autre M. Si c'est le second qui est nul, f est nilpotent. Si c'est le premier qui est nul, f^n est injectif, d'image M, donc f^n est un automorphisme. Donc f aussi. □

Théorème 9.6. *Si $\mathrm{End}(M)$ est un anneau local, alors M est indécomposable. La réciproque est vraie si M est un module artinien et noetherien.*

Démonstration. 1. Supposons que $\mathrm{End}(M)$ soit local. Soit $e \in \mathrm{End}(M)$ un idempotent. Alors e ou $1-e$ est inversible. Si e est inversible, $e^2 = e$ implique $e = 1$. Si $1 - e$ est inversible, alors $(1 - e)x = 1$, donc $e = e1 = e(1 - e)x = (e - e^2)x = 0$. Donc $\mathrm{End}(M)$ n'a que deux idempotents, et il s'ensuit que M est indécomposable (corollaire 9.2).

2. Supposons que M soit un module indécomposable, artinien et noetherien. On sait que tout endomorphisme f de M est soit nilpotent, soit un automorphisme. Si $f^n = 0$, alors $1 - f$ est inversible. Si f est un automorphisme, f est inversible. Donc $\mathrm{End}(M)$ est un anneau local, par la proposition 9.4. □

9.6 Suites de composition

Un module non nul est dit *simple* s'il n'a pas d'autre sous-module que 0 et lui-même.

Définition 9.5. *1. Une* suite normale *dans un module M est une suite finie de sous-modules*

$$0 \subset M_1 \subset M_2 \subset \cdots \subset M_n = M. \tag{5}$$

La longueur *de cette suite est n. Les* quotients *de cette suite sont les modules M_i/M_{i-1}, $i = 1, \ldots, n$.*

2. Deux suites normales sont dites équivalentes *si elles ont même longueur n et s'il existe une permutation σ de $1, 2, \ldots, n$ telle que $M_i/M_{i-1} \cong M'_{\sigma(i)}/M'_{\sigma(i-1)}$ pour tout $i = 1, \ldots, n$.*

3. Une suite de composition est dite simple *si tous ses quotients sont des modules simples.*

Théorème 9.7. *Un module possède une suite de composition si et seulement s'il est artinien et noetherien.*

Démonstration. 0. Tout module artinien non nul possède un sous-module simple ; car, M étant artinien, l'ensemble (non vide) de ses sous-modules non nuls possède un élément minimal, et celui-ci est simple .

1. Soit M un module qui est artinien et noetherien. S'il est nul, on a fini. Sinon, M possède un sous-module simple M_1. Le quotient M/M_1 est artinien et noetherien. Il a donc une suite de composition $0 \subset N_2 \subset \cdots \subset N_n = M/M_1$. L'image réciproque par $M \to M/M_1$ de chaque N_i est un sous-module M_i de M, et on obtient ainsi une suite de composition de M : $0 \subset M_1 \subset M_2 \subset \cdots \subset M_n = M$ (on utilise le théorème 11.11 (ii) pour montrer que les quotients sont simples).

2. Supposons que M ait une suite de composition de longueur n. Si $n = 0$, M est nul et c'est clair. Si $n > 0$, on considère une suite de composition (5). Alors M_{n-1} a une suite de composition de longueur $n-1$, donc par hypothèse de récurrence, M_{n-1} est artinien et noetherien. De plus M/M_{n-1} est simple, donc il est artinien et noetherien. Donc M est artinien et noetherien par 9.2. □

Nous nous acheminons maintenant vers le théorème affirmant que deux suites de compositions sont toujours équivalentes. Commençons par un lemme.

Lemme 9.2. *Soient A, B, C des sous-modules de M tels que $C \subset B$. Alors $(C + A) \cap B = C + (A \cap B)$.*

Démonstration. Soit $b \in (C + A) \cap B$. Donc $b = c + a \in B$, et $a = b - c \in B$, car $b, c \in B$. Ainsi $a \in A \cap B$ et donc $b = c + a \in C + (A \cap B)$.

Réciproquement, $C \subset (C+A) \cap B$, puisque C est inclus dans les deux ensembles ; de plus, $A \cap B \subset (C+A) \cap B$ car $A \subset C+A$. Donc $C+(A \cap B) \subset (C+A) \cap B$. □

Théorème 9.8. *(Zassenhaus) On considère des sous-modules U, V, U', V' de M tels que $V \subset U$ et $V' \subset U'$. Alors*

$$\frac{(U+V') \cap U'}{(V+V') \cap U'} \cong \frac{U \cap U'}{(U' \cap V) + (U \cap V')} \cong \frac{(U'+V) \cap U}{(V'+V) \cap U}.$$

Démonstration. On considère la composition de morphismes

$$U \cap U' \hookrightarrow (U+V') \cap U' \twoheadrightarrow \frac{(U+V') \cap U'}{(V+V') \cap U'}.$$

Son noyau est

$$(U \cap U') \cap ((V+V') \cap U') = U' \cap (V+V') \cap U.$$

En appliquant le lemme à $A = V, B = U', C = V'$, on trouve que $U' \cap (V + V') = V' + (V \cap U')$, donc le noyau est

$$(V' + (V \cap U')) \cap U.$$

En appliquant le lemme à $A = V', B = U, C = V \cap U'$, on trouve que le noyau est

$$(V \cap U') + (V' \cap U).$$

Montrons que la composition ci-dessus est surjective. Prenons un élément quelconque $u + v' = u'$ de $(U+V') \cap U'$; comme $V' \subset U'$, $u = u' - v' \in U'$, donc $u \in U \cap U'$, et $v' \in (V+V') \cap U'$, donc notre élément est congru à un élément de $U \cap U'$ modulo $(V+V') \cap U'$. D'où la surjectivité et le premier isomorphisme, et le second est symétrique. □

Théorème 9.9. *(Jordan-Hölder) (1) Deux suites normales d'un module possèdent des raffinements qui sont des suites normales équivalentes.*

(2) Deux suites de composition d'un module sont équivalentes.

Démonstration. Il suffit de prouver (1). Soit donc deux suites normales de M

$$0 = M_0 \subset M_1 \subset M_2 \subset \cdots \subset M_r = M,$$

et

$$0 = M'_0 \subset M'_1 \subset M'_2 \subset \cdots \subset M'_s = M.$$

Entre M_i et M_{i+1}, on insère $(M'_j + M_i) \cap M_{i+1}$, $j = 0, 1, \ldots, s$, et entre M'_j et M'_{j+1}, on insère $(M_i + M'_j) \cap M'_{j+1}$, $i = 0, 1, \ldots, r$. On a par exemple

$$M_i = (M'_0 + M_i) \cap M_{i+1} \subset (M'_1 + M_i) \cap M_{i+1} \subset (M'_2 + M_i) \cap M_{i+1}$$

$$\subset \cdots \subset (M'_s + M_i) \cap M_{i+1} = M_{i+1}.$$

Par le théorème de Zassenhaus

$$\frac{(M'_j + M_i) \cap M_{i+1}}{(M'_{j-1} + M_i) \cap M_{i+1}} \cong \frac{(M_{i+1} + M'_{j-1}) \cap M'_j}{(M_i + M'_{j-1}) \cap M'_j}.$$

□

9.7 Théorème de Krull-Remak-Schmidt

Théorème 9.10. *Soit M_i, N_j des modules dont les anneaux d'endomorphismes sont des anneaux locaux. Si $\bigoplus_{1 \le i \le m} M_i \cong \bigoplus_{1 \le j \le n} N_j$, alors $m = n$ et il existe une permutation σ de $\{1, 2, \ldots, n\}$ telle que $M_i \cong N_{\sigma(i)}$ pour tout i.*

Ce théorème et le théorème 9.6 impliquent le

Corollaire 9.5. *Soit M un module artinien et noetherien. Sa décomposition en somme directe finie de sous-modules indécomposables (qui existe par la proposition 9.3) est unique à isomorphisme de ces sous-modules près.*

Preuve du théorème 9.10. (récurrence sur m) Rappelons que tous les modules M_i, N_j sont indécomposables (théorème 9.6). Si $m = 1$, alors $M_1 \cong N_{\sigma(i)}$, et comme M_1 est indécomposable, on doit avoir $n = 1$ et $M_1 \cong N_1$. Supposons que $M > 1$. Définissons

$$\alpha_j : N_j \hookrightarrow M \twoheadrightarrow M_1, \beta_j : M_1 \hookrightarrow M \twoheadrightarrow N_j.$$

Donc $\mathrm{id}_{M_1} = \alpha_1 \circ \beta_1 + \alpha_2 \circ \beta_2 + \cdots + \alpha_n \circ \beta_n$. D'après le corollaire 9.3, un des $\alpha_j \circ \beta_j$ doit être inversible. Il n'y a pas de mal à supposer que $j = 1$. Donc $\alpha_1 \circ \beta_1$ est un automorphisme de M_1, noté θ. Considérons $\omega = \theta^{-1} \circ \alpha_1 : N_1 \to M_1$. On a $\omega \circ \beta_1 = \theta^{-1} \circ \alpha_1 \circ \beta_1 = \mathrm{id}_{M_1}$. De plus, $\beta_1 \circ \omega$ est un endomorphisme de N_1, dont le carré est $(\beta_1 \circ \omega)^2 = \beta_1 \circ (\omega \circ \beta_1) \circ \omega = \beta_1 \circ \omega$. Comme $\mathrm{End}(N_1)$ est local, on doit avoir $\beta_1 \circ \omega = 0$ ou 1. Mais $\beta_1 \circ \omega = 0$ implique que $\beta_1 = 0$, car ω est surjectif (puisque $\omega \circ \beta_1 = \mathrm{id}_{M_1}$), donc $\beta_1 \circ \omega = \mathrm{id}_{N-1}$. Finalement, β_1 et ω sont inverses l'un de l'autre, et par suite $M_1 \cong N_1$.

Nous pouvons supposer que $M = \bigoplus_{1\leq i\leq m} M_i = \bigoplus_{1\leq j\leq n} N_j$. Nous montrons maintenant que $M = N_1 \oplus M_2 \oplus \cdots \oplus M_m$. Notons $proj_{M_1}$ la projection $M \to M_1$ correspondant à la décomposition de M en la somme directe des M_i. De même pour $proj_{N_1}$. Soit $x \in N_1 \cap \bigoplus_{2\leq i\leq m} M_i$; alors $proj_{M_1}(x) = 0$; de plus $x \in N_1$, et on peut donc lui appliquer $\omega : N_1 \to M_1$; or $\omega = \theta^{-1} \circ \alpha_1$ et $\alpha_1 = proj_{M_1} \circ inj_{N_1}$, où inj_{N-1} est l'injection canonique de N_1 dans M_1 ; on a donc, comme $x \in N_1$, $\alpha_1(x) = 0$, et donc $\omega(x) = 0$; mais comme ω est un isomorphisme, $x = 0$, et finalement $N_1 \cap \bigoplus_{2\leq i\leq m} M_i = 0$.

Montrons maintenant que $M = N_1 + \bigoplus_{2\leq i\leq m} M_i$. Il suffit de montrer que M_1 est inclus dans la somme à droite. Soit donc $y \in M_1$. Comme $\alpha_1 \circ \beta_1$ est inversible, α_1 est surjective. Il existe donc $x \in N_1$ tel que $y = \alpha_1(x) = proj_{M_1}(x) = x - proj_{M_2}(x) - \cdots - proj_{M_m}(x) \in N_1 + M_2 + \cdots + M_m \in N_1 + \bigoplus_{2\leq i\leq m} M_i$.

Nous avons donc $N_1 \oplus M_2 \oplus \cdots \oplus M_m = N_1 \oplus N_2 \oplus \cdots \oplus N_n$, et en quotientant par le premier terme, nous obtenons $\bigoplus_{2\leq i\leq m} M_i \cong \bigoplus_{2\leq j\leq n} N_j$, ce qui permet de conclure par récurrence. □

10 Modules semisimples

10.1 Modules semi-simples

Un module est dit *semi-simple* s'il est somme de sous-modules simples.

Tout espace vectoriel est semi-simple.

Théorème 10.1. *Soit M un module. Les conditions suivantes sont équivalentes :*

(i) M est semi-simple ;

(ii) M est somme directe de sous-modules simples ;

(iii) Tout sous-module de M est un facteur direct de M.

Lemme 10.1. *Soit N un sous-module d'un sous-module M, lequel est égal à la somme $\sum_{i\in I} M_i$, où les modules M_i sont simples. Alors il existe $J \subset I$ tel que $M = N \oplus \bigoplus_{i\in J} M_i$.*

Démonstration. Posons $E = \{J \subset I, N + \sum_{i\in J} S_i \text{ est une somme directe}\}$. L'ensemble E est non vide car il contient l'ensemble vide (ha ! ha !). Si on ordonne E par inclusion, c'est un ensemble inductif. En effet, soit F une partie totalement ordonnée de E. On définit alors $\mathcal{J} = \cup_{J\in F} J$. Alors $\mathcal{J}$ est dans E : en effet, si l'on a $n + \sum_{i\in\mathcal{J}} m_i = 0$, avec $m_i \in S_i$, alors, cette somme étant de support fini, il y a un $J \in F$ qui contient tous les m_i satisfaisant $s_i \neq 0$; on a alors $n + \sum_{i\in J} m_i = 0$, et comme la somme $N + \sum_{i\in J} S_i$ est

directe, on obtient que tous les m_i sont nuls. Clairement $\mathcal{J}$ est un majorant de F, et E est donc inductif.

Par le lemme de Zorn, E a un élément maximal, soit J. Pour obtenir le lemme, il suffit de montrer que $M = N + \sum_{i\in J} M_i := H$. Et pour cela, il suffit de montrer que chaque M_i est contenu dans H. Si l'un des M_i n'était pas inclus dans H, alors $i \notin J$, et $M_i \cap H$ est un sous-module propre de M_i, lequel doit être nul, car M_i est simple. Mais alors $H + M_i$ est une somme directe, ce qui contredit la maximalité de J. □

Lemme 10.2. *Soit M un module tel que tout sous-module de M est un facteur direct de M. Tout sous-module non nul N de M contient un sous-module simple.*

Démonstration. On peut supposer N de type fini (même cyclique). Alors M contient un sous-module propre maximal M' (lemme de Zorn, car M' est de type fini). Par hypothèse, il existe P sous-module de M tel que $M = M' \oplus P$. Alors la somme $M' + (P \cap N)$ est directe, et donc $P \cap N \cong (M' + (P \cap N))/M'$. De plus, par le lemme 9.2, cette somme est égale à $(M' + P) \cap N$ et ceci vaut $M \cap N = N$. Rassemblant tout ceci, nous avons $P \cap N \cong N/M'$. Ce dernier module est simpls (M' maximal), donc $P \cap N$ est simple, ce qui implique le lemme. □

Preuve du théorème 10.1. (i) implique (ii) (resp. (iii)) : cela découle du lemme 10.1 avec $N = 0$ (resp. N sous-module de M).

(ii) implique (i) : découle de la définition de "semi-simple".

(iii) implique (i) : Soit M' la somme de tous les sous-modules simples de M. Il existe par hypothèse un sous-module de M tel que $M = M' \oplus L$. Si L est non nul, L contient un sous-module simple S, et on doit avoir $L \subset M'$, contradiction avec la somme directe. En conclusion, $L = 0$, $M' = M$,qui est donc semi-simple. □

Corollaire 10.1. *Un module est semi-simple si et seulement s'il est isomorphe à une somme directe de modules simples.*

Corollaire 10.2. *Toute somme directe de modules semi-simples est semi-simple*

Corollaire 10.3. *Si $M \cong \bigoplus_{i\in I} S_i$, avec S_i simple, alors pour tout sous-module N de M, il existe $J \subset I$ tel que $N \cong \bigoplus_{i\in J} S_i$.*

Démonstration. D'après le théorème, il existe un sous-module L de M tel que $M = N \oplus L$. Par le lemme 10.1, il existe $J \subset I$ tel que $M = L \oplus_{i\in J} S_i$. En quotientant les deux expressions de M par L, on trouve que $N \cong \oplus_{i\in J} S_i$. □

Corollaire 10.4. *Tout sous-module d'un module semi-simple est semi-simple.*

Corollaire 10.5. *Tout quotient d'un module semi-simple est semi-simple.*

Démonstration. On applique le lemme 10.1, et un des corollaires précédents. □

Corollaire 10.6. *Si $\mathbb{A}$ comme $\mathbb{A}$-module à gauche sur lui-même est semi-simple, alors tout module à gauche sur $\mathbb{A}$ est semi-simple.*

Démonstration. Tout $\mathbb{A}$-module libre est une somme directe d'un certains nombres de copies de $\mathbb{A}$. Donc le résultat suit. □

Corollaire 10.7. *Si $\mathbb{A}$ comme $\mathbb{A}$-module à gauche est une somme directe finie de sous-modules à gauche simples $S_1 \oplus S_2 \oplus \cdots \oplus S_t$, alors tout module à gauche de type fini sur $\mathbb{A}$ est isomorphe à une somme directe finie de sous-modules dont chacun est isomorphe à l'un des modules S_i.*

Remarquons qu'un sous-module à gauche simple de $\mathbb{A}$ n'est rien d'autre qu'un idéal à gauche *minimal*, c'est-à-dire un idéal à gauche non nul dont le seul sous-idéal à gauche propre est nul.

Démonstration. Nous pouvons écrire $M \cong \mathbb{A}^n/K$, où K est un sous-module de $\mathbb{A}^n$. Comme $\mathbb{A}^n$ est semi-simple, il a un sous- module N tel que $\mathbb{A}^n = K \oplus N$. Donc $M \cong N$. Mais M est la somme directe des sous-modules simples $0^{j-1} \times S_i \times 0^{n-j+1}$ $(j = 1, \ldots, n,\ i = 1, \ldots, t)$, et ce dernier est isomorphe à S_i. On applique alors le corollaire 10.3. □

Le résultat qui suit montre entre autres que l'hypothèse du corollaire 10.6 implique celle du corollaire 10.7.

Proposition 10.1. *(a) Si $\mathbb{A}$ comme $\mathbb{A}$-module à gauche sur lui-même est semi-simple, alors $\mathbb{A}$ est une somme directe* finie *de sous-modules simples (d'idéaux à gauches minimaux).*

(b) Dans ce cas, $\mathbb{A}$ est artinien et noetherien.

Démonstration. (a) En effet, si $\mathbb{A} = \bigoplus_{i \in I} S_i$, alors 1 s'écrit $1 = \sum_{i \in I} s_i$, $s_i \in S_i$, avec des s_i presque tous nuls ; donc $I = \{i \in I, s_i \neq 0\}$, sinon il existe un $j \in I$ avec $s_j = 0$, et on peut prendre $x \in S_j$, $x \neq 0$; alors on a $x = x \cdot 1 = \sum_{i \in I, s_i \neq 0} x s_i$, ce qui contredit la somme directe.

(b) On a $\mathbb{A} = S_1 \oplus S_2 \oplus \cdots \oplus S_t$, où les S_i sont des modules simples. Alors $\mathbb{A}$ admet la suite de composition

$$0 \subset S_1 \subset S_1 + S_2 \subset \cdots \subset S_1 + S_2 + \cdots + S_t.$$

On applique le théorème 9.7. □

Pour usage ultérieur, mentionnons le lemme suivant.

Lemme 10.3. *Soit M un module artinien et semi-simple.*
(a) M est une somme finie de modules simples ;
(b) M a une suite de composition ;
(c) M est noetherien.

Démonstration. (a) Si M est non nul, il a, étant artinien, un sous-module simple S_1. Comme M est semisimple, on a $M_0 = M = S_1 \oplus M_1$, T_1 sous-module. Si M_1 est nul, c'est fini, sinon on continue avec M_1 qui est semi-simple et artinien : $M_1 = S_2 \oplus M_2$. Et ainsi de suite. Les sous-modules M_i décroissent, donc il y a un M_{i+1} qui est nul. On obtient alors $= S_1 \oplus \cdots \oplus S_i$.

(b) La suite de composiiton s'obtient en considérant les sommes partielles dans (a).

(c) Théorème 9.7. □

Exercice 10.1. *Montrer que le théorème 10.1 implique que tout espace vectoriel a une base.*

10.2 Théorème de Wedderburn-Artin

Théorème 10.2. *(lemme de Schur) Soit $f : M \to N$ un homomorphisme de modules ; on suppose f non nul.*
(a) si M est simple, f est injectif ;
(b) si N est simple, f est surjectif ;
(c) si M, N sont simples, f est un isomorphisme.

Démonstration. Cela découle immédiatement de la définition d'un module simple : dans (a), $\mathrm{Ker}(f)$ est un sous-module propre de M, donc il est nul ; dans (b), $f(M)$ est un sous-module non nul de N donc $f(M) = N$. □

Corollaire 10.8. *Si M est un module simple,* $\mathrm{End}(M)$ *est un corps.*

Théorème 10.3. *Tout $\mathbb{A}$-module à gauche simple est de la forme $\mathbb{A}/I$, où $\mathbb{A}$ est vu comme un module à gauche sur lui-même, et I est un idéal à gauche maximal de $\mathbb{A}$. Réciproquement, tout module de cette forme est simple.*

On voit ainsi que des modules simples existent, car les idéaux à gauche maximaux existent par le lemme de Zorn.

Démonstration. 1. Soit M un module simple, et x un élément non nul de M. Alors $\mathbb{A}x = M$, et la fonction $\mathbb{A} \to M, a \mapsto ax$ est surjective. C'est un homomorphisme de modules à gauche, et son noyau est un idéal à gauche de $\mathbb{A}$. Il doit être maximal, sinon il existe un idéal à gauche J tel que $I \subset J \subset \mathbb{A}$, avec des inégalités strictes, et l'image de J par la fonction précédente est un sous- module non nul et propre de M, contradiction.

2. Réciproquement, soit $M = \mathbb{A}/I$ où I est un idéal à gauche maximal de $\mathbb{A}$. Alors, par le théorème de correspondance 8.2, il n'y a aucun sous-module propre non nul dans M. Donc M est simple. □

Théorème 10.4. *(Artin-Wedderbun) Les conditions suivantes sont équivalentes :*

(a) $\mathbb{A}$ comme module à gauche sur lui-même est semi-simple ;

(b) $\mathbb{A}$ est isomorphe en tant qu'anneau à un produit fini d'anneaux de la forme $\mathbb{K}^{n\times n}$, où $\mathbb{K}$ est un corps.

Démonstration. (b) implique (a) : exercices 10.2 et 10.3.

(a) implique (b) D'après les exercices 10.4 et 10.5, il suffit de montrer que $\mathrm{End}_{\mathbb{A}}(\mathbb{A})$ est un anneau satisfaisant la condition (b). On est donc ramené à montrer que si un module M est une somme directe finie de sous-modules simples, alors $\mathrm{End}(M)$ est un anneau satisfaisant (b). Nous écrivons d'abord $M = \bigoplus M_{ij}$, où les sous-modules M_{ij} sont simples, où les M_{ij} pour i fixés sont isomorphes entre eux, et où M_{ij} et $M_{i'j'}$ ne sont pas isomorphes pour $i \neq i'$. Puis nous définissons $M_i = \bigoplus_j M_{ij}$. Alors $M = \bigoplus M_i$, somme directe finie de sous-modules. D'après le lemme de Schur (théorème 10.2), tout homomorphisme de M_{ij} vers $M_{i'j'}$ est nul quand $i \neq i'$; donc tout homomorphisme $M_i \to M_{i'}$ aussi, en vertu de la composition d'homomorphismes naturels $M_{ij} \hookrightarrow M_i \to M_{i'} \hookrightarrow M_{i'j'}$.

D'après l'exercice 10.6, on est donc ramené au cas où il y a un seul i, c'est-à-dire au cas où M est une somme directe finie de sous-modules simples $S_1, \ldots, S_t$. A COMPLETER □

Exercice 10.2. *Soit $\mathbb{A} = \mathbb{K}^{n\times n}$, où $\mathbb{K}$ est un corps. Montrer que $\mathbb{A}$ est somme directe des idéaux à gauches I_j, où I_j est l'ensemble des matrices dont les éléments en dehors de la colonne j sont nuls. Montrer que I_j est un sous-module simple (un idéal à gauche non nul minimal).*

Exercice 10.3. *Montrer que si $\mathbb{A}_i$, $i = 1, 2$, est un anneau qui est semi-simple comme module à gauche sur lui-même, il en est de même pour $\mathbb{A}_1 \times \mathbb{A}_2$.*

Exercice 10.4. *Montrer que l'anneau opposé de* $\mathbb{A}$ *est isomorphe à* $\mathrm{End}_{\mathbb{A}}(\mathbb{A})$. *Indication : l'isomorphisme envoie* $a \in \mathbb{A}$ *sur* f_a, *avec* $f_a(x) = xa$.

Exercice 10.5. *Montrer que* $\mathbb{A}$ *satisfait la condition (b) du théorème 10.4 si et seulement si l'anneau opposé satisfait cette condition.*

Exercice 10.6. *Montrer que si* $M = M_1 \oplus M_2$ *(somme directe de sous-modules), tel que tout homomorphisme de* M_1 *vers* M_2, *et tout homomorphisme de* M_2 *vers* M_1, *est nul, alors l'anneau* $\mathrm{End}(M)$ *est isomorphe au produit direct des anneaux* $\mathrm{End}(M_1)$ *et* $\mathrm{End}(M_2)$.

10.3 Radical de Jacobson

Définition 10.1. *On appelle* annulateur *d'un* $\mathbb{A}$*-module à gauche* M *l'ensemble* $Ann(M) = \{a \in \mathbb{A}, aM = 0\}$.

De manière équivalente, $a \in Ann(M) \Leftrightarrow aM = 0$.

Proposition 10.2. $Ann(M)$ *est un idéal bilatère. Le module* M *a une structure naturelle de* $\mathbb{A}/Ann(M)$*-module à gauche.*

Démonstration. $Ann(M)$ est le noyau de l'homomorphisme d'anneaux naturel de $\mathbb{A}$ dans $\mathrm{End}_{\mathbb{Z}}(M)$, défini par la structure de $\mathbb{A}$- module de M (voir Proposition 8.1 (ii)). C'est donc un idéal bilatère de $\mathbb{A}$.

Pour la deuxième assertion, on définit l'action de $a+Ann(M)$ sur $m \in M$ par am ; cela ne dépend pas du représentant choisi de la classe de a modulo $Ann(M)$, car si $b \in Ann(M)$, alors $bm = 0$. □

Définition 10.2. *Le* radical de Jacobson *d'un anneau* $\mathbb{A}$, *noté* $rad(\mathbb{A})$ *est l'intersection des annulateurs de tous les modules à gauche simples.*

C'est donc un idéal bilatère.

Théorème 10.5. $rad(\mathbb{A})$ *est l'intersection de tous les idéaux maximaux à gauche de* $\mathbb{A}$.

Démonstration. Soit $x \in rad(\mathbb{A})$. Soit I un idéal à gauche maximal de $\mathbb{A}$. Alors $M = \mathbb{A}/I$ est un module simple (théorème 10.3), donc $xM = 0$; ce qui signifie que $x(a + I) \subset I$ pour tout $a \in A$, donc $xa \in I$, et donc (avec $a = 1$), $x \in I$. Donc x est dans tous les idéaux à gauches maximaux de $\mathbb{A}$.

Réciproquement, soit x satisfaisant la dernière phrase. Soit M un module simple. Soit $m \in M$, non nul ; alors $\mathbb{A}m = M$ (car $\mathbb{A}m$ est un sous-module non nul de M et M est simple ; donc la fonction $a \mapsto am$ de $\mathbb{A}$ dans M

est un homomorphisme surjectif de module ; donc son noyau est un idéal à gauche maximal, x s'y trouve, et donc $xm = 0$. Donc $xM = 0$ et enfin $x \in rad(\mathbb{A})$. □

Le résultat qui suit montre entre autres qu'on aurait pu définir le radical en utilisant les modules à droites, ou les idéaux à droite, et qu'on obtiendrait le même radical.

Théorème 10.6. *$rad(\mathbb{A})$ est l'ensemble des a dans $\mathbb{A}$ tels que $1 - xay$ est inversible quels que soient x, y dans $\mathbb{A}$.*

Lemme 10.4. *Si $a \in rad(\mathbb{A})$, alors $1 - a$ est inversible à gauche.*

Démonstration. Supposons que $J = \mathbb{A}(1 - a) \neq \mathbb{A}$. Alors J est un idéal à gauche propre de $\mathbb{A}$, donc il est contenu dans un idéal à gauche maximal I. Donc $J + rad(\mathbb{A}) \subset I$, ce qui est impossible puisque $1 = (1 - a) + a \in J + rad(\mathbb{A})$. Donc $J = \mathbb{A}(1 - a) = \mathbb{A}$ et $1 - a$ est inversible à gauche. □

Théorème 10.7. *(Lemme de Nakayama) Si M est un module de type fini satisfait $rad(\mathbb{A})M = M$, alors $M = 0$.*

Démonstration. Soit $m_1, \ldots, m_n$ des générateurs de M, avec n minimum. Si $n = 0$, alors $M = 0$, et c'est fini. Supposons, par l'absurde, que $n \geq 1$. Par hypothèse, $m_n \in rad(\mathbb{A})M = M$. Il existe donc des scalaires $a_i \in rad(\mathbb{A})$ tels que $m_n = \sum_{1 \leq i \leq n} a_i m_i$ (voir exercice 10.10). Alors $(1 - a_n)m_n = \sum_{1 \leq i \leq n-1} a_i m_i$. D'après le lemme, $1 - a_n$ a un inverse à gauche, soit b. Alors $m_n = \sum_{1 \leq i \leq n-1} b a_i m_i$. Donc M est engendré par $m_1, \ldots, m_{n-1}$, une contradiction. □

Preuve du théorème 10.6. 1. Soit $a \in rad(\mathbb{A})$. Alors pour tout x, y dans $\mathbb{A}$, $b = xay$ est dans $rad(\mathbb{A})$. Or $1 - b$ est inversible par le lemme, et il existe donc $c \in \mathbb{A}$ tel que $c(1 - b) = 1$. Donc $1 - c = -cb \in I$. Donc par le lemme, $c = 1 - (1 - c)$ a un inverse à gauche. Comme c a déjà un inverse à droite, qui est $1 - b$, c'est aussi son inverse à droite, et ainsi $1 - b$ est inversible.

2. Supposons que $1 - xay$ soit inversible quels que soient x, y dans $\mathbb{A}$. Par l'absurde, supposons que $a \notin rad(\mathbb{A})$. Il existe alors un idéal à gauche maximal I tel que $a \notin I$. Par maximalité $I + \mathbb{A}a = \mathbb{A}$. Alors $1 = y + xa, y \in I, x \in \mathbb{A}$. Mais $y = 1 - xa$ est inversible par hypothèse, donc $I = \mathbb{A}$, une contradiction. □

10.4 Radical, artiniaté et semi-simplicité

Le *produit* IJ de deux parties de $\mathbb{A}$ est par définition le sous-groupe additif de $\mathbb{A}$ engendré par les éléments xy, $x \in I, y \in J$. Le produit ainsi défini des parties de $\mathbb{A}$ est associatif, et on définit I^n par récurrence sur $n \geq 1$.

Un idéal (à gauche, à droite, bilatère) I est dit *nilpotent* s'il existe $n \geq 1$ tel que $I^n = 0$.

Théorème 10.8. *Si $\mathbb{A}$ est artinien, alors son radical est nilpotent.*

Démonstration. Soit $J = rad(\mathbb{A})$. On a $J \supseteq J^2 \supseteq j^3 \supseteq \cdots$. Tous ces idéaux sont bilatères (exercice 10.11), et comme $\mathbb{A}$ est artinien, il existe $n \geq 1$ tel que $J^n = J^{n+1} = J^{n+2} = \cdots$. Nous montrons que $J^n = 0$.

Supposons par l'absurde que $J^n \neq 0$. Soit E l'ensemble des idéaux à gauche I tels que $I^n J \neq 0$. Comme $\mathbb{A}$ est artinien, il existe un élément minimal dans E, soit I. Il existe alors $x \in I$ tel que $J^n x \neq 0$. Alors $J^n x\mathbb{A} \neq 0$, $x\mathbb{A} \subset I$, et $x\mathbb{A} \in E$, donc $I = x\mathbb{A}$ par minimalité.

De plus, $J^n(J^n I) = J^{2n} I = J^n I \neq 0$, donc $J^n I \in E$ et comme $J^n \subset I$, on $J^n I = I$ par minimalité. Mais $I \supseteq JI \supseteq J^n I = I$, donc $JI = I$ et $I = 0$ par le lemme de Nakayama. Donc $J^n I = 0$, une contradiction. □

Nous examinons maintenant le rapport entre la semi-simplicité et la nullité du radical.

Théorème 10.9. *(1) Si $\mathbb{A}$ est semi-simple en tant que module à gauche sur lui-même, son radical est nul.*

(2) Si $rad(\mathbb{A})$ est nul, et si $\mathbb{A}$ est artinien, alors $\mathbb{A}$ est semi-simple en tant que module à gauche sur lui-même.

Lemme 10.5. *Si $rad(\mathbb{A}) = 0$, alors pour tout idéal à gauche minimal J de $\mathbb{A}$, il existe un idéal à gauche I tel que $\mathbb{A} = I \oplus J$.*

Démonstration. Comme $rad(\mathbb{A}) = 0$, I n'est pas contenu dans $rad(\mathbb{A})$, et donc par le théorème 10.5, il existe un idéal à gauche maximal J tel que J ne contient pas I. Montrons que $\mathbb{A} = I \oplus J$. L'intersection $I \cap J$ doit être nulle, sinon c'est un sous-module non nul de I, donc égal à I, et donc $I \subset J$, une contradiction. De plus, $I + J$ est un sur-module de J, donc par maximalité de celui-ci, $I + J = \mathbb{A}$. □

Corollaire 10.9. *Pour tout idéal à gauche H et tout idéal à gauche minimal I contenu dans H, il existe un idéal à gauche J contenu dans H tel que $H = I \oplus J$.*

Démonstration. Il existe par le lemme un idéal à gauche J' tel que $\mathbb{A} = I \oplus J'$. Posons $J = J' \cap H$. Alors la somme $I + J$ est directe. Montrons qu'elle est égal à H. Soit $h \in H$. Alors $h = i + j'$, $i \in I, j' \in J'$. Mais $i, h \in H$. Donc $j' \in H$ et enfin $j' \in J$. Donc $H \subset I + J$ et l'inclusion inverse est claire. □

Preuve du théorème 10.9. (1) Par la proposition 10.1, $\mathbb{A}$ est une somme directe $S_1 \oplus \cdots \oplus S_t$ d'idéaux à gauche minimaux, qui sont des modules simples. Soit $x \in rad(\mathbb{A})$. Alors x est dans l'annulateur de S_I, pour tout $i = 1, \ldots, t$. Comme $1 = s_1 + \cdots + s_t$ ($s_i \in S_i$), on obtient que $x = x \cdot 1 = xs_1 + \cdots + xs_t = 0$.

(2) Soit I_1 un idéal à gauche minimal de $\mathbb{A}$; il existe car $\mathbb{A}$ est artinien. Par le corollaire appliqué à $H = \mathbb{A}$, on trouve un sous-module J_1 tel que $\mathbb{A} = I_1 \oplus J_1$. Si J_1 est non nul, il contient un idéal à gauche minimal de $\mathbb{A}$, car $\mathbb{A}$ est artinien ; on applique le corollaire à J_1, et on trouve $\mathbb{A} = I_1 \oplus I_2 \oplus J_2$, I_2 sous-module simple et J_2 sous-module. Ce processus ne peut pas continuer indéfiniment, car les sous-modules J_i décroisssent strictement, et l'un d'eux va être nul, car $\mathbb{A}$ artinien. Donc il existe t tel que $\mathbb{A} = I_1 \oplus \cdots \oplus I_t$, avec des I_j sous-modules simples, et $\mathbb{A}$ satisfait la conclusion de (2). □

Pour usage dans la preuve du théorème de Hopkins-Levitzki, nous prouvons la

Proposition 10.3. *Soit $J = rad(\mathbb{A})$. Tout $\mathbb{A}/J$-module est un $\mathbb{A}$-module, annulé par J. Réciproquement, tout $\mathbb{A}$-module annulé par J est un $\mathbb{A}/J$-module. Sous cette correspondance, les modules simples sur $\mathbb{A}/J$ ou $\mathbb{A}$ sont les mêmes.*

Démonstration. En effet, l'homomorphisme $A \to \mathrm{End}_{\mathbb{Z}}(M)$ qui définit la structure de $\mathbb{A}$-module sur M s'obtient comme composition $\mathbb{A} \to \mathbb{A}/rad(\mathbb{A}) \to End_{\mathbb{Z}}(M)$, où le premier est la projection canonique et le second l'homomorphisme qui définit la structure de $\mathbb{A}/rad(\mathbb{A})$-module sur M.

La deuxième assertion s'obtient car si le $\mathbb{A}$-module M est annulé par J, alors on peut décomposer $\mathbb{A} \to \mathrm{End}_{\mathbb{Z}}(M)$ comme ci- dessus.

La dernière assertion découle de ce qu'un module est simple si et seulement s'il est isomorphe au quotient de l'anneau par un idéal à gauche maximal. Sachant qu'un tel idéal contient le radical de l'anneau, et en utilisant la bijection naturelle entre les idéaux de $\mathbb{A}$ et ceux de $\mathbb{A}/rad(\mathbb{A})$ qui contiennent $rad(\mathbb{A})$, on obtient qu'il y a bijection entre les idéaux à gauches maximaux de $\mathbb{A}$ et ceux de $\mathbb{A}/rad(\mathbb{A})$. □

Exercice 10.7. *Montrer que le radical de $\mathbb{Z}$ est nul.*

Exercice 10.8. *Montrer que* $rad(\mathbb{A}/rad(\mathbb{A})) = 0$.

Exercice 10.9. *Montrer que* $rad(\mathbb{A}^{n\times n}) = (rad(\mathbb{A}))^{n\times n}$.

Exercice 10.10. *Soit* I *un idéal à gauche* $\mathbb{A}$. *On note* IM *le sous-module du module* M *engendré par les éléments* am, $a \in I, m \in M$. *Montrer que si* M *est engendré par* $m_1, \ldots, m_n$, *alors* IM *est engendré par les élément*am_i, $a \in I, i = 1, \ldots, n$.

Exercice 10.11. *Montrer que si* I *est un idéal à gauche et* $J \subset \mathbb{A}$, *alors* IJ *est un idéal à gauche. Montrer que si* I *est un idéal à gauche et* J *un idéal à droite, alors* IJ *est un idéal bilatère.*

10.5 Théorème de Hopkins-Levitzki

Théorème 10.10. *Tout anneau artinien est noetherien.*

Démonstration. Soit $\mathbb{A}$ un anneau artinien en tant que module à gauche sur lui-même, et J son radical. Par le théorème 10.8, on a la chaîne décroissante de sous-modules à gauche de l'anneau :

$$\mathbb{A} = J^0 \supset J \supset J^2 \supset \cdots \supset J^n = 0.$$

Pour montrer que $\mathbb{A}$ est noetherien, il suffit par le théorème 9.7, de montrer qu'il a un suite de composition, et pour cela, que chaque module $M_i = J^i/J^{i+1}$, $i = 0, \ldots, n-1$, en a une. Soit $\mathbb{B} = \mathbb{A}/J$; $\mathbb{B}$, comme module à gauche sur lui-même, est un module semi-simple (théorème 10.9), car le radical de l'anneau $\mathbb{B}$ est nul (exercice 10.8), et qu'il est artinien (proposition 9.2). On $JM^i = 0$, donc M^i est un $\mathbb{B}$-module. Donc, par le corollaire 10.6, M_i est un module semi-simple ; il est aussi artinien, comme quotient d'un sous-module d'un module artinien (proposition 9.2). Par suite M_i (lemme 10.3) est somme directe finie de $\mathbb{B}$-modules simples. Ces modules sont aussi des $\mathbb{A}$-modules simples (proposition 10.3). Donc M_i a une suite de composition en tant que $\mathbb{A}$-module. □

11 Modules sur un anneau commutatif principal intègre

On considère dans ce chapitre un *anneau commutatif intègre et principal* $\mathbb{A}$: tout idéal de $\mathbb{A}$ est engendré par un élément, donc est de la forme $a\mathbb{A}$, $a \in \mathbb{A}$. Les exemples typiques sont $\mathbb{Z}$ et $\mathbb{K}[x]$, $\mathbb{K}$ corps commutatif. Les modules seront notés à gauche.

Exercice 11.1. *Montrer qu'un anneau commutatif, vu comme module sur lui-même, est un module libre, si et seulement si c'est un anneau est principal.*

Exercice 11.2. *Montrer que l'idéal de $\mathbb{Z}[x]$ engendré par 2 et x n'est pas principal. En déduire que $\mathbb{Z}[x]$ n'est pas un anneau principal.*

11.1 Torsion

Soit M un module à gauche. L'*annulateur* $\{a \in \mathbb{A} \mid am = 0\}$ d'un élément $m \in M$ est un idéal de $\mathbb{A}$. L'*annulateur* $\{a \in \mathbb{A} \mid aN = 0\}$ d'un sous-module N de M est un idéal de $\mathbb{A}$.

Un module est *sans torsion* si l'annulateur de tout élément est nul ; de manière équivalente, l'annulateur de M est nul. Au contraire, on dit qu'un module est *de torsion* si tout élément a un annulateur non nul.

Tout module libre est sans torsion, faire l'exercice 11.3.

Exercice 11.3. *Montrer que tout module libre est sans torsion. En déduire l'existence de $\mathbb{Z}$-modules non libres, et plus généralement, pour tout anneau commutatif qui n'est pas un corps (utiliser un quotient de l'anneau).*

11.2 Mise sous forme diagonale des matrices sur $\mathbb{A}$

On considère les opérations de lignes et de colonnes sur les matrices à coefficients dans $\mathbb{A}$. Les *opérations de lignes* sont de trois sortes :

(i) échanger les lignes i et j, opération notée (ij) ;

(ii) multiplier la ligne i par un scalaire a inversible. Notation : aL_i ;

(iii) ajouter à la ligne i la ligne j multipliée par a, avec $i \neq j$; Notation : $L_i + aL_j$.

Les *opérations de colonnes* sont similaires, et notées avec des C.

Théorème 11.1. *Soit M une matrice à coefficients dans $\mathbb{A}$. Par des opérations de lignes et de colonnes, on peut transformer M en une matrice de la forme*

$$\begin{bmatrix} d_1 & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & d_2 & 0 & \cdots & \cdots & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & & & \vdots \\ 0 & \cdots & 0 & d_r & 0 & \dots & 0 \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \end{bmatrix} \tag{6}$$

où $r \geq 0$, les d_i sont des éléments non nuls de $\mathbb{A}$ avec $d_1|d_2|\cdots|d_r$.

On appellera qu'une matrice est sous *forme diagonale* si elle a cette forme, avec la condition sur la divisibilité. On appelle *diviseurs principaux* les éléments $d_1, \ldots, d_r$.

La preuve ci-dessous donne un algorithme pour mettre la matrice sous forme diagonale ; dans la pratique, on n'a pas besoin de suivre strictement cet algorithme, et l'algorithme est très rapide (du moins sur $\mathbb{Z}$) ; cela vient du fait que l'algorithme euclidien est rapide (de basse complexité).

Démonstration. Nous ne prouvons ce théorème que dans le cas $\mathbb{A} = \mathbb{Z}$, avec la propriété supplémentaire que les d_i sont des entiers naturels. Le cas général n'est pas très différent, mais l'avantage de travailler avec les entiers, c'est que chaque idéal de $\mathbb{Z}$ est engendré par un unique entier naturel, et qu'on pourra faire une récurrence facile sur ceux-ci.

On peut supposer M non nulle. On va montrer qu'on peut transformer M par des opérations lignes et de colonnes en une matrice ayant la forme par blocs

$$\begin{pmatrix} d_1 & \mathbf{0} \\ \mathbf{0} & B \end{pmatrix}, \tag{7}$$

où d_1 est un entier naturel non nul qui divise chaque coefficient de la matrice B (les 0 en gras représentent des matrices lignes et colonnes de la taille appropriée). Par hypothèse de récurrence (sur la taille de la matrice), ce sera suffisant ; en effet, si les coefficients d'une matrice sont divisibles par un entier a, cette propriété est préservée par opérations de lignes et de colonnes.

1. Par permutation de lignes et de colonnes, et par multiplication par -1 au besoin, on peut se ramener à $m_{11} > 0$, et à $m_{11} \leq |m_{ij}|$ pour tous i, j tels que m_{ij} est non nul.

2. Dans la suite de l'algorithme, $|m_1 1|$ n'augmentera pas. A chaque étape de cet algorithme, si la matrice obtenue a un coefficient non nul de valeur absolue plus petite que son coefficient $1, 1$, on retournera à l'étape 1. Cela ne peut se produire qu'un nombre fini de fois.

3. On choisit dans la première colonne un coefficient m_{i1}, avec $i > 1$, et on fait la division euclidienne par m_{11} : $m_{i1} = m_{11}q + r_i$, $0 \leq r_i \leq m_{11}$. On fait l'opération de lignes $L_i - qL_1$, ce qui a pour effet de remplacer m_{i1} par r_i. Si $r_i \neq 0$, on retourne à l'étape 1. Si $r_i = 0$, on prend un autre i. En répétant cette procédure, on obtient comme première colonne

$$\begin{pmatrix} m_{11} \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

4. On fait de même pour la première ligne, avec des opérations de colonnes, ce qui ne modifie pas la première colonne déjà obtenue. On est alors ramené à la forme (7), mais avec la possibilité qu'un coefficient b de B ne soit pas divisible par m_{11}, et on peut se ramener à $b > 0$. On ajoute alors la colonne de b à la première et on obtient comme première colonne

$$\begin{pmatrix} m_{11} \\ \vdots \\ b \\ \vdots \end{pmatrix},$$

avec b sur la ligne i. On retourne à l'étape 3 avec ce i, ce qui a pour effet de remplacer m_{i1} par r_i avec $0 < r_i < m_{11}$, et on retourne à l'étape 1. □

Définition 11.1. *On appelle groupe linéaire d'ordre n de $\mathbb{A}$ le groupe des matrices inversibles dans $\mathbb{A}^{n\times n}$. Notation : $GL_n(\mathbb{A})$.*

Une matrice est dans $GL_n(A)$ si et seulement si son déterminant est inversible dans $\mathbb{A}$.

Corollaire 11.1. *Soit M une matrice de taille $n \times p$. Il existe des matrices $P \in GL_n(\mathbb{A})$ et $Q \in GL_p(\mathbb{A})$ telles que PMQ soit sous forme diagonale.*

Démonstration. Il suffit de montrer que les opérations de colonnes sont simulées par des multiplications par la gauche par des matrices inversibles, et semblablement pour les colonnes. Ceci est tout-à-fait semblable au cas où l'anneau est le corps des réels, voir par exemple [**?**] Proposition 12.5. □

Exercice 11.4. *Mettre sous forme diagonale les matrices suivantes :*

$$\begin{pmatrix} 3 & 1 \\ -1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}, \begin{pmatrix} 3 & 1 & -4 \\ 2 & -3 & 1 \\ -4 & 6 & -2 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}.$$

11.3 Unicité de la forme diagonale

Théorème 11.2. *La forme diagonale du théorème 11.1 est unique. De manière précise, r est le rang de la matrice dans le corps des fractions de $\mathbb{A}$ et les idéaux $d_i\mathbb{A}$ sont complètement déterminés par la matrice : $d_i\mathbb{A}$ est l'idéal engendré par les mineurs d'ordre i de la matrice.*

On peut aussi dire que les éléments d_i sont déterminés à association près : a, b dans $\mathbb{A}$ sont *associés* si et seulement si $a\mathbb{A} = b\mathbb{A}$ si et seulement s'il exste $u \in A$ inversible tel que $a = ub$.

Exemple 11.1.

$$\begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix} \to \begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix}.$$

Le 1-mineurs engendrent $\mathbb{Z}$ et le 2-mineur est 5.

Notons $H_i(M)$ l'idéal engendré par les i-mineurs de M.

Démonstration. 1. Le rang d'une matrice ne change pas après opération de lignes ou de colonnes, d'après le corollaire 11.1. De plus, le rang de la matrice sous la forme diagonale du théorème 11.1 est r. Ceci prouve l'assertion sur le rang.

2. Nous montrons que lors d'une opération élémentaire de lignes ou de colonnes $M \to M'$, on a $H_i(M) = H_i(M')$. On peut déjà s'en convaincre pour les 1-mineurs : le cas le moins facile est une opération de lignes $L_i + aL_j$ (pour les colonnes c'est analogue) ; dans ce cas $m'_{ik} = m_{ik} + am_{jk}$ et les autres m_{sk} sont inchangés, en particulier les m_{jk}, ce qui implique que l'idéal engendré par les coefficients de la matrice est inchangé.

Regardons le cas $i = 2$, auquel nous nous restreindrons, pour simplifier. Une opération de lignes (ij) laisse les 2-mineurs globalement invariants, sauf à multiplier certain d'entre eux par -1. Une opération aL_i laisse certains mineurs invariants et multiple certains d'entre eux pas l'élément inversible a. Considérons une opération de lignes $L_i + \alpha L_j$, et nous prenons $i = 1, j = 2$ pour simplifier ; les 2-mineurs sont inchangés, sauf s'ils sont logés dans les lignes 1 et k, $k \geq 3$, et nous prenons $k = 3$ pour simplifier. On a alors

$$M = \begin{pmatrix} a & b & \cdots \\ c & d & \cdots \\ e & f & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix} \to M' = \begin{pmatrix} a + \alpha c & b + \alpha d & \cdots \\ c & d & \cdots \\ e & f & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix}$$

Le 2-mineur de M' logé en les lignes 1 et 3, et dans les deux premières colonnes (pour simplifier, les autres cas sont similaires) est

$$\begin{vmatrix} a + \alpha c & b + \alpha d \\ e & f \end{vmatrix} = \begin{vmatrix} a & b \\ e & f \end{vmatrix} + \alpha \begin{vmatrix} c & d \\ e & f \end{vmatrix},$$

ce qui implique que $H_2(M) = H_2(M')$.

3. Nous montrons maintenant que si M est sous la forme diagonale du théorème 11.1, alors $H_i(M) = d_1 \cdots d_i \mathbb{A}$ pour $i = 1, \ldots, r$. On voit en effet que les seuls mineurs non nuls de cette matrice sont les mineurs principaux, c'est-à-dire, dont la diagonale sur la diagonal principale de M. Un tel mineur,

s'il est d'ordre i, est, par la propriété de divisibilité, un multiple de $d_1 \cdots, d_i$. Donc $H_i(M) = d_1 \cdots d_i \mathbb{A}$ dans ce cas.

4. Le théorème découle des trois parties précédentes. □

Exercice 11.5. *Retrouver les formes diagonales des matrices de l'exercice 11.4 en utilisant le théorème 11.2.*

Exercice 11.6. *Montrer qu'une matrice carrée sur $\mathbb{A}$ est inversible si et seulement si sa forme diagonale est l'identité.*

Exercice 11.7. *Une matrice élémentaire sur $\mathbb{A}$ est une matrice obtenue par une opération de lignes à partir d'une matrice identité. Montrer que la définition est équivalente si on remplace "lignes" par "colonnes". Montrer que toute matrice inversible sur $\mathbb{A}$ est un produit de matrices élémentaires.*

Exercice 11.8. *Utiliser la mise sous forme diagonale pour résoudre sur $\mathbb{A}$ un système d'équations linéaires sur $\mathbb{A}$.*

11.4 Sous-modules de $\mathbb{A}^p$

Théorème 11.3. *Pour tout sous-module H d'un $\mathbb{A}$-module L libre de rang p, il existe une base $x_1, \ldots, x_p$ de L, $r \geq 0$, et des éléments $d_1, \ldots, d_r$ non nuls de $\mathbb{A}$ tels que $d_1 | d_2 | \cdots | d_r$, et que $d_1 x_1, \ldots, d_r x_r$ est une base de H.*

Lemme 11.1. *Soit H un sous-module de $\mathbb{A}^p$. Il est finiment engendré.*

Démonstration. Si $p = 0$, c'est clair, car $\mathbb{A}^0 = \{0\}$. Supposons $p \geq 1$. Soit $\pi : \mathbb{A}^p \to \mathbb{A}$ la première projection. Alors $\pi(H)$ est un sous-module de $\mathbb{A}$, c'est-à dire un idéal, donc $\pi(H) = a\mathbb{A}$, $a \in \mathbb{A}$. Soit $y \in H$ tel que $\pi(y) = a$.

Par hypothèse de récurrence, $H' = H \cap \{0\} \times \mathbb{A}^{p-1}$ est finiment engendré, car $\{0\} \times \mathbb{A}^{p-1}$ est isomorphe à $\mathbb{A}^{p-1}$.

Nous montrons que y et H' engendrent H, et ça suffira pour montrer que H est finiment engendré. Soit $x \in H$. Alors il existe $b \in \mathbb{A}$ tel que $p(x) = ba$. Alors $p(x - by) = p(x) - bp(y) = ba - ba = 0$. Donc $z = x - by \in H'$, et comme $x = by + z$, nous avons prouvé que y et H' engendrent M. □

Etant donnée une matrice M de taille $n \times p$ sur $\mathbb{A}$, et une base $x_1, \ldots x_p$ d'un module libre L, nous notons $K(M, x)$ le sous-module de $\mathbb{A}^p$ engendré par les vecteurs dont les lignes de M sont les coefficients de ces vecteurs dans cette base.

Lemme 11.2. *Soit $M \to N$ une opération de lignes ou de colonnes de. Si c'est une transformation de lignes, alors $K(M,x) = K(N,x)$. Si c'est une transformation de colonnes, alors il existe une base $y_1, \dots, y_p$ de L telle que $K(M,x) = K(N,y)$.*

Démonstration. Par définition, $K(M,x)$ est engendré par les n vecteurs $v_i = \sum_j m_{ij}x_j$, $i = 1 \dots, n$, correspondant aux n lignes de M.

Clairement, si on échange deux lignes, $K(M,x) = K(N,x)$, car on échnage simplement v_i et v_j parmi les générateurs du sous-module ; si on multiplie une ligne par a inversible, on a clairement l'égalité, car l'un des v_i est multiplié par a ; enfin une opération de lignes $L_i + aL_j$ revient à remplacer v_i par $v_i + av_j$, les autres v_k restant inchangés, et on a donc toujours l'égalité.

Passons aux opérations de colonnes. Si c'est une opération (i,j), alors on prend comme nouvelle base la base obtenue en échangeant x_i et x_j. Si c'est une opération aC_i, a inversible, on remplace x_i par $a^{-1}x_i$. Si c'est une opération $L_s + aL_t$, on remplace x_t par $x_t - ax_s$, les autres inchangés, et ça marche, car $m_{is}x_s + m_{it}x_t = (m_{is} + am_{it})x_s + m_{it}(x_t - ax_s)$.

□

Preuve du théorème 11.3. Le module libre L de rang p est isomorphe à $\mathbb{A}^p$. Nous savons donc grâce au lemme 11.1 que H a un système générateur fini. Choisissons une base $x_1, \dots, x_p$ de L. Prenons ces générateurs et définissons une matrice M dont les n lignes sont les coefficients de ces générateurs dans la base de L choisie ; M est alors une matrice $n \times p$ sur $\mathbb{A}$. Les lignes de M engendrent le sous-module H. On a donc $H = K(M,x)$.

On applique alors itérativement le lemme précédent, et la mise sous forme diagonale de N, et on trouve une base $y_1, \dots, y_p$ de L, telle $K(N,y) = H$. Si $d_1, \dots, d_r$ désignent les diviseurs principaux, on trouve que $d_1y_1, \dots d_ry_r$ engendrent H, et ils en forment une base, puisqu'ils ont linéairement indépendants, car $\mathbb{A}$ est intègre. □

Corollaire 11.2. *Tout sous-module d'un $\mathbb{A}$-module libre finiment engendré d'un module libre de rang p est un module libre de rang $\leq p$.*

On notera que, réciproquement, si un anneau satisfait à la propriété du corollaire, alors il est nécessairement principal.

Exercice 11.9. *Montrer que si f est une application linéaire d'un $\mathbb{A}$-module libre M vers un autre N, tous deux finiment engendrés, alors il existe une base $m_1, \dots, m_p$ de M et une base $n_1, \dots, n_l$ de N, telles que $f(m_i) = d_in_i$*

pour $i = 1, \dots, r$ et $f(n_i) = 0$ pour $i > r$, où les d_i sont des scalaires non nuls et $d_1|d_2|\dots|d_r$.

Exercice 11.10. *Trouver une base du sous-groupe de $\mathbb{Z}^3$ engendré par $(1, 0, -1), (2, -3, 1), (0, 3, 1)$ et $(3, 1, 5)$.*

11.5 Structure des $\mathbb{A}$-modules finiment engendrés

Théorème 11.4. *Tout $\mathbb{A}$-module finiment engendré M est isomorphe à un module de la forme*

$$\mathbb{A}^s \times \mathbb{A}/c_1\mathbb{A} \times \cdots \times \mathbb{A}/c_t\mathbb{A}, \tag{8}$$

où $s, t \in \mathbb{N}$, et où les $c_i \in \mathbb{A}$ sont non nuls, non inversibles, et satisfont $c_1|\cdots|c_t$.

Démonstration. Supposons que M soit engendré par p vecteurs. Il existe un module libre de rang p, un homomorphisme surjectif de $\mathbb{A}$-modules $\pi : L \to M$. Alors M est isomorphe à L/H où $H = \mathrm{Ker}(\pi)$. Il existe une base $x_1, \dots, x_p$ de $L, r \in \mathbb{N}$, et des éléments non nuls $d_1, \dots, d_r$ tels que $d_1|\cdots|d_r$ et que $d_1x_1, \dots, d_rx_r$ est une base de H. Par isomorphisme, on est ramené à $L = \mathbb{A}^p$ et que H est le sous-module engendré par $d_1e_1, \dots, d_re_r$, où les e_i forment la base canonique de $\mathbb{A}^p$ (voir exercice 11.11).

Donc M est isomorphe à $N = A^p/(d_1\mathbb{A}) \times \cdots (d_r\mathbb{A}) \cdots \{0\}^{p-r}$. Considérons l'homomorphisme canonique de $\mathbb{A}$-modules

$$\varphi : \mathbb{A}^p \to \mathbb{A}/d_1\mathbb{A} \times \cdots \times \mathbb{A}/d_r\mathbb{A} \times \mathbb{A}^{p-r}.$$

Son noyau est $(d_1\mathbb{A}) \times \cdots (d_r\mathbb{A}) \cdots \{0\}^{p-r}$, c'est-à-dire H. Donc M est isomorphe N.

Il suffit pour conclure de voir que si d_i est inversible, alors $d_i\mathbb{A} = \mathbb{A}$ et donc $\mathbb{A}/d_i\mathbb{A} = \{0\}$. De plus, si d_i non inversible, alors ses multiples ne le sont pas non plus. Il existe donc k tels que $d_1, \dots, d_k$ sont inversibles et $d - k + 1, \dots, d_r$ ne le sont pas. On posera donc $t = r - k$, $s = p - r$, $c_1 = d_{k+1}, \dots, c_t = d_r$. □

Corollaire 11.3. *Tout module finiment engendré sans torsion est libre.*

Rappelons qu'un élément p de $\mathbb{A}$ est dit *irréductible* s'il n'est pas nul ni inversible, et si toute factorisation $p = qr$ dans $\mathbb{A}$ implique que q ou r est inversible.

Corollaire 11.4. *Tout module finiment engendré est isomorphe à un produit d'un module libre par un produit de modules de la forme $\mathbb{A}/p^k\mathbb{A}$, p irréductible dans $\mathbb{A}$, $k \geq 1$.*

Lemme 11.3. *(Théorème chinois) Si* $c = p_1^{k_1} \cdots p_n^{k_n}$, *où les* p_i *sont irréductibles et distincts dans* $\mathbb{A}$ *et où les* k_i *sont* ≥ 1, *alors*

$$\mathbb{A}/c\mathbb{A} \simeq \prod_{1 \leq i \leq n} \mathbb{A}/p_i^{k_i}\mathbb{A}.$$

Exercice 11.11. *Montrer que si on a un isomorphisme de modules* $L_1 \to L_2$, *qui envoie le sous-module* H_1 *sur* H_2, *alors il induit un isomorphisme* $L_1/H_1 \to L_2/H_2$.

11.6 Unicité de cette structure

Théorème 11.5. *Dans le théorème 11.4,* s, t *et les idéaux* $c_i\mathbb{A}$ *ne dépendent que du module* M.

Exercice 11.12. *Montrer que* $\{m \in M \mid \exists a \in \mathbb{A}, a \neq 0, am = 0\}$ *est un sous-module du module* M.

11.7 Application 1 : groupes abéliens finiment engendrés

On prend $\mathbb{A} = \mathbb{Z}$. Comme $\mathbb{Z}$-modules = groupes abéliens, on obtient le

Théorème 11.6. *Soit* G *un groupe abélien finiment engendré.*

(i) $G \simeq L \times G_*$, *où* L *est libre de rang fini et* G_* *est fini.*

(i) Il existe des entiers $t \geq 0$ *et* $2 \leq c_1 | c - 2 | \ldots | c_t$, *entièrement déterminés par la classe d'isomorphisme de* G, *tels que*

$$G_* \simeq \prod_{1 \leq i \leq t} \mathbb{Z}/d_i\mathbb{Z}.$$

(ii) Il existe un multi-ensemble fini F *de puissances non triviales de nombres premiers, entièrement déterminé par la classe d'isomorphisme de* G, *tel que*

$$G_* \simeq \prod_{p^k \in P} \mathbb{Z}/p^k\mathbb{Z}.$$

(iii) G *est libre si et seulement s'il est sans torsion.*

Exercice 11.13. *Trouver les classes d'isomorphisme des groupes abéliens d'ordre 400.*

Exercice 11.14. *A quelle condition un groupe abélien fini contient-il un sous-groupe isomorphe à $\mathbb{Z}/2\mathbb{Z}$? A $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$?*

Exercice 11.15. *Si G est comme dans (8), avec $\mathbb{A} = \mathbb{Z}$, quel est l'ordre maximum d'un élément de G ?*

Exercice 11.16. *Montrer qu'un sous-groupe de $\mathbb{Z}^2$, de rang 2, a une unique base de la forme $(a, 0), (c, d)$, où a, c, d sont des entiers avec $a, d > 0$ et $0 \leq c < a$. Montrer que l'index du sous-groupe (c'est-à-dire la cardinalité du quotient) est ad. Montrer que le nombre de sous-groupes de $\mathbb{Z}^2$ d'index n est égal à la somme des diviseurs de n.*

11.8 Application 2 : réduction d'un endomorphisme d'un espace vectoriel

On prend

$$\mathbb{A} = \mathbb{K}[x],$$

où $\mathbb{K}$ est un corps commutatif. On considère dans la suite un espace vectoriel V fixé sur $\mathbb{K}$ et un endomorphisme fixé f de V. Rappelons la notation $P(f)$ si $P \in \mathbb{K}[x]$, obtenue en remplaçant x par f dans le polynôme P. Alors $P(f)$ désigne un endomorphisme de V.

L'espace V devient un $\mathbb{A}$-module par l'action $Pv = P(f)(v)$, $P \in \mathbb{A}, \in V$. Notons que la structure d,espace vectoriel de V s'obtient de sa structure de $\mathbb{A}$-module en restreignant l'opération externe de celui-ci au sous-corps $\mathbb{K}$ de $\mathbb{A}$. Autrement dit, si P est un polynôme constant, la notation Pv désigne le produit externe, dans le $\mathbb{K}$-espace vectoriel V, du scalaire $P \in \mathbb{K}$ par le vecteur v.

Le $\mathbb{A}$-module V est un module de torsion, car les endomorphismes $f^n, n \in \mathbb{N}$ ne peuvent pas être linéairement indépendants sur $\mathbb{K}$. En fait, par le théorème de Cayley-Hamilton, le polynôme caractéristique est dans l'annulateur de tout $v \in V$; en fait, $P(f) = 0$ si P est le polynôme caractéristique

Il existe un polynôme P, de coefficient dominant 1, de degré minimum, tel que $P(f) = 0$, et c'est le polynôme minimal de f. Le polynôme minimal divise le polynôme caractéristique, et il est le générateur de l'idéal de $\mathbb{A}$ formé de polynômes qui sont dans l'annulateur de tous les éléments de V. Voir le cours d'algèbre linéaire 2 [**?**].

Rappelons qu'un espace vectoriel est dit *cyclique* sous l'action de f s'il existe $v \in V$ tel que les $f^n(v)$ engendrent V comme espace vectoriel. Autrement dit, V est un $\mathbb{A}$-module cyclique (ou monogène).

Théorème 11.7. *Si V est cyclique, alors le polynôme minimal de f est égal à son polynôme caractéristique, soit P, et V comme $\mathbb{A}$-module est isomorphe à $\mathbb{A}/P\mathbb{A}$. Modulo cet isomorphisme, V a pour base les classes de $1, x, \ldots, x^{n-1}$, $\deg(P) = n$. Si $P = x^n - a_1x^{n-1} - \cdots - a_0$, alors l'action de f sur V est entièrement décrite sur cette base par $1 \to x, x \to x^2, \ldots, x^{n-2} \to x^{n-1}, x^{n-1} \to a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$; autrement dit , la matrice de f dans cette base est la matrice compagne de P.*

Voir [**?**], chapitre 16. Appelons *diviseur* ce polynôme P, dans le cas où V est cyclique sous l'action de f ; c'est un polynôme non constant (en excluant le cas où $V = 0$).

En général, un espace vectoriel n'est pas cyclique, mais on a le résultat suivant, dont la première assertion découle immédiatement du théorème 11.4

Théorème 11.8. *L'espace V est une somme directe de sous-espaces cycliques, avec diviseurs $P_1|P_2|\cdots|P_k$. Ceux-ci sont uniquement déterminés par f, si on les prend unitaires. De plus, P_k est le polynôme minimal de f et son polynôme caractéristique est $P_1 \cdots P_k$.*

On appellera *invariants* de f les polynômes $P_1, \ldots, P_k$. On peut aussi déduire la forme de Jordan du Corollaire 11.4.

Corollaire 11.5. *Si $\mathbb{K}$ est algébriquement clos, il existe une base de Jordan pour f.*

Démonstration. D'après le corollaire cité, le $\mathbb{A}$-module V est somme directe se $\mathbb{A}$-modules de la forme $\mathbb{A}/(x-\lambda)^k\mathbb{A}$, puisque les polynômes irréductibles dans $\mathbb{K}[x]$ sont de degré 1. Ce dernier $\mathbb{K}$-espace vectoriel a pour base $e_1 = 1, e_2 = x - \lambda, \ldots, e_k = (x-\lambda)^{k-1}$ modulo $x - \lambda$. Et on a modulo $(x-\lambda)^k$: $xe_1 = x = x - \lambda + \lambda = e_2 + \lambda e_1$, $xe_2 = x(x-\lambda_2) = (x-\lambda)^2 + \lambda(x-\lambda) = e_3 + \lambda e_2$, $\ldots$, $xe_k = x(x-\lambda)^{k-1} = (x-\lambda)^k + \lambda(x-\lambda)^{k-1} = \lambda e_k$. Ce qui domne un bloc de Jordan d'ordre k avec valeur propre λ. □

On peut calculer les diviseurs de f de la manière suivante.

Théorème 11.9. *Soit M la matrice de f dans une base $v_1, \ldots, v_n$ de V, de dimension n. Les invariants de f sont les diviseurs non constants de la matrice $xI_n - M$.*

Démonstration. 1. Considérons l'homomorphisme u de $\mathbb{A}$-module qui envoie l'élément e_i de la base canonique de $\mathbb{A}^n$ sur v_i. Il existe car $\mathbb{A}$ est un $\mathbb{A}$-module libre. Nous identifions dans la suite $\mathbb{A}^n$ avec $\mathbb{A}^{n\times 1}$ (matrices-colonnes). Nous montrons que le noyau de u est engendré comme $\mathbb{A}$-module par les colonnes

de la matrice $xI_n - M$. On a en effet $f(v_j) = \sum_i m_{ij} v_i$, donc $u(xe_j - \sum_i m_{ij} e_i) = xu(e_j) - \sum_i m_{ij} u(e_i) = xv_j - \sum_i m_{ij} v_i = f(v_j) - \sum_i m_{ij} v_i = 0$. Donc la j-ème colonne de $xI_n - M$ est dans le noyau de u.

Soit H le sous-$\mathbb{A}$-module de $\mathbb{A}^n$ engendré par les colonnes de $xI_n - M$. Nous venons de voir que H est contenu dans le noyau de u. Pour prouver l'inclusion réciproque, notons que, considérant $\mathbb{K}^n$ somme un sous- ensemble de $\mathbb{A}^n$, on a $\mathrm{Ker}(u) \cap \mathbb{K}^n = 0$; en effet, si $m \in \mathrm{Ker}(u) \cap \mathbb{K}^n$, alors $m = \sum_i a_i e_i$, $a_i \in \mathbb{K}$, et on a $0 = u(m) = \sum_i a_i v_i$ (u est $\mathbb{A}$-linéaire, donc $\mathbb{K}$ linéaire), et les a_i doivent être nuls, et m aussi. Nous avons $xe_j \equiv \sum_i m_{ij} e_i$ modulo H ; il s'ensuit récursivement que tout $m \in \mathbb{A}^n$ est congru modulo H à une combinaison $\mathbb{K}$-linéaire $\sum_i a_i e_i$. Prenons $m \in \mathrm{Ker}(u)$; on aura alors $m \equiv \sum_i a_i e_i$ modulo H. Mais comme $H \subset \mathrm{Ker}(u)$, $\sum_i a_i \in \mathrm{Ker}(u)$, donc les a_i son tous nuls. Donc $m \equiv 0$ modulo H, et $m \in H$.

2. Nous revenons à la notation usuelle pour A^n, dont les éléments sont donc des lignes. Alors $\mathrm{Ker}(u) = K(xI_n - {}^tM)$, avec les notations de la section 11.4. Le théorème se déduit alors de la démarche suivie dans la preuve des théorèmes 11.3 et 11.4, en remarquant que les diviseurs d'une matrice et de sa transposée sont les mêmes. □

Ce théorème permet entre autres de calculer le polynôme minimal d'un endomorphisme ou d'une matrice carrée : c'est en effet le premier invariant de $xI_n - M$.

Corollaire 11.6. *Deux endomorphismes de V sont conjugués si et seulement s'ils ont même invariants.*

Démonstration. Ils ont en effet la même matrice dans deux bases de V. □

Corollaire 11.7. *Soient A, B deux matrices carrées de même ordre sur $\mathbb{K}$ et $\mathbb{L}$ un sur-corps de $\mathbb{K}$. Alors A, B sont sont conjuguées dans $\mathbb{K}^{n\times n}$ si et seulement si elle sont conjuguées dans $\mathbb{L}^{n\times n}$.*

Démonstration. A cause de leur unicité, calculer les diviseurs de $xI_n - M$ dans $\mathbb{K}[x]$ ou dans $\mathbb{L}[x]$, c'est la même chose. □

Exercice 11.17. *Montrer qu'un espace est cyclique si et seulement si le polynôme caractéristique de f est égal à son polynôme minimal.*

Exercice 11.18. *Montrer que V est irréductible (c'est-à-dire n'a pas de sous-espace stable sous f, autre que 0 est V) si et seulement si le polynôme caractéristique de f est irréductible.*

Quatrième partie

Solution de certains exercices

6.9 L'injection $\mathbb{Q} \to \mathbb{R}$.

9.2 On définit une fonction $f : E \to \mathcal{P}^*(E)$ par $f(P) = \{Q \in E, Q \subset P, P \neq Q\}$. Soit $F : \mathcal{P}^*(E) \to E$ une fonction de choix. On définit $g : E \to E, g = F \circ f$. Alors la suite de sous-modules $g^n(P)$, $n \in \mathbb{N}$, est strictement décroissante.

Références

[1] Luc Bélair, Algèbre, Notes de cours, UQAM. 3

Index

$\mathbb{A}^{op}$, 21

anneau opposé, 21
annulateur, 40
artinien, 28
associé, 47
axiome du choix, 5

base, 22
bon ordre, 9

catégorie, 10
chaine, 6
classe, 10
comparables, 6
complets, 29
coproduit, 14
cyclique, 24

diviseurs principaux, 46
dual, 21
duale, 11
décomposition de l'identité, 29

essentiellement surjectif, 17

final, 12
finiment engendré, 22
foncteur, 14
foncteur contravariant, 15
foncteur covariant, 15
fonction de choix, 5

homomorphisme de module, application linéaire, 21

inductif, 7
initial, 12
invariants, 54
irréductible, 51
isomorphisme, 12
isomorphisme naturel, 16

libre, 22
linéairement indépendants, 22
localement petite, 11
longueur, 32

majoré, 6
maximal, 6, 8
mesure de Lebesgue, 5
minimal, 37
module, 19
monogène, 24
monomorphisme, 12
morphismes, 10

nilpotent, 42
noetherien, 28

objet, 10
opérations de colonnes, 45
opérations de lignes, 45
orthogonaux, 29

partie fractionnaire, 6
pleinement fidèle, 17
produit, 13, 42
propriété universelle, 13, 22, 23

quotients, 32

radical de Jacobson, 40
rang, 22

sans torsion, 45
section, 4
semi-simple, 35

simple, 31, 32
simplifiable, 12
sous-groupe dérivé, 15
sous-module, 21
suite normale, 32
support, 24

théorème de Hilbert, 29
torsion, 45
transformation naturelle, 16
type fini, 22

épimorphisme, 12
équivalentes, 32