Cours de mathématiques

TOME V

ALGÈBRE LINÉAIRE

Mathématiques générales

France $\sim$ 2024

Écrit et réalisé par Louis Lascaud

Table des matières

1 Théorie générale des espaces vectoriels 7

1.1 Applications linéaires . . . 7

1.1.1 Noyaux . . . 7

1.1.2 Théorème du rang . . . 7

1.1.3 Formes linéaires . . . 8

1.1.3.1 Propriétés fondamentales . . . 8

1.1.3.2 Considérations cardinales . . . 9

1.2 Théorie de la dimension . . . 9

1.2.1 Dimension quelconque . . . 9

1.3 Espaces vectoriels quotients . . . 12

1.4 Matrices . . . 16

1.4.1 Définition générale de $\mathfrak{M}_{I\times J}(E)$ . . . 16

1.4.1.1 Définition de l'objet matriciel . . . 16

1.4.2 Classes de matrices particulières . . . 16

1.4.2.1 Matrices triangulaires . . . 16

1.4.3 Matrices à coefficients dans un anneau . . . 18

1.4.3.1 Opérations sur les matrices . . . 18

1.4.3.2 Matrices élémentaires . . . 18

1.4.4 Propriétés algébriques des anneaux de matrices . . . 19

1.4.4.1 Commutant . . . 19

2 Réduction 21

2.1 Généralités . . . 22

2.1.1 Relation de similitude des matrices . . . 22

2.1.2 Notion de stabilité par un endomorphisme . . . 24

2.1.3 Éléments propres . . . 25

2.2 Diagonalisation . . . 27

2.3 Réduction des endomorphismes auto-adjoints . . . 27

2.4 Jordanisation . . . 28

2.4.1 Généralités sur la jordanisation . . . 28

2.4.2 Preuve du théorème de Jordan . . . 28

2.4.3 Opérations sur les blocs de Jordan . . . 28
2.5 Décompositions factorielles de matrices . . . 29
2.5.1 Décomposition J_r . . . 30
2.5.2 Décomposition LU . . . 30
2.5.3 Décomposition de Cholesky (LU pour les $\mathcal{S}_n^{++}$ . . . 30
2.5.4 Décomposition QR (ou décomposition d'Iwasawa) et décomposition de Householder . . . 30
2.5.5 Décomposition ΩS (ou décomposition polaire) . . . 30

3 Compléments de topologie matricielle 31
3.1 Normes matricielles . . . 31
3.1.1 Normes subordonnées matricielles . . . 31
3.1.2 Localisation des valeurs propres . . . 32

4 Théorie des modules 33
4.1 Modules sur un anneau . . . 33
4.1.1 Premières considérations . . . 33
4.1.1.1 Définition . . . 33
4.1.1.2 Sous-modularité . . . 36
4.1.1.3 Le module nul . . . 38
4.1.1.4 Morphismes de modules . . . 38
4.1.1.5 Produits et sommes de modules . . . 41
4.1.1.6 Somme de sous-modules . . . 43
4.1.1.7 Modules quotients . . . 44
4.1.1.8 Suites exactes de modules . . . 45
4.1.1.9 Bimodules . . . 47
4.1.2 Produit tensoriel entre modules . . . 48
4.1.2.1 Introduction : cas des espaces vectoriels . . . 48
4.1.2.2 Produit tensoriel de deux modules . . . 49
4.1.2.3 Produit tensoriel d'algèbres . . . 53
4.1.2.4 Produits tensoriels infinis, algèbre tensorielle . . . 53
4.1.2.5 Extension du corps de base, complexification . . . 53
4.2 Produit extérieur entre modules . . . 54
4.2.1 Algèbre extérieure . . . 54
4.3 Théorie de la dimension des modules . . . 54
4.3.1 Module de type fini . . . 54
4.3.1.1 Anneaux finis sur un autre . . . 57
4.3.1.2 Lemme de Nakayama . . . 57
4.3.2 Module noethérien . . . 59
4.3.2.1 Théorème de transfert de Hilbert . . . 62

4.3.3 Module cyclique . . . 63
4.3.4 Algèbre de type fini . . . 64
4.3.5 Module libres et module de torsion . . . 66
4.3.5.1 Vocabulaire de la dimension pour les modules . . . 66
4.3.5.2 Annulateur d'un module . . . 69
4.3.5.3 Preuve du théorème fondamental de la dimension . . . 70
4.3.5.4 Notion de torsion . . . 71
4.3.5.5 Modules de fractions . . . 77
4.3.5.6 Preuve du théorème du supplémentaire . . . 80
4.3.5.7 Suites exactes courtes scindables entre modules . . . 81
4.3.6 Modules sur un anneau principal . . . 84
4.3.6.1 Résultats généraux sur la principalité sur les modules . . . 84
4.3.6.2 Modules de torsion sur un anneau principal . . . 86
4.3.6.3 Décomposition des parties p-primaires et facteurs invariants d'un module . . . 88
4.3.6.4 Classification des modules de type fini sur un anneau principal : théorème de Kronecker . . . 88
4.3.6.5 Détermination pratique du rang partiel et des facteurs invariants dans la décomposition de Kronecker . . . 89
4.3.7 Projectivité, platitude . . . 90
4.3.7.1 Modules projectifs . . . 90
4.3.7.2 Modules plats . . . 91
4.3.7.3 Modules injectifs . . . 93

5 Espaces préhilbertiens 95
5.1 Matrices symétriques, hermitiennes ; orthogonales, unitaires . . . 95
5.1.1 Vocabulaire des espaces préhilbertiens réels ou complexes . . . 95
5.2 Topologie des espaces préhilbertiens . . . 97
5.2.1 Inégalité de Bessel, égalité de Parseval . . . 97

6 Théorie de Lie 99
6.1 Introduction aux algèbres de Lie et à leurs représentations . . . 100
6.1.1 Définitions générales . . . 100
6.1.1.1 Algèbres de Lie, crochet de Lie . . . 100
6.1.1.2 Sous-algèbres de Lie, algèbres de Lie quotients . . . 101
6.1.1.3 Morphismes d'algèbres de Lie . . . 101
6.1.1.4 Opposition d'algèbres de Lie . . . 102
6.1.1.5 Sommes d'algèbres de Lie . . . 102
6.1.1.6 Quelques exemples d'algèbres de Lie . . . 103
6.1.1.7 Notion de représentation adjointe (un peu tôt) . . . 105

6.1.1.8 Dérivations de Lie . . . 106
6.1.1.9 Idéaux de Lie . . . 106
6.1.1.10 Algèbres de Lie abéliennes . . . 107
6.1.1.11 Séries dérivées, centrales . . . 108
6.1.1.12 Normalisateurs, centralisateurs dans une algèbre de Lie . . . 109
6.1.1.13 Représentations fidèles d'algèbres de Lie . . . 110
6.1.1.14 Extensions d'algèbres de Lie . . . 111
6.1.1.15 Produits semi-directs d'algèbres de Lie . . . 112
6.1.1.16 Algèbres enveloppantes . . . 113
6.1.2 Représentation des algèbres de Lie . . . 115
6.1.3 Classification des algèbres de Lie semi-simples . . . 118
6.1.4 Classification des représentations des algèbres de Lie semi-simples . . . 118
6.1.5 Formule des caractères de Weyl . . . 118
6.2 Théorie des représentations des algèbres de Lie semi-simples . . . 118
6.2.1 Aspects catégories . . . 118
6.2.2 Catégorie $\mathcal{O}$ . . . 118
6.3 Représentations et géométrie algébrique . . . 118
6.3.1 Groupes algébriques . . . 118
6.3.2 Variétés de drapeaux . . . 118
6.3.3 Théorie de Springer . . . 118

7 Exercices **119**

Chapitre 1

Théorie générale des espaces vectoriels

Résumé

Voici la théorie de base des espaces vectoriels telle qu'elle est enseignée actuellement dans les petites classes : généralités sur la structure linéaire, applications entre espaces vectoriels, notion de décomposition, théorie de la dimension, formalisme matriciel, multilinéarité.

1.1 Applications linéaires

1.1.1 Noyaux

1.1.2 Théorème du rang

Lemme. ***(Théorème d'isomorphisme noyau-image)***

Soient E,F deux K-espaces vectoriels et soit $u : E \to F$ une application linéaire. Alors tout supplémentaire de $\mathrm{Ker}(u)$ dans E est isomorphe à $\mathrm{Im}(f)$.

Exercice 1 *(Nilpotents d'ordre 2 dans $\mathbb{R}^3$)*

Soit f un endormorphisme de l'espace à trois dimensions tel que $f \circ f = 0$. Montrer qu'il existe un vecteur $v \in \mathbb{R}^3$ et une forme linéaire g telle que $f : u \mapsto g(u)v$.

▷ **Éléments de réponse.**

Remarquer que $r = \mathrm{rg}(f) = 1$. En effet, $\mathrm{Im}(f) \subseteq \mathrm{Ker}(f)$ d'où $r \leqslant 3 - r$, soit $r \leqslant \frac{3}{2}$. On a donc deux petits cas à traiter.

Conséquence. ***(Factorisation des noyaux emboîtés)***

Soient E,F,G trois K-espaces vectoriels. Soient $u \in \mathcal{L}(E,F)$ et $w \in \mathcal{L}(E,G)$ tels que $\mathrm{Ker}(u) \subseteq \mathrm{Ker}(w)$. Alors il existe $v \in \mathcal{L}(F,G)$ tel que $w = v \circ u$.

▷ Soit E_0 un supplémentaire de $\mathrm{Ker}(u)$ dans E. Alors il existe un isomorphisme $u' : E_0 \to \mathrm{Im}(u)$. Soit F_0 un supplémentaire de $\mathrm{Im}(u)$ dans F. On définit v sur F en la posant nulle sur F_0 et pour $x \in \mathrm{Im}(u)$, $v(x) = w(u'^{-1}(x))$. Alors sur $\mathrm{Ker}(u)$, $v \circ u$ est bien nulle et sur E_0, on a bien $v(u(x)) = w(u'^{-1}(u(x))) = w(x)$. ■

Citons semblablement :

Conséquence. ***(Factorisation des images emboîtées)***

Soient E,F,G trois K-espaces vectoriels. Soient $u \in \mathcal{L}(E,G)$ et $w \in \mathcal{L}(F,G)$ tels que $\mathrm{Im}(u) \subseteq \mathrm{Im}(w)$. Alors il existe $v \in \mathcal{L}(E,F)$ tel que $u = w \circ v$.

▷ Notons w' l'inverse à gauche de w, qui est un morphisme, car les morphismes injectifs dans k-Vect sont rétractables (il suffit de définir l'inverse à gauche nul sur un complémentaire de l'image). Posons $v = w' \circ u$. Alors si $x \in E$, $u(x) \in \mathrm{Im}(u) \subseteq \mathrm{Im}(w)$, soit $v(x) = w(t)$ pour un $t \in E$, puis $w \circ w' \circ w(t) = w(t) = v(x)$ d'où $w \circ v = u$. ■

1.1.3 Formes linéaires

1.1.3.1 Propriétés fondamentales

Propriété. ***(Noyau d'une forme linéaire)***

Le noyau d'une forme linéaire non nulle est un hyperplan.

Propriété. ***(Réciproque au noyau d'une forme linéaire)***

Tout hyperplan d'un espace est le noyau d'au moins une forme linéaire, ipso facto non nulle.

▷ Soit E est un espace vectoriel et H un hyperplan de E. Alors par définition, E/H est de dimension 1, donc isomorphe à K. En prenant un vecteur non nul de E/H, on a donc une injection $E/H \hookrightarrow K$ que l'on peut donc relever en $\varphi : E \to K$ de noyau H. ■

On a également :

Propriété

Soient f_1,...,f_r et f des formes linéaire sur un espace vectoriel E sur un corps k avec $r \in \mathbb{N}$. Alors f est combinaison linéaire des f_1,...,f_r si et seulement si $\bigcap_{i=1}^{r} \mathrm{Ker}(f_i) \subseteq \mathrm{Ker}(f)$.

▷ Le sens direct ne pose pas problème. Réciproquement, on considère $u(x) = (f_1(x),...,f_(x))$. Alors $\mathrm{Ker}(u) \subseteq \mathrm{Ker}(f)$ donc il existe par un lemme précédent une forme linéaire v sur K^n, qui s'écrit donc $v(k_1,...,k_n) = \sum \lambda_i k_i$, avec $f = v \circ u$, autrement dit $f = \sum \lambda_i f_i$. ■

Corollaire

Deux formes linéaires non nulles sont proportionnelles si et seulement si elles définissent le même hyperplan.

1.1.3.2 Considérations cardinales

Remarquer que, même s'il facilite les choses en dimension finie, on n'a pas du tout besoin du théorème du rang.

Propriété. ***(Injectivité des formes linéaires)***

Soit E un $\mathbb{K}$-espace vectoriel, $\mathbb{K}$ un corps. On suppose que E est de dimension $\geqslant 2$. Une forme linéaire sur E ne peut être injective.

▷ Une forme linéaire est en particulier une application linéaire de E dans $\mathbb{K}$. Or $\mathbb{K}$ est de dimension 1 sur $\mathbb{K}$, et par hypothèse, E est de dimension > 1. Ainsi, par dimension, cette forme linéaire ne peut être injective. ■

Propriété. ***(Surjectivité des formes linéaires)***

Soit E un $\mathbb{K}$-espace vectoriel, $\mathbb{K}$ un corps. Toute forme linéaire non nulle sur E est surjective.

▷ L'image d'une forme linéaire est un sous-espace vectoriel de l'espace d'arrivée. Or les sous-espaces vectoriels de $\mathbb{K}$ sont $\{0\}$, ce qui correspond au cas où la forme est nulle, ou $\mathbb{K}$ lui-même, ce qui termine la preuve. ■

1.2 Théorie de la dimension

1.2.1 Dimension quelconque

Commençons par établir le résultat fondamental de la dimension infinie quelconque que nous connaissons déjà en dimension finie.

Théorème. ***(Théorème de la base incomplète)***

Dans un espace vectoriel E quelconque sur $\mathbb{K}$, de toute famille génératrice $\mathcal{G}$, pour toute famille libre $\mathcal{L}$ incluse dans $\mathcal{G}$, on peut trouver une famille de vecteurs contenue dans $\mathcal{G}$ et contenant tous les vecteurs de $\mathcal{L}$ qui soit une base de E.

▷ Cet énoncé est plus précis que ce dont nous avons besoin, mais nous le montrons sous cette forme cependant. Soit E un espace vectoriel sur $\mathbb{K}$, $\mathcal{G}$ une famille génératrice de vecteurs de E, c'est-à-dire telle que tout vecteur de E se décompose comme combinaison linéaire finie de vecteurs

de $\mathcal{G}$, et $\mathcal{L}$ une famille libre de vecteurs de E, c'est-à-dire telle que toute combinaison linéaire d'un nombre fini de ses vecteurs et nulle soit triviale.

Soit $\mathcal{F}$ l'ensemble des familles libres telles que $\mathcal{L} \subseteq \mathcal{L}' \subseteq \mathcal{G}$, en identifiant sans problème une famille à l'image de son support. L'ensemble $\mathcal{F}$ est alors partiellement ordonné par l'inclusion en tant que sous-ensemble de l'ensemble des parties de E. Montrons que $\mathcal{F}$ est un ensemble inductif. Il est non vide, car par hypothèse, il contient $\mathcal{L}$. Soit C une chaîne de $\mathcal{F}$, c'est-à-dire une partie de $\mathcal{F}$ totalement ordonnée, et montrons qu'elle est majorée dans $\mathcal{F}$. Cette chaîne, on peut l'écrire : $C = \{\mathcal{L}_i \mid i \in I\}$ où I est totalement ordonné, avec donc pour tous $i,j \in I$, $i \leqslant j \implies \mathcal{L}_i \subseteq \mathcal{L}_j$. Dans ce cas, la famille $\mathcal{L}' = \bigcup_{i\in I} \mathcal{L}_i$ est libre. En effet, si $x_1,...,x_n$ appartiennent à $\mathcal{L}'$, si l'on a des scalaires vérifiant $\lambda_1 x_1 + ... \lambda_n x_n = 0$, pour tout $j \in [\![1,n]\!]$, il existe $i_j \in I$ tel que $x_j \in \mathcal{L}_{i_j}$. Soit $i_0 = \max_{1\leqslant j\leqslant n} i_j$. Puisque la famille $(\mathcal{L}_i)_{i\in I}$ est totalement ordonnée, on a $x_1,...,x_n \in \mathcal{L}_{i_0}$. La famille $\mathcal{L}_{i_0}$ étant libre, on en déduit $\lambda_1 = ... = \lambda_n = 0$. Ainsi, la famille $\mathcal{L}$ est libre et vérifiant évidemment $\mathcal{L} \subseteq \mathcal{L}' \subseteq \mathcal{G}$, on a $\mathcal{L}' \in \mathcal{F}$. Comme $\mathcal{L}_i \subseteq \mathcal{L}'$ pour tout i, $\mathcal{L}'$ est un majorant de C.

D'après le lemme de Zorn, l'ensemble $\mathcal{F}$ possède un élément maximal $\mathcal{B}$. On va montrer que cette famille est une base de E, telle que $\mathcal{L} \subseteq \mathcal{B} \subseteq \mathcal{G}$. Par définition, c'est une famille libre et par construction elle vérifie les inclusions précédentes. Il ne reste donc qu'à voir qu'elle est génératrice. Soit $x \in E$ et montrons que x s'écrit comme combinaison linéaire d'éléments de $\mathcal{B}$. Il suffit de traiter le cas où $x \in \mathcal{G}$, puisque $\mathcal{G}$ est-elle même génératrice de E. Si $x \in \mathcal{B}$, il n'y a rien à faire. Supposons donc $x \notin \mathcal{B}$. Si la famille $\mathcal{B} \cup \{x\}$ était libre, alorsce serait un élément de $\mathcal{F}$ contenant strictement $\mathcal{B}$, ce qui contredit la maximalité de $\mathcal{B}$. Ainsi, la famille $\mathcal{B} \cup \{x\}$ est liée, et c'est terminé, en effet : il existe des scalaires $\mu_1,...,\mu_n,\mu$ tels que $\mu_1 x_1 + ... + \mu_n x_n + \mu x = 0$ où $\mu_1,...,\mu_n$ sont non tous nuls et $x_1,...,x_n \in \mathcal{B}$. Si $\mu = 0$, alors puisque $\mathcal{B}$ est libre, tous les scalaires jusqu'à n sont nuls, donc tous les μ_i, μ sont nuls ce qui est exclu. Ainsi, on peut écrire $x = -\mu^{-1}(\mu_1 x_1 + ... + \mu_n x_n)$. x s'écrit donc comme combinaison linéaire d'éléments de $\mathcal{B}$, ce qu'il fallait montrer. ■

Propriété

Tout espace vectoriel admet des bases.

▷ Rappelons pour commencer que l'espace nul a pour base la famille vide. Ce cas pathologique ayant été exclu, on peut considérer un vecteur non nul $x_0 \in E$, et dans ce cas, $\{x_0\}$ forme une famille libre. Elle est incluse dans la famille trivialement génératrice $(x)_{x\in E}$. On applique alors le théorème de la base incomplète, et c'est terminé. ■

Théorème. *(Théorème de la dimension)*

Dans tout espace vectoriel, le cardinal de toute partie libre est inférieur au sens de l'ordre cardinal au cardinal de toute partie génératrice de E.

▷ Soient $\mathcal{L}$ une partie libre de E et $\mathcal{G}$ une partie génératrice. Dans le cas où $\mathcal{G}$ est finie, par définition E est de dimension finie et le théorème d'échange du programme garantit que $\mathcal{L}$ est elle-même finie de cardinal inférieur à celui de $\mathcal{G}$. Dans le cas général, pour tout vecteur $l \in \mathcal{L}$, avec l'axiome du

choix, choisissons une partie finie $f(l)$ de G telle que l appartienne à $\mathrm{Vect}(f(l))$. Pour tout $K \in \mathrm{Fin}(\mathcal{G})$ l'ensemble des parties finies de $\mathcal{G}$, d'après le cas fini, on a $\mathrm{card}(f^{-1}(\{K\})) \leqslant \mathrm{card}(K) \leqslant \aleph_0$, dont on déduit que $\mathrm{card}(\mathcal{L}) = \sum_{K\in\mathrm{Fin}(\mathcal{G})} \mathrm{card}(f^{-1}(\{K\})) \leqslant \sum_{K\in\mathrm{Fin}(\mathcal{G})} \aleph_0 \leqslant \mathrm{card}(\mathrm{Fin}(\mathcal{G}))\aleph_0 = \mathrm{card}(\mathrm{Fin}(\mathcal{G})) = \mathrm{card}(\mathcal{G})$ d'après les propriétés de l'arithmétique cardinale, soit $\mathrm{card}(\mathcal{G}) \geqslant \mathrm{card}(\mathcal{L})$. ■

Corollaire. ***(Unicité de la dimension)***

Sur un espace vectoriel quelconque, toutes les bases ont le même cardinal. Celui-ci définit alors la *dimension* de l'espace vectoriel considéré.

▷ Soient $\mathcal{B}, \mathcal{B}'$ deux bases d'un espace vectoriel E. Alors $\mathcal{B}$ est libre et $\mathcal{B}'$ est génératrice, donc d'après ce qui précède, $\mathrm{card}(\mathcal{B}) \leqslant \mathrm{card}(\mathcal{B}')$. Mais ces deux bases ayant un rôle rigoureusement symétrique, on a $\mathrm{card}(\mathcal{B}') \leqslant \mathrm{card}(\mathcal{B})$. En utilisant le théorème de Cantor-Bernstein, c'est-à-dire par antisymétrie de l'ordre cardinal, on a $\mathrm{card}(\mathcal{B}) = \mathrm{card}(\mathcal{B}')$, ce qu'il fallait montrer. Notons que la définition de la dimension est ainsi univoque grâce aux résultats conjoints du corollaire du théorème de la base incomplète, qui garantit l'existence, et du théorème de la dimension pour les espaces vectoriels, qui garantit l'unicité. ■

On termine la théorie élémentaire de la dimension infinie par un résultat très intéressant.

Corollaire. ***(Caractérisation des classes d'isomorphie : un invariant fondamental)***

Deux espaces vectoriels sont isomorphes si et seulement s'ils ont la même dimension.

▷ Rappelons que pour que deux espaces vectoriels soient isomorphes, il suffit qu'il existe une application linéaire bijective de l'un vers l'autre, la réciproque d'une telle application étant nécessairement un morphisme d'après le cours. Supposons que E,F soient deux espaces vectoriels sur $\mathbb{K}$ qui soient isomorphes, par f de E dans F. On vérifie aisément (voir ci-dessous la preuve du $\mathbb{K}$-Vect-théorème de Cantor-Bernstein) qu'un isomorphisme f transforme un famille libre en famille libre et une famille génératrice en famille génératrice. Il transforme donc une base en une base. Puisqu'une bijection préserve le cardinal, par définition, on a donc une base de F de même cardinal qu'une base de E. Par unicité de la dimension, E et F sont de même dimension. Réciproquement, si E est de dimension I, où I est un ensemble quelconque, alors E est isomorphe à $\mathbb{K}^{(I)}$ l'ensemble des applications de I dans $\mathbb{K}$ à support fini. Par transitivité sur cet ensemble, deux espaces de même dimension sont isomorphes. Justifions enfin que $E \simeq \mathbb{K}^{(I)}$. L'isomorphisme à considérer est celui qui à tout vecteur de E envoie la famille de ses composantes dans une base de cardinal I fixée, cette famille étant à support fini par définition du caractère générateur. On vérifie facilement qu'elle est linéaire, surjective par les axiomes de stabilité des espaces vectoriels, et pour l'injectivité, celle-ci vient de la liberté des bases. ■

On peut maintenant conclure.

Lemme. ***(Majoration du cardinal des familles libres)***

Dans un espace vectoriel quelconque, toute famille libre est de cardinal inférieur à cette dimension.

▷ C'est déjà fait. ■

1.3 Espaces vectoriels quotients

Nous terminons nos considérations algébriques sur les structures quotients avec le cas des espaces vectoriels quotients. Celui-ci est d'autant plus intéressants que les deux précédents pour les groupes et les anneaux, car, non seulement nous l'utilisons pour donner de nouvelles preuves de résultats au programme, mais mieux encore, il est la façon naturelle d'introduire le concept de codimension (c'est d'ailleurs de cette manière que, sans vergogne, Xavier Gourdon la définit dans *Les maths en tête*, collection censée être un ouvrage manuel pour les classes préparatoires... bien que la notion de quotient soit sortie des programmes au cours d'un autre millénaire). La co-dimension (que l'on sait être la dimension commune à tous les supplémentaires d'un sous-espace vectoriel) d'un sous-espace vectoriel F est également la dimension de l'espace quotient E/F.

Exercice 2

Soient A,B,C des matrices.

1. *(Inégalité de Frobenius)* Montrer que $\mathrm{rg}(AB)+\mathrm{rg}(BC)\leqslant \mathrm{rg}(ABC)+\mathrm{rg}(B)$.
2. *(Inégalité de Sylvester)* En déduire, pour des matrices carrées A,B de taille n, $\mathrm{rg}(A)+\mathrm{rg}(B)-n\leqslant \mathrm{rg}(AB)$.

▷ **Éléments de réponse.**

C'est dur, hein ?

L'inégalité de Frobenius ne se montre qu'au moyen des espaces vectoriels quotients, que nous allons voir. Cependant, l'inégalité de Sylvester est un grand classique des classes préparatoires.

Nous recommençons le procédé habituel pour la structure des espaces vectoriels. Le théorème de compatibilité est facilité par ce que, comme pour les anneaux, les sous-espaces vectoriels sont automatiquement des sous-groupes distingués, puisqu'en milieu commutatif, et il n'y a pas question de bilatéralité (la loi externe n'est défini que dans un sens bien sûr !).

Soit V un espace vectoriel sur un corps K. Soit W un sous-espace vectoriel de V.

Théorème. ***(Congruences compatibles avec la structure d'espace vectoriel)***

(On définit la compatibilité avec la loi externe par : $\vec{u} \sim \vec{v} \implies \forall \lambda \in K \quad \lambda.\vec{u} \sim \lambda.\vec{v}$.) Toute relation des classes à gauche (ou à droite, peu importe) selon un sous-espace vectoriel est compatible avec l'addition et la loi externe, et réciproquement, toute relation ainsi compatible est relation de classes à gauche (ou à droite) modulo un sous-espace vectoriel.

▷ En exercice. ■

Théorème. ***(Espace vectoriel quotient)***

Le groupe V/W admet une unique structure d'espace vectoriel sur K telle que la projection canonique $\pi : V \longrightarrow V/W$ soit une application linéaire.

▷ On veut avoir, par définition de la notion d'application linéaire, $\pi(\lambda x) = \lambda\pi(x)$ et $\pi(x+y) = \pi(x) + \pi(y)$ pour tous x,$y \in V$ et $\lambda \in K$. La première identité définit univoquement la loi externe sur V/W en tant que K-espace vectoriel : pour $a \in V/W$, si x est un représentant de a, on doit donc poser $\lambda a = \overline{\lambda x}$ et cette définition ne dépend pas du choix du représentant x de a, puisque si $x \sim x'$, $x - x' \in W$, donc $\lambda x - \lambda x' \in W$, donc $\lambda x \sim \lambda x'$. Cela signifie de plus que la relation $\sim$ sur V est compatible avec la loi externe. On vérifie alors aisément que, ceci dit, on a un espace vectoriel (la loi additive est déjà déterminée par le groupe commutatif V, avec $\overline{x+y} = \overline{x} + \overline{y}$). Par analyse-synthèse, on a existence et unicité de la structure d'espace vectoriel sur le quotient. ■

On retient la définition des lois sur le quotient, très intuitive : pour tous $\overline{x}, \overline{y} \in V/W$, pour tout $\lambda \in K$,

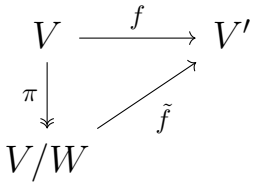
$$\overline{x} +' \overline{y} = \overline{x+y} \text{ et } \lambda.'\overline{x} = \overline{\lambda.x}.$$

Dans ce qui suit, les théorèmes concernant les quotients d'espaces vectoriels découlent de deux choses très simples : l'application des théorèmes sur les groupes pour la loi additive, qui est immédiate sachant que tous les sous-groupes (c'est-à-dire ici, sous-espaces vectoriels) additifs sont tous distingués, le groupe additif étant commutatif par axiome ; d'autre part, la vérification chaque fois des compatibilités avec la loi externe, comme nous venons de le faire. Nous ne détaillons pas celle-ci.

Théorème. ***(Théorème de factorisation pour les espaces vectoriels)***

Soit f une application linéaire entre deux espaces vectoriels V vers V'. Soit W un sous-espace vectoriel de V. W est dans $\mathrm{Ker}(f)$ si et seulement s'il existe un unique morphisme $\tilde{f}$ tel que $f = \tilde{f} \circ \pi$ (se qui se réécrit $f(u) = \tilde{f}(\overline{u})$ pour tout $u \in V$), en notant π la projection canonique (linéaire) de V dans V/W.

Une petite illustration des familles :



Le théorème de factorisation carré s'applique également (nous invitons le lecteur à l'énoncer). Dans le cas où le départ et l'arrivée sont les mêmes, on obtient un corollaire intéressant.

Corollaire

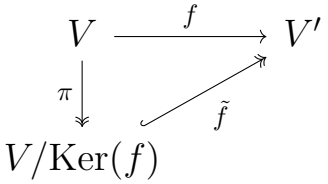
Si f est un endomorphisme de V et W un sous-espace vectoriel stable par f, l'application linéaire quotient est un endomorphisme de V/W.

Les deux théorèmes d'isomorphismes repris pour les anneaux s'énoncent pour les espaces vectoriels. Le deuxième théorème d'isomorphisme pour les groupes proprement dit n'admet pas de généralisation, puisqu'aucune opérateur multiplicative n'est possible entre sous-espaces vectoriels à part l'addition. On reprend les notations précédentes.

Théorème. ***(Premier théorème d'isomorphisme pour les espaces vectoriels)***

Soit $f : V \longrightarrow V'$ une application linéaire. Les espaces vectoriels $V/\mathrm{Ker}(f)$ et $\mathrm{Im}(f) \subseteq V'$ sont isomorphes par l'application linéaire quotient, qui est un isomorphisme.

Ceci s'exprime synthétiquement :



D'autre part :

Théorème. ***(Deuxième théorème d'isomorphisme pour les espaces vectoriels)***

Soient $G \subseteq F \subseteq E$ des sous-espaces vectoriels. Alors F/G est un sous-espace vectoriel de E/G et $\frac{E/G}{F/G} \simeq \frac{E}{F}$.

Exercice 3

Peut-on énoncer un théorème d'isomorphisme pour les algèbres ?

Nous terminons avec la seule justification de tout ce chapitre dans le cas des classes préparatoires (lol). Il faut s'attarder sur la preuve, quoique très succincte, car elle est la clef, comme d'habitude.

Théorème. ***(Théorème fondamental de la codimension)***

Soit W un sous-espace vectoriel de V ; soit W' un supplémentaire de W dans V. Alors W' est isomorphe à V/W.

▷ L'isomorphisme à exhiber est la restriction à W' de la projection canonique de V sur V/W. Celle-ci est linéaire par restriction, d'une application linéaire. Reste à montrer qu'elle est injective et surjective. Pour l'injectivité, on utilise la caractérisation par le noyau : l'ensemble des $x \in W'$ tels que $\pi(x) = W$ le neutre de V/W est réduit à l'élément neutre, car ils sont dans W' ainsi que dans le noyau de π qui est W, et $W \cap W'$ est réduit au neutre car deux espaces supplémentaires sont indépendants. Pour la surjectivité, on a l'image de cette restriction qui égale exactement $\pi(W') = \pi(W) + \pi(W')$, car $\pi(W)$ est le neutre dans V/W. Par linéarité (prolongée sur les parties), $\pi(W) + \pi(W') = \pi(W + W')$ et $W + W' = V$ par complémentarité, donc $\pi(W') = pi(V) = V/W$ par surjectivité de la projection canonique en entier. Et c'est tout. ■

On en déduit ce qui suit, tant attendu :

Corollaire. ***(Unicité de la codimension)***

Soit W un sous-espace vectoriel de V, alors tous les supplémentaires de W dans V (il en existe au moins un, d'après le théorème de la base incomplète) sont isomorphes. En particulier, ceux-ci ont la même dimension, appelée *codimension* de W, notée $\mathrm{codim}_V(W)$ qui égale $\dim_K(V/W)$.

Comme la dimension, la codimension dépend tout à fait de l'espace ambiant, d'où la précision dans la notation.

On termine avec quelques propriétés faciles qui en découlent.

Définition. ***(Hyperplan)***

Un hyperplan est un sous-espace vectoriel de codimension 1.

Propriété. ***(Majoration de la codimension d'une intersection)***

Soient W_1,W_2 deux sous-espaces vectoriels de V de codimensions finies. Alors $\mathrm{codim}(W_1 \cap W_2) \leqslant \mathrm{codim}(W_1) + \mathrm{codim}(W_2)$.

Propriété. ***(Majoration de l'intersection d'hyperplans)***

L'intersection de k hyperplans est un sous-espace vectoriel de codimension inférieur ou égale à k.

Propriété. ***(Lien noyau-image pour la codimension)***

Soit $f : V \longrightarrow V'$ une application linéaire. $\mathrm{Ker}(f)$ est de codimension finie si et seulement si $\mathrm{Im}(f)$ est de dimension finie, et dans ce cas, $\mathrm{codim}(\mathrm{Ker}(f)) = \dim(\mathrm{Im}(f))$.

Propriété

Si V' est de dimension finie, $\mathrm{Ker}(f)$ est de dimension finie et $\mathrm{codim}(\mathrm{Ker}(f)) \leqslant \dim(V')$, avec l'égalité dans le cas seul où f est surjective.

Citons enfin :

Théorème. ***(Théorème de correspondance pour les espaces vectoriels)***

Soit V un K-espace vectoriel, K un corps, et W un sous-espace vectoriel de W. Alors l'ensemble des sous-espaces vectoriels de V/W est en bijection avec l'ensemble des sous-espaces vectoriels de V contenant W par l'application $V' \longmapsto V'/W$.

1.4 Matrices

1.4.1 Définition générale de $\mathfrak{M}_{I\times J}(E)$

1.4.1.1 Définition de l'objet matriciel

1.4.2 Classes de matrices particulières

1.4.2.1 Matrices triangulaires

Définition. ***(Matrice triangulaire supérieure)***

Une matrice carrée $A \in \mathfrak{M}_n(E)$, $n \in \mathbb{N}$, E un groupe, est dite *triangulaire supérieure* si tous les coefficients strictement au-dessus (à droite) de la diagonale principale sont nuls.

Propriété

Une matrice carrée $A \in \mathfrak{M}_n(E)$, $n \in \mathbb{N}$, E un groupe, est triangulaire supérieure si et seulement si pour tous $i,j \in [\![1,n]\!]$, $i < j \implies A_{ij} = 0_E$.

Conseils

- ◇ Pour se rappeler le sens de l'inégalité, regarder les coefficients dans les coins.
- ◇ Pour se rappeler si l'inégalité est stricte, voir ce qui se passe sur la diagonale.

Définition. ***(Matrice triangulaire inférieure)***

Une matrice carrée $A \in \mathfrak{M}_n(E)$, $n \in \mathbb{N}$, E un groupe, est dite *triangulaire inférieure* si tous les coefficients strictement en dessous (à gauche) de la diagonale principale sont nuls.

Propriété

Une matrice carrée $A \in \mathfrak{M}_n(E)$, $n \in \mathbb{N}$, E un groupe, est triangulaire supérieure si et seulement si pour tous $i,j \in [\![1,n]\!]$, $i > j \implies A_{ij} = 0_E$.

Définition. ***(Matrice triangulaire)***

Une matrice carrée $A \in \mathfrak{M}_n(E)$, $n \in \mathbb{N}$, E un groupe, est dite *triangulaire* si elle est triangulaire supérieure ou inférieure.

Définition. ***(Matrice triangulaire supérieure stricte)***

Une matrice carrée $A \in \mathfrak{M}_n(E)$, $n \in \mathbb{N}$, E un groupe, est dite *triangulaire supérieure stricte* si tous les coefficients au-dessus (à droite) de la diagonale principale sont nuls.

Remarque. Cette fois-ci, on demande également que les coefficients diagonaux soient nuls, de même que ci-dessous.

Propriété

Une matrice carrée $A \in \mathfrak{M}_n(E)$, $n \in \mathbb{N}$, E un groupe, est triangulaire supérieure si et seulement si pour tous $i,j \in [\![1,n]\!]$, $i \leqslant j \implies A_{ij} = 0_E$.

Définition. ***(Matrice triangulaire inférieure stricte)***

Une matrice carrée $A \in \mathfrak{M}_n(E)$, $n \in \mathbb{N}$, E un groupe, est dite *triangulaire inférieure stricte* si tous les coefficients en dessous (à gauche) de la diagonale principale sont nuls.

Propriété

Une matrice carrée $A \in \mathfrak{M}_n(E)$, $n \in \mathbb{N}$, E un groupe, est triangulaire supérieure si et seulement si pour tous $i,j \in [\![1,n]\!]$, $i \geqslant j \implies A_{ij} = 0_E$.

Définition. *(Matrice triangulaire stricte)*

Une matrice carrée $A \in \mathfrak{M}_n(E)$, $n \in \mathbb{N}$, E un groupe, est dite *triangulaire stricte* si elle est triangulaire supérieure stricte ou inférieure stricte.

Évidemment :

Observation

Toute matrice triangulaire stricte est triangulaire (large), pour les matrices supérieures comme pour les matrices inférieures.

Exercice 4

Caractériser symboliquement les matrices triangulaires et les matrices triangulaires strictes.

1.4.3 Matrices à coefficients dans un anneau

1.4.3.1 Opérations sur les matrices

1.4.3.2 Matrices élémentaires

Propriété. *(Multiplication à gauche par une matrice élémentaire)*

Soient n,p,q trois entiers naturels et A un anneau unitaire. Soient $i \in [\![1,n]\!]$ et $j \in [\![1,p]\!]$. On considère $E_{ij} \in \mathfrak{M}_{n,p}(A)$ et $A \in \mathfrak{M}_{p,q}(A)$. Alors $E_{ij}A$ est la matrice nulle, sauf sur sa i-ième ligne qui est remplie par la j-ième ligne de A.

Propriété. *(Multiplication à droite par une matrice élémentaire)*

Soient n,p,q trois entiers naturels et A un anneau unitaire. Soient $i \in [\![1,p]\!]$ et $j \in [\![1,q]\!]$. On considère $E_{ij} \in \mathfrak{M}_{p,q}(A)$ et $A \in \mathfrak{M}_{n,p}(A)$. Alors AE_{ij} est la matrice nulle, sauf sur sa j-ième colonne qui est remplie par la i-ième colonne de A.

Mnémonik : pour se rappeler ces deux propriétés, réfléchir ainsi : l'action des matrices élémentaires normale est celle qui s'effectue à gauche, comme pour les opérations élémentaires sur les systèmes. Dans ce cas, tout se passe bien et dans l'ordre, et sur les lignes (qui viennent toujours en premier). Par contre, lorsqu'on inverse le sens, tout s'inverse : à la fois i et j mais aussi les lignes pour les colonnes. Toutefois il est hors de question que l'on mélange ligne et colonne : c'est la marque d'une dissymétrie opératoire grande sur les matrices que les simples matrices élémentaires sont incapables de produire. De plus, le résultat est valable pour des matrices rectangulaires, ce qui ne permet pas de changer une ligne pour une colonne pour cause de taille.

Définition. ***(Matrice d'échange)***

La *matrice d'échange* (des lignes i et j) par $P_{ij} = I_n - E_{ii} - E_{jj} + E_{ij} + E_{ji} =$

$$\begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 0 & & 1 & & \\ & & & \ddots & & & \\ & & 1 & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}.$$

1.4.4 Propriétés algébriques des anneaux de matrices

1.4.4.1 Commutant

On rappelle que dans un anneau A, le commutant d'une partie E est l'ensemble des éléments de A qui commutent avec tous les éléments des E. On note $\mathrm{Com}(E)$ si le contexte de A est clair.

Lemme. ***(Commutant des matrices inversibles)***

Soit K un corps et n un entier naturel non nul. Alors $\mathrm{Com}(GL_n(K)) = \mathrm{Com}(\mathfrak{M}_n(K))$.

▷ Soit $A \in \mathrm{Com}(GL_n(K))$. Alors pour toute matrice $M \in GL_n(K)$, la fonction $f(M) = AM - MA$ définie sur $\mathfrak{M}_n(K)$ est nulle. Mais f est continue par opérations usuelles et $GL_n(K)$ est dense dans $\mathfrak{M}_n(K)$. Ainsi f est nulle sur $\mathfrak{M}_n(K)$ ce qui signifie que A commute avec toute matrice de $\mathfrak{M}_n(K)$. ■

Propriété. ***(Centre de l'espace des matrices)***

Soit K un corps et n un entier naturel non nul. Alors $\mathrm{Com}(\mathfrak{M}_n(K)) = \{\lambda I_n, \lambda \in K\}$.

▷ En multipliant par des matrices élémentaires à gauche et à droite, on trouve qu'une matrice du centre de $\mathfrak{M}_n(K)$ doit être diagonale. En multipliant par la matrice $Diag(1,1,0,...,0)$, on trouve que les deux premiers coefficients sont égaux. Petit à petit, on trouve que la matrice est scalaire : le centre de $\mathfrak{M}_n(K)$ est constitué des matrices d'homothéties. ■

Chapitre 2

Réduction

Résumé

Théorie aujourd'hui fermée, la réduction d'endomorphismes et de matrices est guidée par un projet unique : simplifier l'expression de ces objets. Du point de vue des endomorphismes, il s'agit de voir l'espace muni d'une base dont l'application linéaire considérée « préserve les directions » (notion d'*éléments propres*) ; du point de vue des matrices, il s'agit, de façon tout à fait équivalente d'ailleurs, nous le verrons, de trouver une matrice structurellement simple qui soit *semblable* à la matrice considérée. La réduction est une théorie fermée en ce sens, qu'il existe une réduction applicable à toute matrice sur un corps quelconque : la réduction de Jordan. Avant d'exposer et de démontrer ce théorème fondamental, nous nous intéresserons à des réductions plus restrictives, mais également plus pratiques, auxquelles il faudra s'intéresser donc sous couvert de conditions de réductibilité.

Soit $n \in \mathbb{N}$. On considère aussi un corps $\mathbb{K}$ muni de lois que l'on notera par les notations habituelles. Dans toute la suite,

- l'ensemble $\mathfrak{M}_n(\mathbb{K})$ est muni de la structure d'algèbre sur $\mathbb{K}$: nous notons la multiplication matricielle, la multiplication par un scalaire, et la multiplication dans $\mathbb{K}$ de la même manière, sans risque de confusion ;
- cet ensemble est isomorphe à l'ensemble des endomorphismes de E pour tout espace vectoriel E de dimension n dont nous notons les lois encore avec les notations évidentes. En particulier, $\mathcal{L}(E)$ est muni d'une structure d'algèbre.

Nous croyons que la similitude des notations $(\mathbb{K}, +, \times)$, $(\mathfrak{M}_n(\mathbb{K}), +, \times, \cdot\,)$ et $(\mathcal{L}(E), +, \circ, \cdot\,)$ est sans problème tant que le lecteur prend garde à tout moment de connaître l'ensemble habité par les éléments qu'il manipule.

2.1 Généralités

2.1.1 Relation de similitude des matrices

Définition. ***(Similitude)***

Deux matrices $A,B \in \mathfrak{M}_n(\mathbb{K})$ sont dites *semblables* s'il existe $P \in GL_n(\mathbb{K})$ telle que $A = P^{-1}BP$. (Il est tout à fait équivalent d'écrire à la place $A = PBP^{-1}$.)

Définition. ***(Équivalence)***

Deux matrices $A,B \in \mathfrak{M}_n(\mathbb{K})$ sont dites *équivalentes* s'il existe $P,Q \in GL_n(\mathbb{K})$ telle que $A = Q^{-1}BP$. (Il est tout à fait équivalent d'écrire à la place $A = QBP$.)

Remarques.

1. La similitude et l'équivalence sont toutes deux des relations d'équivalence sur $\mathfrak{M}_n(\mathbb{K})$ (le redémontrer).
2. La similitude entraîne l'équivalence.
3. La trace, le déterminant, le rang sont des invariants de similitude. On aura l'occasion de rencontrer d'autres invariants de similitude dans la suite de notre cours. Ceux-ci ont une grande importance pour nous, en ce qu'ils commencent de répondre à cette question centrale pour la réduction des matrices : pour quels invariants, l'identité de ces invariants entraîne-t-elle la similitude ?
4. Deux matrices sont équivalentes si et seulement si elles ont le même rang[1].

Propriété

Si $A,B \in \mathfrak{M}_n(\mathbb{K})$ sont semblables, alors pour tout $\lambda \in \mathbb{K}$, $A - \lambda I_n$ et $B - \lambda I_n$ sont semblables.

▷ Par hypothèse, il existe $P \in GL_n(\mathbb{K})$ telle que $B = P^{-1}AP$. Or $P^{-1}\lambda I_n P = \lambda I_n P^{-1}P = \lambda I_n$, d'où, par distributivité, $B - \lambda I_n = P^{-1}AP - P^{-1}\lambda I_n P = P^{-1}(A - \lambda I_n)P$, ce qui signifie que $B - \lambda I_n$ et $A - \lambda I_n$ sont semblables par la matrice de passage P. ■

Exercice 5

Montrer que les matrices $A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 3 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$ sont semblables.

[1] Ceci est *grosso modo* l'énoncé de la décomposition J_r des matrices dont nous donnerons un énoncé et une démonstration parmi l'annexe sur les décompositions factorielles des matrices.

▷ **Éléments de réponse.**

Deux matrices semblables ont les mêmes invariants de similitude. Ici, A et B ont la même trace, ce qui ne permet pas de conclure. On applique le résultat précédent : si A et B sont semblables, alors $A - I_3$ et $B - I_3$ le sont également. Il suffit de calculer le déterminant de chacune de ces matrices, respectivement $0 \neq 7$, pour terminer.

Dans toute la suite, toutes les matrices sont prises dans $\mathfrak{M}_n(\mathbb{K})$.

Propriété. ***(Interprétation géométrique de la similitude)***

Soit E un $\mathbb{K}$-espace vectoriel de dimension n. Deux matrices A,B sont semblables si et seulement s'il existe deux bases $\mathcal{B}, \mathcal{B}'$ de E et un endomorphisme $f \in \mathcal{L}(E)$ tel que $A = \mathrm{Mat}_{\mathcal{B}}(f)$ et $B = \mathrm{Mat}_{\mathcal{B}'}(f)$.

Remarque importante. On peut reformuler cette vision des choses par une phrase très simple : deux matrices sont semblables iff elles représentent le même endomorphisme (dans des bases a priori différentes).

Exemple. ***(Expliciter la similitude par changement de base)***

Soient les matrices $A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$. Elles sont semblables.

En effet, si l'on prend E un $\mathbb{K}$-espace vectoriel de dimension 3, $\mathcal{B} = (e_1,...,e_3)$ une base de E, et $f \in \mathcal{L}(E)$ tel que $A = \mathrm{Mat}_{\mathcal{B}}(f)$, on a alors $\begin{cases} f(e_1) = e_2 \\ f(e_2) = e_3 \\ f(e_3) = e_1 \end{cases}$ (il faut savoir écrire une matrice dans une base et donner l'image d'une base par une application à partir de sa matrice représentative !). Il faut alors poser $\mathcal{B}' = (e'_1,e'_1,e'_3) = (e_1, e_3, e_2)$ pour avoir $\begin{cases} f(e'_1) = f(e_1) = e_2 = e'_3 \\ f(e'_2) = f(e_3) = e_1 = e'_1 \\ f(e'_3) = f(e_2) = e_3 = e'_1 \end{cases}$, soit $B = \mathrm{Mat}_{\mathcal{B}'}(f)$.

De plus, on a $B = P^{-1}AP$ avec $P = P_{\mathcal{B},\mathcal{B}'} = \mathrm{Mat}_{\mathcal{B}}(\mathcal{B}') = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$.

Corollaire. ***(Similitude des matrices de permutation)***

L'ensemble des matrices de permutation est inclus dans une seule classe de similitude et contient toutes les matrices de passage entre deux matrices de permutation.

▷ La permutation des éléments d'une base donne une autre base. Les détails ont été traités sur l'exemple ci-dessous. ■

2.1.2 Notion de stabilité par un endomorphisme

Soient E un $\mathbb{K}$-espace vectoriel et $f \in \mathcal{L}(E)$.

Définition. ***(Sous-espace stable)***

Un sous-espace F de E est dit *stable par* f, si $f(F) \subseteq F$, c'est-à-dire : $\forall x \in F \quad f(x) \in F$. On dit aussi que f *stabilise* F.

Proposition. ***(Endomorphisme induit)***

Soit F un sous-espace vectoriel de E. Il existe un endomorphisme $\tilde{f} : F \longrightarrow F$ tel que $\forall x \in F \quad \tilde{f}(x) = f(x)$, si et seulement si, f stabilise F.

▷ Seul le sens indirect nous intéresse vraiment, mais la connaissance de la réciproque clarifie beaucoup le cours pour l'étudiant. Si f stabilise F, $f_{|F}$ est à valeurs dans F et il est immédiat que c'est encore une application linéaire, donc c'est un endomorphisme qui convient pour ce qui précède. Réciproquement, si l'on suppose l'existence de $\tilde{f}$, alors pour tout $x \in F$, par définition de l'espace d'arrivée de $\tilde{f}$, $\tilde{f}(x) \in F$, mais $\tilde{f}(x) = f(x)$, donc $f(x) \in F$, c'est-à-dire que F est stable par f. ■

Remarque. Ainsi, on ne peut définir d'endomorphisme induit sur un sous-espace vectoriel **que** si l'endomorphisme initial le stabilise. Il faudra vérifier cette propriété, souvent simple à établir, de façon systématique.

Exercice 6

On prend $E = \mathbb{K}[X]$, $f : P \mapsto P + P'$. Montrer que pour tout $n \in \mathbb{N}$, $\mathbb{K}_n[X]$ est stable par l'endomorphisme f.

▷ **Éléments de réponse.**

Comment majorer le degré d'une somme ?

Théorème. ***(Interprétation matricielle de la stabilité)***

Soient E un $\mathbb{K}$-espace vectoriel de dimension n, F un sous-espace vectoriel de E et $f \in \mathcal{L}(E)$. Si F est stable par f et si $\mathcal{C} = (e_1,...,e_p)$ est une base de F qu'on complète en $\mathcal{B} = (e_1,...,e_n)$ base de E, alors $\mathrm{Mat}_{\mathcal{B}}(f)$ est de la forme $\begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$ où $A = \mathrm{Mat}_{\mathcal{C}}(\tilde{f})$, $\tilde{f}$ l'endomorphisme induit par f sur F. Réciproquement, si $\mathcal{B} = (e_1,...,e_n)$ base de E et

si $\mathrm{Mat}_{\mathcal{B}}(f)$ est de la forme suivante : $\begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$ avec $A \in \mathfrak{M}_p(\mathbb{K})$, alors le sous-espace vectoriel $F = \mathrm{Vect}(e_1,...,e_p)$ est stable par f et $A = \mathrm{Mat}_{(e_1,...,e_p)}(\tilde{f})$.

▷ Si F est stable par f, alors pour tout $j \in \{1,...,p\}$, $f(e_j) \in F = \mathrm{Vect}(e_1,...,e_p)$ d'où le résultat.

Réciproquement si $\mathcal{B} = (e_1,...,e_n)$ est une base de E et si $\mathrm{Mat}_{\mathcal{B}}(f)$ est de la forme suivante : $\begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$ avec $A \in \mathfrak{M}_p(\mathbb{K})$, alors :

$$\forall j \in \{1,...,p\}, f(e_j) \in \mathrm{Vect}(e_1,...,e_p) = F$$

d'où $f(F) = f(\mathrm{Vect}(e_1,...,e_p)) = \mathrm{Vect}(f(e_1),...,f(e_p)) \subseteq F$. ■

Exercice 7

Soient E un $\mathbb{K}$-espace de dimension 3, $\mathcal{B} = (e_1,...,e_3)$ une base de E et $f \in \mathcal{L}(E)$ tel que $\mathrm{Mat}_{\mathcal{B}}(f) = \begin{pmatrix} 2 & 2 & 1 \\ -2 & 1 & 2 \\ 1 & -2 & 2 \end{pmatrix} = A$. Montrer que le plan F d'équation $x_1 + x_3 = 0$. Écrire A dans $\mathcal{B}' = (e_2, e_1 - e_3, e_1)$.

2.1.3 Éléments propres

Soit E un $\mathbb{K}$-espace vectoriel. Soit f un endomorphisme de E.

Définition. ***(Valeur propre)***

On dit que $\lambda \in \mathbb{K}$ est *valeur propre* de f s'il existe un vecteur **non nul** $x \in E$ tel que $f(x) = \lambda x$.

Remarque importante. Si l'on acceptait $x = 0$, tous les éléments de $\mathbb{K}$ seraient valeurs propres associées au vecteur nul.

Définition. ***(Vecteur propre)***

Dans la relation précédente, on dit que x est UN *vecteur propre* de f, *associé* à la valeur propre λ.

Remarque. Un vecteur propre ne peut être, d'après l'égalité dans la définition, associé qu'à une seule valeur propre.

Définition. ***(Spectre d'un endomorphisme)***

On appelle *spectre* de f l'ensemble des valeurs propres de f. On note : $\mathrm{Sp}(f)$.

Définition. ***(Sous-espace propre associé à une valeur propre)***

Soit $\lambda \in \mathbb{K}$. Le *sous-espace propre de f associé à λ* est défini comme $E_\lambda(f) = \mathrm{Ker}(f - \lambda id)$.

Proposition

Pour tout $\lambda \in \mathbb{K}$, $E_\lambda(f) \iff \lambda \in \mathrm{Sp}(f)$.

▷ Simple reformulation à partir de la définition du noyau de $f - \lambda id$.. ■

Exercice 8

Montrer que l'application linéaire définie sur $\mathbb{R}^2$ par $f(e_1) = e_1 + 2e_2$ et $f(e_2) = 2e_1 + 1e_1$ a pour valeur propre 3 associée au vecteur propre (1,1).

Méthode. ***(Recherche des éléments propres)***

Pour l'instant, la recherche des éléments propres, c'est-à-dire des valeurs et des vecteurs propres.

À ce point, on a uniquement donné le bagage théorique de la réduction ; c'est dans la section suivante que l'on s'intéresse à ce pourquoi l'on est venu. Remarquons que ces notions auraient pu (et dû) être introduites en première année universitaire ; elles auraient grandement clarifié la notion un peu sombre alors de similitude.

Dès maintenant, on s'intéresse à décomposer l'espace vectoriel considéré en sous-espaces propres. D'après les définitions précédentes, cette décomposition dépend évidemment de l'application linéaire considérée ; dès lors, on pourrait croire que c'est beaucoup de bruit pour rien : on déclenche tout un processus de décomposition qui ne vaut que dans une situation (très) particulière (en fait, pour toute une classe de matrices semblables également). Et bien, en physique et en ingénierie, ce procédé est très important : il prendra toute son importante en constatant par exemple qu'un système à paramètres linéaire ou système d'équations différentielles linéaires peut être modélisé par une application linéaire, à qui l'on appliquera une réduction.

2.2 Diagonalisation

Reformulation pratique

Soit $A \in \mathfrak{M}_n(\mathbb{K})$. La matrice A est diagonalisable si et seulement si elle possède n vecteurs propres $u_1,...,u_n$ linéairement indépendants. Dans ce cas on peut écrire $A = PDP^{-1}$ où D est diagonale, avec pour coefficients diagonaux les valeurs propres de A dans l'ordre précédent des vecteurs propres et P une matrice dont la i-ième colonne est le vecteur u_i.

2.3 Réduction des endomorphismes auto-adjoints

Théorème. ***(Théorème spectral)***

Soit $A \in \mathfrak{M}_n(\mathbb{K})$. La matrice A est normale si et seulement s'il existe une matrice unitaire U telle que $A = UDU^*$ où D est diagonale. En particulier, une matrice normale est diagonalisable et ses vecteurs propres sont orthogonaux.

Conséquence. ***(Réduction des matrices symétriques)***

Toute matrice symétrique est diagonalisable et la matrice de passage peut être choisie orthogonale. De plus, ses valeurs propres sont réelles.

Une matrice orthogonale n'est pas nécessairement diagonalisables sur $\mathbb{R}$. Ses valeurs propres sont toutes de module 1 *(voir ci-dessous)*.

Conséquence. ***(Réduction des matrices hermitiennes)***

Toute matrice hermitienne est diagonalisable et la matrice de passage peut être choisie unitaire. De plus, ses valeurs propres sont réelles.

Conséquence. ***(Réduction des matrices unitaires)***

Toute matrice unitaire est diagonalisable et la matrice de passage peut être choisie unitaire. De plus, ses valeurs propres sont de module 1.

Conséquence. ***(Réduction des matrices antihermitiennes)***

Une matrice antihermitienne ($A^* = -A$) est diagonalisable et la matrice de passage peut être choisie unitaire. De plus, ses valeurs propres sont imaginaires pures.

Une matrice antisymétrique n'est pas nécessairement diagonalisable sur $\mathbb{R}$, mais ses valeurs propres sont toujours imaginaires pures.

2.4 Jordanisation

2.4.1 Généralités sur la jordanisation

Définition. ***(Bloc de Jordan)***

Une *matrice de Jordan* ou *bloc de Jordan* est une matrice $J \in \mathfrak{M}_n(C)$ de la forme :

$$J = J(\lambda) = \begin{pmatrix} \lambda & 1 & & & \\ 0 & \lambda & 1 & (0) & \\ & \ddots & \ddots & \ddots & \\ & (0) & \ddots & \ddots & 1 \\ & & & 0 & \lambda \end{pmatrix}$$

où λ est un scalaire.

Théorème. ***(Jordan)***

Toute matrice carrée est diagonalisable par blocs, les blocs étant les $J(\lambda_1),...,J(\lambda_n)$ où $\mathrm{Sp}(A) = \{\lambda_1,...,\lambda_n\}$.

Reformulation pratique. ***(Jordan)***

Toute matrice à coefficients dans un corps $\mathbb{K}$ est réductible dans $\mathbb{K}$ à une matrice triangulaire supérieure dont la première diagonale ne comporte que des 0 ou des 1.

Remarques.

1. Dans le cas diagonalisable, tous les blocs peuvent être et doivent être ! de taille 1.
2. L'écriture par blocs de Jordan révèle immédiatement une et donc la décomposition de Dunford de A comme somme d'une matrice diagonalisable et d'une matrice nilpotente qui commutent : $J_k(\lambda) = \lambda I_k + J_k(0)$.

2.4.2 Preuve du théorème de Jordan

2.4.3 Opérations sur les blocs de Jordan

Définition. ***(Matrice H)***

On note $H = (\delta_{i+1,j})_{(i,j)\in[\![1,n]\!]^2}$.

Propriétés

- Pour tout $m \in \mathbb{N}$, $H^m = (\delta_{i+m,j})_{(i,j)\in[\![1,n]\!]^2}$.
- Dès que $m > n$, $H^m = 0$.

Soient λ, λ' deux scalaires et m un entier naturel.

Propriété. ***(Réécriture d'un bloc de Jordan)***

$$J(\lambda) = \lambda I_n + H.$$

Propriété. ***(Somme de blocs de Jordan)***

$$J(\lambda) + J(\lambda') = 2J\left(\frac{\lambda + \lambda'}{2}\right).$$

Propriété. ***(Dilatation d'un bloc de Jordan)***

Pour tout $\mu \in \mathbb{K}^*$, $J(\mu\lambda) = \mu J(\lambda) + \frac{1}{\mu}H$.

Propriété. ***(Produit de blocs de Jordan)***

$$J(\lambda)J(\lambda') = \lambda\lambda' I_n + (\lambda + \lambda')H + H^2.$$

Propriété. ***(Puissance d'un bloc de Jordan)***

$$J(\lambda)^m = \sum_{p=0}^{m} \binom{m}{p} \lambda m - pH^p = \sum_{p=0}^{\min(m,n-1)} \binom{m}{p} \lambda m - pH^p.$$

Lemme. ***(Les blocs de Jordan < 1)***

$(J(\lambda)^m)_{m\in\mathbb{N}}$ tend vers O si et seulement si $|\lambda| < 1$.

2.5 Décompositions factorielles de matrices

Il s'agit de décompositions annexes, dont les démonstrations s'écartent de la théorie de la réduction bien que les résultats s'inscrivent naturellement dans l'exposé de ce cours.

En règle générale, nous cherchons un nombre fini de matrices A_1,...,A_d telle que $A = A_1...A_d$ produit de ces d matrices (souvent, $d = 2$) dès que A vérifie certaines hypothèses, fréquemment relatives à une certaine classe de matrices.

2.5.1 Décomposition J_r

2.5.2 Décomposition LU

2.5.3 Décomposition de Cholesky (LU pour les $\mathcal{S}_n^{++}$

2.5.4 Décomposition QR (ou décomposition d'Iwasawa) et décomposition de Householder

2.5.5 Décomposition ΩS (ou décomposition polaire)

Chapitre 3

Compléments de topologie matricielle

3.1 Normes matricielles

3.1.1 Normes subordonnées matricielles

Définition. ***(Norme matricielle)***

Pour certains auteurs, une norme matricielle n'est rien d'autre qu'une norme sur un espace de matrices (carrées). La majorité rajoute cependant l'hypothèse supplémentaire que cette norme doive être *d'algèbre* (ou *sous-multiplicatives*) : $\|AB\| \leqslant \|A\| \, \|B\|$.

Propriété. ***(Norme matricielle euclidienne)***

La norme euclidienne matricielle peut se récrire : $\|A\|_2 = \sqrt{\rho(AA^*)}$.

Propriété. ***(Norme associée à une matrice HDP)***

Soit une matrice $A \in \mathfrak{M}_n(\mathbb{C})$ hermitienne définie positive. L'application définie par $\varphi_A(x) = \sqrt{\langle x, Ax \rangle}$ est une norme.

Propriété. ***(Provenance des normes de Hölder)***

Pour $p \in [1, +\infty[$, la norme sur l'espace des matrices $\| \cdot \|_p$ est subordonnée à la norme vectorielle correspondante. En particulier, elles sont sous-multiplicative.

3.1.2 Localisation des valeurs propres

Définition. ***(Matrice à diagonale dominante)***

Une matrice $A \in \mathfrak{M}_n(\mathbb{K})$ est dite *à diagonale dominante* si pour tout $i \in [\![1,n]\!]$, $|a_{ii}| \geqslant \sum_{\substack{j=1 \\ j\neq i}}^{n} |a_{ij}|$.

Définition. ***(Matrice à diagonale strictement dominante)***

Une matrice $A \in \mathfrak{M}_n(\mathbb{K})$ est dite *à diagonale strictement dominante* si pour tout $i \in [\![1,n]\!]$, $|a_{ii}| > \sum_{\substack{j=1 \\ j\neq i}}^{n} |a_{ij}|$.

Définition. ***(Matrice à diagonale fortement dominante)***

Une matrice $A \in \mathfrak{M}_n(\mathbb{K})$ est dite *à diagonale fortement dominante* si A est à diagonale dominante et s'il existe $i \in [\![1,n]\!]$ tel que $|a_{ii}| > \sum_{\substack{j=1 \\ j\neq i}}^{n} |a_{ij}|$.

Lemme. ***(Hadamard)***

Toute matrice à diagonale strictement dominante est inversible.

Théorème. ***(Gerschgorin)***

Toute valeur propre d'une matrice complexe A appartient à l'un des disques de Gerschgorin $D_i = \left\{ z \in \mathbb{C}, |A_{ii} - z| \leqslant \sum_{j\neq i} |A_{ij}| \right\}$ pour i allant de 1 à n.

Chapitre 4

Théorie des modules

Résumé

La théorie des modules, bien qu'elle paraisse marginale ou calculatoire, généralise grossièrement en une fois trois notions importantes de l'algèbre commutative : la notion d'idéal d'un anneau, les anneaux noethériens et en fait à moins forte raison les espaces vectoriels (qui correspondent au cas trivial des modules). On y inclut en particulier la notion de groupe abélien !

4.1 Modules sur un anneau

4.1.1 Premières considérations

4.1.1.1 Définition

Soit A un anneau unitaire commutatif, dont on note les lois communément, avec éventuellement des conflits dans la suite (mais bénins).

Définition. ***(Module sur un anneau commutatif)***

Un *A-module* $(M, +, \cdot)$, ou *module (sur A)* est la donnée d'un ensemble M muni d'une loi de composition interne $+$ et d'une loi de composition externe $\cdot : A \times M \longrightarrow M$ telles que :

(1) $(M,+)$ est un groupe abélien ;
(2) $\forall x \in M\ \forall (a,b) \in A^2 \quad (ab) \cdot x = a \cdot (b \cdot x)$;
(2′) $\forall x \in M \quad 1_A \cdot x = x$;
(3) $\forall a \in A\ \forall (x,y) \in M^2 \quad a \cdot (x+y) = a \cdot x + a \cdot y$;
(3′) $\forall x \in M\ \forall (a,b) \in A^2 \quad (a+b) \cdot x = a \cdot x + b \cdot x$.

⟶ *Notation.* On notera, bien que cela engendre un conflit, $a \cdot x = ax$.

Remarque. Si A est un corps, un A-module est exactement un A-espace vectoriel. En fait, la définition de A-module est exactement celle d'espace vectoriel où le corps de base est remplacé,

sans résistance aucune, par un anneau commutatif.

Reformulation pratique

Soit $a \in A$. On note :

$$\begin{aligned} \rho(a) : \quad M &\longrightarrow M \\ x &\longmapsto a \cdot x. \end{aligned}$$

La deuxième propriété énonce que $\rho(a)$ est un morphisme de groupes abéliens pour tout A.

Ceci justifie la définition dans la reformulation suivante :

Reformulation pratique

Soit $a \in A$. On note :

$$\begin{aligned} \rho : \quad A &\longrightarrow \mathrm{End}(M) \\ a &\longmapsto \rho(a). \end{aligned}$$

Les propriétés $(2')$, (3) et $(3')$ énoncent que ρ est un morphisme d'anneaux.

Théorème. ***(Définition équivalente des modules)***

Se donner une structure de A-module sur M, revient à se donner une structure de groupes abéliens $(M, +)$ et un morphisme d'anneaux de A dans $\mathrm{End}(M)$.

▷ À écrire, conséquence de la reformulation précédente. ■

On peut, à la lumière de ce résultat, formuler le fait suivant en se rappelant qu'il existe un unique homomorphisme d'anneaux de $\mathbb{Z}$ dans tout anneau donné.

Théorème. ***(Structure de $\mathbb{Z}$-module sur un groupe abélien)***

Tout groupe abélien est naturellement muni d'une unique structure de $\mathbb{Z}$-module.

Corollaire. ***(Description de la catégorie des $\mathbb{Z}$-modules)***

La catégorie des $\mathbb{Z}$-modules est équivalente à la catégorie des groupes abéliens.

▷ Il suffit d'écrire quels sont les foncteurs mis en jeu. ■

Remarque. Cette analogie fondamentale permet de confondre la théorie des groupes abéliens avec une théorie de la dimension adaptée aux $\mathbb{Z}$-modules. C'est pour cette raison qu'en présence d'un groupe abélien G, on parle parfois d'*anneau de groupe*.

On construit des modules très simples à partir de A lui-même, de même qu'on le faisait dans les espaces vectoriels.

Propriété. ***(Tout anneau est un module sur lui-même)***

$(A, +, \times)$ est un A-module.

Propriété. ***(Puissance cartésienne d'un anneau)***

Pour tout $n \in \mathbb{N}$, $(A^n, +, \times)$ est un A-module.

Exercice 9

Justifier que pour un anneau B, $A \times B$ est muni de la structure de A-module.

Exemples

1. Pour $A = \mathbb{Z}$, pour tout $n \in \mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$ est un $\mathbb{Z}$-module. Ainsi A ne s'injecte pas dans tout A-module, contrairement au cas des corps.
2. Pour $A = \mathbb{K}[X]$, $\mathbb{K}$ un corps, pour tout $P \in \mathbb{K}[X]$, $\mathbb{K}[X]/(P)$ est un $\mathbb{K}[X]$-module.
3. Pour A quelconque, pour tout idéal I de A, A/I est un A-module.
4. Les idéaux de A sont des A-modules.
5. Toute A-algèbre est naturellement munie de la structure de A-module.
6. Anticipons sur la suite. D'après la théorie de la dimension pour les espaces vectoriels, tout espace de dimension finie (mais la dimension infinie s'y raccroche relativement), sera isomorphe à un certain $\mathbb{K}^n$. Ce n'est plus le cas pour les modules, où cette propriété sera étudiée sous le nom de *liberté*.
   Donnons un exemple où l'isomorphie est forcément mis en défaut. Prenons $A = \mathbb{Z}[X]$ et posons $M = \mathbb{Z}[X]/X^2$. Par division euclidienne, on a l'isomorphisme en tant que $\mathbb{Z}$-module $\mathbb{Z}[X]/X^2 \simeq \mathbb{Z}\langle 1, X\rangle \simeq \mathbb{Z}^2$ qui n'est pas isomorphe à un anneau de polynômes.

On revient sur les points **1.** et **4.** qui sont fondamentaux. Dans la théorie des espaces vectoriels sur un corps $\mathbb{K}$, tout espace E qui n'est pas l'espace nul admet un sous-espace de dimension 1 de la forme $\mathbb{K}x$ pour un certain $x \in \mathbb{K}$. En particulier, $\mathbb{K}$ s'injecte dans tout espace vectoriel non nul sur $\mathbb{K}$ (en fait, grâce à la propriété d'inversibilité qui donne que $\lambda \cdot x = 0$ ssi $\lambda = 0$ ou $x = 0$; le phénomène généré par l'absence de cette propriété dans les modules étant appelé *torsion*). Cette propriété donne une certaine rigidité à la catégorie des $\mathbb{K}$-espaces vectoriels qui n'est plus dans celle des A-modules pour un anneau (même intègre !) A qui n'est pas un corps. (On verra même que dans ce cas, il existe toujours un A-module dont tous les éléments sont de torsion.)

En effet, premièrement, les idéaux de A sont des A-modules, donc, déjà, il existe des A-modules strictement plus petit que A au sens ensembliste ! (Ceci n'a plus cours sinon puisque les idéaux d'un corps sont triviaux.)

Deuxièmement, lorsqu'on introduira la théorie de la dimension pour les modules, on verra très simplement que A est un A-module de dimension 1, puisque généré par 1. Dès qu'un idéal de A n'est pas principal, il ne pourra pas être de dimension inférieure à A en tant que A-module ; en particulier, pour que la théorie soit cohérente, il ne pourra pas admettre de base : c'est un module *non libre*, phénomène interdit pas le théorème de la base incomplète, absent pour les modules. D'autre part, on pourra même avoir des sous-modules strict de même dimension que le module de départ, par exemple, $2\mathbb{Z}$ dans $\mathbb{Z}$.

Troisièmement, dès qu'un idéal de A n'est pas de type fini, on aura même un sous-module de A, trivialement de type fini, qui n'est pas engendré par une famille finie, d'où une réelle dissymétrie avec la notion de sous-espace vectoriel qui vient de ce que la notion d'idéal d'un anneau est très peu rigide par rapport à celle de sous-espace linéaire.

Ainsi tous les grands problèmes de la théorie dimensionnelle des modules sont déjà présents à cause de la notion d'idéal de l'anneau A. On peut les extrapoler, pour les esprits retors, à des modules plus grands que A en observant que si I est un idéal de A, alors $I \times ... \times I$ est un idéal de A^n.

On enchaîne avec la notion de sous-module.

4.1.1.2 Sous-modularité

Définition. ***(Sous-module)***

Soit M un A-module. Une partie N de M est un *sous-module* de M si :

- $(N,+)$ est un sous-groupe de $(M,+)$;
- $\forall a \in A, n \in N \quad a \cdot n \in N$.

Propriété. ***(Caractérisation linéaire des sous-modules)***

Une partie N d'un module M est un sous-module de M, si et seulement si, $0_M \in N$ et pour tous $\lambda \in A$, pour tous $x,y \in N$, $\lambda x + y \in N$.

Le cas particulier des anneaux donne un parallèle intéressant.

Propriété. ***(Sous-modules d'un anneau)***

Les sous-modules d'un anneau sont ses idéaux.

▷ Découle mot à mot de la définition de sous-module et d'idéal. ■

Propriété. ***(Sous-modules d'un groupe abélien)***

Les sous-modules d'un groupe commutatif vu en tant que $\mathbb{Z}$-module sont exactement ses sous-groupes vus en tant que $\mathbb{Z}$-modules.

Propriétés. ***(Sous-modules triviaux)***

Si M est un A-module, alors $\{0\}$ et M sont des A-sous-modules de M.

▷ Rien de particulier. ■

Comme pour toute structure algébrique, la notion de sous-module est stable par intersection quelconque.

Propriété. ***(Intersection de sous-modules)***

Soit $(N_i)_{i\in I}$ une famille de sous-modules de M indexée par un ensemble I quelconque. Alors $\cap N_i$ est un sous-module de M.

▷ Même vérification que d'habitude. ■

On en déduit ceci :

Propriété. ***(Sous-module engendré)***

Soit X une partie de M. Alors il existe un plus petit sous-module de M contenant X.

▷ C'est l'intersection de tous ces modules : $\langle X\rangle = \bigcap_{\substack{X\subseteq N\subseteq M \\ N \text{ sous-module de } M}} N$. ■

De même que pour les espaces vectoriels, la caractérisation linéaire des sous-modules permet la caractérisation suivante du sous-module engendré :

Propriété. ***(Caractérisation linéaire du sous-module engendré)***

Soit X une partie de M. Alors on peut décrire :

$$\langle X\rangle = \{\sum_{i\in I} a_i x_i, I \text{ fini}, a_i \in A, x_i \in X \qquad \forall i \in I\}.$$

Remarque. Pour certains auteur, la *somme* d'une famille infinie de sous-modules de M est le sous-module engendré par leur union. C'est en fait la même terminologie que pour les idéaux.

Exercice 10

Sous quelle condition la réunion de deux sous-modules est encore un sous-module de A ?

▷ **Éléments de réponse.**

Même chose que d'habitude.

4.1.1.3 Le module nul

Soit A un anneau commutatif. Alors $\{0_A\}$, en tant qu'idéal de A, est un A-module. Il est fini, de type fini, libre, admettant pour base $\emptyset$.

4.1.1.4 Morphismes de modules

Définition. ***(Morphisme de modules, application linéaire entre modules)***

Soient M,N deux A-modules. Une application $f : M \longrightarrow N$ est dite *A-linéaire* si :

1. $f : (M, +) \longrightarrow (N, +)$ est un morphisme de groupes abéliens ;
2. $\forall a \in A, \forall m \in M \quad f(am) = af(m)$.

On dit également que f est un *morphisme de A-modules* de M vers N.

On peut l'énoncer de façon beaucoup plus pratique, comme dans le cas des espaces vectoriels (encore...).

Reformulation pratique. ***(Caractérisation linéaire des morphismes)***

Une application $f : M \longrightarrow N$, pour M,N deux A-modules, est linéaire si et seulement si, pour tous $\lambda \in A$, pour tous x,$y \in M$, $f(\lambda x + y) = \lambda f(x) + f(y)$.

Des considérations immédiates qui ne font aucune différence avec la théorie des applications linéaires entre espaces vectoriels.

Définition. ***(Isomorphisme de modules)***

Soient M,N deux A-modules. Une application $f : M \longrightarrow N$ est un *isomorphisme de A-modules* si c'est une application A-linéaire qui soit de plus bijective.

Définition. ***(Endomorphisme de modules)***

Soit M un A-module. Un *endomorphisme de A-modules* est une application linéaire de M dans M.

Définition. ***(Automorphisme de modules)***

Soit M un A-module. Un *automorphisme de A-modules* est un endomorphisme bijectif de M. Ce qui revient au même, c'est un isomorphisme de M dans M.

Propriété. ***(Composition de morphismes de modules)***

Soient M_1,M_2,M_3 trois A-modules Soit $f : M_1 \longrightarrow M_2$ et $g : M_2 \longrightarrow M_3$ deux applications linéaires. Alors $g \circ f$ est une application A-linéaire.

Remarque. Notons de façon très peu excitante que la composition d'isomorphismes (resp. d'endomorphismes, d'automorphismes) est encore un isomorphisme (resp. un endomorphisme,

un automorphisme).

Propriété. ***(Réciproque d'un isomorphisme de A-modules)***

L'application réciproque d'un isomorphisme de A-modules est un isomorphisme de A-modules.

Cette proposition, comme on la voit souvent, rassure.

Propriété. ***(Injection linéaire d'une sous-structure de module)***

Soit M un A-module et N un sous-module de M. Soit i l'injection $N \hookrightarrow M$ canonique. Il existe une unique structure de A-module sur N telle que i est A-linéaire.

On étudie, comme dans le cas de l'algèbre linéaire, le noyau et l'image des applications linéaires.

Propriété. ***(Noyau d'une application linéaire)***

Le noyau $\mathrm{Ker}(f)$ d'une application linéaire f entre A-modules est un sous-module du départ.

Propriété. ***(Image d'une application linéaire)***

L'image $\mathrm{Im}(f)$ d'une application linéaire f entre A-modules est un sous-module d'arrivée.

▷ À faire les deux, juste pour se réveiller. ■

On rappelle que, dans le cas des anneaux, le noyau n'est pas un sous-anneau mais un idéal. C'est bien cohérent avec le fait que les sous-modules d'un anneau soient ses idéaux et non ses sous-anneaux. On traitera à profit l'exercice suivant pour se clarifier les idées...

Exercice 11

Une forme linéaire non nulle d'un module est-elle nécessairement surjective ?

De même :

Propriété. ***(Image réciproque d'un module)***

Soient M,M' deux A-modules et $f : M \longrightarrow M'$ linéaire. Alors $f^{-1}(A)$ est un sous-module de M.

Propriété. ***(Image directe d'un module)***

Soient M,M' deux A-modules et $f : M \longrightarrow M'$ linéaire. Alors $f(A)$ est un sous-module de M'.

On dispose des deux propriétés-en-une-seule suivantes, dont la généralité mérite que l'on y reste quelques secondes.

Propriété. ***(Restriction, extension des scalaires)***

Soient A,B deux anneaux commutatifs. Soit $\eta : A \longrightarrow B$ un morphisme d'anneaux. Alors si M est un B-module, M est un A-module.

▷ Par caractérisation abstraite des modules, M est un B-module, c'est-à-dire qu'il existe un morphisme d'anneaux $\rho : B \longrightarrow \mathrm{End}(M,+)$. Par composition de morphismes d'anneaux, $\rho \circ \eta : A \longrightarrow \mathrm{End}(M,+)$ est également un morphisme d'anneaux, donc M est aussi un A-module. ■

Corollaire. ***(Module sur un sous-anneau)***

Soient $A' \subseteq A$ deux anneaux, A' un sous-anneau de A. Si M est un A-module, alors M est naturellement un A'-module.

Corollaire. ***(Transmission de la modularité)***

Soient A,B deux anneaux commutatifs tels qu'il existe un morphisme d'anneaux de $A \longrightarrow B$. Alors B est un A-module.

Exercice 12

Soient K_1 et K_2 deux corps où K_1 est un sous-corps strict de K_2. K_1 est-il un K_2 espace vectoriel ? Expliquer en quoi cela ne contredit pas la propriété précédente.

▷ **Éléments de réponse.**

Que dire d'un morphisme d'anneaux entre deux corps ?

Corollaire. ***(Modularité des idéaux d'un autre anneaux)***

Soient A,B deux anneaux commutatifs tels qu'il existe un morphisme d'anneaux de $A \longrightarrow B$. Alors tous les idéaux de B sont des A-modules.

Remarque. Naturellement, les suites à coefficients A^I et les suites à support fini $A^{(I)}$ sont des A-modules, parce que ce sont des A-algèbres.

Les morphismes de modules permettent de construire d'autres modules, ainsi que des A-algèbres.

Propriété. ***(Groupe des automorphismes de modules)***

Soit M un module. Alors $(\mathrm{Aut}(M), \circ)$ est un groupe.

Propriété. ***(Algèbre des endomorphisme de modules)***

Soit M un module. Alors $(\mathrm{End}(M), +\circ)$ est muni de la structure de A-algèbre.

On peut pour finir réénoncer la propriété universelle des polynômes dans le cadre général des A-modules. Elle a ça d'intérêt qu'elle donne une *base* sur cet espace en le plaçant au centre de la théorie de la dimension des modules de type I, pour un ensemble I.

Propriété. ***(Propriété universelle des suites à support fini)***

Soient A un anneau commutatif et I un ensemble. Le A-module $A^{(I)}$ muni de la structure canonique vérifie la propriété universelle : pour tout A-module M, pour tout $(x_i)_{i\in I} \in M^I$, il existe une unique application A-linéaire

$$\phi : A^{(I)} \longrightarrow M$$

vérifiant $\phi(e_i) = x_i$ pour tout $i \in I$, en notant $e_i = (d_i^j)_{j\in I}$ pour tout $i \in I$.

Ceci introduit en douceur la partie suivante, dont l'austérité du formalisme sera aisément évitée en pensant à l'analogie avec les espaces connus (prendre $A = \mathbb{R}$ et $M = \mathbb{R}^2$, par exemple).

4.1.1.5 Produits et sommes de modules

On introduit le notion de produit, pour pouvoir parler de somme (directe externe), qui ouvre la théorie de la dimension linéaire. Notons que les considérations de cette partie sont très semblables à celles des espaces vectoriels, la bifurcation ayant lieu ensuite.

Définition-propriété. ***(Produit quelconque de modules)***

Soient I un ensemble et $(M_i, +_I, \cdot_I)_{i\in I}$ une famille de A-modules. L'ensemble $\prod_{i\in I} M_i$ est un A-module lorsque muni des opérations $+$ et $\cdot$ suivantes, pour tous $a \in A$, $(x_i)_{i\in I} = x, (y_i)_{i\in I} = y \in \prod_{i\in I} M_i$:

$$x + y = (x_i +_I y_i)_{i\in I} a \cdot x = (a \cdot x_i)_{i\in I}.$$

C'est le *A-module produit des $(M_i)_{i\in I}$*.

Propriété. ***(Régularité des projections)***

De plus pour tout $j \in I$, la projection $p_j : \prod_{i\in I} M_i \longrightarrow M_j$ est A-linéaire.
$(x_i)_{i\in I} \longmapsto x_j$

La structure produit est munie de la propriété universelle suivante :

Propriété. ***(Propriété universelle du produit de A-modules)***

Soient $(M_i)_{i\in I}$ une famille de A-modules et M le module produit. Soit M' un A-module et pour tout $i \in I$, $f_i : M' \longrightarrow M_i$ une application A-linéaire. Pour tout $j \in I$, on note p_j la j-ième projection canonique de M. Alors il existe une unique application A-linéaire

$$f : M' \longrightarrow M$$

telle que $p_j \circ f = f_j$ pour tout $j \in I$.

▷ On doit définir f par $f(x) = (f_i(x))_{i\in I}$ pour tout $x \in M'$! ■

Remarque. On peut écrire $A^I = \prod_{i\in I} A$ et l'on se ramène de l'étude de A^I à l'étude du produit de modules.

Définition-propriété. ***(Somme directe (externe) de sous-modules)***

Soit I un ensemble et $(M_i)_{i\in I}$ une famille quelconques de A-modules. Le sous-ensemble de $\prod_{i\in I} M_i$ constitué des familles presque nulles est un sous-module de $\prod M_i$, noté $\bigoplus_{i\in I} M_i$, appelé *somme directe* des M_i, ou *somme directe externe* pour plus de clarté par rapport aux sommes de sous-espaces, même si c'est fondamentalement pareil... est encore un A-module.

Remarque. Lorsque I est fini, $\prod_{i\in I} M_i = \bigoplus_{i\in I} M_i$.

Propriété. ***(Propriété universelle de la somme directe de A-modules)***

Soient $(M_i)_{i\in I}$ une famille de A-modules et M le module produit. Soit M' un A-module et pour tout $i \in I$, $f_i : M' \longrightarrow M_i$ une application A-linéaire. Pour tout $j \in I$, on note $\iota_j : M_j \longrightarrow \bigoplus_{i\in I} M_i$. Alors il existe une unique application A-linéaire
$x \longmapsto (x_i)_{i\in I} = (\delta_i^j x)_{i\in I}$

$$f : \bigoplus_{i\in I} M_i \longrightarrow M'$$

telle que $f \circ \iota_j = f_j$ pour tout $j \in I$.

Cette propriété abstraite est très semblable à celle qui définit le produit tensoriel ; on tâchera de la retenir, pour sa conception.

Essayons de retenir le fait général suivant : pour le produit, les choses se passent bien avec les surjections projections ; pour la somme directe (qui n'est autre que le co-produit), les choses se passent bien avec les injections inclusions.

4.1.1.6 Somme de sous-modules

La proposition suivante nous donne sous quelles conditions un module est somme de quelques uns de ses sous-modules, et pressent par là une théorie de la décomposition.

Propriété. ***(Critère de décomposition d'un module en somme de sous-modules)***

Soit M un A-module. Soit $(M_i)_{i\in I}$ une famille sous-module de M. On a l'équivalence entre :

(i) $f : \bigoplus_{i\in I} M_i \longrightarrow M$ est un isomorphisme,

(ii) $M = \sum_{i\in I} M_i$ et pour tout $j \in I$, $M_j \cap \sum_{i\in I\setminus\{j\}} M_i = \{0\}$.

Ce formalisme, qui est le même que pour les espaces vectoriels, n'est sans doute pas celui avec lequel l'étudiant est familier. Rappelons-lui qu'en construction, on a bien pourtant : $\mathbb{R} \oplus \mathbb{R} = \mathbb{R}^2$.

Définition. ***(Module, algèbre graduée)***

Soient A un anneau et M un A-module ou une A-algèbre. On dit que M est *gradué* si $M = \bigoplus_{n\in\mathbb{N}} M_n$ avec les M_n des sous-A-modules ou algèbres de M.
Dans ce cas, M_n est la *composante* de M de *degré* n. On dit qu'un élément $x \in M$ est *homogène* s'il est non nul et à appartient à l'un des M_n, et son *degré* est n.

Ceci dit, on peut bien définir la supplémentarité qui sera directement utilisée dans la proposition suivante.

Définition. ***(Supplémentaire)***

Soient M un A-module et M', M'' deux de ses sous-A-modules. On dit que M'' est supplémentaire de M' dans M, si $M = M' \oplus M''$.

Définition. ***(Facteur direct)***

Soient M un A-module et M' un sous-A-module de M. On dit que M' est un *facteur direct* s'il admet un supplémentaire.

Un sous-module n'est pas toujours un facteur direct, contrairement au cas des espaces vectoriels. En effet, soit $I = 2\mathbb{Z}$ sous-$\mathbb{Z}$-module de $\mathbb{Z}$. Soit J un supplémentaire, $J = b\mathbb{Z}$. Alors en particulier $I + J = \mathbb{Z}$, donc $\text{pgcd}(2,b) = 1$. Il n'y a jamais unicité des coefficients de Bézout, donc la somme n'est pas directe ; on aurait aussi pu dire : $I \cap J = \text{ppcm}(2,b)\mathbb{Z} = 2b\mathbb{Z} \neq \{0\}$.

4.1.1.7 Modules quotients

On rappelle que l'on prend un anneau A **commutatif**.

Définition-propriété. ***(Quotient d'un module par un sous-module)***

Soit M un A-module. Soit $(M', +)$ un sous-groupe abélien de $(M,+)$. Les deux conditions suivantes sont équivalentes :

(i) M' est un sous-module de M ;

(ii) il existe sur le groupe quotient M/M' une structure de A-module telle que la surjection canonique $\pi : M \longrightarrow M/M'$ soit A-linéaire.

En outre, si une telle structure de A-module existe sur M/M', elle est unique. Muni d'elle, M/M' est appelé *module quotient* de M par M'.

▷ La projection $M \longrightarrow M/M'$ est un morphisme de groupes abéliens où l'on rappelle que M/M' est l'ensemble des classes d'équivalence pour la relation sur les $(x,y) \in M^2$ donnée par xRy si et seulement si $x - y \in M'$. Rappelons aussi que $\text{Ker}(\pi) = M'$.

Supposons qu'il existe $A \times M/M' \longrightarrow M/M'$, la loi externe seule nous intéressant d'après l'hypothèse sur les groupes, une structure de A-module sur M/M' telle que $\pi : M \longrightarrow\!\!\!\!\!\rightarrow M/M'$ soit A-linéaire. On voit que cette structure est unique, car pi est injective : pour $a \in A$, $m \in M$, $M/M' \ni a \cdot \overline{m} = a\pi(m) = \pi(am)$ d'où l'unicité. De plus $M' = \text{Ker}(\pi)$ est bien un (sous-)A-module.

Supposons que M' est un sous-A-module. On veut définir une structure de A-module sur M/M'. Posons $(a, \overline{m}) \longrightarrow \pi(am)$ de $A \times M/M' \longrightarrow M/M'$. On vérifie que ceci est bien défini en ne dépendant pas du choix de m, puis qu'elle munit M/M' de la structure de A-module, telle que $\pi : M \longrightarrow M/M'$ soit A-linéaire et le tour est joué. ■

Sans surprise :

Propriété. ***(Premier théorème d'isomorphisme pour les modules)***

Soit $f : M \longrightarrow M'$ un morphisme de A-modules. Alors il existe un unique morphisme $\overline{f} : M/\mathrm{Ker}(f) \longrightarrow M'$ de A-module tel que

$$\begin{array}{ccc} M & \xrightarrow{f} & M' \\ {\scriptstyle\pi}\downarrow & \nearrow_{\overline{f}} & \\ M/\mathrm{Ker}(f) & & \end{array}$$

commute, soit $\overline{f} \circ \pi = f$. De plus, $\mathrm{Im}(f) = \mathrm{Im}(\overline{f})$ et $\overline{f}$ est un isomorphisme sur son image.

Propriété. ***(Théorème de factorisation pour les modules)***

Soit $f : M \longrightarrow M'$ un morphisme de A-modules. Soit N un sous-module de M et $\pi : M \longrightarrow M/N$ la projection canonique. Alors les conditions suivantes sont équivalentes :

(i) $N \subseteq \mathrm{Ker}(f)$;

(ii) il existe un unique morphisme $g : M/N \longrightarrow M'$ de A-modules tel que $g \circ \pi = f$, soit

$$\begin{array}{ccc} M & \xrightarrow{f} & M' \\ {\scriptstyle\pi}\downarrow & \nearrow_{\overline{f}} & \\ M/N & & \end{array}$$

commute.

Remarquons que le premier énoncé découle du second e prenant $N = \mathrm{Ker}(f)$ et en montrant également, mais c'est facile, que les images coïncident. On montre donc le deuxième énoncé.

Preuve.

▷ Il suffit de vérifier que le morphisme donné pour le théorème de factorisation sur les groupes est bien un morphisme de modules. ■

4.1.1.8 Suites exactes de modules

On définit, de même que dans le cas des groupes et des espaces vectoriels, la notion de suites exactes. Elle est fondamentale pour montrer les propriétés de la théorie de la dimension des modules.

Définition. ***(Suite exacte de A-modules)***

Une *suite exacte de A-modules* est typiquement la donnée de trois A-modules M,M',M'' tels que $M' \xrightarrow{f} M \xrightarrow{g} M''$ où $\mathrm{Im}(f) = \mathrm{Ker}(g)$.
Plus généralement, c'est une collection de A-modules $(M_i)_{i\in\mathbb{N}}$ et de morphismes de A-modules $f_i : M_i \longrightarrow M_{i+1}$ tels que $M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1}$ et pour tout $i \in \mathbb{N}^*$, $\mathrm{Ker}(f_i) = \mathrm{Im}(f_{i-1})$.

Attention ! Il n'y a aucune raison que les f,g soient uniques.

Propriété. ***(Exactitude à gauche)***

Soit $f : M_1 \longrightarrow M_2$ A-linéaire. Alors $M_1 \xrightarrow{f} M_2 \longrightarrow 0$ est exacte si et seulement si f est surjective.

On rappelle que, comme dans toute catégorie habituelle, il existe une unique flèche partant du module nul vers tout module, et qu'elle est injective (non surjective, sauf si le module d'arrivée est nul), et qu'il existe une unique flèche partant de tout module vers le module nul, et qu'elle est surjective (non injective, sauf si le module de départ est nul). En particulier, il existe une unique flèche du module nul dans lui-même, et c'est un isomorphisme.

Propriété. ***(Exactitude à droite)***

Soit $f : M_1 \longrightarrow M_2$ A-linéaire. Alors $0 \longrightarrow M_1 \xrightarrow{f} M_2$ est exacte si et seulement si f est injective.

Le vocabulaire est le même qu'en toute généralité.

Définition. ***(Suite exacte courte de A-modules)***

Une suite exacte courte (ou *(A-Mod)-sec*) est une suite exacte à trois termes non nuls partant et arrivant à zéro :

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0.$$

Propriété. ***(Exactitude des suites courtes)***

$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$ est exacte ssi f injective, g surjective et $\mathrm{Ker}(g) = \mathfrak{Im}(f)$.

Dans le cas particulier des modules qui nous intéresse, ce lemme donne :

Propriété. ***(Encadrement exact de la somme de sous-modules)***

$0 \longrightarrow M_1 \longrightarrow M_1 \oplus M_2 \longrightarrow M_2 \longrightarrow 0$ est exacte.

Une dernière chose :

Propriété

Soit $f : M_1 \longrightarrow M_2$ un morphisme de A-modules. Si la suite courte

$$0 \longrightarrow \mathrm{Ker}(f) \hookrightarrow M_1 \xrightarrow{f} \mathrm{Im}(f) \longrightarrow 0$$

est exacte, alors

$$0 \longrightarrow M_1/\mathrm{Ker}(f) \overset{\overline{f}}{\hookrightarrow} M_2 \twoheadrightarrow M_2/\mathrm{Im}(f) \longrightarrow 0$$

est également une suite exacte courte.

Notons que le premier théorème d'isomorphisme donne une suite exacte courte :

Propriété. ***(Sec du premier théorème d'iso)***

On a, pour tous modules M' sous-module de M,

$$0 \longrightarrow M' \hookrightarrow M \twoheadrightarrow M/M' \longrightarrow 0$$

qui est une suite exacte.

Cette notion de cohomologie se révèlera utile en théorie abstraite des modules.

4.1.1.9 Bimodules

Définition. ***(Bimodule)***

Soient R,S deux anneaux. Un *R-S-bimodule* est un groupe abélien $(M,+)$ tel que M est un R-module à gauche et M est un S-module à droite, avec la condition de compatibilité suivante, dite *pseudo-associativité* :

$$\forall r \in R\ \forall s \in S\ \forall m \in M \quad (r._R m).{}_S s = r._R(m._S s).$$

On note parfois M_A^B où ${}_B^A M$ un bimodule M sur A-B. Pour bien faire comprendre le sens d'action, on note parfois ${}_A M_B$ ou ${}^A M^A$ ou encore ${}_A M_B$ ou ${}^A M^B$.

⟶ *Convention.* Un R-R-bimodule est tout simplement appelé un *R-bimodule*.

Exemples. ***(Bimodules)***

1. Si R et S sont commutatifs, un R-S-bimodule est exactement la donnée d'un R-module qui est aussi un S-module. Si S est commutatif, un R-S-bimodule est un R-module à gauche qui est aussi un S-module à gauche. Si R est commutatif, un R-S-bimodule est un S-module à droite qui est aussi un R-module à droite.
2. Réciproquement, tout R-module M où R est commutatif est canoniquement un R-bimodule. En effet, si M est un R-module à gauche, on peut définir la multiplication à droite comme la même multiplication qu'à gauche, et cela fonctionne. De même en inversant les rôles. Cependant, tous les R-bimodules sur des anneaux commutatifs

ne sont pas décrits de cette manière : on peut faire différer les lois à gauche et à droite a priori.

3. Toute algèbre A sur un anneau R est canoniquement munie de la structure de R-bimodule. Si φ est le morphisme canonique, il suffit de poser $r.a = \varphi(r)a$ et $a.r = a\varphi(r)$ pour tous $r \in R, a \in A$.
4. En particulier, tout anneau R est un R-bimodule. Dans ce cas, la pseudo-associativité traduit l'associativité dans R.
5. Tout idéal bilatère d'un anneau R en est un R-bimodule.
6. Si M est un R-module à gauche, alors M est un R-$\mathbb{Z}$-bimodule avec la loi d'itération évidente sur $\mathbb{Z}$. De même, si M est un R-module à droite, alors M est un $\mathbb{Z}$-R-bimodule avec la loi d'itération évidente sur $\mathbb{Z}$.
7. Si R est un sur-anneau de S, alors S est un R-R-bimodule, un R-S-bimodule et un S-R-bimodule.

4.1.2 Produit tensoriel entre modules

Dans toute la suite, on fixe A un anneau commutatif.

4.1.2.1 Introduction : cas des espaces vectoriels

Soient E,F deux espaces vectoriels sur un corps K. Alors il existe un espace vectoriel $E \otimes F$ et une application bilinéaire $\phi : E \times F \longrightarrow E \otimes F$, et l'on pose $\phi(x,y) = x \otimes y$, vérifiant la propriété universelle suivante : pour tout espace vectoriel G sur le corps K, pour toute application bilinéaire g de $E \times F$ dans G, il existe une et une seule application linéaire $\tilde{g} : E \otimes F \longrightarrow G$ telle que $g = \tilde{g} \circ \varphi$.

L'espace $E \otimes F$ est appelé *produit tensoriel* de E et de F. De même, on note $x \otimes y$ le produit tensoriel de x et y.

Intuitivement, le produit tensoriel permet de transformer des applications bilinéaires en application linéaire sur un certain espace (bien que plus compliqué).

Dans la section suivante, on donne une construction explicite de cet objet.

4.1.2.2 Produit tensoriel de deux modules

Définition. ***(Produit tensoriel)***

Soient M,N deux A-modules. On note $C = A^{(M\times N)}$ le A-module des applications de $M\times N$ dans A presque partout nulles, vu comme l'espace des combinaisons linéaires formelles d'éléments de $M \times N$. Alors C est un A-module libre de base canonique $(e_{(x,y)})_{(x,y)\in M\times N}$ où $e_{(x,y)}(u,v) = \delta^{(u,v)}_{(x,y)}$.

On note D le sous-module de C engendré par les éléments de la forme :

- $e_{(x+y,z)} - e_{(x,z)} - e_{(y,z)}$, x,$y \in M$, $z \in N$,
- $e_{(x,y+z)} - e_{(x,y)} - e_{(x,z)}$, $x \in M$, y,$z \in N$,
- $e_{(\alpha x,y)} - \alpha e_{(x,y)}$, $x \in M$, $y \in N$, $\alpha \in A$,
- $e_{(x,\alpha y)} - \alpha e_{(x,y)}$, idem,

pour les parcourant. (On veut en effet que ces éléments soient nuls par bilinéarité.)

Sous ces conditions, on appelle *produit tensoriel* de M et N, et l'on note $M \otimes N$, ou $M \otimes N$ s'il n'y a pas d'ambiguïté, le A-module C/D. La projection fournit une application bilinéaire $\varphi : M \times N \to M \otimes N, (x,y) \mapsto x \otimes y$.

Pour un module N donné, *tensorialiser* un module M par N revient à prendre le produit tensoriel $M \otimes N$.

Reformulation pratique. ***(Identités dans le produit tensoriel)***

Soient M,N deux A-modules. Soient x,$x' \in M$, y,$y' \in N$, λ,$\mu \in A$. Alors :

1. *(Biadditivité 1)* $(x + x') \otimes y = x \otimes y + x' \otimes y$;
2. *(Biadditivité 2)* $x \otimes (y + y') = x \otimes y + x \otimes y'$;
3. $(x + y) \otimes (x' + y') = x \otimes y + x \otimes y' + x' \otimes y + x' \otimes y'$;
4. *(Unicité de l'action de A)* $\lambda(x \otimes y) = (\lambda x) \otimes y = x \otimes (\lambda y)$;
5. $(\lambda x) \otimes (\mu y) = \lambda\mu(x \otimes y)$.

Cette construction répond trivialement au problème de l'introduction.

Propriété. ***(Propriété universelle du produit tensoriel)***

Soient A un anneau, M,N deux A-modules. Le produit tensoriel $(N \otimes M, \varphi)$ vérifie la propriété universelle suivante : pour tout K-module, pour toute application bilinéaire f de $M \times N$ dans G, il existe une et une seule application linéaire $\tilde{f} : M \otimes N \to G$ telle que $f = \tilde{f} \circ \varphi$, autrement dit telle que le diagramme

$$\begin{array}{ccc} M \times N & & \\ {\scriptstyle\varphi}\downarrow & \searrow^{f} & \\ NM \otimes N & \xrightarrow[\tilde{f}]{} & G \end{array}$$

commute. En particulier, il est unique à isomorphisme près.

Définition-propriété. ***(Produit tensoriel d'applications linéaires)***

Si M,N,M',N' sont des A-modules et $f : M \to M'$ et $g : N \to N'$ sont des applications linéaires, alors il existe une unique application linéaire dite *produit tensoriel de f et g* $f \otimes g : M \otimes N \to M' \otimes N'$ telle que $(f \otimes g)(x \otimes y) = f(x) \otimes g(y)$.

Propriété. ***(Bifonctorialité du produit tensoriel)***

Soient M,N,M',N' sont des A-modules. Tout morphisme $f : M \to M'$ de A-modules et tout morphisme $g : N \to N'$ de A-modules induisent des morphismes de A-modules :

$$f \otimes id_N : M \otimes N \to M' \otimes N$$

tel que $(f \otimes id_N)(m \otimes n) = f(m) \otimes n$ pour tous $m \in M, n \in N$ et

$$id_M \otimes g : M \otimes N \to M \otimes N'$$

tel que $(id_M \otimes g)(m \otimes n) = m \otimes g(n)$.
Ces applications $f \mapsto f \otimes id_N$ et $g \mapsto id_M \otimes g$ sont fonctorielles, c'est-à-dire qu'elles préservent les morphismes identités et la composition. De plus, on a un diagramme :

$$\begin{array}{ccc} M \otimes N & \xrightarrow{f \otimes id_N} & M' \otimes N \\ {\scriptstyle id_M \otimes g}\downarrow & & \downarrow{\scriptstyle id_{M'} \otimes g} \\ M \otimes N' & \xrightarrow[f \otimes id_{N'}]{} & M' \otimes N' \end{array}$$

commutatif. Autrement dit, le produit tensoriel est bifonctoriel.

▷ On applique la propriété universelle à l'application bilinéaire $(x,y) \mapsto f(x) \otimes g(y)$. ■

Fait. ***(Tenseurs purs)***

Par définition, un élement de M,N est une somme finie $\sum_{i=1} nm_i \otimes n_i$ où les $m_i \otimes n_i$ sont appelés *tenseurs purs* ou *propres*.

Très simple à écrire soi-même. En effet, l'ensemble des éléments du produit tensoriel l'engendre, et un coefficient scalaire peut être stocké dans l'un ou l'autre des membres d'un tenseur pur.

Propriété. ***(Base du produit tensoriel)***

Soient M,N deux A-modules libres de type fini. Soient $(e_1,...,e_m)$ et $(f_1,...,f_n)$ des bases respectives de M et N avec $m,n \in \mathbb{N}$. Alors la famille $(e_i \otimes f_j)_{(i,j) \in [\![1,m]\!] \times [\![1,n]\!]}$ est une base

de $M \otimes_A N$. En particulier, le produit de deux modules libres est libre.

▷ Rien de compliqué. ■

Corollaire. ***(Dimension du produit tensoriel)***

Soient E,F deux K-espaces vectoriels de dimension finie. Alors $\dim(E \otimes_K F) = \dim(E)\dim(F)$.

Corollaire. ***(Identification du produit tensoriel d'espaces vectoriels)***

Soient E,F deux K-espaces vectoriels de dimension finie. Alors $E \otimes_K F = Ł_K(E,F)$.

Exercice 13 *(Produit tensoriel et applications linéaires)*

Expliciter un isomorphisme entre $E \otimes F$ et $\mathcal{L}(E,F)$. Cet isomorphisme est-il encore disponible en dimension finie ?

Propriété. ***(Commutativité du produit tensoriel)***

Soient M,N deux A-modules. Alors $M \otimes_A N \simeq N \otimes_A M$.

Propriété. ***(Associativité du produit tensoriel)***

Soient M,N,P trois A-modules. Alors $M \otimes (N \otimes P) \simeq (M \otimes N) \otimes P$.

Remarque. En un sens, le produit tensoriel est la construction la plus général d'opération associative.

Propriété. ***(Neutralité de l'anneau pour le produit tensoriel)***

Soit M un A-module avec A unitaire.. Alors $A \otimes_A M \simeq M$.

▷ Il suffit d'exhiber $\varphi : M \to A \otimes_A M, m \mapsto 1 \otimes m$ et $\psi : A \otimes_A M \to M, (a \otimes m) \mapsto am$ induite par l'application bilinéaire $A \times M \to M, (a,m) \mapsto am$, et de remarquer que $\psi \circ \varphi = id_{A \otimes_A M}$ et $\varphi \circ \psi = id_M$. ■

Heuristique

Le produit tensoriel est un espace dans lequel l'anneau de base n'existe pas : il se fond dans les tenseurs.

Propriété. ***(Absorbance du module nul pour le produit tensoriel)***

Soit M un A-module. On note 0_A le module nul sur A. Alors $0_A \otimes_A M \simeq 0_A$.

Propriété. ***(Récupération de produit tensoriel)***

Soient V,Y,Z,W des modules sur un même anneau. Alors $(V \otimes Z) \cap (Y \otimes W) = (V \cap Y) \otimes (Z \cap W)$.

Deux petites propriétés utiles pour expliciter des exemples :

Propriété

Soient A un anneau, I un idéal de A et M un A-module. Alors $A/I \otimes_A M \simeq M/IM$.

▷ On peut vérifier la bonne définition de $\tilde{a} \otimes m \mapsto \tilde{am}$ et que c'est un isomorphisme, de réciproque également bien définie $\tilde{m} \mapsto \tilde{1} \otimes m$. ■

Heuristique

La torsion dans l'un des membres du produit tensoriel se répercute sur les autres par unicité de l'action de l'anneau de base.
En particulier, $0 \otimes y = 0$ et $x \otimes 0 = 0$ pour tous x,y.

Propriété

Soient A un anneau, I,J deux idéaux de A. Alors $A/I \otimes_A A/J \simeq A/(I+J)$.

▷ On peut vérifier la bonne définition de $\tilde{a} \otimes \tilde{b} \to \tilde{ab}$ et que c'est un isomorphisme, de réciproque également bien définie $a \cdot (1\ [I]) \otimes (1\ [J])$. On aura là utilisé la pseudo-distributivité de $\mathbb{Z}$ quant à son action sur $\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z}$. ■

Heuristique

Dans un produit tensoriel, les produits s'effacent. En effet, et c'est souvent possible, il faut essayer de les stocker dans l'action de l'anneau de base.

Exemples. ***(Produits tensoriels)***

1. $\mathbb{Z}/n\mathbb{Z} \otimes_Z \mathbb{Q}$ et $\mathbb{Z}/n\mathbb{Z} \otimes_Z (\mathbb{Q}/\mathbb{Z})$ sont nuls.
   Conséquence de la propriété suprécédente. En effet, $\mathbb{Q}$ et $\mathbb{Q}/\mathbb{Z}$ sont n-divisibles, *i.e.* $n\mathbb{Q} = \mathbb{Q}$ et $n(\mathbb{Q}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z}$.
2. En tant que groupes abéliens, $\mathbb{Z}/n\mathbb{Z} \otimes_Z \mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/\text{pgcd}(n,m)\mathbb{Z}$.
   Conséquence de la propriété précédente.

3. $\mathbb{Q} \otimes_Z \mathbb{Q} \simeq \mathbb{Q}$.
   Même idée : il suffit d'observer que $1 \otimes_{\mathbb{Z}} (qq') = q \otimes_{\mathbb{Z}} q'$ pour tous $q,q' \in \mathbb{Q}$.
4. Pour tout anneau R, $R[X] \otimes_R R[Y] \simeq R[X,Y]$. C'est presque pour cela que l'on a introduit le produit tensoriel ! On peut identifier X à $X \otimes 1$, Y à $1 \otimes X$, et XY à $X \otimes Y$.
5. Soit $\mathbb{H}$ la $\mathbb{R}$-algèbre des quaternions. Alors $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{C} \simeq \mathfrak{M}_2(\mathbb{C})$ en tant que $\mathbb{C}$-algèbre. De même, $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{H} \simeq \mathfrak{M}_4(\mathbb{R})$.
   En exercice.

Propriété. ***(Produit tensoriel par un localisé)***

Soient A un anneau, S une partie multiplicative de A et M un A-module. Alors $S^{-1}A \xrightarrow{\sim} \otimes_A M \simeq S^{-1}M$ par $m/1 \mapsto 1 \otimes m$, et cet isomorphisme est fonctoriel en M.

Propriété. ***(Produit tensoriel de bimodules)***

Soient R,S,T trois anneaux. Si M est un S-R-bimodule et N est un R-T-bimodule, alors $M \otimes_R N$ est un S-T-bimodule.

4.1.2.3 Produit tensoriel d'algèbres

Propriété. ***(Homomorphismes d'algèbres d'un produit tensoriel)***

Soient k un corps et A,B,C trois k-algèbres. Alors

$$\mathrm{Hom}_{k\text{-alg.}}(A \otimes_k B,C) = \mathrm{Hom}_{k\text{-alg.}}(A,C) \times \mathrm{Hom}_{k\text{-alg.}}(B,C).$$

4.1.2.4 Produits tensoriels infinis, algèbre tensorielle

Définition-propriété. ***(Algèbre tensorielle)***

Soit V un K-espace vectoriel. On note $T(V)$ l'espace vectorielle $\bigoplus_{n\in\mathbb{N}} V^{\otimes n}$ où $V^{\otimes n} = V \otimes_K ... \otimes_K V$ le produit tensoriel de n copies de V. Alors $T(V)$ est une K-algèbre, dite *algèbre tensorielle* de V, où pour $x = x_0 + x_1 + ...$ et $y = y_0 + y_1 + ...$ avec $x_n,y_n \in V^{\otimes n}$, $xy := \sum_{n,m} x_n \otimes y_n$.

4.1.2.5 Extension du corps de base, complexification

Propriété. ***(Extension du corps de base)***

Soit k un sous-corps de K et E un k-e.v. Alors $E \otimes_k K$ est un K-espace vectoriel. Vu comme k-espace vectoriel, k se plonge dedans par une application linéaire.

Définition. ***(Complexifié)***

Soit E un $\mathbb{R}$-espace vectoriel. On note $\tilde{E}$, et l'on appelle *complexifié*, le $\mathbb{C}$-espace vectoriel $E \otimes \mathbb{C}$.
E s'identifie alors à un sous-espace de $\tilde{E}$ vu comme $\mathbb{R}$-espace vectoriel.

4.2 Produit extérieur entre modules

4.2.1 Algèbre extérieure

Définition. ***(Algèbre extérieure)***

Soit V un K-espace vectoriel. L'*algèbre extérieure* sur V est le quotient de l'algèbre tensorielle $T(V)$ par l'idéal engendrée par les $v \otimes v, v \in V$. On la note $\bigwedge V$.

Propriété. ***(Alternance du produit extérieur)***

Soient u,$v \in V$. Alors $u \wedge v = -v \wedge u$.

4.3 Théorie de la dimension des modules

On se donne toujours un anneau commutatif unitaire A.

4.3.1 Module de type fini

Définition. ***(Typage fini de modules)***

Un A-module M est de *type fini* s'il est engendré par un nombre fini d'éléments, c'est-à-dire s'il existe une partie X de M finie telle que $M = \langle X \rangle$.

Remarquons le fait suivant :

Reformulation pratique. ***(Module de type fini)***

Un module M sur A est de type fini si et seulement s'il existe $n \in \mathbb{N}^*$ et une application A-linéaire surjective $\pi : A^n \twoheadrightarrow M$.

▷ Preuve : il suffit de l'écrire. ■

Corollaire. ***(Type fini en dimension 1)***

A est de type fini sur lui-même.

On verra que même un module de type 1, n'admet pas nécessairement de base... et parfois même des sous-modules de types minimaux plus grand (dans un cas très simple pourtant : trouverez-vous lequel ?)

Corollaire. ***(Dimension $n \in \mathbb{N}$ des modules)***

Pour tout $n \in \mathbb{N}^*$, le module A^n est de type fini.

On peut énoncer sans problème les quelques propriétés suivantes.

Propriété. ***(Transfert du type fini par surjection)***

Soit $M \longrightarrow M'$ une surjection A-linéaire entre les deux modules M,M'. Si M est de type fini, alors M' est de type fini.

▷ Si M est de type fini, c'est qu'il existe $n \in \mathbb{N}$ et $\pi : A^n \longrightarrow M$ surjective. Alors $f \circ \pi : A^n \longrightarrow M'$ est A-linéaire et surjective, donc M' est de type fini par caractérisation. ■

Corollaire. ***(Transfert du type fini sur l'image)***

Soit $M \longrightarrow M'$ une application A-linéaire entre les deux modules M,M'. Si M est de type fini, alors $f(M)$ est un sous-module de M' de type fini.

D'autre part :

Propriété. ***(Transfert du type fini par encadrement sur les suites exactes)***

Si $M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$ est une suite exacte, et si M' et M'' sont de type fini, alors M l'est.

▷ Soient $\xi_1,...,\xi_n$ des générateurs de M'' où n est un entier naturel. Soient $y_1,...,y_m$ des générateurs de M' où m est un entier naturel. Puisque g est surjective, il existe des $x_i \in M$, $i \in [\![1,n]\!]$, tels que $g(x_i) = \xi_i$ pour tout i. Soit $x \in M$. Alors par linéarité de g, $g(x) = \sum_{i=1}^{n} a_i x_i = \sum_{i=1}^{n} a_i g(x_i) = g(\sum_{i=1}^{n} a_i x_i)$ pour des $a_i \in A$ pour tous $i \in [\![1,n]\!]$ certains. Posons $x' = x - \sum_{i=1}^{n} a_i x_i$. Alors $g(x') = 0$ d'après le calcul précédent, donc $x' \in \mathrm{Ker}(g) = \mathrm{Im}(f)$. Ainsi, pour des certains $b_i \in A$ pour tous $i \in [\![1,n]\!]$, $x' = f(\sum_{i=1}^{m} b_i y_i) = \sum_{i=1}^{m} b_i f(y_i)$. Or $x = \sum_{i=1}^{m} b_i f(y_i) + \sum_{i=1}^{n} a_i x_i$ par définition de x'. Donc la concaténation des $(x_i)^n$ et des $(f(y_j))^m$ engendre M. ■

Pour formuler une propriété analogue à celle de surjection pour une injection, on a besoin d'une propriété de noethérianité, dont on verra ensuite que c'est une propriété fondamentale pour les modules. Notons bien que contrairement à ce qui se passe ensemblistement, l'existence d'une surjection dans un sens entre modules n'implique pas celle d'une injection dans l'autre.

Propriété. ***(Transfert du type fini par injection en milieu noethérien)***

Soit $M \longrightarrow M'$ une injection A-linéaire entre les deux modules M,M'. **On suppose que A est noethérien.** Si M' est de type fini, alors M est de type fini.

▷ On suppose donc A noethérien. D'après la reformulation initiale de la définition du typage fini, on veut montrer que tout sous-module d'un module de type fini est de type fini.

Si $M = A$, c'est vrai ; c'est la définition d'être noethérien.

Montrons par récurrence que tout sous-module de A^n est de type fini. Soit $A^{n-1} \xrightarrow{f} A^n \xrightarrow{g} A$ ou $g : (x_1,...,x_n) \mapsto x_n$ et $f : (x_1,...,x_{n-1}) \mapsto (x_1,...,x_{n-1},0)$. La suite est exacte, car $\mathrm{Ker}(g) = \mathrm{Ker}(f)$. Soit N un sous-module de A^n. Alors $N'' = g(N)$ est de type fini, car A est noethérien. De plus, $N' = f^{-1}(N)$ est un sous-module de A^{n-1}. Par hypothèse de récurrence, $f^{-1}(N)$ est de type fini. Ceci donne $f_0 : N' \longrightarrow N$ et $g_0 : N \longrightarrow N''$ dont on vérifie qu'elles sont respectivement injective et surjective et que $\mathrm{Ker}(g_0) = \mathrm{Im}(f_0)$. D'après la propriété précédente, l'encadrement dans une suite exacte courte donne que, puisque N', N'' sont de type fini, N est de type fini. Pour finir, il existe une surjection $\sigma : A^n \longrightarrow M$, car M est de type fini. Pour N un sous-module de M, $\sigma^{-1}(N)$ est un sous-module de type fini de A^n. Il est donc de type fini. Ainsi la restriction $\sigma_0 : \sigma^{-1}(N) \longrightarrow N$ est surjective donc puisque $\sigma^{-1}(N)$ est de type fini, N aussi. ■

Heuristique

On comprend bien que, si l'anneau de base A n'est pas noethérien, un idéal de type non infini va engendrer un truc de dimension finie. Il y aurait donc un problème dès les coefficients, a fortiori dans le module.

Exercice 14

Trouver un contre-exemple à ce qui précède dans le cas d'un anneau noethérien.

▷ **Éléments de réponse.**

Soit A un anneau non noethérien : on sait qu'il en existe, par exemple $\mathbb{R}[(X_i)_{i\in\mathbb{N}}]$. Soit I un idéal de type non fini de A. Alors I est un A-module qui s'injecte naturellement dans le A-module A. Pourtant, il n'est clairement pas de type fini comme A-module, puisqu'en fait les deux notions coïncident alors. Cependant, A est de type fini sur lui-même, engendré par 1 ! Contre-exemple.

Heuristique

Finalement, comme on a dit, dans le cas des modules, contrairement aux espaces vectoriels, les sous-modules d'un module de type fini ne sont pas forcément de type fini (et la proposition précédente dit que c'est vrai si l'anneau de base est noethérien, en utilisant qu'un sous module M' de M s'injecte canonique $M' \hookrightarrow M$.

Ce qui est plus surprenant que les sous-modules d'un module de type fini ne soient pas tous de type fini, c'est que la condition A noethérien suffise !

4.3.1.1 Anneaux finis sur un autre

Définition. ***(Finitude d'un anneau sur un autre)***

Soient A,B deux anneaux et $\varphi : A \to B$. On dit que B est *fini* sur A si B est de type fini en tant que A-module.

Propriété. ***(Tour d'anneaux finis)***

Soient A,B,C trois anneaux. Si B est fini sur A et C est fini sur B alors C est fini sur A.

4.3.1.2 Lemme de Nakayama

Définition. ***(Sous-module engendré par un idéal)***

Soient A un anneau commutatif, M un A-module et I un idéal de A. On note IM l'ensemble des sommes finies d'éléments de la forme $a_i m_i$ avec $a_i \in I$ et $m_i \in M$.

Fait

Avec les notations précédentes, on a toujours $IM \subseteq M$. Ainsi : $IM = M \iff M \subseteq IM$, ce qui n'est pas le cas a priori.

Fait

Si M est de type fini engendré par x_1,...,x_n, alors IM est l'ensemble des sommes de la forme $a_i x_i$, $i \in [\![1,n]\!]$, $a_i \in I$.

Lemme. ***(Nakayama, 1951)***

Soient A un anneau commutatif, M un A-module de type fini et I un idéal de A. Soit N un sous-A-module de M tel que $M \subseteq IM + N$. Alors il existe un élément a de I tel que $(1+a)M \subseteq N$ (autrement dit, un élément r de A tel que $r \cong 1$ $[I]$ et $rM = 0$).

▷ On se place dans le cas particulier où N est nul. On a donc $M \subseteq IM$ et l'on veut montrer qu'il existe $a \in I$ tel que $(1+a)M = 0$. Puisque M est de type fini, on peut prendre x_1,...,x_n des générateurs de M, $n \in \mathbb{N}$. Pour tout $i \in [\![1,n]\!]$, $x_i \in M = IM$ donc $x_i = \sum_{j=1}^{n} y_{i,j} x_j$ pour une certaine matrice $Y = (y_{i,j})_{i,j \in [\![1,n]\!]^2}$. En notant X le vecteur colonne des x_i, on a $YX = X$ d'où $ZX = 0$ avec $Z = I_n - Y$. En multipliant par la comatrice de Z, on a $\det(Z)X = 0$, autrement dit, en prenant $d = \det(Z)$, $dx_i = 0$ pour tout $i \in [\![1,n]\!]$, d'où $dM = 0$. Reste à montrer que $d - 1 \in I$, ce qui

s'observe[1] en développant le déterminant de Z : $d = \begin{vmatrix} 1-y_{1,1} & y_{1,2} & \cdots & y_{1,n} \\ y_{2,1} & 1-y_{2,2} & & \\ \vdots & & \ddots & \\ y_{n,1} & & & 1-y_{n,n} \end{vmatrix}$. En développant par rapport à la première colonne, on obtient $(1-y_{1,1})d_{n-1}+a$ où $a \in A$ au vu de $n-1$ derniers termes la première colonne de Z, qui sont tous dans A : nommément, $a = -y_{2,1}M_{2,1} + ... + (-1)^n y_{n,1}M_{n,1}$. En recommençant le processus au rang $n-1$, puis par récurrence descendante, on obtient facilement (en développant de tête des produits imbriqués...) que $d = (1-y_{1,1})...(1-y_{n,n}) + a_0$, $a_0 \in A$. Il est clair que $(1-y_{1,1})...(1-y_{n,n})$ s'écrit $1+a'$ où $a' \in A$, d'où le résultat.

Revenons au cas général. Le A-module $N' = M/N$ est encore de type fini et vérifie $N' \subseteq IN'$; il suffit d'appliquer ce qui précède pour trouver $a \in I$ tel que $(1+a)N' = (1+a)M/N = 0$, ce qui signifie exactement $(1+a)M \subseteq N$ par les propriétés du quotient. ■

Ainsi on a déjà montré :

Corollaire. ***(Lemme de Nakayama faible)***

Soient A un anneau commutatif, M un A-module de type fini et I un idéal de A. On suppose que $M \subseteq IM$. Alors il existe un élément a de I tel que $(1+a)M = 0$.

Mnémonik : $IM = M \implies im = m \iff (1-i)m = 0$.

On peut énoncer le lemme de Nakayama de diverses manières.

Corollaire. ***(Énoncés autres du lemme de Nakayama)***

Soient A un anneau commutatif, M un A-module de type fini et I un idéal de A. Soit aussi N un sous-A-module de M

1. *(Avec le Jacobson)* Supposons $I \subseteq R$ le radical de Jacobson de A. Si $IM = M$, alors $M = 0 := \{0\}$.
2. *(Avec le Jacobson faible)* Si $RM = M$, alors $M = 0$.
3. *(Avec le Jacobson et les sous-modules)* Si $M = N + RM$, alors $M = N$.

[1] Voici une façon moins crasseuse de conclure. On écrit $d = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} (\delta_{i,\sigma(i)} - y_{i,\sigma(i)})$. Pour un terme de cette somme, si σ ne fixe aucun point, on obtient un produit d'éléments de I qui est donc dans I. Sinon, on obtient, modulo dilatation par un élément de I, une somme d'éléments de 1 additionnée d'un 1. Le signe de ce terme sera $\varepsilon(\sigma) \times (-1)^{D(\sigma)}$ où $D(\sigma)$ est le nombre de points non fixés par σ. À la fin, on pourra écrire $d = y + \sum_{\sigma \in \mathfrak{S}_n, \sigma \notin D_n} \varepsilon(\sigma) \times (-1)^{D(\sigma)}$ où y est dans I et D_n est l'ensemble des dérangements de $\mathfrak{S}_n$. Or cette somme vaut 1, car si l'on en extrait $id_{[\![1,n]\!]}$, dont le terme associé vaut 1, on a une bijection entre les permutations paires qui ne sont pas des dérangements ni l'identité et les permutations impaires qui ne sont pas des dérangements : étant donné $\sigma \neq id$ paire qui n'est pas un dérangement, il y a donc deux points $a,b \in [\![1,n]\!]$ qu'elle fixe ; on associe alors $\sigma\tau_{ab}$. Cette bijection est assez clairement compatible avec $\sigma \mapsto D(\sigma)$. Ces deux sous-sommes ont donc le même nombre d'éléments, et leurs termes sont deux à deux opposés grâce au facteur signature. Il ne reste plus que $\varepsilon(id)(-1)^0 = 1$, ce qu'il fallait montrer.

4. *(Cas local)* Supposons A local et soit I un idéal propre de A. Si $IM = M$, alors $M = 0$.
5. *(Cas local avec les sous-modules)* Supposons A local et notons $\mathfrak{m}$ sont unique idéal maximal. Si $M = N + \mathfrak{m}N$, alors $N = M$.
6. *(Nakayama en termes de générateurs)* On suppose que les images dans M/RM d'éléments $m_1,...,m_n$ engendrent M/RM en tant que R-module ; alors $m_1,...,m_n$ engendrent M en tant que R-module.

▷ Les liens viennent des faits suivants : si $a \in R$, alors $1+a$ est inversible ; l'astuce permettant de passer de Nakayama faible à Nakayama ; dans un anneau local, R est l'unique idéal maximal de A. Le dernier énoncé s'obtient en appliquant Nakayama Jacobson-sous-modules à $N = \langle m_1,...,m_n \rangle$. ■

4.3.2 Module noethérien

Nous pouvons énoncer les définition et propriété suivante :

Définition. ***(Module noethérien)***

Un A-module M est *noethérien* si tout sous-module de M est de type fini.

Heuristique

La noethérianité est une propriété de finitude.

Fait. ***(Noethérien implique de type fini)***

Un module noethérien est de type fini. Tout module est un sous-module de lui-même.

De plus :

Fait. ***(Noethérianité pour un anneau)***

Un anneau est noethérien si et seulement s'il est noethérien en tant que module sur lui-même. Vient de ce que les sous-modules d'un anneau sont ses idéaux et qu'un idéal est de type fini si et seulement s'il est de type fini en tant que A-module.

On rappelle que le typage fini pour un anneau entier est inintéressant : un anneau est toujours de type fini en tant qu'idéal de lui-même ou en tant que module sur lui-même, car il est engendré par 1.

Propriété. ***(Noethérianité d'un module de type fini sur un anneau noethérien)***

Soit M un A-module de type fini. Alors M est noethérien si A est un anneau noethérien.

▷ Si A est noethérien, la proposition précédente a montré que les sous-modules de M qui est de type fini sont également de type fini, donc M est noethérien. ■

Exercice 15

Montrer que la réciproque est fausse.

Proposition. ***(Notion de noethérianité a fortiori)***

Soit B un anneau contenant un anneau A. Si B est un A-module noethérien, alors B est un anneau noethérien.

▷ Par hypothèse, ses idéaux sont de type fini sur A, donc sur B, donc B est un anneau noethérien. ■

Exercice 16

Montrer que la réciproque est fausse.

▷ **Éléments de réponse.**

On cherche un anneau noethérien B, c'est-à-dire noethérien en tant que B-module, qui ne le soit pas en tant que A-module. Le troisième exemple donné ci-dessous convient *(remarque Attention)*.

On montre la propriété déjà partiellement démontrée pour les anneaux, généralisée au cas des modules noethériens.

Théorème. ***(Caractérisation des modules noethériens)***

Soit A un anneau et M un A-module. Les conditions suivantes sont équivalentes :

1. Toute famille non vide de sous-modules admet un élément maximal pour l'inclusion.
2. Toute suite croissante de sous-modules de M est stationnaire.
3. Tout sous-module de M est de type fini (*i.e.* M est noethérien).

▷ Montrons que (1) $\implies$ (3). Soit E un sous-module de M. Soit $\mathcal{A}$ l'ensemble des sous-modules de type fini de E. Il est non vide, car contient le sous-module nul. Par hypothèse, il existe N maximal dans $\mathcal{A}$. Si $N \subsetneq E$, soit $x \in E$, $x \notin N$. Alors $N' = N + Ax$ est un sous-module de E de type fini contenant N strictement, ce qui contredit la maximalité de N, absurde, donc $N = E$ et E est de type fini.

Montrons que (3) $\implies$ (2). Soit $(M_n)_{n\in\mathbb{N}}$ une suite croissante de sous-modules. Alors $\bigcup_{n\geqslant 0} M_i$ est un sous-module de M (en effet, si $x \in M_i, y \in M_j, x+y \in M_{\max(i,j)}$...). Il est donc de type fini engendré par disons x_1,...,x_r où pour tout i entre 1 et r, il existe n_i tel que $x_i \in M_{n_i}$. Pour $n = \max(n_i)$, $x_i \in M_n$ pour tout i donc $\cup M_i = \sum_{i=1}^{r} Ax_i \subseteq M_n$ donc pour tout $k \geqslant n$, $M_k \subseteq M_n$ et par croissance $M_k = M_n$.

Montrons enfin que (2) $\implies$ (1). Par l'absurde, soit σ un ensemble non vide de sous-modules de M qui n'a pas d'élément maximal. Soit donc $M_0 \in \sigma$. Comme M_0 n'est pas maximal, donc il existe $M_1 \in \sigma$ tel que $M_0 \subsetneq M_1$. De même M_1 n'est pas maximal, et de fil en anguille on construit une suite non stationnaire de sous-modules de M, ce qui contredit (2). ■

La noethérianité admet cette propriété de dévissage.

Théorème. ***(Noethérianité des modules par dévissage)***

Soit A un anneau et M un A-module, $M' \subseteq M$ un sous-A-module de M. Alors M est noethéien, si et seulement si, M' et M/M' sont noethériens.

▷ Si M est noethérien, alors tout sous-module de M' est un sous-module de M donc de type fini. D'autre part, tout sous-module de M/M' est de la forme N/M' où N est un sous-module de M contenant M'. Donc N est de type fini et si $(x_1,...,x_n)$ engendre N, alors il est clair que leurs classes modulo M' engendrent N/M', qui est donc de type fini.

Réciproquement, soit N un sous-module de M. On ne pas raisonner directement puisque N ne contient pas nécessairement M'. On force en prenant l'intersection, ce qui pousse à invoquer le second théorème d'isomorphisme $N/(N \cap M') \simeq (N + M')/M'$. Or celui-ci est un sous-module de M/M' noethérien, donc de type fini, donc $N/(N \cap M')$ est de type fini. Ainsi, il est engendré par $\overline{x_1},...,\overline{x_r}$. Ainsi, $N = Ax_1 + ... + Ax_r + N \cap M'$. Or $N \cap M'$ est de type fini comme sous-module de M', donc de type fini, donc N est de type fini. ■

Corollaire. ***(Quotient d'un module noethérien)***

Tout quotient d'un module noethérien est noethérien. Plus généralement (ou pas), si $M \twoheadrightarrow N$ deux modules et M est noethérien, alors N est noethérien.

▷ Immédiat. ■

Corollaire. ***(Somme directe finie de modules noethériens)***

Soit A un anneau et $(M_i)_{i\in[\![1,n]\!]}$ un A-module noethérien. Alors $\prod_{i=1}^{n} M_i$ est aussi noethérien.

▷ On a la suite exacte : $0 \longrightarrow M_i \longrightarrow (\prod_{i=1}^{n} M_i) \longrightarrow (\prod_{i=1}^{n} M_i)/M_1 \longrightarrow 0$. Or $(\prod_{i=1}^{n} M_i)/M_1 \simeq \prod_{i=2}^{n} M_i$. On raisonne donc par récurrence si $n > 2$, et directement si $n = 2$ par la propriété précédente, d'où le résultat. ■

On retrouve le théorème fondamental grâce à la propriété de dévissage.

Corollaire

Soit A un anneau noethérien et M un A-module. Alors M est de type fini si et seulement si M est un A-module noethérien.

▷ Le sens réciproque est vrai indépendamment de A via la définition. Réciproquement, soit $x_1,...,x_r$ une famille génératrice. On considère la suite $0 \longrightarrow \mathrm{Ker}(\phi) \longrightarrow A^r suite exT \phi M \longrightarrow 0$ où $\phi : (a_i) \mapsto \sum a_i x_i$, $\phi \in \mathrm{Hom}_{A\text{-Mod}}(A^2, M)$. Comme A^r est un produit fini de A-modules noethériens, il est noethérien par le corollaire précédent. Donc M est quotient d'un module noethérien, donc noethérien. ■

Exemples. ***(Modules noethériens)***

1. Tous les anneaux noethériens fournissent des exemples de modules noethériens sur eux-mêmes.
2. On renvoie au premier exercice pour des exemples plus élaborés.
3. Si A est noethérien, alors l'anneau $A[X]$ est noethérien (admis pour l'instant ; on en fournit une démonstration plus tard). Conséquemment, si A est anneau noethérien, $A[X_1,...,X_n]$ est un anneau noethérien. Ainsi, si K est un corps, $K[X_1,...,X_n]$ est un anneau noethérien ; $\mathbb{Z}[X_1,...,X_n]$ est également un anneau noethérien.
   Attention ! $A[X]$ n'a aucune chance d'être un A-module noethérien, même si A l'est ! En effet, $\mathbb{R}[X]$ n'est pas du tout de type fini en tant que $\mathbb{R}$-module !
4. Par contre, $K[X_1,...,X_n,...]$ n'est pas un anneau noethérien (évidemment).

4.3.2.1 Théorème de transfert de Hilbert

On en profite pour redémontrer dans le cas des modules le théorème de transfert de Hilbert, qui établit que la noethérianité est héréditaire dans la catégorie des anneaux. On peut formaliser tout à fait ce fait dans le cadre de la théorie des modules.

Théorème. ***(Théorème (de transfert) de Hilbert)***

Soit A un anneau noethérien. Alors $A[X]$ est noethérien.

▷ Supposons A noethérien. Alors de toute manière, $A[X]$ est une A-algèbre. En particulier, $A[X]$ est un A-module. Notons $M_n = \{P \in A[X] \mid \deg(P) \leqslant n\}$. On vérifie que c'est un sous-A-module de $A[X]$, qui est de type fini, engendré par $1,X,...,X^n$. Posons $f_n : M_n \longrightarrow\!\!\!\!\!\rightarrow A$ l'application linéaire qui, à un polynôme, fait correspondre son coefficient dominant. Soit I un idéal de $A[X]$. On pose $I_n = I \cap M_n \subseteq M_n$ un A-module de type fini. Posons $J_n = f_n(I_n)$. Alors J_n est un sous-module de A, c'est-à-dire un idéal de A. Or, $a \in J_n$, si et seulement si, il existe un polynôme $P \in I$ de la forme $P = aX^n + \sum_{i=0}^{n-1} a_i X^i$, $a_i \in A$. La suite des idéaux J_n est croissante. En effet, si $a \in J_n$, alors il existe

$P = aX^n + \sum_{i=0}^{n-1} a_i X^i \in I$. De plus, $XP \in I \cap M_{n+1} = I_{n+1}$, donc $a \in J_{n+1}$. Comme A est noethérien, la suite $(J_n)_{n\in\mathbb{N}}$ est stationnaire. Ainsi il existe $N \in \mathbb{N}$ tel que pour tout $n \geqslant N$, $J_n = J_N$. Soient Q_1,...,Q_l des générateurs du A-module de type fini I_N. On note I' l'idéal de $A[X]$ engendré par les Q_i, $i = 1,...,l$. Montrons que $I = I'$. Il est clair que $I' \subseteq I_N \subseteq I$. Soit donc $P \in I$. Montrons que $P \in I'$ par récurrence sur le degré de P. On sait déjà que $I' \supseteq I_N$. On en déduit que si $P \in I$ et $\deg(P) \leqslant N$, alors $P \in I_n \subseteq I'$ d'où $P \in I'$. Soit donc $P \in I$ avec $\deg(P) = n > N$. On fait l'hypothèse de récurrence forte. Le polynôme P s'écrit sous la forme $P = aX^n + \sum_{i=0}^{n-1} a_i X^i$ donc $P \in J_n = J_N$, l'idéal J_N ayant justement été construit par stabilisation de la suite des idéaux J_n. Il existe donc $P_0 \in I_N$ tel que $P_0 = aX^N + \sum_{i=0}^{N-1} b_i X^i$, $b_i \in A$. Ainsi $I \ni Q = P - X^{n-N}P_0$ avec $\deg(Q) < n$. Par hypothèse de récurrence, $Q \in I'$. Ainsi $I' \ni P = Q + X^{n-N}P_0$ puisque $Q \in I'$ et $P_0 \in I_N \subseteq I'$ donc $X^{n-N}P_0 \in I'$ et c'est terminé. ■

On peut anticiper légèrement sur la suite :

Corollaire. ***(Algèbre de type fini sur un anneau noethérien)***

Une algèbre de type fini sur un anneau noethérien A est un anneau noethérien.

▷ En effet, B est en tant qu'anneau un quotient de $A[X_1,...,X_n]$ qui est noethérien, donc B est noethérien en tant qu'anneau (et donc en tant que B-module). ■

4.3.3 Module cyclique

Définition. ***(Module cyclique)***

Soit M un module de type fini. On dit qu'il est *cyclique* s'il est engendré par un élément.

On anticipe sur la notion de base développée juste après.

Exercice 17

Un module cyclique est-il toujours libre ?

▷ **Éléments de réponse.**

Non ! Le $\mathbb{Z}$-module $\mathbb{Z}/2\mathbb{Z}$ est cyclique, engendré par 1. Pourtant, il n'est pas libre, on le verra bien assez tôt.

On voit ainsi qu'une famille à un élément sur un module n'est pas forcément libre !

Cependant :

Propriété. ***(Liberté des modules cycliques sans torsion)***

Un module cyclique sans torsion est libre.

On anticipe également sur la notion d'annulateur pour énoncer cette caractérisation parfois bien utile :

Proposition. ***(Caractérisation de la cyclicité par l'annulateur)***

Soit M un A-module. Alors M est cyclique si et seulement si M est isomorphe à $A/\mathrm{ann}(M)$.

▷ On note $\mathrm{ann}(M) = \{a \in A, a.x = 0 \quad \forall x \in M\}$. On vérifie facilement que c'est un idéal de A. Soit x un élément de M. On note $\rho_x : a \longmapsto ax$, application linéaire par axiome des modules. Le noyau N de ρ_x est un idéal de A contenant $\mathrm{ann}(M)$. Par théorème d'isomorphisme, on peut factoriser ρ_x sur $\mathrm{ann}(M)$. Cette application est un isomorphisme si et seulement si elle est injective et surjective, c'est-à-dire si et seulement si $\mathrm{ann}(M) = N$ et x engendre M, par construction de ρ_x. Si M est cyclique et x un générateur de M, alors il est clair que l'inclusion réciproque de N dans l'annulateur est vraie, car si $y \in M$, $y = a'x$ puis $ay = aa'x = a'ax = a'0 = 0$. Ceci donne le sens direct du théorème. Réciproquement, supposons que M soit isomorphe à $A/\mathrm{ann}(M)$ par l'application ϕ. Alors M est engendré par l'image de 1_A. En effet, 1_A est un générateur du quotient de A puisque 1_A génère A. ■

4.3.4 Algèbre de type fini

Soit A un anneau et B une A-algèbre par l'homomorphisme $\eta : A \longrightarrow B$.

On rappelle la définition suivante :

Définition. ***(Génération d'une algèbre)***

Soit X une partie de B. On dit que X *engendre* B comme A-algèbre, si le sous-anneau de B engendré par $\eta(A) \cup X$ est B lui-même.

D'où naturellement :

Définition. ***(Algèbre de type fini)***

L'algèbre B est de type fini si elle est générée par une partie finie.

Un exemple très simple : $B = A[X_1,...,X_n]$ est une A-algèbre de type fini, car engendrée par $\{X_1,...,X_n\} = X$, finie.

Attention ! B n'est pas un A-module de type fini dès que $n \geqslant 1$ et $A = \mathbb{R}$!

Exercice 18

Pour les initiés de la partie suivante, ils savent que ce A-module est encore libre. Il peut être intéressant de fournir un contre-exemple de module en tant que B-algèbre de type finie, mais même pas libre en tant que module.

▷ **Éléments de réponse.**

On peut s'intéresser à $\mathbb{Z}[X,Y]/2\mathbb{Z}$.

Ceux qui ont les idées claires voient immédiatement que la réciproque est trivialement vraie.

Proposition. ***(Une algèbre module de type fini est de type fini)***

Soit B une A-algèbre. Alors si B est de type fini comme A-module, c'est une A-algèbre de type fini.

Ceci nous amène à penser la génération des algèbres comme une façon d'écrire les éléments comme des polynômes, en un certain nombre de variables (l'ordre du typage), en certains éléments de l'algèbre, donc en nombre fini. Ceci montre bien que la réciproque de la propriété précédente est illusoire : en tant que A-module de type fini, on autorise la combinaison d'éléments de A pour décrire l'ensemble, mais en tant qu'algèbre, on touchera beaucoup plus d'éléments en autorisant avec des éléments de l'algèbre même, ce qui est possible puisqu'on a un produit sur cette structure.

Reformulation pratique. ***(Typage fini des algèbres)***

Une algèbre B est de type fini sur A si et seulement s'il existe $n \in \mathbb{N}$ et $\phi : A[X_1,...,X_n] \twoheadrightarrow B$ un morphisme de A-algèbres.

En particulier, si B est une A-algèbre de type fini, alors $B \simeq A[X_1,...,X_n]/I$. C'est une conséquence directe du théorème d'isomorphisme en factorisant ϕ par son noyau. Notons que dans cette construction toute théorique, l'expression de I peut être tout à fait horrible. Puisque ces structures sont clairement des algèbres, on a donc le résultat suivant :

Théorème. ***(Description des A-algèbres de type fini)***

Les A-algèbres de type fini n sont, à isomorphisme près, les quotients de $A[X_1,...,X_n]$.

Exercice 19

Soient A,B deux anneaux et $f : A \longrightarrow B$ un morphisme telle que f induise par ses préimages une bijection de l'ensemble des idéaux de B dans l'ensemble des idéaux de A. Alors f est-elle nécessairement surjective ?

▷ **Éléments de réponse.**

Je ne sais pas. Mais cette hypothèse suffit à montrer : si $A \longrightarrow B$ surjective et A noethérien, alors B noethérien, car toute surjection morphique vérifie cette propriété.

Proposition. ***(Transfert de la noethérianité sur les algèbres)***

Si A est noethérien et B une A-algèbre de type fini, alors B est un anneau noethérien.

▷ D'après le théorème de transfert de Hilbert, $A[X_1,...,X_n]/I \simeq B$ est noethérien. ■

Avec ce bagage théorique, on peut pousser la description de toutes les algèbres en mimant la preuve pour le typage fini (remarquer alors que tout ceci n'a finalement absolument rien à voir avec le typage fini) :

Théorème. ***(Description des A-algèbres)***

Les A-algèbres sont, à isomorphisme près, les quotients d'anneaux de polynômes à un nombre quelconque de variables à coefficients dans A. De plus, si la A-algèbre B est engendrée par un nombre I d'éléments, alors B est isomorphe à un quotient de $A[(X_i)_{i\in I}]$.

▷ Simple jeu d'écriture en mimant la preuve du cas du type fini. ■

4.3.5 Module libres et module de torsion

4.3.5.1 Vocabulaire de la dimension pour les modules

Dans cette section, on prend A un anneau et M un A-module. Soit également une famille $\{x_i\}_{i\in I}$ une famille d'éléments de M quelconque.

Soit l'application : ϕ : $\begin{array}{ccc} A^{(I)} & \longrightarrow & M \\ e_i & \longmapsto & x_i \end{array}$, qui est A-linéaire.

Définition. ***(Famille libre d'un module)***

On dit que la famille $\{x_i\}_{i\in I}$ est *libre* dans M, ou M-libre, si le morphisme ϕ est injectif.

Reformulation pratique. ***(Famille libre d'un module)***

Soient M un module sur un anneau commutatif A et $(x_i)_{i\in I}$ une famille d'éléments de M. Elle est *libre* si et seulement si, pour tout sous ensemble J de I fini, pour toute famille $(a_j)_{j\in J}$ d'éléments de A, si $\sum_{j\in J} a_j \cdot x_j = 0_M$, alors (a_j) est identiquement nulle.

Définition. ***(Famille génératrice d'un module)***

On dit que la famille $\{x_i\}_{i\in I}$ *engendre* M, ou M est généré par elle, si le morphisme ϕ est surjectif.

Reformulation pratique. ***(Famille génératrice d'un module)***

Soient M un module sur un anneau commutatif A et $(x_i)_{i\in I}$ une famille d'éléments de M. Elle est *génératrice* si et seulement si, tout élément x de M est combinaison à coefficients dans A d'un nombre fini d'éléments de (x_i).

Remarque. On reformule immédiatement : la famille $(x_i)_{i\in I}$ est génératrice si et seulement si la partie $\{x_i, i \in I\}$, est une partie génératrice de M.

Définition. ***(Base d'un module)***

On dit que la famille $\{x_i\}_{i\in I}$ est une *base* de M si ϕ est un isomorphisme.

Reformulation pratique. ***(Base d'un module)***

Soient M un module sur un anneau commutatif A et $(x_i)_{i\in I}$ une famille d'éléments de M. Elle est *base* si et seulement si, elle est libre et génératrice à la fois.

Tout A-module admet une famille génératrice : $(x)_{x\in M}$. Il est beaucoup plus intéressant de trouver une famille génératrice finie ; ce n'est pas toujours possible, penser aux espaces vectoriels.

Si $A = \mathbb{K}$ est un corps justement, tout A-module admet une base : c'est le théorème de la base incomplète en dimension quelconque, qui nécessite d'ailleurs l'axiome du choix. En fait, dans le cas des modules, ce n'est plus vrai, ce qui rend beaucoup plus difficile (et non fermée !) la théorie de la dimension.

Définition. ***(Module libre)***

On dit que le module M est *libre*, s'il admet une base.

Reformulation pratique. ***(Liberté des modules)***

Un module sur A est libre si $M \simeq A^{(I)}$.

Corollaire. ***(Modules libres de type fini)***

Les modules libres de type fini sont les A^n, à isomorphisme près.

▷ Ce n'est pas évident a priori ! En effet, on pourrait suppose que, M étant un A-module, il est libre, et donc admette une base de cardinal I, mais soit également engendré par une famille elle finie, dont on ne peut pas extraire de base (ça existe : voir (2,3) génératrice de $\mathbb{Z}$ par Bézout, mais pas libre par non-unicité des coefficients de Bézout et dont aucune des sous-familles n'engendre $\mathbb{Z}$ entier). En fait, ce point de vue n'est pas le bon. Supposons que M soit libre : il est isomorphe à un certain $A^{(I)}$ en tant que A-module. Il est aussi de type fini, donc $A^{(I)}$ est de type fini, engendré par $x_1,...,x_n$. On note J la réunion des supports des x_i, ensemble fini. Si I est infini, il existe $i_0 \in I \setminus J$, et alors $i \mapsto \delta^i_{i_0}$ n'est pas dans $\mathrm{Vect}(x_1,...,x_n)$, absurde. Donc I est fini, donc $M \simeq A^{[\![1,p]\!]} \simeq A^p$ pour un certain p. ■

Corollaire. ***(Modules de rang 1)***

Les modules libres engendrés par un unique élément sont isomorphes à A. (On parle de module cyclique.)

Corollaire. ***(Modules libres de type I)***

Soit I un ensemble quelconque. Les modules libres admettant une base de cardinal I sont $A^{(I)}$ à isomorphisme près.

▷ Simples réécritures. ■

Un module de type fini n'est pas forcément libre ! On voit dans les exemples ci-dessous que $\mathbb{Z}/2\mathbb{Z}$ n'est pas libre. Or il est fini, donc de type fini. Le problème par rapport aux espaces vectoriels est la non-rigidité des coefficients : il n'y a pas unicité de la décomposition dans $\mathbb{Z}/2\mathbb{Z}$, car $2.1 = 4.1$, par exemple. Ceci donne également un exemple de module engendré par un élément mais non isomorphe à A.

Exemples. ***(Modules libres)***

1. $A^{(I)}$ est donc un A-module libre ayant pour base la base canonique des (e_i) définie comme précédemment.
2. $A[X_1,...,X_n]$ est libre.
3. Tout anneau de polynômes est libre.

Exemples. ***(Modules non libres)***

1. Le $\mathbb{Z}$-module $\mathbb{Z}/2\mathbb{Z}$ n'est pas libre. En effet, il n'est pas nul et l'ensemble $\mathbb{Z}^{(I)}$ est infini pour tout I non vide. Ainsi $\mathbb{Z}/2\mathbb{Z}$ ne peut lui être isomorphe.
2. $\mathbb{Q}$ en tant que module sur $\mathbb{Z}$ n'est pas libre. C'est une conséquence de ce que $(\mathbb{Q},+)$ tout couple de rationnel est lié par une relation à coefficients entiers, leurs dénominateurs.

On peut énoncer le résultat suivant, d'une généralité navrante.

Théorème. ***(Tout module est un quotient de module libre)***

Tout module est isomorphe au quotient d'un module libre.

▷ Soit M un A-module. Il existe toujours une famille génératrice, il suffit de prendre tous les éléments ponctuellement. Il existe donc une surjection A-linéaire $\phi : A^{(I)} \hookrightarrow M$ pour un certain I, éventuellement $I = M$ et $A^{(I)}$ est libre. Par le premier théorème d'isomorphisme, $M \simeq A^{(I)}/\mathrm{Ker}(\phi)$, ce qu'il fallait montrer. ■

Exemple

Le $\mathbb{Z}$-module $\mathbb{Z}/2\mathbb{Z}$ n'est pas libre. Pourtant on a évidemment une surjection $\mathbb{Z}$-linéaire de $\mathbb{Z}$ dans $\mathbb{Z}/2\mathbb{Z}$ (ne pas se mélanger les pinceaux !). Ainsi $\mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z}$, et l'on est bien avancé (exemple inutile mais d'intérêt pédagogique non nul).

Comme on sait, tout espace vectoriel admet une base. On ne rappelle pas la preuve de ce résultat d'algèbre linéaire qui repose sur l'utilisation du lemme de Zorn.

Théorème. ***(Liberté des modules sur un corps)***

Tout module sur un corps est libre.

On a quand même un théorème de la dimension pour les modules. Par rapport aux espaces vectoriels, celui-ci ne s'énonce pas en toute généralité, mais dit que si un module admet une base, alors le cardinal est un invariant de bases ; c'est donc possible de définir la dimension.

Définition-propriété. ***(Dimension d'un module)***

Soit A un anneau non nul. Si L est un A-module libre, toutes les bases de L ont le même cardinal. Le cardinal d'une base de L est appelé rang de L et est noté $rg(L)$.

Remarque. Il n'y a en fait aucun problème pour l'anneau nul : le théorème s'applique. En effet, il n'y a qu'une application dans $\{0\}^I$, donc si un module sur l'anneau nul est libre, il est de cardinal 1 : c'est un groupe trivial. On a vu que son unique base est l'ensemble vide.

Pour montrer ce théorème, on a besoin de la notion suivante.

4.3.5.2 Annulateur d'un module

Définition. ***(Annulateur d'un module)***

Soit A un anneau et N un A-module. L'*annulateur* du module N est

$$\mathrm{ann}(N) := \{a \ni A \mid ax = 0 \ \forall x \in N\} \subseteq A.$$

On rappelle que la donnée d'un A-module N est celle d'un morphisme d'anneau $\rho : A \longrightarrow \mathrm{End}(N,+)$, dont l'expression est donnée par $a \longmapsto (x \longmapsto ax)$.

Reformulation pratique. ***(Annulateur d'un module)***

On a $\mathrm{ann}(N) = \mathrm{Ker}(\rho)$.

D'où :

Proposition. ***(Structure de l'annulateur)***

L'annulateur d'un module sur A est un idéal de A.

Remarque importante. D'après le théorème de factorisation pour les A-modules, si I est un idéal inclus dans $\mathrm{ann}(N)$, on peut passer au quotient par I dans ρ ce qui donne $\overline{\rho} : A/I \longrightarrow \mathrm{End}(N,+)$. Ceci confère une structure de A/I-module à N.

Remarque. Soit M un A-module et I un idéal de A. Alors IM est un sous-module de M, en notant $IM = \{\sum_{i=1}^{l} a_i m_i, l \in \mathbb{N}^*, (a_i)_{i=1}^{l} \in I^l, (x_i)_{i=1}^{l} \in M^l\}$. On a clairement $I \subseteq \mathrm{ann}(M/IM) \subseteq A$, puisque $\mathrm{ann}(M/IM) = \{a \in A \mid am \in IM \quad \forall m \in M\}$. Par conséquent, M/IM a une structure de A/I-module.

On peut également définir la notion moins forte suivante :

Définition. ***(Annulateur d'un élément)***

Soit A un anneau et N un A-module. L'*annulateur* d'un élément x du module N est

$$\mathrm{ann}(x) := \{a \ni A \mid ax = 0\} \subseteq A.$$

Reformulation pratique. ***(Annulateur d'un élément)***

On a $\mathrm{ann}_x(N) = \mathrm{Ker}(\rho_x)$ où $\rho_x : a \longmapsto ax$.

Proposition. ***(Structure de l'annulateur d'un élément)***

L'annulateur d'un élément d'un module sur A est un idéal de A.

Proposition. ***(Annulateur et annulateur d'un élément)***

Pour tout $x \in N$, $\mathrm{ann}_x(N)$ contient $\mathrm{ann}(N)$.

4.3.5.3 Preuve du théorème fondamental de la dimension

Preuve.

▷ Soit donc L un A-module libre. Soit $\mathfrak{m}$ un idéal maximal de A, donné par le théorème de Krull, et donc le lemme de Zorn, et donc l'axiome du choix. Alors $A/\mathfrak{m} = \mathbb{K}$ est un corps, donc $E = L/\mathfrak{m}L$ est un $\mathbb{K}$-espace vectoriel donc l'existence est garantie par la section précédente. Soit une base de L indexée par I. On va contrer que le cardinal de I est la dimension de E, et ce sera terminé. Puisque L a une base indexée par I, alors $L \simeq A^{(I)}$. Cette isomorphisme induit un isomorphisme de $\mathbb{K}$-espaces vectoriels $L/\mathfrak{m}L \simeq A^{(I)}/mA^{(I)}$. De plus, l'application $\begin{array}{ccc} A^{(I)} & \hookrightarrow & \mathbb{K}^{(I)} \\ (a_i)_{i\in I} & \longmapsto & (\overline{a_i})_{i\in I} \end{array}$ de noyau $\mathfrak{m}^{(I)}$, donc d'après le théorème de factorisation pour les espaces vectoriels, $A(I)/\mathfrak{m}A^{(I)} \simeq \mathbb{K}^{(I)}$, d'où $L/\mathfrak{m}L \simeq \mathbb{K}^{(I)}$ en tant que $\mathbb{K}$-espace vectoriel. Par transitivité, $\dim(L\mathfrak{m}L) = \mathrm{card}(I)$. C'est terminé. ■

Remarque. Dans le type fini, on a quand même besoin du lemme de Zorn. Remarquons aussi que cette preuve s'appuie sur la théorie de la dimension vectorielle : la théorie des modules suit celle des espaces vectoriels. (Ceci est dissymétrique avec le fait que dans le cas du type fini, on n'a pas besoin de l'axiome du choix pour la théorie vectorielle de la dimension, mais on en a besoin pour exhiber un idéal maximal de l'anneau de base. (Dans le cas d'un corps, l'idéal nul est maximal.))

On peut remarquer le fait suivant :

D'un module libre, les sous-modules (même de type fini) ne sont pas forcément tous libres. Soit A un anneau non principal : on sait qu'il en existe, par exemple $\mathbb{K}[X,Y]$ et I un idéal non principal de A. Alors A est un A-module sur lui-même, libre, de rang 1, de base 1_A. Pourtant, l'idéal I est un A-module qui n'est pas libre. En effet, d'après le théorème du supplémentaire que l'on démontrera plus tard, il admettrait une base à un seul élément, mais c'est impossible, car il n'est pas principal par hypothèse.

Remarque. On montrera par contre que tout sous-module d'un module libre sur un anneau principal, est libre. Mais c'est pour plus tard.

4.3.5.4 Notion de torsion

On supposera rapidement l'anneau A intègre, mais on peut définir la première notion en toute généralité.

Définition. ***(Élément de torsion)***

Soit M un A-module. Un élément $x \in M$ est dit *de torsion*, s'il existe $a \in A$ régulier tel que $ax = 0$.

Exercice 20

Soit A un anneau et l'on suppose qu'il existe $a \in A$ non régulier. Montrer que tous les éléments de M sont de torsion.

▷ **Éléments de réponse.**

On répondra plus tard à cette question.

Définition. ***(Module de torsion)***

Soit M un A-module. On dit que M est *de torsion* si tous ses éléments le sont.

Définition. ***(Module sans torsion)***

Soit M un A-module. On dit que M est *sans torsion* si sa seule torsion est le nul.

Observation. ***(Élément de torsion d'un module sur un anneau intègre)***

Soit M un A-module, A intègre. Un élément $x \in M$ est dit de torsion, s'il existe $a \in A$ non nul tel que $ax = 0$.

De même que dans les anneaux intègres :

Propriété. ***(Sous-module d'un module sans torsion)***

Un sous-module d'un module sans torsion est sans torsion.

Mais également :

Propriété. ***(Sous-module d'un module de torsion)***

Un sous-module d'un module de torsion est de torsion.

On observe que :

Fait. ***(Le phénomène de torsion disparaît dans les espaces vectoriels)***

Si l'anneau de base est un corps, le module est automatiquement sans torsion.
C'est une des premières propriétés des espaces vectoriels E sur $\mathbb{K}$: pour $\lambda \in \mathbb{K}$ et $x \in E$, si $\lambda \cdot x = 0$, alors $x = 0$ ou $\lambda = 0$.

Exercice 21

Supposons A non intègre. Le module M peut-il être sans élément de torsion non nul ?

▷ **Éléments de réponse.**

Soit M un module non nul, sans quoi ça n'a aucun intérêt. Puisque A est non intègre, on peut exhiber une paire de diviseurs de zéro associés dans A tels que $ab = 0$. Supposons que M soit sans élément de torsion non nul. Soit donc $x \neq 0$ dans M. Alors $bx \neq 0$. Mais $bx \in M$. De plus, $a.bx = (ab)x = 0x = 0$, donc $bx \in M$ est de torsion non nul, absurde.

On utilise ces notations dès maintenant. Clairement :

Propriété

Un module libre est sans torsion.

▷ Soit $(x_i)_{i\in I}$ une base du A-module libre M. Supposons qu'il existe $a \in A$ régulier et $x \in M$ non nul tel que $ax = 0$. Alors puisque $x = a_1x_1 + ... + a_nx_n$ où $x_1,...,x_n \in \{x_i, i \in I\}$ deux à deux distincts, $n \in \mathbb{N}$, et $a_1,...,a_n \in A$ que l'on peut supposer non nul quitte à enlever des x_i. Ainsi $aa_1x_1 + ... + aa_nx_n = 0$. Or l'un des a_i est non nul, car x est non nul par hypothèse. Par unicité de la décomposition dans une base, on a pour ce a_i, $aa_i = 0 = a.0$, en identifiant à la décomposition de $ax = 0$. Puisque a est régulier, $a_i = 0$, contradiction. ■

On s'intéresse au lien entre torsion et annulateur dans le cas intègre. Une implication est immédiate.

Propriété

Si $\mathrm{ann}(M) \neq \{0\}$ et A est intègre, alors M est de torsion.

▷ Par définition, l'annulateur de M est l'ensemble des $a \in A$ tels que $ax = 0$ pour tout $x \in M$. Par hypothèse, il existe donc $a \in A$ non nul tel que pour tout $x \in M$, $ax = 0$. En particulier, pour tout $x \in M$, il existe $a \in A$ non nul donc régulier tel que $ax = 0$. ■

Remarque. Si l'on ne suppose pas l'anneau A intègre, il n'y a aucune chance que cette implication soit vraie. Il suffit de trouver un anneau ayant un élément absorbant à gauche, c'est-à-dire dans l'annulateur de A vu comme A-module, et alors A est un A-module de torsion.

Dans un cas plus favorable[1], nous pouvons montrer une réciproque.

Propriété

Si M est de torsion et de type fini, alors $\mathrm{ann}(M) \neq \{0\}$.

Remarquons avant de commencer la preuve qu'un module est de torsion si et seulement si tous ses générateurs sont de torsion.

Preuve.

▷ Le module M est engendré par $x_1,...,x_l$ pour un certain entier p et les x_i sont bien évidemment de torsion. Il existe donc des $a_i \in A$ tels que $a_ix_i = 0$ pour tout $i = 1,...l$. Alors $a = \prod_{i=1}^{l} a_i \in \mathrm{ann}(M)$, mais $a \neq 0$. ■

[1] Il est illusoire d'envisager une réciproque générale au vu de la preuve précédente, car nous avons opéré l'interversion grossière $\exists\ \forall \implies \forall\ \exists$. Il nous faut une hypothèse de compacité, ici le typage fini.

Exercice 22

Donner un exemple de module de torsion sur un anneau intègre (nécessairement de type infini) dont l'annulateur est réduit au nul.

▷ **Éléments de réponse.**

Prenons l'entonnoir infini, c'est-à-dire le $\mathbb{Z}$-module $\prod_{n\in\mathbb{N}} \mathbb{Z}/n\mathbb{Z}$. On extrait maintenant l'ensemble A des familles à support fini de ce module. C'est encore un $\mathbb{Z}$-module. En choisissant le ppcm des ordres des composantes d'un élément, on montre qu'il est de torsion. Pourtant, son annulateur est réduit à l'élément nul de A.

Étudions deux exemples fondamentaux :

Exemple. ***(Le $\mathbb{Z}$-module $\mathbb{Q}$)***

Remarquons dès maintenant que $\mathbb{Z}$ est principal et que cet exemple pourra servir dans la section sur les modules sur un anneau principal. On remarque que :

- $\mathbb{Q}$ est sans torsion sur $\mathbb{Z}$. Cela vient de l'intégrité de $\mathbb{Q}$.
- $\mathbb{Q}$ n'est pas de type fini sur $\mathbb{Z}$ (il l'est, bien évidemment, en tant que $\mathbb{Q}$-espace vectoriel puisqu'alors de dimension 1 !). C'est un exercice classique de théorie élémentaire des groupes : on en donne une généralisation juste au-dessous. On aurait pu aussi le déduire de la suite et de la propriété que l'on verra plus tard que tout module sans torsion de type fini sur un anneau principal est libre.
- Le $\mathbb{Z}$-module $\mathbb{Q}$ n'est pas libre. (On ne peut le déduire du point précédent, par contre.) En effet, soit B une famille d'éléments de ce module indexée par I. Alors I n'est pas vide, car $\mathbb{Q}$ n'est pas nul. De plus, $\mathbb{Q} \neq k\mathbb{Z}$ pour tout $k \in \mathbb{Q}$, donc si $\mathrm{card}(I) < 2$ alors B n'est pas génératrice. D'autre part, si $\mathrm{card}(I) \geqslant 2$, soient x,x' deux vecteurs distincts de B. Alors $x = \frac{p}{q}$ et $x' = \frac{p'}{q'}$ pour certains entiers et $-p'q\frac{p}{q} + pq'\frac{p'}{q'} = 0$ d'où une relation de dépendance entre x et x', donc la famille B n'est pas libre, car toute sous-famille d'une famille libre doit être libre. Ainsi B n'est jamais une base du module considéré.
- On peut faire la remarque suivante : pour tous entiers q_1,q_2 non nuls, $(\frac{1}{q_1}) + (\frac{1}{q_2}) = (\frac{1}{q_1 \vee q_2})$. En effet, l'inclusion directe est claire, et réciproquement, si $k \in \mathbb{Z}$, et si l'on a une relation de Bézout $q_1u + q_2v = q_1 \wedge q_2$,

$$\frac{k}{q_1 \vee q_2} = \frac{k(q_1 \wedge q_2)}{q_1q_2} = \frac{k(q_1u + q_2v)}{q_1q_2} = ku\frac{1}{q_2} + kv\frac{1}{q_1}.$$

Proposition

Soit A un anneau factoriel ayant une infinité d'irréductibles deux à deux non associés. Alors $Frac(A)$ est un A-module non de type fini.

▷ Supposons que le module $M = Frac(A)$ soit engendré par $x_1 = \frac{p_1}{q_1}$, ..., $x_r = \frac{p_r}{q_r}$. Soit P l'ensemble fini, par réunion finie d'ensembles finis, des irréductibles apparaissant dans la décomposition en irréductibles à association près des dénominateurs. Soit donc $\pi \notin P$ un irréductible de A. Alors $\frac{1}{\pi}$ n'est pas dans l'espace engendré par les x_1,...,x_r. En effet, si c'était le cas, on pourrait écrire $\pi K = q_1...q_r$ en réduisant les fractions de la forme suivante au même dénominateur : $k_1\frac{p_1}{q_1}, ..., k_r\frac{p_r}{q_r}$. Par lemme d'Euclide, π divise l'un des q_i, contradiction. ■

Exemple. ***(Le tore rationnel ou le $\mathbb{Z}$-module $\mathbb{Q}/\mathbb{Z}$)***

Remarquons dès maintenant que $\mathbb{Z}$ est principal et que cet exemple pourra servir dans la section sur les modules sur un anneau principal. On remarque que :

- $\mathbb{Q}/\mathbb{Z}$ est de torsion. En effet, si $x = \frac{p}{q}$ où $(p,q) \in \mathbb{Z} \times \times^*$, alors $q\overline{x} = \overline{p} = 0$, car $p \in \mathbb{Z}$.
- $\mathbb{Q}/\mathbb{Z}$ n'est pas de type fini. Il suffit d'appliquer la même preuve que précédemment en faisant attention à manipuler les éléments du quotient par $\mathbb{Z}$, ce qui ne défait pas notre argument.
- $\mathbb{Q}/\mathbb{Z}$ n'est pas un $\mathbb{Z}$-module libre. En effet, il est de torsion, et non nul, donc il admet une torsion non nul, or un module libre est sans torsion.

On souhaite maintenant construire des modules de torsion. On voit que les anneaux quotients sont grossièrement des torsions.

Propriété. ***(Les quotients sont des torsions)***

Si I est un idéal non nul de A, alors A/I est de torsion.

▷ Si I est un idéal de A, $\text{ann}(A/IA) = \text{ann}(A/I) = I$, donc s'il est non nul, A/I est un A-module de torsion. ■

En utilisant le théorème de Krull, on obtient le résultat d'existence suivant :

Conséquence. ***(Existence de A-modules de torsion si A n'est pas un corps)***

Soit A un anneau qui n'est pas un corps. Alors il existe toujours un A-module de torsion non nul.

Plus généralement, on peut définir la *torsion* d'un module. On a maintenant besoin de **l'intégrité de A**.

Définition. ***(Torsion d'un module))***

] Soit M un A-module. L'ensemble des éléments de torsion sur A de M est noté M_{tor}.

Propriété. ***(Structure de la torsion)***

La torsion d'un module **sur un anneau intègre** en est un sous-module.

▷ Si x,$y \in M$ sont de torsions, alors il existe a,$b \in A$ non nuls tels que $ax = bx = 0$. Puisque l'anneau A est intègre, $ab \neq 0$. Ainsi $ab(x+y) = b(ax) + a(by) = 0$. Donc $x+y$ est de torsion. Si $x \in M$ est de torsion, il existe a non nul tel que $ax = 0$. Ainsi pour tout $\lambda \in A$, $a(\lambda x) = \lambda ax = 0$ donc λ_x est de torsion. ■

On suppose donc maintenant que A est intègre.

Remarque importante. On a la suite exacte courte :

$$0 \longrightarrow M_{\text{tor}} \hookrightarrow M \twoheadrightarrow M/M_{\text{tor}} \longrightarrow 0,$$

qui permet de voir que M/M_{tor} n'a pas d'élément de torsion non nul.

Propriété. ***(Quotient par la torsion)***

Un module sur un anneau intègre quotienté par sa torsion est un module sans torsion.

▷ Soit $\overline{x} \in M/M_{\text{tor}}$. On suppose qu'il existe $a \in A$ non nul tel que $a\overline{x} = 0$. Alors $\overline{ax} = 0$ par construction du module quotient, donc ax est dans la torsion de M. Ainsi il existe b non nul tel que $b(ax) = 0$ d'où $(ba)x = 0$, où ba est non nul par intégrité de A, donc x est dans la torsion de M. Donc $\overline{x}$ est nul. ■

On voudrait en fait que le module ainsi construit soit plus fortement libre, mais ce n'est vrai que si l'anneau A est principal.

Exercice 23

Fournir un contre-exemple.

▷ **Éléments de réponse.**

Car je n'en ai pas trouvé.

On peut maintenant énoncer un théorème fondamental, bien qu'il n'en ait pas tout à fait l'air :

Théorème. ***(Théorèmes du supplémentaire pour les modules)***

Soit A intègre et L un A-module libre de rang fini n. Soit L' un A-sous-module de L supposé également libre. Alors :

1. $\text{rg}(L') \leqslant n$,
2. il existe un sous-module libre L'' de L vérifiant $L' \cap L'' = \{0\}$ avec $\text{rg}(L') + \text{rg}(L'') = n$,
3. $\text{rg}(L') = n$ ssi L/L' est de torsion.

Exemple fondamental. *(Z et Z^2)*

On se place dans la catégorie des $\mathbb{Z}$-modules. On considère le $\mathbb{Z}$-module $L = \mathbb{Z}^2$, clairement libre de rang 2 (ayant pour base la base canonique) et l'on considère également $L' = 2\mathbb{Z} \times \{0\}$, également $\mathbb{Z}$-module libre de rang 1 et de base $\{(2,0)\}$. Si l'on pose aussi $L'' = \{0\} \times \mathbb{Z}$, on a $\mathrm{rg}(L'') = 1$ et clairement $L' \cap L''$ est réduit au nul ; de plus $\mathrm{rg}(L') + \mathrm{rg}(L'') = 2 = \mathrm{rg}(L)$. Soit $\tilde{L}$ le sous-module de L engendré par L' et L''. On voit que $\tilde{L} = 2\mathbb{Z} \times \mathbb{Z}$. Ainsi le rang de $\tilde{L}$ est 2, de base (2,1). De plus :

$$L/\tilde{L} = \mathbb{Z}/2\mathbb{Z} \times \{0\} \simeq \mathbb{Z}/2\mathbb{Z} \text{ et } L/L' = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}.$$

Ainsi $L/\tilde{L}$ est de torsion, puisqu'en effet $\tilde{L}$ est de rang 2, et L/L' n'est pas de torsion, puisqu'en effet L' n'est pas de rang $\mathrm{rg}(L)$.

Remarque. Il n'y a même pas besoin de fournir de contre-exemple, car lorsque L n'est pas libre, on peut imaginer un sous-module qui n'est pas libre, et l'on ne peut plus parler de rang (*i.e.* de dimension), et tout ceci n'a plus aucun sens.

Ceci n'implique pas que le L'' du deuxième point, même dans le cas d'un module libre de type fini, soit un supplémentaire de L'. Le contre-exemple est donné par la construction précédente : en effet $2\mathbb{Z} \times \{0\} \oplus \{0\} \times \mathbb{Z} \simeq 2\mathbb{Z} \times \mathbb{Z}$ n'est pas $\mathbb{Z}^2$.

Ces remarques donnent la considération suivante :

Proposition

Un idéal d'un anneau A est un A-module libre, si et seulement si, il est principal et son générateur ne divise pas zéro.

▷ Si un idéal I de A n'est pas principal, il ne peut être libre, sinon, A étant libre de rang 1, on aurait le rang I inférieur à 1, donc égal à 1 ou I nul. De plus, si I est libre, il est sans torsion, donc il n'existe aucun $b \in A$ tel que $ba = 0$ où a est un générateur de I, $a \in I$. Réciproquement, si I est principal et son générateur ne divise pas zéro, on vérifie que I est cyclique sans torsion donc libre. ■

La preuve du théorème précédent nécessite l'introduction de la notion suivante.

4.3.5.5 Modules de fractions

Dans cette section, on cherche à généraliser la construction du localisé au module. En général, étant donné un anneau et un localisé, le localisé correspondant du module sera un module sur le localisé de l'anneau.

Soit donc A un anneau et S une partie multiplicative de A. On rappelle que $S^{-1}A$ est une A-algèbre par $a \longrightarrow a/1$, en particulier, c'est un A-module.

Soit M un A-module. On va construire un $S^{-1}A$-module $S^{-1}M$, le *module de fractions* de S. De même que dans le cas des anneaux, on munit $S \times M$ de la relation $\mathcal{R}$ donnée par $(s,m)\mathcal{R}(s',m')$ si et seulement si $\exists \sigma \in S \quad \sigma s'm = \sigma sm'$. C'est une relation d'équivalence et on note $S^{-1}M$ le quotient de M par cette relation. La classe d'un élément (s,m) est notée $\frac{m}{s}$.

On a que si $(\frac{m}{s}, \frac{m'}{s'}) \in (S^{-1}M)^2$, alors $\frac{ms'+m's}{ss'}$ ne dépend que des classes de $\frac{m}{s}$ et de $\frac{m'}{s'}$. On peut donc définir ainsi la loi $+ : S^{-1}M \times S^{-1}M \longrightarrow S^{-1}M$. De plus, si $(\sigma,a) \in S \times A$ et $(s,m) \in SM$, alors $\frac{am}{\sigma s}$ ne dépend que des classes de $\frac{a}{\sigma}$ et $\frac{m}{s}$ d'où la bonne définition d'une loi externe $S^{-1}A \times S^{-1}M \longrightarrow S^{-1}M$.

Théorème

Les deux opérations ainsi définies munissent $S^{-1}M$ d'une structure de $S^{-1}A$ module.

De plus, si A est intègre,

Proposition

L'application $\eta_M : \begin{array}{ccc} M & \longrightarrow & S^{-1}M \\ m & \longmapsto & \frac{m}{1} \end{array}$ un morphisme injectif de A-modules.

Ainsi

Proposition

M est un sous-A-module de $S^{-1}M$.

Pour que les choses soient claires :

Définition. *(Module de fractions)*

On appelle le $S^{-1}A$-module $S^{-1}M$ le *S-module de fractions* de M.

Le module de fractions de M vérifie la propriété universelle suivante :

Propriété. *(Propriété universelle des modules de fractions)*

Soit M un A-module, N un $S^{-1}A$-module. Pour tout application $f : M \longrightarrow N$ A-linéaire, il existe une unique application $\tilde{f} : S^{-1}M \longrightarrow N$ $S^{-1}A$-linéaire telle que $f = \tilde{f} \circ \eta_M$.

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ {\scriptstyle \eta_M}\downarrow & \nearrow_{\tilde{f}} & \\ S^{-1}M & & \end{array}$$

Remarques.

1. Soient M,M' deux A-modules et $f : M' \longrightarrow M$ A-linéaire. Alors $\eta_M \circ f : M' \longrightarrow S^{-1}M$ A-linéaire. D'après la propriété universelle, il existe un unique $S^{-1}f : S^{-1}M' \longrightarrow S^{-1}M$ $S^{-1}A$-linéaire vérifiant

$$\begin{array}{ccc} M' & \xrightarrow{\eta_M \circ f} & S^{-1}M \\ {\scriptstyle \eta_{M'}}\downarrow & \nearrow_{S^{-1}f} & \\ S^{-1}M' & & \end{array}$$

i.e.

$$\begin{array}{ccc} M' & \xrightarrow{f} & M \\ {\scriptstyle \eta_{M'}}\downarrow & & \downarrow{\scriptstyle \eta_M} \\ S^{-1}M' & \xrightarrow{S^{-1}f} & S^{-1}M. \end{array}$$

2. Si $g : M'' \longrightarrow M'$ et $f : M' \longrightarrow M$ et A-linéaire. On montre que $S^{-1}(f \circ g) = S^{-1}(f) \circ S^{-1}(g)$. De même, $S^{-1}(id_M) = id_{S^{-1}M}$.

Nous allons maintenant localiser des sommes directes.

Propriété. ***(Localisation d'une somme directe)***

Soient A un anneau et S une partie multiplicative de A. Soit $(M_i)_{i\in I}$ une famille quelconque de A-modules. On a un isomorphisme de $S^{-1}A$-module entre $\bigoplus_{i\in I} S^{-1}M_i \simeq S^{-1}(\bigoplus_{i\in I} M_i)$.

▷ On pose l'injection $a_j : M_j \longrightarrow \bigoplus_{i\in I} M_i$ A-linéaire. Alors naturellement $S^{-1}a_j : S^{-1}M_j \longrightarrow S^{-1}(\bigoplus_{i\in I} M_i)$ est A-linéaire. Par propriété universelle, la somme directe $\phi : \bigoplus_{i\in I} S^{-1}M_i \longrightarrow S^{-1}(\bigoplus_{i\in I} M_i)$ où ϕ est $S^{-1}A$-linéaire et $\phi \circ \iota_i = S^{-1}a_i$. D'autre part, l'application $\begin{array}{ccc} \bigoplus_{i\in I} M_i & \longrightarrow & \bigoplus_{i\in I} M_i S^{-1}M_i \\ (a_i)_{i\in I} & \longmapsto & (\eta_{M_i}(a_i))_{i\in I} \end{array}$ est A-linéaire. Enfin, par propriété universelle, j'ai une application $S^{-1}A$-linéaire $\psi : S^{-1}(\bigoplus_{i\in I} M_i) \longrightarrow \bigoplus_{i\in I} S^{-1}M_i$. On constate que ϕ et ψ sont inverses l'un de l'autre. ■

Propriété. ***(Localisation d'une suite exacte courte)***

Soient A un anneau et S une partie multiplicative de A. Soit M, M', M'' des A-modules et une suite exacte $M' \xrightarrow{f} M \xrightarrow{g} M''$ une suite exacte. Alors $S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M''$ est une suite exacte de $S^{-1}A$-module.

▷ Les flèches du haut sont A-linéaires, celles du bas sont $S^{-1}A$-linéaires, et celles qui descendent sont A-linéaires (forcément !).

$$\begin{array}{ccccc} M' & \longrightarrow & M & \longrightarrow & M'' \\ \downarrow{\scriptstyle \eta_{M'}} & & \downarrow{\scriptstyle \eta_M} & & \downarrow{\scriptstyle \eta_{M''}} \\ S^{-1}M' & \xrightarrow{S^{-1}f} & S^{-1}M & \xrightarrow{S^{-1}g} & S^{-1}M'' \end{array}$$

Par hypothèse, $\mathrm{Ker}(g) = \mathrm{Im}(f)$. En particulier, $g \circ f = 0$. On obtient facilement $S^{-1}g \circ S^{-1}f = 0$. On en déduit par caractérisation que $\mathrm{Ker}(S^{-1}g) \subseteq \mathrm{Im}(S^{-1}f)$. Montrons l'inclusion inverse. Soit $\frac{m}{s} \in \mathrm{Ker}(S^{-1}g)$ avec les notations évidentes. Cela signifie $S^{-1}g\left(\frac{m}{s}\right) = 0$, soit $\frac{1}{s}S^{-1}g(\frac{m}{1}) = 0$. Mais $S^{-1}g(\frac{m}{1}) = \frac{g(m)}{1}$! On a donc $\frac{g(m)}{1} = 0$ en multipliant par s. Autrement dit, il existe $\sigma \in S$ tel que $\sigma m \in \mathrm{Ker}(g) = \mathrm{Im}(f)$. Il existe donc $m' \in M'$ tel que $\sigma m = f(m')$. Par suite, $(S^{-1}f)\left(\frac{m'}{s\sigma}\right) = \frac{m}{s}$. La preuve est terminée. ■

Il faut être attentif à ce que deviennent injections, surjections par le procédé de localisation. L'exemple $\mathbb{Z} \longrightarrow \mathbb{Z}/7\mathbb{Z}$ est édifiant, lorsqu'on localise $\mathbb{Z}$ en son corps des fractions : l'homomorphisme valant 1 en 1, ayant pour noyau $7\mathbb{Z}$, devient l'application nulle, puisque le module d'arrivée devient le module nul par localisation !

Corollaire

Si L est un A-module libre alors $S^{-1}L$ est un $S^{-1}A$ module libre et il est de même rang. Si A est intègre et la localisation le corps des fractions, alors $S^{-1}L$ est un $Frac(A)$-espace vectoriel.

▷ Immédiat. ■

4.3.5.6 Preuve du théorème du supplémentaire

D'après le lemme précédent, si l'anneau A est intègre, on peut poser $F = Frac(A) = S^{-1}A$ où $A = A \setminus \{0\}$ est dans ce cas à tout module M sur A, on peut associer le F-espace vectoriel $S^{-1}M$.

Définition. ***(Espace vectoriel des fractions)***

On note $M_0 = S^{-1}M$ selon la construction précédente, qui est un F-espace vectoriel.

On fixe un anneau intègre A.

Lemme

Le A-module M est de torsion si et seulement si $M_0 = 0$.

▷ Pour $x \in M$, $\eta_M(x) = x/1$ est nul si et seulement s'il existe $a \in A$ non nul tel que $ax = 0$. Autrement dit, le noyau de η_M est l'ensemble des éléments de torsion de M. En particulier, si $M_0 = 0$, le module M est de torsion. Inversement, si M est de torsion, alors $\eta_M = 0$. Tout élément de M_0 est alors de la forme $x/s = 1/s\eta_M(x)$, donc nul. ■

On reprend la démonstration du théorème du supplémentaire. Soit L un A-module libre et $L' \subseteq L$ un sous-module libre. Soit $Q = L/L'$.

▷ On a la suite exacte courte de A-modules : $0 \longrightarrow L' \xrightarrow{f} L \xrightarrow{g} Q \longrightarrow 0$. D'après les considérations précédentes, on a donc la suite exacte courte de F-espaces vectoriels $0 \longrightarrow L'_0 \xrightarrow{f_0} L_0 \xrightarrow{g_0} Q_0 \longrightarrow 0$. Or L_0 est un F-espace vectoriel de dimension n. Puisque l'application $f_0 : L'_0 \longrightarrow L_0$ est F-linéaire injective, L'_0 est de dimension $\leqslant n$, autrement dit, $\mathrm{rg}(L') \leqslant n$, d'où le premier point du théorème. ■

On montre maintenant le troisième point du théorème.

▷ De plus, on a $\mathrm{rg}(L') = n \iff L'_0$ et L_0 ont même dimension finie $n \iff f_0$ est surjective $\iff g_0$ est nulle $\iff Q_0 = 0 \iff Q$ est un module de torsion, d'après le lemme, d'où le point 3. ■

Reste à montrer le second point du théorème. Cela se ramène au lemme suivant.

Lemme

Si L est un A-module libre de rang n, toute famille libre de L peut-être complétée en une famille libre à n éléments.

▷ Puisque par hypothèse L est sans torsion, l'application canonique $\eta_L : L \longrightarrow L_0$ est injective ; on peut donc identifier tout élément x de L à son image par η_L. Soit $(e_1,....,e_m)$ une famille d'éléments de L. Cette famille est libre sur A si et seulement si en tant que famille d'éléments de L_0, elle est libre sur F. En effet, toute relation de liaison entre les e_i à coefficients dans A peut-être vue comme une relation de liaison à coefficients dans $F \supseteq A$. Inversement, étant donnée une relation de liaison à coefficients dans F, en multipliant par le plus petit multiple commun des dénominateurs des fractions des coefficients de la relation, on obtient une liaison dans A. Supposons donc la famille $(e_1,...,e_m)$ libre sur A. C'est donc une famille libre du F-espace vectoriel L_0 qui est de dimension n. On peut donc la compléter en une base $(e_1,...,e_m,g_1,...g_{n-m})$ de L_0. Chacun des g_i est de la forme f_i/s_i, où $f_i \in L$ et $s_i \in S$. La famille $(e_1,...,e_m,f_1,...,f_{n-m})$ est encore une base du F-espace vectoriel L_0, donc une famille libre du A-module L. ■

Preuve.

▷ Le lemme permet de conclure comme suit. Soit $(e_1,...,e_m)$ une base de L'. On la complète en une famille libre $(e_1,...,e_m,f_1,...,f_{n-m})$ de L ; il suffit alors de prendre pour L'' le sous-module de L engendré par $(f_1,...,f_{n-m})$. ■

4.3.5.7 Suites exactes courtes scindables entre modules

Dans cette section, on considère une sec de A-modules :

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

notée $(\mathcal{E})$.

Propriété

Les conditions suivantes sont équivalentes :

1. Il existe une application A-linéaire $\tau : M'' \longrightarrow M$ telle que $g\tau = 1_{M''}$.
2. Il existe une application $\sigma : M \longrightarrow M'$ telle que $\sigma f = 1_{M'}$.
3. Il existe un couple (σ, τ) d'applications A-linéaires, avec $\sigma : M \longrightarrow M'$, $\tau : M'' \longrightarrow M$, vérifiant $\sigma f = 1_{M'}$, $g\tau = 1_{M''}$ et $f\sigma + \tau g = 1_M$.

De plus, si σ, τ est un couple vérifiant la dernière condition, l'application suivante est un isomorphisme de A-modules :

$$\begin{array}{rccc} \psi : & M & \longrightarrow & M' \oplus M'' \\ & x & \longmapsto & \sigma(x) + g(x). \end{array}$$

▷ Il est clair que 3 implique 2 et 1.

$$0 \longrightarrow M' \underset{\sigma}{\overset{f}{\rightleftarrows}} M \underset{\tau}{\overset{g}{\rightleftarrows}} M'' \longrightarrow 0$$

Montrons que 1 implique 3. On montre en fait un peu plus : étant donné τ comme voulu, il existe un unique σ tel que (σ,τ) satisfasse à la dernière condition. Si σ existe, il est unique, car $f\sigma = id_M - \tau g$. Puisque f est injective, $g(id_M - \tau g) = g - g\tau g = g - g = 0$. Or $\mathrm{Im}(id_M - \tau g) \subseteq \mathrm{Ker}(g) = \mathrm{Im}(f)$, donc il existe $\sigma : M \longrightarrow M'$ tel que $id_M - \tau g = f\sigma$, définie par le nul sur le reste. Il reste à vérifier $\sigma f = id_{M'}$. Puisque f est injective, il suffit de vérifier que $f\sigma f = f$. Or $f\sigma f = (id_M - \tau g)f = f - \tau g f = f - 0$. De même, on montre que 1 implique 2. Enfin, pour montrer que l'application ψ définie ci-dessus, sous l'une des conditions équivalentes précédentes, est un isomorphisme, on introduit

$$\begin{array}{rccc} \phi : & M' & \longrightarrow & M'' \oplus M \\ & x' + x'' & \longmapsto & f(x') + \tau(x''). \end{array}$$

On a bien $\phi\psi(x) = \phi(\sigma(x) + g(x)) = f\sigma(x) + \tau g(x) = x$. Montrons que ϕ est injective. Si $\phi(x' + x'') = 0$, alors $f(x') + \tau(x'') = 0$ (ce sont en fait des équivalences) d'où $gf(x') + g\tau(x'') = 0$ d'où $x'' = 0$ d'où $f(x') = 0$ d'où $x' = 0$ par surjectivité de g et injectivité de f, par suite exacte courte. ■

Ces conditions ne sont plus équivalentes dans la catégorie des groupes ! En revanche, elle est vérifiée pour les groupes abéliens où le produit semi-direct est facilité. On peut identifier dans la preuve précédente ce qui coince dans la preuve précédente : dans un groupe quelconque, on ne peut écrire $f\sigma = id_M - \tau g$ ou encore $f - \tau g f = f - 0$.

Définition. ***(Scindage d'une suite exacte)***

Un couple (σ, τ) vérifiant la dernière des conditions précédentes est appelé *scindage de la suite exacte* $(\mathcal{E})$.

Définition. ***(Scission ou scindabilité)***

La suite exacte $(\mathcal{E})$ est dite *scindable* ou *scindée* si elle admet un scindage.

Proposition

Si $(\mathcal{E})$ est scindable, $M \simeq M' \oplus M''$.

Exemples

1. Si M_1,M_2 sont deux A-modules, la suite exacte $0 \longrightarrow M_1 \longrightarrow M_1 \oplus M_2 \longrightarrow M_2 \longrightarrow 0$ est scindable. Cet exemple est fondamentale comme le montre le fait suivant.
2. La suite exacte de $\mathbb{Z}$-modules donnée par $0 \longrightarrow \mathbb{Z} \xrightarrow{2\times} \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$ n'est pas scindable. Car la seule application $\mathbb{Z}$-linéaire de $\mathbb{Z}/2\mathbb{Z}$ dans $\mathbb{Z}$ est l'application nulle.

Fait. ***(Représentation des suites scindables)***

Toute suite scindable est essentiellement du premier type ci-dessus. Plus précisément, si $0 \longrightarrow M' \xrightarrow{i} M \xrightarrow{s} M'' \longrightarrow 0$ est une suite exacte courte scindable, alors $i(M')$ admet un supplémentaire N dans M et s_N est un isomorphisme de N sur M''.

Exercice 24 *(Tout est dans les détails)*

On suppose qu'on a une suite exacte $0 \longrightarrow M_1 \longrightarrow M \longrightarrow M_2 \longrightarrow 0$ et que $M \simeq M_1 \oplus M_2$. Montrer que la suite exacte n'est pas forcément scindée.

▷ **Éléments de réponse.**

Remarquons déjà que c'est dû à ce que la suite proposée n'est pas nécessairement la suite canonique de l'exemple **1.** Il suffit de considérer $A = \mathbb{Z}$, $M_1 = \mathbb{Z}$ et $M_2 = (\mathbb{Z}/n\mathbb{Z})^{\mathbb{N}}$. On prend alors $g : M_1 \times M_2 \to M_2$ donnée par $(k, (\overline{k_1},...,\overline{k_n})) \longmapsto (\overline{k}, \overline{k_1}, ..., \overline{k_n})$ et $f : M_1 \longrightarrow M_1 \oplus M_2$ donnée par $k \longmapsto (nk, (0,0,...))$. Trouver une section de g revient à considérer une section de la projection $\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$, mais il n'en existe pas.

Lemme. ***(Condition nécessaire de liberté)***

Soit $(\mathcal{E})$ une suite exacte de A-modules

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

où M'' est un module libre. Alors $(\mathcal{E})$ est scindable.

▷ Soit $(e_i)_{i\in I}$ une base de M''. Pour tout $i \in I$, choisissons grâce à l'axiome du choix $x_i \in M$ tel que $g(x_i) = e_i$. Soit $\tau : M'' \longrightarrow M$ l'unique application linéaire vérifiant $\tau(e_i) = x_i$ pour tout i. Alors $g\tau(e_i) = e_i$, donc $g\tau = 1_{M''}$, ce qui montre d'après la propriété fondamentalee que la suite exacte

est scindable. ■

4.3.6 Modules sur un anneau principal

4.3.6.1 Résultats généraux sur la principalité sur les modules

Théorème. ***(Sous-modules d'un module libre sur un anneau principal, cas fini)***

Tout sous-module d'un module libre de rang fini sur un anneau principal est libre.

▷ Soient donc A un anneau principal, L un A-module libre de type fini, donc de rang n. On peut donc prendre $L = A^n$. On procède par récurrence sur n. Pour $n = 1$, un sous-module de A est un idéal de A. Appelons-le I. Puisque A est principal, $I = (f)$. Si f est nul, I est le A-module nul, il est de rang nul et libre. Sinon, $\{f\}$ est une base de I donc I est libre de rang 1. Supposons maintenant $n > 1$ et montrons la propriété au rang n en la supposant vraie à tout rang $k \leqslant n-1$. Soit la suite $0 \longrightarrow A^{n-1} \xrightarrow{f} A^n \xrightarrow{g} A \longrightarrow 0$ évidente. Soit M un sous-module de A^n. On pose $M' = f^{-1}(M) \subseteq A^{n-1}$ et $M'' = g(M) \subseteq A$, alors $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ est une suite exacte courte, et par hypothèse de récurrence, M' et M'' sont libres. Comme M'' est libre, la suite exacte courte scinde et on a que $M \simeq M' \oplus M''$ et par suite, M est libre. ■

Remarque. Cette propriété est fausse dès que A n'est pas principal ! En effet, s'il existe un idéal non principal de A, s'il était libre, A étant bien sûr libre, il serait de rang 1, donc principal, absurde. Il y a donc équivalence entre la principalité de A et le fait que tout sous-module d'un module libre sur A est libre.

La propriété tient encore pour un module de rang quelconque, seulement, la preuve est plus laborieuse et requiert le lemme de Zorn ; Serge Lang même la donne seulement en annexe de sa petite bible de l'algèbre. Nous la recopions mot pour mot :

Théorème. ***(Sous-modules d'un module libre sur un anneau principal, cas général)***

Tout sous-module d'un module libre sur un anneau principal est libre.

▷ Soit A un anneau principal et L un module libre sur A. Soit L' un sous-A-module de L. On va montrer que, si $\mathcal{B} = (e_i)_{i\in I}$ est une base de L, il existe une base de L' extraite de $\mathcal{B}$. Pour tout sous-ensemble J de I, on note L_J le sous-ensemble de L engendré par les vecteurs indexés par J, et note $L'_J = L_J \cap L'$. On considère l'ensemble des (L'_J, w) pour toute partie J de I, et w est une base de L'_J indexée par *un sous-ensemble* de J. L'ordre naturel sur cet ensemble est donnée par $L'_J \subseteq L'_K$ et la base pour L'_K est une extension de la base de L'_J, autrement dit, la restriction de w' à J est w. Il est clair que cet ensemble est inductif et non vide par hypothèse. Par le lemme de Zorn, on prend L'_J,w un élément maximal. On veut montrer que $J = I$. Supposons le contraire. Soit $k \in I \setminus J$. On note $K = J \cup \{k\}$. Si $L_K \cap L' = L'_J$, alors (L'_K, w) est plus grand que notre élément maximal, contradiction. Autrement, il existe un élément de L'_K de la forme $cv_k + y$ où $y \in L_J$ et $c \in A$ non nul. L'ensemble des

c pour lesquels il existe $y \in L_J$ tel que $cv_k + y \in L'$ est un idéal de A principal ; soit a un générateur de cet idéal, et soit $w_k = av_k + y$ correspondant. Si $z \in L'_K$, alors il existe $b \in A$ tel que $z - bw_k \in L_J$. Mais $z - bw_k \in F$, d'où $z - bw_k \in L'_J$. Ainsi les w_j pour $j \in J$ additionnés de w_k forment une base de L'_K, ce qui contredit encore la maximalité de notre élement... maximal, contradiction. Ceci termine la preuve. ■

Ceci ne permet pas d'extrapoler les théorèmes de la dimension des espaces vectoriels, même dans le cas d'un anneau principal.

Exemple

Dans le $\mathbb{Z}$-module $\mathbb{Z}^3$, la famille de vecteurs donnée par $2I_3$ est libre mais pas génératrice.

On montre maintenant une propriété attendue sur les modules de torsion que l'on a laissée aux anneaux principaux (voir ci-haut pour des contre-exemples).

Théorème. *(Modules sans torsion sur un anneau principal)*

Tout module de type fini sans torsion sur un anneau principal est libre.

▷ Soit M de type fini sur un anneau principal. Soit Γ une partie génératrice finie et soit Λ une partie libre maximale de M, L le sous-module qu'elle engendre. Pour tout $x \in \Gamma \setminus \Lambda$, $\Lambda \cup \{x\}$ n'est pas libre, don cil existe $a_x \in A$ non nul tel que $a_x \cdot x \in L$. On note $a = \prod_{x \in \Gamma \setminus \Lambda} a_x \neq 0$ où $\Gamma \setminus \Lambda$ peut être un ensemble fini par typage fini, et si pour tout $x \in M$, $ax \in L$. Si l'on pose $\varphi : M \longrightarrow L$ qui à $x \longmapsto ax$, φ est injective puisque M est sans torsion et un anneau principal est intègre. Donc M est isomorphe à $\varphi(M)$. Or $\varphi(M)$ est libre comme sous-module d'un module libre, donc M est libre. ■

Exercice 25

On souhaite montrer que les hypothèses de ce théorème sont maximales. Préciser un contre-exemple d'un module non libre dans le cas où primo, M est de type fini sans torsion sur un anneau non principal, secundo, M est sans torsion sur un anneau principal, mais pas de type fini.

▷ **Éléments de réponse.**

Le second contre-exemple est donné par le $\mathbb{Z}$-module $\mathbb{Q}$ étudié précédemment. Quant au premier exemple, il est très simple : il suffit de choisir un idéal non principal de type fini d'un anneau, par exemple, pour $A = \mathbb{R}[X,Y]$, on choisit $M = (X,Y)$. Alors M est de type 2, sans torsion, mais $-Y.X + X.Y = 0$, donc X,Y n'est pas $\mathbb{R}[X,Y]$-libre.

On dispose du théorème suivant :

Théorème. ***(Modules sans torsion sur un anneau principal)***

Soit M un module de type fini sur un anneau principal A. Il existe $L \subseteq M$ libre et $T \subseteq M$ de torsion tel que $M = T \oplus L$. De plus, pour toute telle décomposition, $T = M_{\text{tor}}$ et L est isomorphe à M_{tor}.

▷ $0 \longrightarrow M_{\text{tor}} \longrightarrow M \longrightarrow M/M_{\text{tor}} \longrightarrow 0$ est scindée donc M_{tor} admet un supplémentaire isomorphe à M/M_{tor}. Pour le deuxième point, on suppose $M = T \oplus L$ où T est de torsion et L libre. Clairement, $T = M_{\text{tor}}$ en l'écrivant, d'où l'isomorphisme $\pi_{|L} : L \longrightarrow M/M_{\text{tor}}$ un isomorphisme. ■

Remarque. Il reste à comprendre les modules de type fini de torsion sur un anneau A principal. En effet, on sait que tout module libre de type fini de rang n est isomorphe à A^n !

4.3.6.2 Modules de torsion sur un anneau principal

Les premières définitions peuvent être données pour un anneau commutatif A quelconque.

Définition. ***(Élément p-primaire d'un module)***

Soit $p \in A$ un élément irréductible de A. Soit M un A-module. On dit que $x \in M$ est *p-primaire* s'il existe $n \in \mathbb{N}^*$ tel que $p^n x = 0$.

Définition-propriété. ***(Partie p-primaire d'un module)***

Soit M un A-module et $p \in A$ irréductible. L'ensemble des éléments p-primaires de M forme un sous-module de M et on le note $M(p) \subseteq M_{\text{tor}}$.

▷ L'ensemble $N_n = \{x \in M \mid p^n x = 0\}$ sous-module de M. La suite croissante des sous-modules de $\bigcup_{n\in\mathbb{N}^*} N_n$ est un sous-module de M et justement $M(p) = \bigcup_{n\in\mathbb{N}^*} N_n$. ■

Nous allons démontrer :

Théorème. ***(Module de torsion de type fini sur un anneau principal)***

Soit M un A-module *de torsion* de type fini où A est un anneau principal. Il existe des éléments irréductibles $p_1,\ldots,p_l$ deux à deux non associés tels que pour tout irréductible $p \in A$, $M(p) \neq 0$ si et seulement si $p \sim p_i$ pour au moins i, et l'on a :

$$M = \bigoplus_{i=1} pM(p_i).$$

On a besoin d'une batterie de lemmes, sans surprise, que nous énonçons :

Définition. ***(Contre-annulateur d'un scalaire)***

Le *contre-annulateur* du scalaire $f \in A$ d'un A-module M, A un anneau commutatif, est l'ensemble $E_f = \{x \in M \mid fx = 0\}$.

Lemme. ***(Structure du contre-annulateur)***

Le contre-annulateur d'un scalaire de A est un sous-module de M.

On suppose maintenant l'anneau de base *principal*.

Lemme. ***(Contre-annulateur du ppcm)***

Si $f,g \in A$ et $h = f \vee g$, $E_h = E_f + E_g$.

▷ Facile grâce au théorème de Bézout en décomposant le couple (f,g) par extraction du ppcm. ■

Lemme. ***(Contre-annulateur du pgcd)***

Si $f,g \in A$ et $h = f \wedge g$, $E_h = E_f \cap E_g$.

▷ Facile grâce au théorème de Bézout. ■

Corollaire. ***(Tangence des contre-annulateurs d'étrangers)***

Soient $f,g \in A$ premiers entre eux. Alors $E_f \cap E_g = 0$.

On reprend la preuve générale du théorème :

Preuve.

▷ Soit M un module de type fini et de torsion. Dans ce cas, $A \supseteq \mathrm{ann}(M) \neq \{0\}$. Or, $\mathrm{ann}(A)$ est un idéal de A principal, non nul, d'où $\mathrm{ann}(A) = (a)$ où $a \neq 0$. Par décomposition primaire, $a \sim p_1^{\alpha_1} ... p_l^{\alpha_l}$ des irréductibles deux à deux non associés. On peut alors écrire $M = E_a = \bigoplus_{i=1}^{l} E_{p_i^{\alpha_i}}$. Soit p un irréductible de A. Si p est premier à a, alors $E_a \cap E_{p^n} = \{0\}$ pour tout $n \geqslant 1$, d'où $M(p) = \bigcup_{n \geqslant 2} E_{p^n}$. En effet, si l'on est annulé par une certaine puissance de p, ce qui est vrai par type fini, c'est le cas pour tout puissance supérieure. Si p est associé à p_i, on va montrer que $M(p) = E_{p_i^{\alpha_i}}$. Il est clair qu'il suffit de montrer l'inclusion directe. Soit x p-primaire. On pose la quantité $q'' = \prod_{j \neq i} p_j^{\alpha_j} \sim a/p_i^{\alpha_i}$. On pose également $M' = E_{p_i^{\alpha_i}}$ et $M'' = E_{q''} = \bigoplus_{j \neq i} E_{p_j^{\alpha_j}}$. On note que $x \in M(p) \subseteq M = M' \oplus M''$, d'où la décomposition canonique $x = \underbrace{x'}_{\in M'} + \underbrace{x''}_{\in M''}$. Par définition, il existe $n \in \mathbb{N}^*$ tel que $p^n x = 0$, et on peut le prendre sans souci $n \geqslant a_i$; c'est asymptotique. Par somme directe, $p^n x'' = 0$, puis $x'' = 0$, car $E_{q''} \cap E_{p_i^{\alpha_i}}$. Ainsi $x \in M'$. En particulier, $M(p) = M'$, ce qu'il fallait démontrer. ■

4.3.6.3 Décomposition des parties p-primaires et facteurs invariants d'un module

Théorème. ***(Décomposition des parties p-primaires d'un module)***

Soit p un irréductible de A. Soit M un A-module de type fini p-primaire, c'est-à-dire, qui égale sa partie p-primaire : $M = M(p)$. Il existe un isomorphisme $M \xrightarrow{\sim} \bigoplus_{i=1}^{m} A/(p^{r_i})$ où les entiers $r_1,...,r_n$ vérifient $r_1 \geqslant r_2 \geqslant ... \geqslant r_m \geqslant 1$. De plus, cette suite est unique.

On aura besoin de la notion suivante, fondamentale :

Définition. ***(Période d'un élément d'un module)***

Soit $x \in M$ un A-module. On appelle *période de x*, un générateur de son annulateur sur A.

Remarque. Si x est p-primaire, une période de x est de la forme p^r. En effet, il existe n tel que $p^n x = 0$ et alors $(p^n) \subseteq \{a \in A \mid ax = 0\}$.

▷ On s'intéresse d'abord au cas cyclique. Si M est de type fini, p-primaire et cyclique engendré par x, alors grâce à la surjection $\sigma : A \twoheadrightarrow M$ canonique, si p^r est une période de x, $\mathrm{Ker}(\sigma) = (p^r)$ et $M \simeq A/(p^r)$. On raisonne maintenant par récurrence sur le nombre de générateurs de M. Supposons que M est engendré par X de cardinal $n+1$. On a $\mathrm{ann}(M) = (p^r)$. Tout élément de X est annulé par p^r. Il y en a au moins un qui a pour période p^r. ■

4.3.6.4 Classification des modules de type fini sur un anneau principal : théorème de Kronecker

Théorème. ***(Théorème de décomposition pour les parties de torsion)***

Soient A un anneau principal, M un module de type fini de torsion. Alors $M \simeq \bigoplus_{i=1}^{n} A/(a_i)$ où $(a_1) \subseteq (a_2) \subseteq ... \subseteq (a_n) \neq A$ et la famille $(a_i)_{i \in [\![1,n]\!]}$ est déterminée de manière unique.

▷ Pour le premier point, on remarque que $M = \bigoplus_{i=1}^{l} M(p_i) \simeq \bigoplus_{i=1}^{l} \bigoplus_{j=1}^{n_i} A/(p_i^{r_j})$ où $(r_j^i)_j$ est décroissante et l'on conclut par théorème chinois.

Supposons $M \simeq \bigoplus_{i=1}^{n} A/(a_i) \simeq \bigoplus_{j=1}^{m} A/(b_j)$ où $(a_1) \subseteq (a_2) \subseteq ... \subseteq (a_n)$ et $(b_1) \subseteq (b_2) \subseteq ... \subseteq (b_m)$. Montrons que $n = m$ et que $a_i \sim b_i$. On raisonne par récurrence sur le nombre de facteurs irréductibles de $a_1,...,a_n$. Pour $N = 0$, $M = 0$ d'où $m = 0$ et il n'y a rien à faire. Soit maintenant $N > 0$. Soit p un irréductible de A. Étudions M/pM et pM. Soit $E = A/(q)$ où $q \in A \setminus \{0\}$. Si p est premier à q, soit p inversible dans $A/(q)$, alors $pE = p(A/(q)) = A/(q)$, donc $E/pE = \{0\}$. Si maintenant p divise q, $pE \simeq A/(q/p)$ d'où $E/pE \simeq A/(p)$. Or $A/(p)$ est un corps, donc M/pM étant un $A/(p)$ module, M/pM est un $A/(p)$ espace vectoriel, dont la dimension est $\mathrm{card}(i, p \mid a_i)$. Supposons que p divise tous les a_i. Donc la dimension de M/pM est n ; c'est aussi le nombre de j tel que $p \mid b_j$. Donc

$n \leqslant m$. Par symétrie, $n = m$ et donc p divise b_j pour tout $j = 1,...,m$. Soit n', respectivement m', le nombre d'indice i, respectivement j, pour lesquels a_i, respectivement b_j, n'est pas associé à p. On a $pM \simeq \bigoplus_{i=1}^{n} A/(a_i/p) \simeq \bigoplus_{i=1}^{m'} A/(b_j/p)$. Le nombre de facteurs irréductibles de $\prod_{i=1}^{n'}(a_i/p)$ est strictement inférieur à N. Par hypothèse de récurrence, $n' = m'$ et $\forall n' < i \leqslant n \quad a_i \sim p \sim b_j$. Par hypothèse de récurrence, $\forall 1 = 1...n'$, $\frac{a_i}{p} \simeq \frac{b_i}{p}$ et donc $a_i \sim b_i$. On applique l'hypothèse de récurrence à pM, ce qui permet de terminer la preuve. ■

Remarque. Soient M,M' des modules de type fini sur A principal. Alors $M \simeq M'$ si et seulement si

$$M \simeq A^s \oplus \left(\bigoplus_{i=1}^{n} A/(a_i)\right) \text{ et } M' \simeq A^{s'} \oplus \left(\bigoplus_{i=1}^{m} A/(b_i)\right)$$

où $s = s'$, $n = m$ et $(a_i) = (b_i)$ pour tout i.

On fixe A un anneau intègre principal.

Remarque importante. On en déduit le théorème de Kronecker pour les groupes abéliens finis, par ce que tout groupe abélien est canoniquement muni de la structure de $\mathbb{Z}$-modules !

4.3.6.5 Détermination pratique du rang partiel et des facteurs invariants dans la décomposition de Kronecker

Soit M un A-module de type fini, A principal. Alors A^n se surjecte sur M par σ. Alors Kerσ est un sous-module de A^n libre donc de rang $m \leqslant n$, d'où Ker$\sigma \simeq A^m$. On a $0 \longrightarrow \text{Ker}\sigma \xhookrightarrow{R} A^n \twoheadrightarrow M \longrightarrow 0$ où $R \in \mathfrak{M}_{m,n}(A)$. Ainsi $M \simeq A^n/\text{Im}(R) \simeq A^m/\text{Ker}(\sigma)$.

Remarque. On dispose d'un algorithme effectif en plus de l'algorithme théorique présenté ci-dessus, permettant de trouver la décomposition primaire d'un élément dans le cas où M est un module sur un anneau euclidien ; notons que ceci nous permet de garder l'aspect pratique de la décomposition pour les groupes, puisque notre ami $\mathbb{Z}$ est euclidien. En outre, pour trouver un anneau principal non euclidien, il faut se lever de bonne heure.

Modules et invariants de similitude

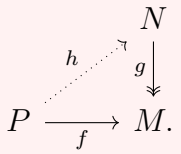
Soit V un espace vectoriel et $f \in \text{End}(V)$. Alors V hérite par f d'une structure de $\mathbb{K}[X]$-module, $K[X]$ principal. On peut donc appliquer à V le théorème de Kronecker. On en déduit la théorie des invariants de similitude de Frobenius.

4.3.7 Projectivité, platitude

4.3.7.1 Modules projectifs

Définition. ***(Module projectif)***

Soit P un A-module. Alors P est dit *projectif* si pour pour tout morphisme $f : P \longrightarrow M$ de A-modules et tout morphisme surjectif $g : N \longrightarrow M$, il existe un morphisme de A-module $h : P \longrightarrow N$ tel que $f = g \circ h$, c'est-à-dire faisant commuter le diagramme :



Autrement, si le foncteur $A \mapsto \mathrm{Hom}(P,A)$ est exact.

Reformulation pratique. ***(Projectivité)***

Un module P est projectif si et seulement si toute suite exacte courte $0 \longrightarrow L \longrightarrow M \longrightarrow P \longrightarrow 0$ est scindée.

▷ En exercice. ■

Reformulation pratique. ***(Projectivité)***

Soit P un A-module. Alors P est projectif si et seulement si le foncteur $\mathrm{Hom}(P,?)$ est exact, autrement dit, si pour toute suite exacte de A-modules $0 \longrightarrow N \longrightarrow M \longrightarrow L \longrightarrow 0$, on a une suite exacte de modules : $0 \longrightarrow \mathrm{Hom}(P,N) \longrightarrow \mathrm{Hom}(P,M) \longrightarrow \mathrm{Hom}(P,L) \longrightarrow 0$.

Remarque importante. Le foncteur covariant $\mathrm{Hom}(P,?)$ est toujours exact à gauche. Ainsi, P est projectif si et seulement si $\mathrm{Hom}(P,?)$ est exact à droite, *i.e.* si pour tout morphisme surjectif de A-modules $M \xrightarrow{f} L$, l'application induite $\mathrm{Hom}(P,M) \to \mathrm{Hom}(P,L)$ (par $u \mapsto f \circ u$) est surjective.

▷ En effet, si $f : N \to M$ est injective, $\tilde{f} : \mathrm{Hom}(P,N) \to \mathrm{Hom}(P,M), u \mapsto f \circ u$ est injective, car f est une application inversible à gauche. Si de plus on a $g : M \to L$, alors $\mathrm{Im}(\tilde{f}) = \mathrm{Ker}(\tilde{g})$, car $\tilde{g}(f \circ u) = (g \circ f) \circ u = 0 \circ u = 0$ pour tout $u : P \to N$ et si $\tilde{g}(v) = 0$, $\mathrm{Im}(v) \subseteq \mathrm{Ker}(g) \subseteq \mathrm{Im}(f)$, et notons $f' : \mathrm{Im}(f) \to N$ l'inverse à gauche de f sur $\mathrm{Im}(f)$, puisque $f : N \to \mathrm{Im}(f)$ est un isomorphisme par le théorème de factorisation, f étant injective ; posons $u = f' \circ v$; alors si $x \in P$, $v(x) \in \mathrm{Im}(f)$, soit $v(x) = f(t)$ puis $f \circ u(x) = f \circ f' \circ f(t) = f(t) = v(x)$ d'où $f \circ u = v$. ■

Propriété. ***(Caractérisation des modules projectifs)***

Un module est projectif si et seulement s'il est facteur direct dans un certain module libre.

▷ Puisque qu'un module est toujours de type quelconque, il existe une application surjective f de $M = A^{(I)}$ module libre dans P. Notons $L = \mathrm{Ker}(f)$. Alors on a une suite exacte courte telle que dans dans la reformulation ; elle est donc scindée si P est projectif, donc $M = L \oplus P$, et P est facteur direct associé à L dans le A-module libre M. Réciproquement, supposons que $P \oplus M$ dans un A-module libre $A^{(I)}$. Soit (e_i) la base canonique de $A^{(I)}$, s l'injection canonique de P et π la projection grâce au facteur direct. Noter que $\pi \circ s = id_P$. Soient alors g,f comme dans la définition. Soit a_i une préimage de $f(\pi(e_i))$ par g pour tout $i \in I$. Alors par propriété universelle des modules libres il existe un unique morphisme $\varphi : A^{(I)} \longrightarrow E$ et $\varphi(e_i) = a_i$ pour tout i. Comme $g \circ \varphi$ et $f \circ \pi$ coïncident sur la base, ils sont égaux. On pose alors $h = \varphi \circ s$. ■

On en déduit directement :

Propriété. ***(Libre $\Longrightarrow$ projectif)***

Tout module libre est projectif.

Ainsi, le défaut de projectivité dans les modules ne se trouve que pour des modules ne répondant pas aux attendus de la théorie de la dimension linéaire.

Contre-exemple. ***(Module projectif non libre)***

Le module $\mathbb{Z} \times \{0\}$ sur l'anneau $\mathbb{Z} \times \mathbb{Z}$ (non intègre) est projectif (prendre la définition) sans être libre, car il n'y a jamais unicité de la décomposition sur A. □

On a la réciproque dans le cas $A = \mathbb{Z}$.

Propriété. ***(Projectivité et liberté dans le cas principal)***

Sur un anneau principal, un module est libre si et seulement s'il est projectif.

Exemples. ***(Modules projectifs)***

1. Tout anneau A est projectif en tant que A-module.
2. Facilement, un coproduit de modules projectifs est projectif. En particulier, tout module libre (comme coproduit de copies de A) est projectif.

4.3.7.2 Modules plats

En un sens, les modules plats généralisent les modules projectifs, comme on va le voir.

Définition. ***(Module plat)***

Soit P un A-module. Alors P est dit *plat* si le foncteur $\otimes P$ est exact, autrement dit, si pour toute suite exacte de A-modules $0 \longrightarrow N \longrightarrow M \longrightarrow L \longrightarrow 0$, on a une suite exacte de modules : $0 \longrightarrow N \otimes P \longrightarrow M \otimes P \longrightarrow L \otimes P \longrightarrow 0$.

Remarque importante. Le foncteur covariant $\otimes_A P$ est toujours exact à droite. Ainsi, P est plat si et seulement si $\otimes_A P$ est exact à gauche, *i.e.* si pour tout morphisme injectif de A-modules $N \xrightarrow{f} M$, l'application induite $N \otimes_A P \to M \otimes_A P$ (par $f(a \otimes b) = f(a) \otimes b$) est injective.

▷ Il n'y a pas de moyen simple de le vérifier à la main (le problème est de montrer que pour $N \xrightarrow{f} L \xrightarrow{g} K$, $\mathrm{Ker}(\tilde{g}) \subseteq \mathrm{Im}(\tilde{f})$). Raisonnement autrement. On a un isomorphisme $\mathrm{Hom}(M \otimes P, A) \simeq \mathrm{Bil}(M \times P, A) \simeq \mathrm{Bil}(P \times M, A) \simeq \mathrm{Hom}(P, \mathrm{Hom}(M, A))$ de sorte que $(M \otimes P)^* \simeq \mathrm{Hom}(P, M^*)$. À partir de la, il suffit de remarquer que la suite $M_1 \to M_2 \to M_3 \to 0$ est exacte si et seulement si $0 \to M_3^* \to M_2^* \to M_1^3$ est exacte. ■

Fait. ***(Cas des modules libres)***

Tout module libre est plat. En particulier, tout espace vectoriel est plat.

En effet, si M est un A-module libre de base $(e_i)_{i \in I}$, alors $M = \bigoplus_{i \in I} Ae_i$, d'où par définition $M \otimes_A N = \bigoplus_i (Ae_i) \otimes_A N$. Ainsi tout élément de $M \otimes_A N$ s'écrit de manière unique comme somme de produit tensoriels de la base avec des y_i formant une famille presque nulle de N. Donc si $N' \longrightarrow N$ est une application injective, le A-morphisme induit $N' \otimes_A M \longrightarrow N \otimes_A M$ reste injectif. D'où le résultat.

Propriété

Un module de type fini sur un anneau local est plat si et seulement s'il est libre.

Propriété. ***(Projectif $\Longrightarrow$ plat)***

Tout module projectif est plat.

▷ Il est clair d'après la reformulation qu'un module projectif est facteur direct dans un module libre. Ceci suffit à créer la suite exacte ci-dessus. ■

Contre-exemple. ***(Module plat non projectif)***

Par exemple, le $\mathbb{Z}$-module $\mathbb{Q}$ est plat (c'est une localisation de $\mathbb{Z}$), mais pas projectif car il n'existe pas d'homomorphisme non nul f de $\mathbb{Q}$ dans un module libre M (en effet, $f(1) = 2^n f(\frac{1}{2^n}) \in 2^n M$ pour tout entier naturel n, ce qui est impliquerait que $f(1) = 0$, et donc $f = 0$). □

Par contre :

Propriété

Tout module plat de présentation finie est projectif.

Propriété. ***(Plat $\Longrightarrow$ sans torsion)***

Tout module plat sur un anneau intègre est sans torsion.

▷ Soit M un A-module de torsion et x un élément de torsion associé à $k \in A$, soit $kx = 0_M$. On a une suite exacte courte $0 \longrightarrow A \longrightarrow A \longrightarrow A/\mathrm{Im}(f) \longrightarrow 0$ où la première flèche non triviale est $f : a \mapsto ka$. Elle est injective puisque A est intègre. Mais si on tensorise par $\otimes_A M$, elle ne l'est plus... D'où le résultat par contraposée. ■

Contre-exemple. ***(Module ni projectif, ni plat)***

Le $\mathbb{Z}$-module $\mathbb{Z}/2\mathbb{Z}$ n'est pas projectif, ni, a fortiori, plat. En effet, il ne peut pas être sous-module d'un module libre sur $\mathbb{Z}$, car il n'est pas libre sur $\mathbb{Z}$ principal. □

4.3.7.3 Modules injectifs

Théorème. ***(Critère de Baer)***

Contre-exemple

$\mathbb{Q}(X)/\mathbb{Z}[X] = M$ est un module divisible qui n'est pas injectif.
Plus précisément, considérons $R = \mathbb{Z}[X]$ et $I = (2,X)$. Soit $f : I \to M$ qui à 2 associe la classe de 0 et à X associe la classe de $\frac{1}{2}$. Ce morphisme est alors nul. Supposons qu'on l'étende à $\tilde{f} : R \to M$. □

Chapitre 5

Espaces préhilbertiens

Résumé

Premier pas vers la géométrie, la structure hilbertienne rajoute la notion de produit scalaire, normalement connue depuis le lycée, à la structure linéaire. En extrayant les propriétés classiques de cette opération, on obtient la notion de bilinéarité, qui, par le biais du théorème de Riesz, se rattache très fortement à la théorie de la dualité. Enfin, en définissant l'angle de la même manière que la définition géométrique du produit scalaire, on espace préhilbertien devient un esace muni d'une distance (par la norme naturellement issue du produit scalaire) et de mesures d'angle, et constitue donc le cadre standard de la géométrie euclidienne en dimensions supérieures.

5.1 Matrices symétriques, hermitiennes ; orthogonales, unitaires

Soient m,n deux entiers naturels. Soit $\mathbb{K}$ un corps.

5.1.1 Vocabulaire des espaces préhilbertiens réels ou complexes

Définition. ***(Produit scalaire hermitien)***

Soit φ une forme sur $E \times E$ où E est un $\mathbb{C}$-espace vectoriel. On dit que φ est un *produit scalaire (hermitien)* sur E si c'est une forme sesquilinéaire hermitienne définie positive. Autrement dit :

(i) la forme φ est sesquilinéaire (*i.e.* « $\frac{3}{2}$-linéaire »), c'est-à-dire linéaire par rapport à la deuxième variable et semi-linéaire par rapport à la première : pour tous x,$y \in E$, $\lambda \in \mathbb{C}$, $\varphi(\lambda x + y) = \overline{\lambda}\varphi(x) + \varphi(y)$;

(ii) la forme φ est hermitienne, c'est-à-dire que pour tous x,$y \in E$, $\varphi(x,y) = \overline{\varphi(y,x)}$.

On remarque que si la forme φ est sesquilinéaire hermitienne, alors pour tout x, $\varphi(x,x) \in \mathbb{R}$.

(iii) la forme φ est positive ;

(iv) la forme φ est définie (on dit aussi *définie positive*).

Définitions

- L'espace E est appelé *espace préhilbertien complexe*.
- Si de plus E est de dimension finie, E est appelé *espace hermitien*.
- Si E est en fait un espace vectoriel sur $\mathbb{R}$, E est appelé *espace préhilbertien réel*.
- Si de plus E est de dimension finie, E est appelé *espace euclidien*.

Astuce !

Pour vérifier qu'un truc est un produit scalaire hermitien, on peut enlever l'axiome de semi-linéarité à gauche (elle découle de la linéarité à droite et du caractère hermitien).

Propriété. *(Matrice adjointe)*

Pour toute matrice $A \in \mathfrak{M}_{m,n}(\mathbb{C})$, en notant $\langle .,. \rangle_n$ le produit scalaire hermitien (ou, si A est réelle, euclidien) canonique de $\mathbb{C}^n$, il existe une unique matrice A^* appelée *adjointe* de A telle que :

$$\forall u,v \in \mathbb{C}^n \quad \langle Au, v \rangle_m = \langle A^* v, u \rangle_n .$$

▷ Ce résultat est vrai pour n'importe quels produits scalaires sur l'espace de départ et l'espace d'arrivée : montrons-le dans ce cadre. ■

Propriété

Pour toute matrice $A \in \mathfrak{M}_{m,n}(C)$, $A^* = \overline{{}^t A}$.

Propriété

Pour toute matrice $A \in \mathfrak{M}_{m,n}(\mathbb{C})$,

- $\mathrm{Ker}(A^*) = (\mathrm{Im}(A))^\perp$;
- $\mathrm{Im}(A^*) = (\mathrm{Ker}(A))^\perp$.

Définition. *(Matrice hermitienne)*

Soit A une matrice carrée. On dit que A est *hermitienne* si elle égale son adjointe.

Définition. *(Matrice symétrique)*

Soit A une matrice hermitienne. Si de plus A est réelle, elle est dite *symétrique*.

Définition. *(Matrice unitaire)*

Soit A une matrice carrée. On dit que A est *unitaire* si son inverse est son adjointe.

Définition. ***(Matrice orthogonale)***

Soit A une matrice unitaire. Si de plus A est réelle, elle est dite *orthogonale*.

Définition. ***(Matrice normale)***

Soit A une matrice carrée. Si $AA^* = A^*A$, A est dite *normale*.

Propriété. ***(Unitaire $\Longrightarrow$ normale)***

Toute matrice unitaire est normale. En particulier, toute matrice orthogonale est normale.

Propriété

Toute matrice de permutation est orthogonale.

Définition. ***(Matrice positive)***

Une matrice hermitienne est dite *positive* ou *semi-définie positive* si et seulement si la forme quadratique associée l'est, c'est-à-dire si pour tout vecteur x, $\langle Ax,x\rangle \geqslant 0$.

Définition. ***(Matrice définie positive)***

Une matrice hermitienne est dite *définie positive* si et seulement si la forme quadratique associée l'est, c'est-à-dire si pour tout vecteur **non nul** x, $\langle Ax,x\rangle > 0$.

Propriété. ***(Caractérisation des matrices positives et définies positives)***

- Une matrice hermitienne est positive si et seulement si toutes ses valeurs propres sont positives.
- Une matrice hermitienne est définie positive si et seulement si toutes ses valeurs propres sont strictement positives.

5.2 Topologie des espaces préhilbertiens

5.2.1 Inégalité de Bessel, égalité de Parseval

Propriété. ***(Identité de Rayleigh)***

Soient $(E, (\ \cdot\ ,\ \cdot\ )$ un espace préhilbertien et $(e_k)_{k\in\mathbb{N}}$ une suite orthonormale totale de vecteurs de E. Pour tout n, on note p_n le projecteur orthogonal sur $\mathrm{Vect}(e_0,\ldots,e_n)$. Alors pour tout $x \in E$, $p_n(x) \underset{n\to\infty}{\longrightarrow} x$, d'où la relation $x = \sum_{k=0}^{\infty} (x, e_k)e_k$.

▷ Soit $x \in E$ et $\varepsilon > 0$. $(e_k)_{k\in\mathbb{N}}$ est totale donc $F = \mathrm{Vect}(e_k)$ est dense dans E, par conséquent il existe $y \in F$ tel que $\|x - y\| < \varepsilon$. $y \in F = \mathrm{Vect}(e_k)$ donc il existe $N \in \mathbb{N}$ tel que $y \in \mathrm{Vect}(e_0,\ldots,e_N)$.

Pour $n \in \mathbb{N}$, on pose $F_n = \text{Vect}(e_0,...,e_n)$. On a $y \in F_N$ donc $d(x,F_N) \leqslant \|x-y\| \leqslant \varepsilon$. De plus, pour tout $n \in \mathbb{N}$, on a $F_N \subseteq F_n$ donc $d(x,F_n) = \|x - p_n(x)\| \leqslant d(x,F_N) \leqslant \varepsilon$, ce qui termine la preuve. ■

Théorème. ***(Égalité de Parseval-Bessel)***

Soient $(E, (\ \cdot\ ,\ \cdot\ )$ un espace préhilbertien et $(e_k)_{k\in\mathbb{N}}$ une suite orthonormale de vecteurs de E. Soit $x \in E$. Alors $\|x\|^2 = \sum_{k=0}^{\infty} |(e_k,x)|^2$ si et seulement si x est adhérent à $\text{Vect}(e_k)_{k\in\mathbb{N}}$.

▷ Dans tous les cas, d'après l'inégalité de Bessel donne $\sum_{k=0}^{\infty} |(e_k,x)|^2 \leqslant \|x\|^2$. Le théorème de Parseval pour une base hilbertienne donne que si x est adhérent à $\text{Vect}(e_k)$, alors on a l'égalité. Réciproquement, supposons l'inégalité inverse. Alors on a l'égalité. Montrons que x est adhérent à $\text{Vect}(e_k)$. Il suffit de montrer que $x = \sum_{k=0}^{\infty} (x, e_k)e_k$. ■

Chapitre 6

Théorie de Lie

Résumé

Pour être franc, je n'ai pas compris l'intérêt.

6.1 Introduction aux algèbres de Lie et à leurs représentations

6.1.1 Définitions générales

On observera nombre de parallèles mot à mot avec la théorie des groupes.

6.1.1.1 Algèbres de Lie, crochet de Lie

Soit k un corps commutatif. Dans la plupart des cas, k sera algébriquement clos, et surtout de caractéristique nulle.

Définition. ***(Algèbre de Lie, crochet)***

Une *k-algèbre de Lie* $\mathfrak{g}$ est un espace vectoriel sur k muni d'une application bilinéaire
$\begin{array}{ccc} \mathfrak{g}\times\mathfrak{g} & \longrightarrow & \mathfrak{g} \\ (x,y) & \longmapsto & [x,y] \end{array}$, dit *crochet de Lie* vérifiant :

- $[x,x]=0$ pour tout $x\in\mathfrak{g}$,
- *(Identité de Jacobi)* $[x,[y,z]]+[y,[z,x]]+[z,[x,y]]=0$ pour tous $x,y,z\in\mathfrak{g}$.

Mnémonik : Dans l'identité de Jacobi, les variables se déplacent vers la gauche.

Une algèbre de Lie n'est a priori pas une algèbre !

Propriété. ***(Opposition du crochet)***

Soit $(\mathfrak{g},[\,\cdot\,,\cdot\,])$ une algèbre de Lie. Alors pour tous $x,y\in\mathfrak{g}$, $[x,y]=-[y,x]$.

Exemple. ***(Algèbre de Lie)***

Si A une k-algèbre (associative, non unitaire) $\mathfrak{g}=(A,[a,b]=ab-ba)$ est une algèbre de Lie.

6.1.1.2 Sous-algèbres de Lie, algèbres de Lie quotients

Définition. ***(Sous-algèbre de Lie)***

Soit $\mathfrak{g}$ une algèbre de Lie et $\mathfrak{h} \subseteq \mathfrak{g}$. On dit que $\mathfrak{h}$ est une *sous-algèbre de Lie* si $\mathfrak{h}$ est un sous-espace vectoriel de $\mathfrak{g}$ stable par le crochet.
C'est évidemment une algèbre de Lie.

Exemples. ***(Sous-algèbres de Lie)***

1. Si A est une algèbre de Lie et une algèbre, et si B est une sous-algèbre de A, alors c'est une sous-algèbre de Lie de A.

Définition-propriété. ***(Algèbre de Lie quotient)***

Soit $\mathfrak{g}$ une algèbre de Lie et $\mathfrak{h}$ une sous-algèbre de Lie. Alors on peut définir l'*algèbre de Lie quotient* $\mathfrak{g}/\mathfrak{h}$. Elle vérifie la propriété universelle du quotient habituelle.

▷ En effet, on dispose de $\mathfrak{g} \twoheadrightarrow \mathfrak{h}$. ■

6.1.1.3 Morphismes d'algèbres de Lie

Définition. ***(Morphisme d'algèbres de Lie)***

Soient $\mathfrak{g},\mathfrak{h}$ deux algèbres de Lie. Un *morphisme de Lie* est une application k-linéaire de $\mathfrak{g}$ dans $\mathfrak{h}$ telle que pour tous $x,y \in \mathfrak{g}$, $f([x,y]) = [f(x),f(y)]$. On note $\mathrm{Hom}_{\mathrm{Lie}}(\mathfrak{g},\mathfrak{h})$ ou plus simplement $\mathrm{Hom}(\mathfrak{g},\mathfrak{h})$ l'ensemble des morphismes de Lie de $\mathfrak{g}$ dans $\mathfrak{h}$.

Exemples. ***(Morphismes de Lie)***

1. Si A une k-algèbre (associative, non unitaire) $\mathfrak{g} = (A, [a,b] = ab - ba)$ est une algèbre de Lie et $\mathrm{Hom}_{\mathrm{Lie}}(\mathfrak{g},\mathfrak{h}) = \mathrm{Hom}(\mathfrak{g},\mathfrak{h})$.
2. En particulier si V est un espace vectoriel, en particulier si c'est une algèbre de Lie $\mathfrak{g}$, alors $\mathrm{End}(V)$ est une algèbre de Lie pour le crochet $[u,v] = u \circ v - v \circ u$ et l'on note $gl(V)$ et $\mathfrak{gl}(\mathfrak{g})$ l'algèbre de Lie ainsi obtenue.

Définition. ***(Isomorphisme d'algèbres de Lie)***

Un *isomorphisme d'algèbres de Lie* est un morphisme bijectif entre algèbres de Lie.

Propriété. ***(Bonne définition de l'isomorphisme d'algèbre de Lie)***

Soit $f : \mathfrak{g} \to \mathfrak{h}$ un isomorphisme d'algèbres de Lie. Alors f^{-1} est un morphisme d'algèbres de Lie.

On définit sans problème la notion de *suite exacte d'algèbres de Lie*.

Propriété. ***(Noyau d'un morphisme de Lie)***

Le noyau d'un morphisme de Lie est une sous-algèbre de Lie de l'algèbre de départ.

Propriété. ***(Image d'un morphisme de Lie)***

L'image d'un morphisme de Lie est une sous-algèbre de Lie de l'algèbre d'arrivée.

Exercice 26

Notons $e = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $f = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ et $h = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Soit $\sigma = \exp(\mathrm{ad},e) \circ \exp(-ad,e)$. Montrer que $\sigma \in \mathrm{Aut}_{\mathrm{Lie}}(\mathfrak{sl}_2(k))$ et calculer σ en e, f et h *(voir la section suivante pour la définition de* $\mathfrak{sl}$*)*.

6.1.1.4 Opposition d'algèbres de Lie

Définition. ***(Algèbre de Lie opposée)***

Soit $\mathfrak{g}$ une algèbre de Lie. On note et appelle $\mathfrak{g}^{\mathrm{op}}$ l'*algèbre de Lie opposée* à $\mathfrak{g}$, l'algèbre de Lie d'espace sous-jacent $\mathfrak{g}$ vu comme k-espace vectoriel avec pour crochet, pour $x,y \in \mathfrak{g}$: $[x,y]_{\mathfrak{g}^{\mathrm{op}}} := -[x,y]_{\mathfrak{g}}$.

Propriété. ***(Algèbre de Lie et algèbre de Lie opposée)***

Pour toute algèbre de Lie $\mathfrak{g}$, $\mathfrak{g} \simeq \mathfrak{g}^{\mathrm{op}}$ par un isomorphisme d'algèbres de Lie.

6.1.1.5 Sommes d'algèbres de Lie

Définition-propriété. ***(Somme d'algèbres de Lie)***

Soient $(\mathfrak{g}_i)_{i\in I}$ une collection d'algèbres de Lie. Alors on peut définir une algèbre de Lie dite *somme des* $\mathfrak{g}_i$, $i \in I$, notée $\bigoplus_{i\in I} \mathfrak{g}_i$ où le crochet est défini terme à terme sur le produit. En particulier, si $\mathfrak{g},\mathfrak{h}$ sont deux algèbres de Lie, pour tous $(a,b) = a\oplus b,(a',b') = a'\oplus b' \in \mathfrak{g}\oplus\mathfrak{h}$ en tant qu'espaces vectoriels, $[(a,b),(a',b')] := ([a,a'],[b,b']) = [a,a'] \oplus [b,b']$.

Exercice 27 *(Décomposition classique de* $\mathfrak{gl}(n)$*)*

Soit $n \in \mathbb{N}$. On note $\mathfrak{s}(n)$ l'algèbre des homothéties de $\mathfrak{M}_n(k)$. Montrer que, si $\mathrm{car}(k) \nmid n$, alors $\mathfrak{gl}(n) = \mathfrak{sl}(n) \oplus \mathfrak{s}(n)$ en tant qu'algèbres de Lie. Que dire en caractéristique n ?

▷ **Éléments de réponse.**

Invoquer le théorème de Dunford.

En caractéristique n, ce ne peut-être vrai : on aurait que toute matrice est une homothétie (comment ?)

La théorie des algèbres de Lie est liée à celle des groupes de Lie, mais pas que. Voyons des exemples pour l'illustrer.

6.1.1.6 Quelques exemples d'algèbres de Lie

Exemples. ***(Algèbres de Lie)***

1. On a déjà vu qu'une algèbre est une algèbre de Lie en puissance. Si la multiplication est commutatif, le crochet est identiquement nul : l'algèbre de Lie est *abélienne*.
2. Un espace vectoriel E muni du produit trivial $[v,w] = 0_E$ pour tous $v,w \in E$ est une algèbre de Lie.
3. $\mathbb{R}^3$ muni du produit vectoriel est une $\mathbb{R}$-algèbre de Lie.
4. Comme on l'a dit, si V est un k-espace vectoriel, $\mathrm{End}(V)$ muni du crochet $[f,g] = f \circ g - g \circ f$ est une k-algèbre de Lie. Munie du crochet $g \circ f - f \circ g$, on obtient encore une k-algèbre de Lie, mais ce n'est certainement pas la même, mais c'est l'algèbre opposée de la première.
5. *(Groupes de Lie)* On fixe $k = \mathbb{R}$ ou $\mathbb{C}$. Si G est un groupe de Lie, alors T_1G l'espace tangent en $1 \in G$ à G est canoniquement une algèbre de Lie. De là viennet la plupart des exemples classiques que nous développons ci-dessous.
6. *(Groupes algébriques)* On suppose k algébriquement clos. Soit G une variété algébrique G muni de lois de groupes qui sont des applications régulières (typiquement, la loi de groupe sur une conique).
7. L'algèbre de Lie du groupe $(\mathbb{C}^*,\times)$ est naturellement identifiée à $\mathbb{C}$. L'algèbre de Lie du groupe S^1 s'identifie au sous-espace vectoriel des imaginaires purs.
8. $\mathfrak{gl}(n,k) = \mathfrak{gl}_n(k) = \mathfrak{gl}(n)$ (où k est alors passé sous silence) est l'algèbre de Lie munie du crochet commutateur sur l'espace vectoriel des matrices $\mathfrak{M}_n(k)$. Elle est de dimension n^2. Si $k = \mathbb{R}$, on montre que c'est l'algèbre de Lie du groupe de Lie $GL_n(\mathbb{R})$, d'où la notation. Même remarque pour les algèbres suivantes. On n'identifie pas forcément $\mathfrak{gl}(n,k)$ à un espace de matrices, et l'on peut garder le formalisme des endomorphismes.
9. $\mathfrak{sl}(n)$ l'ensemble des matrices de trace nulle de $\mathfrak{M}_n(\mathbb{R})$ est une algèbre de Lie munie du crochet induit par $\mathfrak{gl}(n)$. Ceci vaut aussi pour k un corps quelconque. On note souvent : $A_n = \mathfrak{sl}(n+1)$ l'*algèbre des matrices sans trace*. Elle est de dimension $n(n+2)$.
10. $\mathfrak{o}(n) = \mathfrak{so}(n)$ pour $k = \mathbb{R}$ l'ensemble des matrices antisymétriques est une algèbre de Lie munie du crochet induit. On peut écrire pour k de caractéristique nulle :

$\mathfrak{so}(2n+1) = \{x \in \mathfrak{gl}(2n+1) \mid sx = -{}^t xs\}$ où $s = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & I_n \\ 0 & I_n & 0 \end{pmatrix}$ si $\mathrm{car}(k) \neq 0$. On note souvent $B_n = \mathfrak{so}(2n+1)$ l'*algèbre de Lie orthogonale impaire*. De même, $\mathfrak{so}(2n) = \{x \in \mathfrak{gl}(2n) \mid sx = -{}^t xs\}$ où $s = \begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix}$ si $\mathrm{car}(k) \neq 0$. On note souvent $D_n = \mathfrak{so}(2n)$ l'*algèbre de Lie orthogonale paire*. La dimension de $\mathfrak{so}(n)$ est $\frac{n(n-1)}{2}$.

11. $\mathfrak{u}(n)$ pour $k = \mathbb{C}$ l'ensemble des matrices antihermitiennes $\neq \mathfrak{su}(n)$ toujours pour $k = \mathbb{C}$ l'ensemble des matrices antihermitiennes de trace nulle sont des algèbres de Lie munies du crochet induit.

12. $\mathfrak{s}(n)$ pour k quelconque note l'algèbre de Lie, munie du crochet induit, des homothéties de $\mathfrak{M}_n(k)$. Elle n'apparaît pas naturellement associée à un groupe de Lie cependant.

13. $\mathfrak{sp}(n)$ pour n pair, $n = 2k$, est l'algèbre des matrices symplectiques : $\{x \in \mathfrak{gl}(n) \mid sx = -{}^t xs\}$ où $s = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}$, qui est de Lie munie du crochet induit. On note souvent : $C_k = \mathfrak{sp}2k$ l'*algèbre de Lie symplectique*. Elle est de dimension $2n^2$.

14. Si M est une variété lisse, l'espace vectoriel $\mathfrak{X}(M)$ des champs de vecteurs lisses sur M, muni du crochet de Lie $[X,Y]_p(\varphi) := X_p(Y_p(\varphi)) - Y_p(X_p(\varphi))$ est une algèbre de Lie.

15. Si G est un groupe de Lie, $\mathfrak{X}^G(G)$ l'ensemble des champs de vecteurs lisses sur G invariants à gauche est une sous-algèbre de Lie de $\mathfrak{X}(G)$.

16. Si $\mathfrak{g}$ est une algèbre de Lie, $\mathrm{Der}(\mathfrak{g})$ munie du crochet $[\partial_1,\partial_2] = \partial_1 \circ \partial_2 - \partial_2 \circ \partial_1$ est une algèbre de Lie.

Astuce !

Il serait peut-être intelligent de démontrer une bonne fois pour toute qu'un commutateur définit un crochet de Lie.

Contre-exemple. ***(Algèbre de Lie qui n'est pas une algèbre)***

Soit V un k-espace vectoriel de dimension finie. Alors $sl(V) = \{x \in gl(V) = \mathrm{End}(V) \mid \mathrm{tr}(x) = 0\}$ n'est pas une algèbre, mais une sous-algèbre de Lie de $gl(V)$. □

Exercice 28 *(Classification des algèbres de Lie de basse dimension)*

Classifier les algèbres de Lie de dimension 1, 2 et 3. Dans chaque cas, exhiber un plongement dans un certain $\mathfrak{gl}(N)$.

▷ **Éléments de réponse.**

Toute algèbre de Lie sur k de dimension 1 est isomorphe à k. Puisque tous les éléments y sont colinéaires, il n'y a qu'un seul crochet, le crochet nul. On a alors $\mathfrak{g} = k \hookrightarrow \mathfrak{gl}(k^1)$.

En dimension 2, écrivons $\mathfrak{g} = Kx \oplus Ky$ et calculons $[x,y]$. S'il est nul, $\mathfrak{g} \sim k \oplus k$ et le crochet est nul. Si $[x,y] = z$, on peut supposer $x = z$ quitte à changer la base. On a alors $\mathfrak{g} \hookrightarrow \mathfrak{gl}(2)$ en identifiant $\mathfrak{g} = \{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}, a,b \in k\}$.

Le cas $n = 3$ est plus complexe.

Exercice 29 *(Quelques identités en basse dimension)*

Montrer que $A_1 = B_1 = C_1$, que $B_2 = C_2$ et $D_3 = A_3$.

Classification des algèbres de Lie de dimension finie

On peut démontrer que les algèbres de Lie simples de dimension finie sur $\mathbb{C}$ sont isomorphes à l'un des A_n,B_n,C_n,D_n, dites algèbres de Lie *classiques*, ou à certaines *algèbres exceptionnelles*, en nombre fini, notées : E_6,E_7,E_8,F_4,G_2.

6.1.1.7 Notion de représentation adjointe (un peu tôt)

Soit $\mathfrak{g}$ une algèbre de Lie, V un espace vectoriel. Alors $\mathrm{End}(V)$ est une algèbre de Lie (noté ainsi, on parle toujours d'endomorphismes d'espace vectoriel).

Définition. ***(Représentation d'une algèbre de Lie)***

Une *représentation* de $\mathfrak{g}$ dans V est un morphisme d'algèbres de Lie $\mathfrak{g} \xrightarrow{\rho} \mathrm{End}(V)$.

VOC On dit que V est une représentation de $\mathfrak{g}$.

Définition. ***(Représentation adjointe)***

On prend ici $V = \mathfrak{g}$. On définit $\rho_{\mathfrak{g}} = \mathrm{ad}_{\mathfrak{g}} : \mathfrak{g} \to \mathrm{End}(\mathfrak{g})$ par $x \longmapsto [x, \ \cdot\ ] : y \mapsto [x,y]$.

Lemme. ***(Nom de la « représentation » adjointe)***

Soit $\mathfrak{g}$ une algèbre de Lie. Alors $\mathrm{ad}_{\mathfrak{g}}$ est une représentation de $\mathfrak{g}$.

▷ Soient $x,y \in \mathfrak{g}$. Alors $\mathrm{ad}([x,y]) = [\mathrm{ad}(x),\mathrm{ad}(y)] = \mathrm{ad}(x) \circ \mathrm{ad}(y) - \mathrm{ad}(y) \circ \mathrm{ad}(x)$. Soit $z \in \mathfrak{g}$. On a bien $\mathrm{ad}([x,y])(z) = [[x,y],z] = [x,[y,z]] - [y,[x,z]] = [\mathrm{ad}(x),\mathrm{ad}(y)](z)$ en utilisant l'identité de Jacobi. ■

6.1.1.8 Dérivations de Lie

Définition. ***(Dérivation (de Lie))***

Soit $\mathfrak{g}$ une algèbre de Lie et $D \in \mathrm{End}(\mathfrak{g})$. On dit que D est une *dérivation* si $D([x,y]) = [D(x),y] + [x,D(y)]$.
On note $\mathrm{Der}(\mathfrak{g})$ l'ensemble des dérivations de $\mathfrak{g}$.

D'après la définition, une dérivation n'a aucune raison d'être un morphisme de Lie.

Exemples. ***(Dérivations)***

1. Soit $x \in \mathfrak{g}$. Alors $\mathrm{ad}(x) \in \mathrm{End}(\mathfrak{g})$ est une dérivation de $\mathfrak{g}$ car $[x,[y,z]] = \mathrm{ad}(x)([y,z]) = [\mathrm{ad}(x)(y),z] + [y,\mathrm{ad}(x)(z)] = [[x,y],z] + [y,[x,z]]$.

Remarque. On note aussi $\mathrm{ad} : \mathfrak{g} \to \mathrm{Der}(\mathfrak{g}) \subseteq \mathrm{End}(\mathfrak{g})$. Alors $\mathrm{ad}(\mathfrak{g})$ est l'ensemble des *dérivations intérieures* de $\mathfrak{g}$. Les autres sont les *dérivations extérieures* de $\mathfrak{g}$.

Fait

$\mathrm{ad} : \mathfrak{g} \to \mathrm{End}(\mathfrak{g})$ est un morphisme d'algèbres de Lie qui commute aux dérivations :

$$\mathrm{ad}(D(x)) = [D,\mathrm{ad}(x)] \qquad \forall x \in \mathfrak{g}, \forall D \in \mathrm{ad}(\mathfrak{g})$$

et

$$\mathrm{ad}(D(x)) = [D,\mathrm{ad}(x)] \qquad \forall x \in \mathfrak{g}, \forall D \in \mathrm{Der}(\mathfrak{g}).$$

Exercice 30 *(Commutateur de dérivations)*

Montrer que le commutateur de deux dérivations est encore une dérivation.

6.1.1.9 Idéaux de Lie

Définition. ***(Idéal de Lie)***

Soit $\mathfrak{g}$ une algèbre de Lie, $\mathfrak{h}$ un sous-espace vectoriel de $\mathfrak{g}$. On dit que $\mathfrak{h}$ est un *idéal* de $\mathfrak{g}$ si $\mathrm{ad}(x)(\mathfrak{h}) \subseteq \mathfrak{h}$. On note $\mathfrak{h} \triangleleft \mathfrak{g}$.

Définition-propriété. ***(Idéal caractéristique d'une algèbre de Lie)***

Un *idéal caractéristique* d'une algèbre de Lie $\mathfrak{g}$ est un idéal $\mathfrak{h}$ tel que pour tout $D \in \mathrm{Der}(\mathfrak{g})$, $D(\mathfrak{h}) \subseteq \mathfrak{h}$.

Fait. ***(Les idéaux sont des sous-algèbres de Lie)***

Soit $\mathfrak{g}$ une algèbre de Lie. Tout idéal de $\mathfrak{g}$ est une sous-algèbre de Lie de $\mathfrak{g}$.

Exemples. ***(Idéaux de Lie)***

1. Soit G un groupe de Lie et $\mathfrak{g}$ son algèbre de Lie. Soit H un sous-groupe de Lie, c'est-à-dire un sous-groupe qui soit une sous-variété différentielle, et soit $\mathfrak{h}$ l'algèbre de Lie associée. Alors $\mathfrak{h} \subseteq \mathfrak{g}$ est une sous-algèbre de Lie, et si $H \triangleleft G$, alors $\mathfrak{h}$ est un idéal de $\mathfrak{g}$.
2. Un autre exemple typique issu des groupes de Lie. On prend $G = SL_n(k)$ et $\mathfrak{g} = sl(n)$ l'ensemble des matrices $n \times n$ de trace nulle. Alors $H = SO_n(k) = \{A \mid {}^tAA = I_n\}$ le groupe spécial orthogonal est un sous-groupe de Lie de $\mathfrak{g}$. De plus, $\mathfrak{h} = so(n,\sigma) = \{A \in \mathrm{End}(\sigma^n) \mid {}^t(A) + A = 0\}$ est une sous-algèbre de Lie de $\mathfrak{g}$, mais $\mathfrak{h}$ n'est pas un idéal de $\mathfrak{g}$.

Propriétés

Soit $\mathfrak{g}$ une algèbre de Lie.

1. Si $\mathfrak{a},\mathfrak{b} \triangleleft \mathfrak{g}$ (respectivement caractéristiques), alors $[\mathfrak{a},\mathfrak{b}] \subseteq \mathfrak{g}$ est un idéal (respectivement caractéristique).
2. Si $\mathfrak{a} \triangleleft \mathfrak{g}$, alors $\mathfrak{g}/\mathfrak{a}$ est une algèbre de Lie et $0 \longrightarrow \mathfrak{h} \longrightarrow \mathfrak{g} \longrightarrow \mathfrak{g}/\mathfrak{h} \longrightarrow 0$ est une suite exacte d'algèbres de Lie.

▷ Successivement :

1. Si $D \in \mathrm{ad}(g)$ ou $\mathrm{Der}(g)$, $x \in \mathfrak{a}$, $y \in \mathfrak{b}$, montrons que $D([x,y]) \in [\mathfrak{a},\mathfrak{b}]$. Or $D([x,y]) = [D(x),y] + [x,D'y)$ qui est bien dans $[\mathfrak{a},\mathfrak{b}]$.
2. En exercice. ■

Lemme. ***(Tour d'idéaux (caractéristiques) de Lie)***

Soit $\mathfrak{g}$ une algèbre de Lie. Si $\mathfrak{a} \triangleleft \mathfrak{g}$ (respectivement caractéristique) et $\mathfrak{b} \triangleleft \mathfrak{a}$ est **caractéristique**, alors $\mathfrak{b} \triangleleft \mathfrak{g}$ (respectivement caractéristique).

▷ Soit $D \in ad(\mathfrak{g})$, respectivement $D \in \mathrm{Der}(\mathfrak{g})$. Par hypothèse, $D(\mathfrak{a}) \subseteq \mathfrak{a}$, d'où $D \in \mathrm{Der}(\mathfrak{a})$. Ainsi $D(\mathfrak{b}) \subseteq \mathfrak{b}$, car $\mathfrak{b} \triangleleft_{\mathrm{car}} \mathfrak{a}$. respectivement, $\mathfrak{b} \triangleleft_{\mathrm{car}} \mathfrak{a} \triangleleft_{\mathrm{car}} \mathfrak{g}$ d'où le résultat... ■

6.1.1.10 Algèbres de Lie abéliennes

Définition. ***(Algèbre de Lie abélienne)***

On dit qu'une algèbre de Lie $\mathfrak{g}$ est *abélienne* si $\mathfrak{g}^{\mathrm{op}} = G$.

Propriété. ***(Caractérisation de l'abélianité par le crochet)***

Une algèbre de Lie $(\mathfrak{g},[\,\cdot\,,\,\cdot\,])$ est abélienne, si et seulement si, son crochet est nul, *i.e.* pour tous $x,y \in \mathfrak{g}$, $[x,y] = 0$.

6.1.1.11 Séries dérivées, centrales

On introduit une notion semblable à celle des groupes qui permet d'énoncer des propriétés de dévissage sur les algèbres de Lie.

Définition-propriété. ***(Algèbre de Lie dérivée)***

Pour toute algèbre de Lie $\mathfrak{g}$, $[\mathfrak{g},\mathfrak{g}] \triangleleft \mathfrak{g}$ est un idéal caractéristique de $\mathfrak{g}$, appelé *algèbre de Lie dérivée* de $\mathfrak{g}$. On note $D(\mathfrak{g}) = [\mathfrak{g},\mathfrak{g}]$.

Propriété. ***(Abélianisée d'une algèbre de Lie)***

Pour toute algèbre de Lie $\mathfrak{g}$, $\mathfrak{g}/D(\mathfrak{g}) = \mathfrak{g}/[\mathfrak{g},\mathfrak{g}]$ est une algèbre de Lie abélienne.

Exemples. ***(Algèbres de Lie dérivées)***

1. $D(gl(V)) = sl(V)$.
2. S'amuser à en calculer d'autres soi-même !

Définition. ***(Série dérivée d'une algèbre de Lie)***

On appelle *série dérivée* d'une algèbre de Lie $\mathfrak{g}$ la suite décroissante d'algèbre de Lie donnée par $D^0(\mathfrak{g}) = \mathfrak{g}$ et pour tout $i \in \mathbb{N}$, $D^{i+1}(\mathfrak{g}) = [D^i(\mathfrak{g}),D^i(\mathfrak{g})] = D(D^i(\mathfrak{g})) \subseteq D^i(\mathfrak{g})$.

Définition. ***(Série centrale d'une algèbre de Lie)***

ON appelle *série centrale descendante* d'une algèbre de LIe $\mathfrak{g}$ la suite décroissante d'algèbres de Lie donnée par $C^0(\mathfrak{g}) = \mathfrak{g}$ et pour tout $i \in \mathbb{N}$, $C^{i+1}(\mathfrak{g}) = [\mathfrak{g},C^i(\mathfrak{g})]$.

Propriété. ***(Caractéristicité des séries dérivées d'algèbre de Lie)***

Soit $\mathfrak{g}$ une algèbre de Lie. Pour tout $i \in \mathbb{N}$, $D^i(\mathfrak{g}) \triangleleft \mathfrak{g}$ est un idéal caractéristique de $\mathfrak{g}$.

Propriété. ***(Caractéristicité des séries centrales d'algèbre de Lie)***

Soit $\mathfrak{g}$ une algèbre de Lie. Pour tout $i \in \mathbb{N}$, $C^i(\mathfrak{g}) \triangleleft \mathfrak{g}$ est un idéal caractéristique de $\mathfrak{g}$.

Propriété. ***(Morphisme de Lie et série dérivée)***

Soient $\mathfrak{g},\mathfrak{h}$ deux algèbres de Lie. Soit $f \in \mathrm{Hom}_{\mathrm{Lie}}(\mathfrak{g},\mathfrak{h})$. Alors $f(D^i(\mathfrak{g})) \subseteq D^i(\mathfrak{h})$ pour tout $i \in \mathbb{N}$.

Propriété. ***(Morphisme de Lie et série centrale)***

Soient $\mathfrak{g}$,$\mathfrak{h}$ deux algèbres de Lie. Soit $f \in \mathrm{Hom}_{\mathrm{Lie}}(\mathfrak{g},\mathfrak{h})$. Alors $f(C^i(\mathfrak{g})) \subseteq C^i(\mathfrak{h})$ pour tout $i \in \mathbb{N}$.

▷ Par récurrence. ■

6.1.1.12 Normalisateurs, centralisateurs dans une algèbre de Lie

Définition. ***(Centralisateur de Lie)***

Soit $\mathfrak{g}$ une algèrbe de Lie, V un sous-espace vectoriel de $\mathfrak{g}$. On note $z_{\mathfrak{g}}(V)$ le *centralisateur* de V dans $\mathfrak{g}$ donné par $\{x \in \mathfrak{g} \mid [x,y] = 0 \qquad \forall y \in \mathfrak{g}\}$.

Définition. ***(Normalisateur de Lie)***

Soit $\mathfrak{g}$ une algèrbe de Lie, V un sous-espace vectoriel de $\mathfrak{g}$. On note $n_{\mathfrak{g}}(V)$ le *normalisateur* de V dans $\mathfrak{g}$ donné par $\{x \in \mathfrak{g} \mid [x,y] \in V \qquad \forall y \in \mathfrak{g}\}$.

Propriété. ***(Structure d'algèbre du centralisateur de Lie)***

Soit $\mathfrak{g}$ une algèbre de Lie, V un sev de $\mathfrak{g}$. Alors $z_{\mathfrak{g}}(V)$ est une sous-algèbre de Lie de $\mathfrak{g}$.

▷ Soient $x,y \in z_{\mathfrak{g}}(V)$ et $z \in V$. L'identité de Jacobi fournit bien $[[x,y],z] = 0$. ■

Propriété. ***(Structure d'idéal du centralisateur de Lie)***

Soit $\mathfrak{g}$ une algèbre de Lie, V un sev de $\mathfrak{g}$. Alors si $V \lhd \mathfrak{g}$ (respectivement caractéristique), on a $z_{\mathfrak{g}}(V) \lhd \mathfrak{g}$ (respectivement caractéristique).

▷ Soient $x \in z_{\mathfrak{g}}(V)$ et $y \in \mathfrak{g}$. Montrons que $[x,y] \in z_{\mathfrak{g}}(V)$. Soit $z \in \mathbb{V}$. Montrons que $[[x,y],z] = 0$. C'est le cas : on le voit en développant ce crochet par l'identité de Jacobi et en observant deux termes nuls. ■

Propriété. ***(Structure d'idéal du normalisateur de Lie)***

Soit $\mathfrak{g}$ une algèbre de Lie, V un sev de $\mathfrak{g}$. Alors si $V \lhd \mathfrak{g}$, on a $n_{\mathfrak{g}}(V) \lhd \mathfrak{g}$.

▷ Soient $x \in n_{\mathfrak{g}}(V)$, $y \in \mathfrak{g}$ et $z \in V$. À compléter. ■

Exemple fondamental. ***(Centre de Lie)***

Soit $\mathfrak{g}$ une algèbre de Lie. Le *centre* de $\mathfrak{g}$ est $z_{\mathfrak{g}}(\mathfrak{g})$, on le note $z(\mathfrak{g})$. Le centre est toujours caractéristique. De plus, on peut le voir $z(\mathfrak{g}) = \{x \in \mathfrak{g} \mid [x,y] = 0 \qquad \forall y \in \mathfrak{g}\} = \mathrm{Ker}(\mathrm{ad})$.

Exercice 31

Montrer que $z(\mathfrak{gl}(n)) = \mathfrak{s}(n)$.

▷ **Éléments de réponse.**

Une fois la traduction faite... C'est un simple exercice d'algèbre linéaire de bébé ! Attention toutefois à distinguer le cas où $\mathrm{car}(k) = n$.

Exercice 32

Soit $\mathfrak{g}$ une algèbre de Lie de dimension finie avec $z(\mathfrak{g})$ de codimension 1. Montrer que $\mathfrak{g}$ est abélienne.

▷ **Éléments de réponse.**

Copier la preuve pour les groupes de $G/Z(G)$ monogène $\implies$ G abélien.

Exercice 33 *(Des séries dérivées triviales)*

Montrer que, pour $\mathfrak{g} = A_n$, B_n, C_n ou D_n, si $\mathrm{car}(k) = 0$, alors $[\mathfrak{g},\mathfrak{g}] = \mathfrak{g}$.

Exercice 34 *(Dérivée de $\mathfrak{gl}(n)$)*

Montrer que, si $\mathrm{car}(k) \nmid n$, alors $[\mathfrak{gl}(n),\mathfrak{gl}(n)] = \mathfrak{sl}(n)$.

Exercice 35 *(Auto-normalisation)*

On dit qu'une sous-algèbre de Lie est *auto-normalisante* si elle est égale à son normalisateur. Montrer que $\mathcal{T}_n^+(k)$ et $D_n(k)$ sont auto-normalisants dans $\mathfrak{gl}(n)$.

6.1.1.13 Représentations fidèles d'algèbres de Lie

Définition. ***(Représentation fidèle d'une algèbre de Lie)***

Soit $\mathfrak{g}$ une algèbre de Lie. Une *représentation* V de $\mathfrak{g}$ est fidèle si $\mathfrak{g} \to \mathrm{End}(V)$ est injectif. On dit que ad est fidèle si le centre $z(\mathfrak{g}) = \{0\}$.

6.1.1.14 Extensions d'algèbres de Lie

Définition. ***(Extension d'une algèbre de Lie)***

Soient $\mathfrak{a}$,$\mathfrak{b}$ deux algèbres de Lie. Une *extension* de $\mathfrak{b}$ par $\mathfrak{a}$ est une suite exacte d'algèbres de Lie

$$0 \longrightarrow \mathfrak{a} \xrightarrow{f} \mathfrak{g} \xrightarrow{g} \mathfrak{b} \longrightarrow 0.$$

Fait

Puisque $\mathrm{Ker}(g) \triangleleft \mathfrak{g}$ et $\mathrm{Ker}(g) = \mathrm{Im}(f) \simeq \mathfrak{a}$, on a $\mathfrak{a} \triangleleft \mathfrak{g}$.

Définition. ***(Équivalence d'extensions d'algèbres de Lie)***

Soient $\mathfrak{a}$,$\mathfrak{b}$ deux algèbres de Lie. Deux extensions de $\mathfrak{b}$ par $\mathfrak{a}$:

$$0 \longrightarrow \mathfrak{a} \longrightarrow \mathfrak{g} \longrightarrow \mathfrak{b} \longrightarrow 0$$

et

$$0 \longrightarrow \mathfrak{a} \longrightarrow \mathfrak{g}' \longrightarrow \mathfrak{b} \longrightarrow 0$$

sont *équivalentes* ou *isomorphes* si l'on a un diagramme commutatif

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathfrak{a} & \longrightarrow & \mathcal{G} & \longrightarrow & \mathfrak{b} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle id} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle id} & & \\ 0 & \longrightarrow & \mathfrak{a} & \longrightarrow & \mathcal{G}' & \longrightarrow & \mathfrak{b} & \longrightarrow & 0 \end{array}$$

avec $f \in \mathrm{Hom}_{\mathrm{Lie}}(\mathfrak{g},\mathfrak{g}')$, soit deux triangles à vérifier.

Fait

Toute équivalence d'extensions d'algèbre de Lie est un isomorphisme de Lie, *i.e.* $f \in \mathrm{Isom}_{\mathrm{Lie}}(\mathfrak{g},\mathfrak{g}')$.

Fait

L'équivalence d'extensions d'algèbre de Lie est une relation d'équivalence.
L'ensemble de ses classes d'équivalence est noté $\mathrm{Ext}^1_{\mathrm{Lie}}(\mathfrak{a},\mathfrak{b})$.

Définition. ***(Extension scindée d'algèbres de Lie)***

Soient $\mathfrak{a}$,$\mathfrak{b}$ deux algèbres de Lie. L'extension $0 \longrightarrow \mathfrak{a} \xrightarrow{\alpha} \mathfrak{g} \xrightarrow{\beta} \mathfrak{b} \longrightarrow 0$ est scindée si elle est équivalente à $0 \longrightarrow \mathfrak{a} \longrightarrow \mathfrak{a} \oplus \mathfrak{b} \longrightarrow \mathfrak{b} \longrightarrow 0$ donnée par $x \mapsto (x,y)$, $(x,y) \mapsto y$ et $(0,y \hookleftarrow y$.

Remarque. Si $\mathfrak{a}$,$\mathfrak{b}$ sont deux algèbres de Lie, $\mathfrak{a}\oplus\mathfrak{b} = \mathfrak{a}\times\mathfrak{b}$ avec le crochet de Lie $[(x,y),(z,t)] = ([x,z],[y,t])$ avec $x,z \in \mathfrak{a}$ et $y,t \in \mathfrak{b}$. C'est bien une algèbre de Lie.

Propriété

$0 \longrightarrow \mathfrak{a} \xrightarrow{\alpha} \mathfrak{g} \xrightarrow{\beta} \mathfrak{b} \longrightarrow 0$ est scindée si et seulement s'il existe $s \in \mathrm{Hom}_{\mathrm{Lie}}(\mathfrak{b},\mathfrak{g})$ telle que $\beta \circ s = id_{\mathfrak{b}}$ $s(\mathfrak{b}) \lhd \mathfrak{g}$.

Définition. ***(Extension $\frac{1}{2}$-scindée d'algèbres de Lie)***

L'extension $0 \longrightarrow \mathfrak{a} \xrightarrow{\alpha} \mathfrak{g} \xrightarrow{\beta} \mathfrak{b} \longrightarrow 0$ est *$\frac{1}{2}$-scindée* s'il existe s section de β telle que $s(\mathfrak{b})$ soit une sous-algèbre de Lie de $\mathfrak{g}$, *i.e.* $s \in \mathrm{Hom}_{\mathrm{Lie}}(\mathfrak{b},\mathfrak{g})$ tel que $\beta \circ s = id_{\mathfrak{g}}$.

Propriété

$0 \longrightarrow \mathfrak{a} \xrightarrow{\alpha} \mathfrak{g} \xrightarrow{\beta} \mathfrak{b} \longrightarrow 0$ est $\frac{1}{2}$-scindée si et seulement s'il existe une décomposition $\mathfrak{g} = \alpha(\mathfrak{a}) \oplus \mathfrak{c}$ avec $\mathfrak{c}$ une sous-algèbre de Lie.

Définition. ***(Extension centrale d'algèbres de LIe)***

L'extension $0 \longrightarrow \mathfrak{a} \xrightarrow{\alpha} \mathfrak{g} \xrightarrow{\beta} \mathfrak{b} \longrightarrow 0$ est *centrale* si $\alpha(\mathfrak{a}) \subseteq z(\mathfrak{g})$ le centre de $\mathfrak{g}$.

Fait. ***(Extensions centrales $\frac{1}{2}$-scindées)***

Une extension $\frac{1}{2}$-scindée qui est centrale est nécessairement triviale.

6.1.1.15 Produits semi-directs d'algèbres de Lie

Lemme

Les extensions $\frac{1}{2}$-scindées de $\mathfrak{b}$ par $\mathfrak{a}$ sont exactement les produits semi-directs $\mathfrak{a} \rtimes \mathfrak{b} = \mathfrak{g}$.

▷ Montrons le sens direct. Soit $0 \longrightarrow \mathfrak{a} \xrightarrow{f} \mathfrak{g} \xrightarrow{g} \mathfrak{b} \longrightarrow 0$ une extension $\frac{1}{2}$-scindée par la section s de β, soit $\mathfrak{g} = \alpha(\mathfrak{a}) \oplus \mathfrak{c}$ où $\mathfrak{c} = s(\mathfrak{b}) \subseteq \mathfrak{g}$ est une sous-algèbre de Lie. On a $\alpha(\mathfrak{a}) = \mathrm{Ker}(\beta) \lhd \mathfrak{g}$. Alors s fournit un isomorphisme d'espace vectoriel $\mathfrak{g} = \mathfrak{a} \times \mathfrak{b}$. Soient $(a,b),(a',b') \in \mathfrak{g} \simeq \mathfrak{a} \times \mathfrak{b}$. Notons $[(a,b),(a',b')] = (a'',b'')$ où $b = \beta(a,b)$, $b' = \beta(a',b')$. Puisque $\beta \in \mathrm{Hom}_{\mathrm{Lie}}(\mathfrak{g},\mathfrak{b})$, $b'' = [b,b']$. De plus, $a'' = [a,a"] + ([b,a'] - [b',a]) = [a,a'] + \mathrm{ad}(s(b))(a') - \mathrm{ad}(s(b'))(a) = [a,a'] + f(b)(a') + f(b')(a)$: on retrouve le produit semi-direct avec $f : \begin{array}{ccc} \mathfrak{b} & \longrightarrow & \mathrm{Der}(\mathfrak{a}). \\ b & \longmapsto & \mathrm{ad}(s(b)) \end{array}$ D'autre part, l'identité de Jacobi dans $\mathfrak{g}$ donne que l'application f est un morphisme d'algèbre de Lie. ■

Définition-propriété. ***(Produit semi-direct d'algèbres de Lie)***

Le *produit semi-direct* d'algèbres de Lie $\mathfrak{g} = \mathfrak{a} \rtimes \mathfrak{b}$ est l'espace vectoriel $\mathfrak{g} = \mathfrak{a} \oplus \mathfrak{b}$ muni du crochet $[(a,b),(a',b')] = ([a,a'] + f(b)(a') - f(b')(a),[b,b'])$ où $f \in \mathrm{Hom}_{\mathrm{Lie}}(b,\mathrm{Der}(\mathfrak{a}))$.

Remarque. $\mathrm{Der}(\mathfrak{a}) = \{f \in \mathrm{End}_K(\mathfrak{a}) \mid f([x,y]) = [f(x),y] + [x,f(y)] \qquad \forall x,y \in \mathfrak{a}\}$, $\mathrm{End}_K(\mathfrak{a})$ est une algèbre de Lie pour le commutateur et $\mathrm{Der}(\mathfrak{a})$ est une sous-algèbre de Lie de $\mathrm{End}_K(\mathfrak{a})$.

6.1.1.16 Algèbres enveloppantes

Une algèbre enveloppante (universelle) est une façon fonctorielle d'associer une algèbre associative à une algèbre de Lie.

Définition. ***(α-fonction)***

Soit $\mathfrak{g}$ une k-algèbre de Lie et A une algèbre associative (non nécessairement unitaire) sur k. Une application $f \in \mathrm{Hom}_K(\mathfrak{g},A)$ est une *α-fonction* si $f([x,y]) = [f(x),f(y)]$ pour tous $x,y \in \mathfrak{g}$.
De façon équivalente, si $A_{\mathrm{Lie}} = (A,[\ \cdot\ ,\ \cdot\ ])$: A muni du commutateur, il existe un foncteur de la catégorie des algèbres associatives vers la catégorie des algèbres de Lie.

Remarque. Une α-fonction est un morphisme d'algèbres de Lie $\mathfrak{g} \to A_{\mathrm{Lie}}$.

Définition. ***(Algèbre tensorielle d'une algèbre de Lie)***

Soit $\mathfrak{g}$ une algèbre de Lie. L'*algèbre tensorielle* de $\mathfrak{g}$, notée $T(\mathfrak{g})$ est son algèbre tensorielle en tant qu'espace vectoriel, autrement dit $T(\mathfrak{g}) = \bigoplus_{n \geqslant 0} \underbrace{\mathfrak{g} \otimes_k \mathfrak{g} \otimes_k \mathfrak{g} \otimes_k \ldots \otimes_k \mathfrak{g}}_{n \text{ copies de } \mathfrak{g}}$. Notons que si $m,n \in T(\mathfrak{g})$, $m \cdot n = m \otimes n \in T(\mathfrak{g})$.

Définition-propriété. ***(Algèbre enveloppante)***

On note $J(\mathfrak{g})$ l'idéal bilatère engendré par $\{x \otimes y - y \otimes x - [x,y], x,y \in \mathfrak{g}\} \mathrel{\widehat{=}} \mathfrak{g} \otimes \mathfrak{g} - \mathfrak{g}$. Alors $U(\mathfrak{g}) = T(\mathfrak{g})/J(\mathfrak{g})$ est une algèbre associative unitaire[a] sur k dite *algèbre enveloppante (universelle)* de $\mathfrak{g}$. L'application canonique $f_{\mathfrak{g}} : \mathfrak{g} \hookrightarrow T(\mathfrak{g}) \twoheadrightarrow U(\mathfrak{g})$ est une α-fonction.

[a] $1_{U(\mathfrak{g})} = f_{\mathfrak{g}}(1_{T(\mathfrak{g})})$.

▷ En effet $[f_{\mathfrak{g}}(x),f_{\mathfrak{g}}(y)]_{U(\mathfrak{g})} = x \otimes y - y \otimes x = [x,y] = f_{\mathfrak{g}}([x,y])$ pour tous $x,y \in \mathfrak{g}$. ■

Propriété. ***(Propriété universelle de $U(\mathfrak{g})$)***

Soit A une algèbre associative sur K et $f : \mathfrak{g} \to A$ une α-fonction. Alors il existe un unique $g \in \mathrm{Hom}_{\mathrm{Ass}}(U(\mathfrak{g}),A)$ qui fait commuter le diagramme :

$$\begin{array}{ccc} \mathcal{G} & \xrightarrow{f} & A \\ & \searrow^{fg} & \uparrow g \\ & & U(\mathcal{G}). \end{array}$$

De façon équivalente,

$$\begin{aligned} \mathrm{Hom}_{\mathrm{Lie}}(\mathfrak{g},A_{\mathrm{Lie}}) &\xrightarrow{\sim} \mathrm{Hom}_{1\text{-}\mathrm{Ass}}(U(\mathfrak{g}),A) \\ f &\mapsto g \\ f \circ f_{\mathfrak{g}} &\hookleftarrow g. \end{aligned}$$

▷ On rappelle $T(\mathfrak{g}) = k \oplus \bigoplus_{n\geqslant 1} \mathfrak{g}^{\otimes n}$. Soit $g' \in \mathrm{Hom}_{1\text{-}\mathrm{Ass}}(T(\mathfrak{g}),A)$ l'unique fonction telle que $g'(x) = f(x)$ pour tout $x \in \mathfrak{g} \hookrightarrow T(\mathfrak{g})$. Plus précisément, pour $m = \sum_{k=1}^{d} m_k$ avec $m_k = x_1^{(k)} \otimes x_2^{(k)} \otimes ... \otimes x_k^{(k)} \in \mathfrak{g}^{\otimes(k)}$. On a $g'(m) = \sum_{k=1}^{d} f(x_1^{(k)}.f(x_2^{(k)})...f(x_k^{(k)})$. On a $f : \mathfrak{g} \to A$.

$$\begin{array}{ccc} T(\mathcal{G}) & \xrightarrow{g'} & A \\ \downarrow & \nearrow_{g} & \\ U(\mathcal{G}) & & \end{array}$$

Puisque f est une α-fonction, $g'(x \otimes y - y \otimes x - [x,y]) = 0$, soit $g'(J(\mathfrak{g})) = 0$. ■

Fait. ***(Fonctorialité de l'algèbre enveloppante)***

L'application $\mathfrak{g} \mapsto U(\mathfrak{g})$ des algèbres de Lie vers les algèbres associatives unitaires est fonctorielle.

En effet, si $\varphi \in \mathrm{Hom}_{\mathrm{Lie}}(\mathfrak{g},\mathfrak{g}')$, alors il existe un unique $U(\varphi) \in \mathrm{Hom}_{1\text{-}\mathrm{Ass}}(U(\mathfrak{g}),U(\mathbb{G}'))$ tel que le diagramme suivant commute.

$$\begin{array}{ccc} \mathcal{G} & \xrightarrow{\varphi} & \mathcal{G}' \\ {\scriptstyle fg}\downarrow & & \downarrow{\scriptstyle fg'} \\ U(\mathcal{G}) & \xrightarrow{U(\varphi)} & U(\mathcal{G}'). \end{array}$$

La catégorie des algèbres de Lie est munie de $\oplus$, et la catégorie des algèbres associatives est munie de $\otimes_k$, *i.e.*, à A,B on associe $A \otimes_k B$ avec $(a \otimes b) \cdot (a' \otimes b') = (aa') \otimes (bb')$ $((a \otimes 1) \cdot (1 \otimes b) = a \otimes b)$.

Proposition. ***(Algèbre enveloppante d'une somme d'algèbres de Lie)***

Soient $\mathfrak{g}$,$\mathfrak{h}$ deux algèbres de Lie. Alors $U(\mathfrak{g} \oplus \mathfrak{h}) = U(\mathfrak{g}) \otimes U(\mathfrak{h})$.

▷ On souhaite écrire une application $U(\mathfrak{g}) \otimes U(\mathfrak{h}) \to U(\mathfrak{g} \oplus \mathfrak{h})$. Il existe une application $\tilde{i} : U(\mathfrak{g}) \xrightarrow{\sim} U(\mathfrak{g} \oplus \mathfrak{h})$ donnée par la propriété de fonctorialité donnée par le morphisme d'algèbre de Lie $\begin{array}{ccc} \mathfrak{g} & \longrightarrow & \mathfrak{g} \oplus \mathfrak{h} \\ x & \longmapsto & (x,0) \end{array}$. Il existe une fonction $\tilde{j} : U(\mathfrak{h}) \to U(\mathfrak{g} \oplus \mathfrak{h})$. Les images de $\tilde{i}$,$\tilde{j}$ commutent dans $U(\mathfrak{g} \oplus \mathfrak{h})$ car $[\mathfrak{g},\mathfrak{h}] = 0$ dans $\mathfrak{g} \oplus \mathfrak{h}$. L'application linéaire $\begin{array}{rccc} \varphi : & U(\mathfrak{g}) \otimes U(\mathfrak{h}) & \longrightarrow & U(\mathfrak{g} \oplus \mathfrak{h}) \\ & x \otimes y & \longmapsto & \tilde{i}(x) \cdot \tilde{j}(y) \end{array}$ est un morphisme d'algèbres.

D'une part, φ est surjective. En effet, $U(\mathfrak{g})$ est engendrée par 1 et $\mathrm{Im}(f_{\mathfrak{g}})$. Ainsi, $U(\mathfrak{g} \oplus Hj)$ est engendrée par 1 et $G \oplus \mathfrak{h}$ et tous deux appartiennent à $\mathrm{Im}(\varphi)$.

D'autre part, φ est injective. On cherche ψ tel que $\psi : (\mathfrak{g} \oplus \mathfrak{h}) \to U(\mathfrak{g}) \oplus U(\mathfrak{h})$ et $\psi \circ \varphi = id$. Or il existe des morphismes d'algèbres de Lie donné par $\begin{array}{rccc} p : & \mathfrak{g} \oplus \mathfrak{h} & \longrightarrow & \mathfrak{g} \\ & (x,y) & \longmapsto & x \end{array}$ et $\begin{array}{rccc} q : & \mathfrak{g} \oplus \mathfrak{h} & \longrightarrow & \mathfrak{h}. \\ & (x,y) & \longmapsto & y \end{array}$ On en déduit $\tilde{p} : U(\mathfrak{g} \oplus \mathfrak{h}) \to U(\mathfrak{g})$ et $\tilde{q} : U(\mathfrak{g} \oplus \mathfrak{h}) \to U(\mathfrak{h})$. On choisit alors $\psi = \tilde{p} \oplus \tilde{q}$. ■

Propriété. ***(Algèbre enveloppante de $\mathfrak{g}^{\mathrm{op}}$)***

$U(\mathfrak{g}^{\mathrm{op}}) = U(\mathfrak{g})^{\mathrm{op}}$.

▷ La fonction $f : \mathfrak{g}^{\mathrm{op}} \to U(\mathfrak{g})^{\mathrm{op}}$, $x \mapsto f_{\mathfrak{g}}(x) = x$ est une α-fonction. Ainsi, il existe un morphisme d'algèbres associatives $U(\mathfrak{g}^{\mathrm{op}}) \to U(\mathfrak{g})^{\mathrm{op}}$ surjectif and injectif. Notons bien que pour une algèbre A, $A^{\mathrm{op}} = A$ en tant que k-espace vectoriel avec $(x \cdot y)_{A^{\mathrm{op}}} = (y \cdot x)_A$ pour tous $x,y \in A$. ■

6.1.2 Représentation des algèbres de Lie

La théorie des représentations des algèbres de Lie inclut en quelque sorte celle des représentations de groupe. En effet, à tout groupe de Lie, groupe algébrique, on associe une algèbre de Lie par $G \mapsto \mathfrak{g} = T_1 G$.

Définition. ***(Représentation d'une algèbre de Lie)***

Une *représentation* d'une algèbre de Lie $\mathfrak{g}$ sur k dans un espace vectoriel V est un morphisme d'algèbres de Lie $\mathfrak{g} \to gl(V)$.

Remarques.

1. Si $f : G \to GL(V)$ est une représetation d'un groupe de Lie, alors $d_1 f : \mathfrak{g} \to gl(V)$ est une représentation de $\mathfrak{g}$.
2. $\mathrm{ad} : \mathfrak{g} \to \mathfrak{gl}(\mathfrak{g}), x \mapsto \mathrm{ad}(x) = [x, \ \cdot \ ]$ est la représentation adjointe de $\mathfrak{g}$ sur elle-même.

3. Une représentation de $\mathfrak{g}$ sur V est la même chose qu'une application linéaire $\rho : \mathfrak{g} \to \mathrm{End}(V)$ tel que $\rho([x,y]) = \underbrace{[\rho(x),\rho(y)]}_{\rho(x)\circ\rho(y)-\rho(y)\circ\rho(x)}$ pour tous $x,y \in \mathfrak{g}$.
4. L'application $\rho : \mathfrak{g} \to \mathrm{End}(V)$ est une α-fonction où $\mathrm{End}(V)$ est vue comme une algèbre associative. Cette application fournit un morphisme d'algèbres $U(\rho) : U(\mathfrak{g}) \to \mathrm{End}(V)$, et donc, $U(\rho)$ est une représentation de $U(\mathfrak{g})$ dans V. Cette remarque implique le fait suivant.

Fait

L'ensemble des représentations de $\mathfrak{g}$ sur V est l'ensemble des représentations de $U(\mathfrak{g})$ sur V.

Définition. ***(Sous-représentation d'une algèbre de Lie)***

Une *sous-représentation* d'une représentation algèbre de Lie $\mathfrak{g}$ sur V est $W \subseteq V$ tel que pour tous $x \in \mathfrak{g}, w \in W$, on a $x \cdot w \in W$ en notation $\cdot$ l'action de $x \in \mathfrak{g}$ sur $w \in V$

Définition. ***(Représentation simple d'une algèbre de Lie)***

Une représentation d'une algèbre de Lie $\mathfrak{g}$ sur V est *simple* ou *irréductible* si $V \neq \{0\}$ et pour toute sous-représentation W, on a soit $W = \{0\}$ ou W.

Propriété. ***(Réductibilité des représentations d'algèbre de Lie)***

Une représentation V d'une algèbre de Lie $\mathfrak{g}$ est réductible si et seulement s'il existe $V_1,V_2 \subseteq V$ des sous-représentations telles que $V = V_1 \oplus V_2$ et $V_1,V_2 \neq \{0\}$.

Définition. ***(Représentation semi-simple d'une algèbre de Lie)***

Une représentation d'une algèbre de Lie est *semi-simple* ou *complètement réductible* si c'est la somme directe de représentations simples d'algèbre de Lie.

Définition-propriété. ***(Représentation quotient)***

Si $W \subseteq V$ est une sous-représentation d'une algèbre de Lie $\mathfrak{g}$, alors il existe une représentation de $\mathfrak{g}$ sur V/W appelée *représentation quotient*.

Remarques.

1. Si $\rho : \mathfrak{g} \to gl(V)$ une représentation, on note $\rho(x) = x_V$ pour tout $x \in \mathfrak{g}$.
2. Soit $\rho : \mathfrak{g} \to gl(V)$ une représentation et $v \in V$. On note $\mathfrak{g}_V = \{x \in \mathfrak{g} \mid x \cdot v := \rho(x)(v) = 0\}$ le *stabilisateur* de v dans $\mathfrak{g}$. Alors $\mathfrak{g}_V$ est une sous-algèbre de Lie de $\mathfrak{g}$. Pour la représentation adjointe, on retrouve le centralisateur.

Définition. ***(Morphisme de représentations d'algèbres de Lie)***

Soient V,W deux représentations de l'algèbre de Lie $\mathfrak{g}$. Un *morphisme de représentations de* $\mathfrak{g}$ est une application linéaire de V dans W telle que $f(xv) = xf(v)$ pour tout $x \in \mathfrak{g}$, pour tout $v \in V$.

Fait. ***(Catégorie des représentations d'une algèbre de Lie)***

Grâce aux notions de sous-représentations, de représentations quotients et de morphismes de représentations, on peut définir la catégorie $\mathrm{Rep}(\mathfrak{g})$ des représentations de $\mathfrak{g}$ qui est une catégorie abélienne.

Définition. ***(Somme directe de représentations d'une algèbre de Lie)***

Il existe évidemment un foncteur *somme directe de représentations* $\oplus$ de $\mathrm{Rep}(\mathfrak{g}) \times \mathrm{Rep}(\mathfrak{g}) \to \mathrm{Rep}(\mathfrak{g})$ donné par $(V,W) \mapsto V \oplus W$ la somme directe d'espaces vectoriels, de sorte que $\mathfrak{g} \mapsto gl(V \oplus W)$ et $x \mapsto x_{V\oplus W} = x_V \oplus x_W = \begin{pmatrix} x_v & 0 \\ 0 & x_w \end{pmatrix}$.

Définition. ***(Produit tensoriel de représentations)***

Étant donné deux représentations $V,W \in \mathrm{Rep}(\mathfrak{g}) = \mathrm{Rep}(U(\mathfrak{g}))$, le *produit tensoriel des deux représentations*, noté $V \otimes W \in \mathrm{Rep}(\mathfrak{g})$ évidemment donné par $V \otimes W$ en tant qu'espace vectoriel avec l'action de $\mathfrak{g}$ donnée par $x_{V\otimes W} = x_V \otimes id_W + id_V \otimes x_W \in \mathrm{End}(V \otimes W) = \mathrm{End}(V) \otimes \mathrm{End}(W)$ pour tout $x \in \mathfrak{g}$.

En général, $\mathrm{Rep}(A)$ où A est une algèbre associative, n'a pas de produit tensoriel. (Il sera nécessaire que A soit une algèbre de Hopf.)

Définition. ***(Représentation duale d'une algèbre de Lie)***

$V^\times = V^V = \mathrm{Hom}_k(V,k)$ avec l'action de $\mathfrak{g}$ ci-dessus est appelée *représentation duale* de V.

Remarque. En particulier, $\mathfrak{g}$ agit sur $\mathrm{Hom}_k(V \otimes V,k)$ l'ensemble des formes bilinéaires $V \times V \to k$.

Remarque. $b \in \mathrm{Hom}_k(V \otimes V,k)$ est dite $\mathfrak{g}$-*invariante* si elles appartient à $\mathrm{Hom}_k(V \otimes V,k)^\mathfrak{g} = \{b \mid xb = 0 \quad \forall x \in \mathfrak{g}\} = \{b : V \times V \to A \mid b(xv,w) + b(v,xw) = 0 \quad \forall x \in y, \forall v,w \in U\} = \{b \in V \times V \to k \mid b(x.u) = 0 \quad \forall x \in y, \forall u \in V \times V\} = \mathrm{Hom}_\mathfrak{g}(V \otimes V,k)$ où $V \otimes V$ est la représentation tenseur et k la 0-représentation : $x.b = 0$.

De façon similaire, on a $(V^V)^\mathfrak{g} = \mathrm{Hom}_k(V,k)^\mathfrak{g} = \mathrm{Hom}_\mathfrak{g}(V,k)$ ou $\mathrm{Hom}_k(V,W)^\mathfrak{g} = \mathrm{Hom}_\mathfrak{g}(U,W) = ...$

⟶ *Notation.* Étant donné $b \in \mathrm{Hom}_k(V \otimes V,k)$, on peut considérer l'algèbre de Lie $z_{\{b\}}(\mathfrak{g})$ le stabilisateur de b dans $\mathfrak{g}$, soit $\{x \in \mathfrak{g} \mid x.b = 0\}$.

Exemples

1. Si b est antisymétrique non dégénérée et $V = k^{2n}$, alors $z_{\{b\}}(gl(V)) = \mathfrak{sp}(n,k)$.
2. Si b est symétrique non dégénérée et $V = k^n$, alors $z_{\{b\}}(gl(V)) = \mathfrak{so}(n,k)$.
3. Sur $k \neq \mathbb{C}$, il peut y avoir plusieurs algèbres de Lie orthogonales non isomorphes.

Exercice 36 *(Nilpotence des matrices sans trace)*

Montrer que $\mathfrak{sl}_2(k)$ est nilpotente si et seulement si $\mathrm{car}(k) = 2$.

6.1.3 Classification des algèbres de Lie semi-simples

6.1.4 Classification des représentations des algèbres de Lie semi-simples

6.1.5 Formule des caractères de Weyl

6.2 Théorie des représentations des algèbres de Lie semi-simples

6.2.1 Aspects catégories

6.2.2 Catégorie $\mathcal{O}$

6.3 Représentations et géométrie algébrique

6.3.1 Groupes algébriques

6.3.2 Variétés de drapeaux

6.3.3 Théorie de Springer

Chapitre 7

Exercices

Difficulté des exercices :

- ● ○ ○ ○ ○ Question de cours, application directe, exercice purement calculatoire sans réelle difficulté technique
- ● ● ○ ○ ○ Exercice faisable, soit intuitivement, soit en employant des moyens rudimentaires ou des techniques déjà vues
- ● ● ● ○ ○ Exercice relativement difficile et dont la résolution appelle à une réflexion plus importante à cause d'obstacles techniques ou conceptuels, qui cependant devraient être à la portée de la plupart des étudiants bien entraînés
- ● ● ● ● ○ Exercice très exigeant, destiné aux élèves prétendant aux concours les plus difficiles, exercice « classique ».
- ● ● ● ● ● La résolution de l'exercice requiert un raisonnement et des connaissances extrêmement avancés, dépassant les attentes du prérequis. Il est presque impossible de le mener à terme sans indication. Bien qu'exigibles à très peu d'endroits, ces exercices sont très intéressants et présentent souvent des résultats forts.

Appendice

Bibliographie

[1] *Titre du livre*, Auteur du livre, date, maison d'édition

Table des figures

Liste des tableaux