Master de sciences, mention mathématiques
Année 2008–2009

INTRODUCTION À LA THÉORIE DES REPRÉSENTATIONS

UFR de mathématique et d'informatique — Université Louis Pasteur
7, rue René Descartes — 67084 Strasbourg Cedex

Table des matières

Introduction

Ce cours fondamental commence par présenter le langage des modules sur un anneau. Cette notion se retrouve partout en algèbre moderne, de la géométrie algébrique à la topologie algébrique, en passant naturellement par la théorie des représentations. Pour simplifier, disons que les modules sont aux anneaux ce que les actions sont aux groupes. Après un aperçu des définitions et des constructions de base, nous étudions la structure des modules en les découpant en morceaux plus ou moins petits. Puis nous regardons une classe particulière de modules, les modules complètement réductibles, qui sont ceux qui peuvent être reconstitués à partir de leurs plus petits constituants. Enfin nous définissons le produit tensoriel de deux modules.

Dans le deuxième chapitre, nous introduisons des outils d'étude des anneaux : radical de Jacobson et idempotents. Ensuite nous nous lançons dans l'étude d'une classe particulière d'anneaux, les anneaux semi-simples artiniens. Ils sont caractérisés par le fait que tous leurs modules sont complètement réductibles. Le théorème de Wedderburn-Artin décrit complètement leur structure : ce sont des produits d'anneaux de matrice à coefficients dans un anneau à division. (« Anneau à division » est l'appellation officielle pour « corps non-commutatif ».) Ensuite, nous étudions des anneaux artiniens généraux. Cette partie du cours est assez abstraite, faute de temps pour en développer les applications.

Le troisième chapitre concerne les algèbres. Essentiellement, une algèbre est un anneau contenant un corps, comme par exemple l'anneau des matrices à coefficients dans un corps k. On peut alors faire varier ce corps, par exemple passer des matrices $n \times n$ à coefficients dans $\mathbf{R}$ aux matrices $n \times n$ à coefficients dans $\mathbf{C}$. Le point culminant de ce chapitre est le théorème de Wedderburn-Malcev, qui dit que si A est une algèbre de dimension finie sur un corps k parfait (disons, de caractéristique nulle), alors on peut casser A en deux morceaux $A = B \oplus J(A)$, où B est une sous-algèbre semi-simple de A (un morceau à priori sympathique) et où $J(A)$ est un idéal nilpotent de A. Cette décomposition généralise la décomposition de Dunford des endomorphismes d'un espace vectoriel en partie semi-simple plus partie nilpotente.

Avec le quatrième chapitre, nous en arrivons enfin à des problèmes concrets, avec la notion de représentation de groupes. Notre exposé est assez classique, si ce n'est que nous tirons partie du vocabulaire mis en place jusque là. Au programme : les représentations des groupes finis, avec la théorie classique des caractères de Frobenius, Schur et Burnside, et la preuve du théorème de Burnside qui affirme que tout groupe d'ordre $p^a q^b$ est résoluble. Puis vient la notion de représentation induite, un procédé important de construction de représentations. Le chapitre se clôt sur la théorie de Peter-Weyl, qui affirme que si G est un groupe compact, alors les coefficients des représentations complexes continues de dimension finie de G fournissent une base hilbertienne de l'espace $L^2(G)$ des fonctions de carré intégrable sur G pour la mesure invariante (mesure de Haar).

Nous illustrons toute cette théorie dans le cinquième chapitre sur les exemples classiques du groupe symétrique et du groupe unitaire. De façon peut-être surprenante de prime abord, les deux cas peuvent être étudiés à l'aide d'une même combinatoire, celle des partitions, des tableaux et des fonctions symétriques. Une autre relation entre les représentations du groupe unitaire et celles du groupe symétrique, sans doute plus directe mais moins explicite, est apportée par la dualité de Schur-Weyl, dont l'exposé conclut ce cours.

1 Modules sur un anneau

Introduction

Un groupe n'existe que quand il agit : ce leitmotiv de tout enseignement de théorie des groupes résume d'une part les applications de la théorie, d'autre part les deux principales méthodes d'études des groupes, à savoir les opérations d'un groupe sur un ensemble ou sur un espace vectoriel. L'idée est d'obtenir des renseignements sur un groupe abstrait à partir des groupes symétriques et des groupes linéaires, qui sont concrets et prétendument bien connus. De façon analogue, une méthode fructueuse d'étude d'un anneau, commutatif ou non, consiste à examiner ses actions sur un groupe abélien. Une telle action s'appelle un module sur l'anneau. La pertinence de cette méthode vient de ce qu'on remplace un objet quadratique (la multiplication dans un anneau est bilinéaire) par des objets linéaires.

L'algèbre linéaire, vue comme l'étude des espaces vectoriels, est le cas particulier de la théorie des modules quand l'anneau est un corps. Nous retrouverons du reste quelques outils et concepts de l'algèbre linéaire dans la théorie des modules. Mieux : la donnée d'un espace vectoriel de dimension finie sur un corps k muni d'un endomorphisme est équivalente à la donnée d'un $k[X]$-module artinien et noethérien. Toute la théorie de la réduction des endomorphismes se trouve ainsi englobée dans l'étude des $k[X]$-modules, ce qui explique à posteriori l'importance donnée aux sous-espaces stables et aux polynômes d'endomorphismes. Continuant ainsi, on peut ramener la réduction simultanée d'une famille d'endomorphismes sur un espace vectoriel à l'étude des modules sur une algèbre. Un cas particulier de ceci est l'action d'un groupe sur un espace vectoriel, appelée représentation linéaire du groupe.

L'ensemble des modules sur un anneau et des homomorphismes de modules forme ce qu'on appelle une catégorie abélienne. C'est là le domaine des suites exactes courtes et longues, de la chasse au diagramme et de l'*abstract nonsense,* des résolutions et de l'algèbre homologique, de la théorie basculante et des équivalences de catégories dérivées. Ces outils, parmi les plus puissants en algèbre aujourd'hui, n'ont malheureusement pas leur place dans un cours d'introduction.

1.1 Le langage des modules

1.1.1 Rappels sur les anneaux

Par convention, un anneau a toujours un neutre multiplicatif, et un homomorphisme d'anneaux préserve toujours le neutre multiplicatif. On note $A^\times$ l'ensemble des éléments inversibles de l'anneau A : c'est un groupe. Un homomorphisme d'anneaux de A dans B induit un homomorphisme de groupes de $A^\times$ dans $B^\times$.

Exemple. Si M et N sont deux groupes abéliens, alors l'ensemble des homomorphismes de groupes de M dans N est un groupe abélien, qu'on note $\mathrm{Hom}_{\mathbf{Z}}(M,N)$. Pour $M=N$, on parle d'endomorphismes et on note $\mathrm{End}_{\mathbf{Z}}(M)$ plutôt que $\mathrm{Hom}_{\mathbf{Z}}(M,M)$. Le produit de composition munit $\mathrm{End}_{\mathbf{Z}}(M)$ d'une structure d'anneau, le neutre multiplicatif étant l'application identité.

Anneau opposé : soit A un anneau. On désigne par A^{op} l'anneau opposé à A : il a le même groupe additif sous-jacent que A, mais le produit ab dans A^{op} de deux éléments a et b est égal au produit ba calculé dans A.

Idempotent : un élément e d'un anneau A est appelé idempotent s'il est non-nul et si $e^2 = e$. Alors $eAe = \{x \in A \mid x = xe = ex\}$ est un anneau, de neutre e.

Anneau à division : un anneau A est dit à division si $A^\times$ est l'ensemble des éléments non-nuls de A. On parlait jadis de « corps non-commutatif ».

Anneau local : un anneau A est dit local si l'ensemble $A \setminus A^\times$ des éléments non-inversibles est un idéal bilatère.

L'anneau nul, réduit au seul élément 0, n'est ni local, ni un anneau à division. C'est le seul anneau dans lequel 0 est inversible.

Anneau de matrices : soit A un anneau et n un entier strictement positif. L'ensemble des matrices carrées $n \times n$ à coefficients dans A est un anneau, noté $\mathbf{Mat}_n(A)$. Attention : les trois anneaux $\mathbf{Mat}_n(A^{\mathrm{op}})$, $\mathbf{Mat}_n(A)$ et $\mathbf{Mat}_n(A)^{\mathrm{op}}$ ont même groupe additif sous-jacent mais ont des produits différents.

La définition d'anneau local adoptée ci-dessus est commode pour la preuve du théorème de Krull-Schmidt 1.2.2.6. La notion peut cependant être présentée de façon différente ; d'autres caractérisations sont ainsi données dans la proposition 2.3.1.1.

Exercices.

(1) Soit e un idempotent d'un anneau A, de sorte que eAe est un anneau de neutre multiplicatif e. Alors pour tout idéal bilatère I de A, l'ensemble eIe est un idéal bilatère de eAe et $eIe = I \cap eAe$. Tout idéal bilatère de eAe est de cette forme.

(2) Soient A un anneau et n un entier strictement positif. Les idéaux bilatères de $\mathbf{Mat}_n(A)$ sont de la forme $\mathbf{Mat}_n(I)$, où I est un idéal bilatère de A.

1.1.2 Définition d'un module

La tâche d'insérer la phrase « Soit A un anneau » devant la plupart des énoncés suivants est laissée au lecteur.

A-module : un A-module à gauche est un groupe abélien M muni d'une opération externe de A de sorte que pour tous $a, b \in A$ et tous $m, n \in M$, on ait

$$a(m+n) = am + an,\ (a+b)m = am + bm,\ (ab)m = a(bm),\ 1m = m.$$

En d'autres termes, on demande la donnée d'un homomorphisme d'anneaux de A dans $\mathrm{End}(M)$. Pour alléger les énoncés, la précision « à gauche » sera parfois omise des énoncés. Pour indiquer que M est un A-module à gauche, on écrit parfois ${}_AM$.

Homomorphismes de A-modules : soient M et N deux A-modules. Un homomorphisme de A-modules de M dans N est un homomorphisme de groupes abéliens $f : M \to N$ qui commute à l'action de A : pour tout $a \in A$ et tout $m \in M$, on doit avoir $f(am) = af(m)$.

On note $\mathrm{Hom}_A(M,N)$ l'ensemble des homomorphismes de A-modules de M dans N ; c'est un sous-groupe de $\mathrm{Hom}_{\mathbf{Z}}(M,N)$. Pour $M=N$, on note $\mathrm{End}_A(M)=\mathrm{Hom}_A(M,M)$; c'est un sous-anneau de $\mathrm{End}_{\mathbf{Z}}(M)$.

Exemples.

(1) $A=\mathbf{Z}$. Un groupe abélien est un $\mathbf{Z}$-module, et réciproquement. La notation $\mathrm{Hom}_{\mathbf{Z}}(M,N)$ n'est pas ambiguë.

(2) A est un corps k. Un A-module est la même chose qu'un k-espace vectoriel.

(3) $A=k[X]$, où k est un corps. Un A-module est la donnée d'un k-espace vectoriel E muni d'un endomorphisme u : l'action d'un polynôme $P\in k[X]$ sur un vecteur $x\in E$ est $P(u)(x)$. Un homomorphisme du $k[X]$-module donné par le couple (E,u) dans le $k[X]$-module donné par le couple (F,v) est une application k-linéaire $f:E\to F$ telle que $v\circ f=f\circ u$.

Annulateur d'un A-module : l'annulateur d'un A-module M est le noyau de l'homomorphisme d'anneaux de A dans $\mathrm{End}_{\mathbf{Z}}(M)$ définissant la structure de A-modules sur M. C'est un idéal bilatère de A noté $\mathrm{ann}\,M$.

Deux modules importants sur un anneau A quelconque :

(1) Le A-module à gauche régulier est le groupe abélien $(A,+)$, sur lequel les éléments de A agissent par multiplication à gauche. Pour distinguer le A-régulier de l'anneau A, on note celui-là ${}_AA$. Pour tout A-module à gauche M, l'application $f\mapsto f(1)$ est un isomorphisme de groupes abéliens de $\mathrm{Hom}_A({}_AA,M)$ sur M. L'application $f\mapsto f(1)$ est un isomorphisme d'anneaux de $\mathrm{End}_A({}_AA)$ sur A^{op}, de réciproque $a\mapsto(b\mapsto ba)$.

(2) Soit I un ensemble. Le A-module $A^{(I)}$ (ou ${}_AA^{(I)}$) est l'ensemble de toutes les familles $(a_i)_{i\in I}$ d'éléments de A n'ayant qu'un nombre fini d'éléments non-nuls. La somme et l'action de A par multiplication à gauche se font composante par composante. À chaque $i\in I$ correspond un élement $e_i\in A^{(I)}$; c'est la famille formée de zéros, avec juste un 1 en position i. Alors pour tout A-module M, l'application $f\mapsto(f(e_i))_{i\in I}$ est un isomorphisme de groupes abéliens de $\mathrm{Hom}_A(A^{(I)},M)$ sur M^I.

Soit M un A-module. Une famille $(m_i)_{i\in I}$ d'éléments de M est dite génératrice si chaque élément $m\in M$ s'écrit comme combinaison linéaire $\sum_{i\in I}a_im_i$ des éléments de cette famille, avec $(a_i)\in A^{(I)}$. On dit que c'est une base si pour tout m, il y a existence et unicité de $(a_i)_{i\in I}$. Autrement dit, l'homomorphisme de A-modules $f\in\mathrm{Hom}_A(A^{(I)},M)$ tel que $f(e_i)=m_i$ est surjectif si $(m_i)_{i\in I}$ est génératrice, et est un isomorphisme si $(m_i)_{i\in I}$ est une base. Un A-module qui possède une base est dit libre. Évidemment, tout module possède une famille génératrice (la façon la plus brutale de voir cela est de prendre tous les éléments du module), donc tout module est l'image d'un module libre par un homomorphisme surjectif.

Exercice. Soit A un anneau commutatif non-nul et M un A-module libre. Montrer que toutes les bases de M ont même cardinal. (Indication : en rang fini, on peut procéder avec des matrices et des déterminants de la façon suivante. Soit $(e_1,\dots,e_n)$ une base de M et $(f_1,\dots,f_m)$ une famille génératrice de M. Écrivons $e_i=\sum_j a_{ij}f_j$ et $f_j=\sum_i b_{ji}e_i$. Alors $AB=I_n$. La formule de Binet-Cauchy sur les déterminants de matrices interdit alors $m<n$.

En rang infini, le plus simple est de considérer un idéal maximal $\mathfrak{m}$ de A. Si I et J sont deux ensembles, un isomorphisme de A-modules entre $A^{(I)}$ et $A^{(J)}$ induit un isomorphisme de $A/\mathfrak{m}$-espaces vectoriels entre $A^{(I)}/\mathfrak{m}A^{(I)} \cong (A/\mathfrak{m})^{(I)}$ et $A^{(J)}/\mathfrak{m}A^{(J)} \cong (A/\mathfrak{m})^{(J)}$. On s'est alors ramené au cas des espaces vectoriels sur un corps.)

1.1.3 Constructions catégoriques

Module 0.

Produit $\prod_{t\in T} M_t$ et coproduit (somme directe externe)

$$\coprod_{t\in T} M_t = \left\{ (m_t) \in \prod_{t\in T} M_t \;\middle|\; m_t = 0 \text{ sauf pour un nombre fini d'indices} \right\}$$

d'une famille $(M_t)_{t\in T}$ de modules. La somme de deux éléments et l'action d'un élément de A se calculent composante par composante. On dispose d'homomorphismes canoniques $p_u : \prod_{t\in T} M_t \to M_u$ et $i_u : M_u \to \coprod_{t\in T} M_t$ pour $u \in T$; p_u donne la u-ième composante d'un T-uplet appartenant au produit, i_u envoie un élément m de M_u sur le T-uplet comportant des 0 partout, sauf à la position u où on trouve m. Les applications

$$\left(\begin{array}{c} \mathrm{Hom}_A\left(N, \prod_{t\in T} M_t\right) \xrightarrow{\simeq} \prod_{t\in T} \mathrm{Hom}_A(N, M_t) \\ f \mapsto (p_t \circ f)_{t\in T} \end{array} \right) \text{ et } \left(\begin{array}{c} \mathrm{Hom}_A\left(\coprod_{t\in T} M_t, N\right) \xrightarrow{\simeq} \prod_{t\in T} \mathrm{Hom}_A(M_t, N) \\ g \mapsto (g \circ i_t)_{t\in T} \end{array} \right)$$

sont des isomorphismes de groupes abéliens ; de fait, on vérifie sans peine que ces homomorphismes admettent des bijections réciproques, qui à $(f_t)_{t\in T} \in \prod_{t\in T} \mathrm{Hom}_A(N, M_t)$ et $(g_t)_{t\in T} \in \prod_{t\in T} \mathrm{Hom}_A(M_t, N)$, associent respectivement

$$\Big(n \mapsto (f_t(n))_{t\in T}\Big) \in \mathrm{Hom}_A\left(N, \prod_{t\in T} M_t\right) \text{ et } \left((m_t)_{t\in T} \mapsto \sum_{t\in T} g_t(m_t)\right) \in \mathrm{Hom}_A\left(\coprod_{t\in T} M_t, N\right).$$

Remarques.

(1) Il est fréquent d'écrire $\bigoplus$ plutôt que $\coprod$. Cet abus de notation ne prête quasiment jamais à confusion.

(2) Le module $A^{(I)}$ du paragraphe précédent est le coproduit $\coprod_{i\in I\ A} A$ d'une famille de copies du module à gauche régulier. Dans ce cadre, le second isomorphisme de groupes abéliens ci-dessus redonne l'isomorphisme $\mathrm{Hom}_A(A^{(I)}, M) \cong M^I$ du paragraphe précédent.

Sous-module : un sous-module N d'un A-module M est un sous-groupe additif stable par l'action de A. Le groupe quotient M/N devient un A-module si l'on pose $a(m+N) = am+N$, pour $a \in A$ et $m + N \in M/N$. (On vérifie facilement que cela est bien défini.) L'injection de N dans M et la surjection canonique de M sur M/N sont évidemment des homomorphismes de A-modules. Un sous-module N d'un A-module M est dit maximal si $N \subsetneq M$ et s'il n'existe pas de sous-module P coincé strictement entre N et M.

Exemples.

(1) Les sous-modules du A-module à gauche régulier ${}_AA$ sont les idéaux à gauche de A.

(2) Soit E un espace vectoriel sur un corps k. La donnée d'un endomorphisme u de E définit une structure de $k[X]$-module sur E. Un sous-$k[X]$-module de E est un sous-espace de E stable par u ; la structure de $k[X]$-module sur E/F est définie par l'endomorphisme que u induit sur E/F.

(3) Combinant les deux exemples précédents, considérons un corps k et un polynôme unitaire $P = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + X^n$ de degré n à coefficients dans k. Le $k[X]$-module $E = k[X]/(P)$, quotient du module régulier, est le k-espace vectoriel E muni de l'endomorphisme u donné par la multiplication par X. Dans la base $(\overline{1}, \overline{X}, \ldots, \overline{X^{n-1}})$, la matrice de u est la matrice compagnon de P

$$\begin{pmatrix} 0 & \ldots & \ldots & 0 & -a_0 \\ 1 & \ddots & & \vdots & -a_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_{n-2} \\ 0 & \ldots & 0 & 1 & -a_{n-1} \end{pmatrix}.$$

(4) Soient A un anneau, I un idéal bilatère de A, M un A-module. Alors

$$IM = \{a_1m_1 + \cdots + a_nm_n \mid n \in \mathbf{N}, (a_i) \in I^n, (m_i) \in M^n\}$$

est un sous-module de M. De plus, l'idéal I est inclus dans le noyau de l'homomorphisme d'anneaux de A dans $\mathrm{End}(M/IM)$. Ce dernier se factorise donc à travers le quotient A/I, ce qui permet de dire que M/IM est un A/I-module.

Soit $f : M \to N$ un homomorphisme de A-modules. L'image par f d'un sous-module de M est un sous-module de N ; la préimage par f d'un sous-module de N est un sous-module de M. On définit ainsi deux sous-modules $\ker f = \{x \in M \mid f(x) = 0\}$ et $\mathrm{im}\, f = \{f(x) \mid x \in M\}$ de M et N, respectivement, appelés noyau et image de f. Le conoyau de f est le module $N/\mathrm{im}\, f$. Un homomorphisme est injectif si et seulement si son noyau est nul ; on dit alors que f est un monomorphisme. Un homomorphisme est surjectif si et seulement si son conoyau est nul ; on dit alors que f est un épimorphisme [1].

Soit M un A-module et P un sous-module. Les sous-modules de M/P sont de la forme N/P avec N sous-module de M contenant P. (Pour voir cela, examiner la préimage par l'homomorphisme canonique de M sur M/N.) Un module comme N/P peut ainsi être vu soit comme quotient du sous-module N de M, soit comme sous-module du quotient M/P de M ; pour cette raison, on dit que N/P est un sous-quotient de M.

1. Les notions de mono- et d'épimorphisme peuvent être définies dans un cadre catégorique général, où injectivité et surjectivité n'ont plus de signification. Les équivalences « monomorphisme si seulement si le noyau est nul » et « épimorphisme si et seulement si le conoyau est nul » restent toutefois valables dans les catégories abéliennes.

Soit M un A-module, soit $(M_i)_{i\in I}$ une famille de sous-modules de M. On dispose alors d'homomorphismes canoniques

$$\begin{pmatrix} \coprod_{i\in I} M_i \to M \\ (m_i)_{i\in I} \mapsto \sum_{i\in I} m_i \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} M \to \prod_{i\in I} M/M_i \\ m \mapsto (m + M_i)_{i\in I} \end{pmatrix}.$$

La somme des M_i, notée $\sum_{i\in I} M_i$ est l'image du premier homomorphisme ; l'intersection des M_i est le noyau du second ; la somme et l'intersection des M_i sont donc des sous-modules de M. On dit que les M_i sont en somme directe si le premier homomorphisme est injectif ; on écrit alors $\bigoplus_{i\in I} M_i$ plutôt que $\sum_{i\in I} M_i$. Pour que M soit la somme directe de deux sous-modules M' et M'', il faut et il suffit que $M' \cap M'' = 0$ et que $M' + M'' = M$; on dit alors que M' et M'' sont supplémentaires l'un de l'autre. Un sous-module possédant un supplémentaire est appelé facteur direct (*direct summand* en anglais).

Théorème de factorisation : un homomorphisme $f : M \to N$ de A-modules se factorise en

$$\begin{array}{ccc} M & \xrightarrow{\quad f \quad} & N. \\ & \searrow \quad \nearrow & \\ & M/\ker f \xrightarrow{\simeq} \operatorname{im} f & \end{array}$$

Isomorphismes canoniques : si N, N' et P sont des sous-modules d'un A-module M tels que $P \subseteq N$, alors $(N + N')/N' \cong N/(N \cap N')$ et $(M/P)/(N/P) \cong M/N$.

Suite exacte : une suite d'homomorphismes

$$M_0 \xrightarrow{f_1} M_1 \xrightarrow{f_2} \cdots \xrightarrow{f_n} M_n$$

est dite exacte en M_i si $\operatorname{im} f_i = \ker f_{i+1}$. On a alors $f_{i+1} \circ f_i = 0$. Elle est dite exacte si elle est exacte en M_1, en M_2, ..., et en M_{n-1}.

Exemple. Soit $f : M \to N$ un homomorphisme de A-modules. Alors on dispose d'une suite exacte

$$0 \to \ker f \to M \xrightarrow{f} N \to \operatorname{coker} f \to 0.$$

Suite exacte courte : une suite exacte courte est une suite exacte de la forme $0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$. On a ainsi f injective, g surjective, $L \cong \ker g$, $N \cong \operatorname{coker} f$, $\operatorname{im} f = \ker g$.

1.1.3.1 Proposition. *Étant donnée une suite exacte courte* $0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$, *les trois conditions suivantes sont équivalentes :*

(i) $\operatorname{im} f$ $(= \ker g)$ *possède un supplémentaire.*

(ii) Il existe $h \in \operatorname{Hom}_A(M, L)$ *tel que* $h \circ f = \mathrm{id}_L$.

(iii) Il existe $k \in \operatorname{Hom}_A(N, M)$ *tel que* $g \circ k = \mathrm{id}_N$.

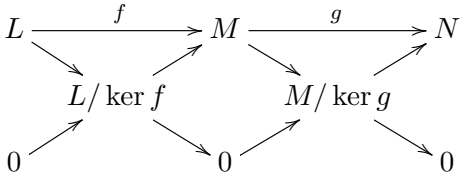
Preuve. Montrons d'abord que (i) entraîne (ii) et (iii)). Supposons (i). Il existe donc un sous-module X dans M tel que $M = X \oplus \operatorname{im} f$. Alors la restriction de g à X est un isomorphisme de X sur N. La composée k de l'inverse de cet isomorphisme avec l'injection de X dans M vérifie $g \circ k = \mathrm{id}_N$. Cela montre (iii). Par ailleurs, f induit un isomorphisme entre L et $\operatorname{im} f$. En composant l'inverse de celui-ci par la projection de M sur $\operatorname{im} f$ parallèlement à X, on obtient un homomorphisme h de M sur L tel que $h \circ f = \mathrm{id}_L$. Cela montre (ii).

Réciproquement, supposons (ii). Il existe donc $h \in \mathrm{Hom}_A(M, L)$ tel que $h \circ f = \mathrm{id}_L$. Je dis qu'alors $M = \ker h \oplus \operatorname{im} f$. L'égalité $\ker h \cap \operatorname{im} f = 0$ vient du fait que tout élément x dans cette intersection s'écrit $f(y)$ avec $y \in L$, puis alors que $0 = h(x) = h \circ f(y) = y$, de sorte que $x = f(0) = 0$. L'égalité $M = \ker h + \operatorname{im} f$ vient de ce que tout élément x de M s'écrit $x = f \circ h(x) + (x - f \circ h(x))$, avec $x - f \circ h(x) \in \ker h$. Bref on a bien $M = \ker h \oplus \operatorname{im} f$, ce qui entraîne (i).

Il reste à montrer que (iii) entraîne (i), autrement dit que l'existence d'un $k \in \mathrm{Hom}_A(N, M)$ tel que $g \circ k = \mathrm{id}_N$ entraîne celle d'un supplémentaire X de $\ker g$ dans M. Pour voir cela, on constatera qu'avec les notations ainsi mises en place, on a $M = \ker g \oplus \operatorname{im} k$. □

Une suite exacte courte qui satisfait les hypothèses de la proposition est dite scindée.

Toute suite exacte se casse en suites exactes courtes. La méthode pour le faire est d'introduire les noyaux et les conoyaux des homomorphismes de la suite exacte $L \xrightarrow{f} M \xrightarrow{N}$ de départ, comme sur le diagramme suivant :



avec $L/\ker f \cong \operatorname{im} f = \ker g$

$M/\ker g = \operatorname{coker} f \cong \operatorname{im} g.$

On voit alors apparaître la suite exacte courte

$$0 \to L/\ker f \to M \to M/\ker g \to 0,$$

que l'on peut compléter aux bords par les deux suites

$$0 \to \ker f \to L \to L/\ker f \to 0$$

$$0 \to M/\ker g \to N \to \operatorname{coker} g \to 0.$$

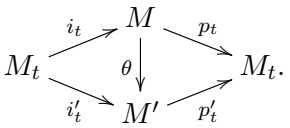
En partant d'une suite exacte comportant $n + 2$ modules, le même procédé fournit n suites exactes courtes, plus toujours les deux au bord.

Exercices.

(1) Soit $(M_t)_{t \in T}$ une famille finie de modules sur un anneau A. Appelons M la somme directe externe des (M_t) ; elle vient avec des homomorphismes $i_t : M_t \to M$ de A-modules. Comme M est aussi le produit des $(M_t)_{t \in T}$, on dispose également d'homomorphismes canoniques $p_t : M \to M_t$.

(i) Vérifier les relations $p_t \circ i_t = \mathrm{id}_{M_t}$, $p_t \circ i_u = 0$ si $t \neq u$, $\sum_{t\in T} i_t \circ p_t = \mathrm{id}_M$.

(ii) Montrer que réciproquement, si M' est un A-module, s'il existe des homomorphismes $i'_t : M_t \to M'$ et $p'_t : M' \to M_t$ vérifiant les mêmes relations entre eux que les i_t et les p_t du (a), alors il existe un unique isomorphisme $\theta : M \to M'$ rendant commutatif pour tout t le diagramme



(2) Soit M un A-module. Supposons que M soit la somme directe d'une famille finie $(M_i)_{i\in I}$ de sous-modules de M. Pour $i \in I$, notons $e_i : M \to M_i$ la projection sur M_i parallèlement à $\sum_{j\neq i} M_j$; autrement dit $e_i(m)$ est nul si m appartient à un M_j avec $j \neq i$ et est m si $m \in M_i$. Montrer que $e_i^2 = e_i$, que $e_i \circ e_j = 0$ si $i \neq j$, et que $\sum_{i\in I} e_i = \mathrm{id}_M$.

(3) (Lemme des cinq court) On considère un diagramme commutatif d'homomorphismes de A-modules de la forme suivante, où les deux lignes forment des suites exactes :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L & \longrightarrow & M & \longrightarrow & N & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & L' & \longrightarrow & M' & \longrightarrow & N' & \longrightarrow & 0 \end{array}$$

Montrer que si, parmi les trois homomorphismes f, g et h, deux sont des isomorphismes, alors le troisième est aussi un isomorphisme.

(4) (Lemme du serpent) On considère un diagramme commutatif d'homomorphismes de A-modules de la forme suivante, où les deux lignes forment des suites exactes :

$$\begin{array}{ccccccccc} & & L & \xrightarrow{u} & M & \xrightarrow{v} & N & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & L' & \xrightarrow[u']{} & M' & \xrightarrow[v']{} & N'. & & \end{array}$$

Montrer qu'il existe une suite exacte canonique

$$\ker f \to \ker g \to \ker h \xrightarrow{\delta} \operatorname{coker} f \to \operatorname{coker} g \to \operatorname{coker} h.$$

(Indication : les deux premières flèches sont induites par u et v ; les deux dernières par u' et v'. Soit $x \in \ker h$; on peut écrire $x = v(y)$, avec $y \in M$; il existe alors un unique $z \in L'$ tel que $u'(z) = g(y)$. On vérifie que la classe $z + \operatorname{im} f$ ne dépend que de x et pas du choix de y, ce qui autorise à poser $\delta(x) = z$. L'homomorphisme δ étant ainsi défini, il faut vérifier que la suite obtenue est exacte. C'est longuet, mais ne présente pas de difficulté particulière. Note : δ est appelé homomorphisme de liaison.)

(5) Soient deux homomorphismes $g : M \to N$ et $g' : M' \to N$ de A-modules. Appelons L le noyau de l'homomorphisme $\begin{pmatrix} g & -g' \end{pmatrix} : M \oplus M' \to N$, où la notation matricielle par blocs reflète la décomposition en somme directe du module de gauche. Autrement dit, L est le sous-module $\{(n, n') \mid g(n) = g(n')\}$ de $M \oplus M'$. On dispose alors d'homomorphismes $f : L \to M$ et $f' : L \to M'$ obtenus en composant l'injection de L

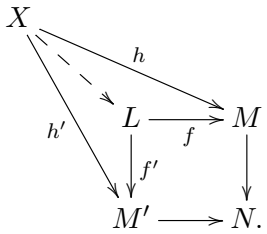
dans $M \oplus M'$ avec les surjections de ce dernier sur M et M', et ainsi d'un diagramme commutatif appelé « pullback »

$$\begin{array}{ccc} L & \xrightarrow{f} & M \\ {\scriptstyle f'}\downarrow & & \downarrow{\scriptstyle g} \\ M' & \xrightarrow[g']{} & N. \end{array}$$

(i) Pour tout diagramme commutatif

$$\begin{array}{ccc} X & \xrightarrow{h} & M \\ {\scriptstyle h'}\downarrow & & \downarrow{\scriptstyle g} \\ M' & \xrightarrow[g']{} & N \end{array}$$

d'homomorphismes de A-modules, il existe un unique homomorphisme de X dans L rendant le diagramme suivant commutatif :



(ii) Montrer que f' induit un isomorphisme de $\ker f$ sur $\ker g'$ et que si g' est surjectif, alors f est surjectif.

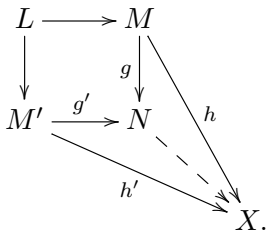
(6) Soient deux homomorphismes $f : L \to M$ et $f' : L \to M'$ de A-modules. Appelons N le conoyau de l'homomorphisme $\begin{pmatrix} f \\ -f' \end{pmatrix} : L \to M \oplus M'$, où la notation matricielle par blocs reflète la décomposition en somme directe du module de droite. Autrement dit, N est le quotient de $M \oplus M'$ par le sous-module $\{(f(m), -f'(m)) \mid m \in L\}$. On dispose alors d'homomorphismes $g : M \to N$ et $g' : M' \to N$ obtenus en composant les injections de M et M' dans $M \oplus M'$ avec l'homomorphisme canonique de ce dernier sur N, et ainsi d'un diagramme commutatif appelé « pushout »

$$\begin{array}{ccc} L & \xrightarrow{f} & M \\ {\scriptstyle f'}\downarrow & & \downarrow{\scriptstyle g} \\ M' & \xrightarrow[g']{} & N. \end{array}$$

(i) Pour tout diagramme commutatif

$$\begin{array}{ccc} L & \xrightarrow{f} & M \\ {\scriptstyle f'}\downarrow & & \downarrow{\scriptstyle h} \\ M' & \xrightarrow[h']{} & X \end{array}$$

d'homomorphismes de A-modules, il existe un unique homomorphisme de N dans X rendant le diagramme suivant commutatif :



(ii) Montrer que g induit un isomorphisme de coker f sur coker g' et que si f est injectif, alors g' est injectif.

1.1.4 Le (bi)foncteur Hom

Dans ce paragraphe, A et B sont des anneaux.

Commençons par motiver notre étude. Soit $f : L \to M$ un homomorphisme de A-modules. Alors pour tous A-modules X et Y, on dispose d'homomorphismes de groupes abéliens

$$f_* : \begin{pmatrix} \mathrm{Hom}_A(X,L) \to \mathrm{Hom}_A(X,M) \\ h \mapsto f \circ h \end{pmatrix} \quad \text{et} \quad f^* : \begin{pmatrix} \mathrm{Hom}_A(M,Y) \to \mathrm{Hom}_A(L,Y) \\ h \mapsto f \circ h. \end{pmatrix}$$

Si en outre $f' : L \to M$ et $g : M \to N$ sont des homomorphismes de A-modules, alors

$$(f+f')_* = f_* + f'_*, \quad (f+f')^* = f^* + f'^*, \quad (g \circ f)_* = g_* \circ f_* \quad \text{et} \quad (g \circ f)^* = f^* \circ g^*.$$

Foncteur : un foncteur covariant de la catégorie des A-modules dans la catégorie des B-modules est une règle F attribuant un B-module $F(M)$ à tout A-module M, et un homomorphisme $F(f) : F(M) \to F(N)$ à tout homomorphisme $f : M \to N$. On demande que $F(\mathrm{id}_M) = \mathrm{id}_{F(M)}$ pour tout A-module M, et que pour f et g des homomorphismes, $F(g \circ f) = F(g) \circ F(f)$ chaque fois que cela a un sens [2].

Un foncteur contravariant est défini de façon analogue, à ceci près qu'il renverse les flèches. Si G est un foncteur contravariant, alors l'image par G d'un homomorphisme $f \in \mathrm{Hom}_A(M,N)$ appartient à $\mathrm{Hom}_B(G(N), G(M))$. Si la composée $g \circ f$ de deux homomorphismes f et g a un sens, alors on demande que $G(g \circ f) = G(f) \circ G(g)$.

Un foncteur F de la catégorie des A-modules dans la catégorie des B-modules est dit additif si les applications $F : \mathrm{Hom}_A(M,N) \to \mathrm{Hom}_B(F(M), F(N))$ sont des homomorphismes de groupes. Un foncteur additif envoie le module 0 sur le module 0 (car 0 est le seul module M pour lequel $\mathrm{id}_M = 0$). On montre qu'un foncteur additif respecte les sommes directes (utiliser l'exercice (1) du paragraphe 1.1.3).

2. La notion de foncteur et de catégorie est bien plus générale que celle exposée ici dans le cadre des modules sur un anneau. Néanmoins la définition que nous verrons bientôt de foncteur additif n'a de sens que pour des foncteurs entre des catégories additives, et la notion de foncteur exact est réservée aux foncteurs entre deux catégories abéliennes. La catégorie des modules sur un anneau A est l'exemple prototypique d'une catégorie abélienne.

Un foncteur additif F est dit exact s'il envoie chaque suite exacte de A-modules sur une suite exacte de B-modules.

Un foncteur covariant F est dit exact à gauche si l'exactitude de $0 \to L \to M \to N$ entraîne celle de $0 \to F(L) \to F(M) \to F(N)$. Un foncteur contravariant G est dit exact à gauche si l'exactitude de $L \to M \to N \to 0$ entraîne celle de $0 \to G(N) \to G(M) \to G(L)$. On définit de façon analogue la notion de foncteur exact à droite.

Exemple. $\mathrm{Hom}_A(X, ?)$ est un foncteur additif covariant de la catégorie des A-modules dans la catégorie des $\mathbf{Z}$-modules ; notre application f_* du début du paragraphe doit donc être notée $\mathrm{Hom}_A(X, f)$. De manière analogue, $\mathrm{Hom}_A(?, Y)$ est un foncteur additif contravariant entre les mêmes catégories ; notre application f^* du début du paragraphe doit être notée $\mathrm{Hom}_A(f, Y)$.

1.1.4.1 Proposition. *Soient X et Y deux A-modules. Alors les foncteurs* $\mathrm{Hom}_A(X, ?)$ *et* $\mathrm{Hom}_A(?, Y)$ *sont exacts à gauche.*

Preuve. Partons d'une suite exacte $0 \to L \xrightarrow{f} M \xrightarrow{g} N$. En appliquant le foncteur $\mathrm{Hom}_A(X, ?)$, nous obtenons une suite de groupes abéliens

$$0 \to \mathrm{Hom}_A(X, L) \xrightarrow{f_*} \mathrm{Hom}_A(X, M) \xrightarrow{g_*} \mathrm{Hom}_A(X, M)$$

dont nous voulons voir qu'elle est exacte. L'injectivité de f entraîne celle de f_* : la vérification de cette assertion facile est omise. L'égalité $g \circ f = 0$ implique que $g_* \circ f_* = (g \circ f)_* = 0$, d'où $\mathrm{im}\, f_* \subseteq \ker g_*$. Il nous reste à montrer l'inclusion opposée. Prenons $h \in \ker g_*$. Dans le diagramme

$$\begin{array}{ccccccc} & & & & X & & \\ & & & k \swarrow & \big\downarrow h & & \\ 0 & \longrightarrow & L & \xrightarrow{f} & M & \xrightarrow{g} & N, \end{array}$$

la composée $g \circ h$ est nulle. Ainsi $\mathrm{im}\, h \subseteq \ker g = \mathrm{im}\, f$. Puisque f réalise une bijection entre L et $\mathrm{im}\, f$, il existe pour chaque $x \in X$ un unique élément $k(x) \in L$ tel que $f(k(x)) = h(x)$. L'application k, obtenue en composant h avec l'inverse de la restriction de f à son image, est un homomorphisme de A-modules, et on a $h = f_*(k) \in \mathrm{im}\, f_*$. Ceci achève notre preuve de l'exactitude à gauche de $\mathrm{Hom}_A(X, ?)$. La preuve de l'exactitude à gauche de $\mathrm{Hom}_A(?, Y)$ est analogue. □

Les foncteurs $\mathrm{Hom}_A(X, ?)$ et $\mathrm{Hom}_A(?, Y)$ ne sont pas exacts ; on peut le voir en examinant leur comportement sur la suite exacte courte $0 \to \mathbf{Z} \to \mathbf{Z} \to \mathbf{Z}/m\mathbf{Z} \to 0$ avec $A = \mathbf{Z}$ et $X = Y = \mathbf{Z}/m\mathbf{Z}$ (la flèche de $\mathbf{Z}$ dans lui-même est la multiplication par m).

Exercices.

(1) Soit A un anneau, soit F un foncteur additif covariant de la catégorie des A-modules vers la catégorie des $\mathbf{Z}$-modules, et soit M un A-module. Montrer que l'application $F : \mathrm{End}_A(M) \to \mathrm{End}_{\mathbf{Z}}(F(M))$ est un homomorphisme d'anneaux et que $F(M)$ est muni d'une structure naturelle de $\mathrm{End}_A(M)$-module à gauche.

(2) Soient A et B deux anneaux et F un foncteur covariant de la catégorie des A-modules vers la catégorie des B-modules.

(i) Pour que F soit exact à gauche, il faut et il suffit que pour chaque suite exacte courte $0 \to L \to M \to N \to 0$, la suite $0 \to F(L) \to F(M) \to F(N)$ soit exacte.

(ii) Pour que F soit exact à droite, il faut et il suffit que pour chaque suite exacte courte $0 \to L \to M \to N \to 0$, la suite $F(L) \to F(M) \to F(N) \to 0$ soit exacte.

(iii) Montrer que les conditions suivantes sont équivalentes :
— F est exact.
— F est exact à gauche et exact à droite.
— F envoie toute suite exacte courte sur une suite exacte courte.

(3) Soient A un anneau et L, M, N, P quatre A-modules. Soient $f \in \mathrm{Hom}_A(L, M)$ et $g \in \mathrm{Hom}_A(N, P)$. Montrer que le diagramme suivant commute

$$\begin{array}{ccc} \mathrm{Hom}_A(M,N) & \xrightarrow{\mathrm{Hom}_A(M,g)} & \mathrm{Hom}_A(M,P) \\ \downarrow{\scriptstyle \mathrm{Hom}_A(f,N)} & & \downarrow{\scriptstyle \mathrm{Hom}_A(f,P)} \\ \mathrm{Hom}_A(L,N) & \xrightarrow[\mathrm{Hom}_A(L,g)]{} & \mathrm{Hom}_A(L,P). \end{array}$$

(Note : on note habituellement $\mathrm{Hom}_A(f, g) : \mathrm{Hom}_A(M, N) \to \mathrm{Hom}_A(L, P)$ l'application composée.)

1.1.5 Le (bi)foncteur Ext^1_A

Donnons-nous deux A-modules M et N. On note $Ext^1_A(M, N)$ la classe des suites exactes courtes de premier et dernier termes N et M, respectivement. Étant donnés deux élements

$$\xi : \ 0 \to N \xrightarrow{f} E \xrightarrow{g} M \to 0 \quad \text{et} \quad \xi' : \ 0 \to N \xrightarrow{f'} E' \xrightarrow{g'} M \to 0$$

de $Ext^1_A(M, N)$, on écrit $\xi \sim \xi'$ si on peut inclure ξ et ξ' dans un diagramme commutatif

$$\begin{array}{ccccccc} & & & & E & & & & \\ & & & \nearrow & \downarrow{\scriptstyle \theta} & \searrow & & & \\ 0 & \longrightarrow & N & & & & M & \longrightarrow & 0. \\ & & & \searrow & & \nearrow & & & \\ & & & & E' & & & & \end{array}$$

La situation impose en fait à l'homomorphisme $\theta : E \to E'$ d'être un isomorphisme. Ainsi $\sim$ est une relation d'équivalence sur $Ext^1_A(M, N)$; on peut montrer que le quotient $\mathrm{Ext}^1_A(M, N) = Ext^1_A(M, N)/\sim$ est un ensemble [3]. Pour $\xi \in Ext^1_A(M, N)$, on note $[\xi] \in \mathrm{Ext}^1_A(M, N)$ sa classe d'équivalence.

3. On peut trouver un A-module libre F et un épimorphisme $h : F \to M$. Pour toute suite exacte ξ, cet épimorphisme h se factorise à travers E et s'écrit donc $g \circ k$, avec $k : F \to E$. Alors $\begin{pmatrix} f & k \end{pmatrix} : N \oplus F \to E$ est encore un épimorphisme, de noyau disons K. L'extension ξ est alors équivalente à une extension de la forme $0 \to N \to (N \oplus F)/K \to M \to 0$. On se ramène ainsi à une description à l'intérieur d'ensembles : ensemble des sous-modules de $N \oplus F$, groupes d'homomorphisme.

On munit $\mathrm{Ext}^1_A(M,N)$ d'une structure de groupe abélien de la façon suivante. Prenons deux extensions

$$\xi:\ 0\to N\xrightarrow{f} E\xrightarrow{g} M\to 0 \quad\text{et}\quad \xi':\ 0\to N\xrightarrow{f'} E'\xrightarrow{g'} M\to 0.$$

Définissons deux sous-modules de $E\oplus E'$ par

$$K=\{(e,e')\mid g(e)=g'(e')\}\quad\text{et}\quad L=\{(f(n),-f'(n))\mid n\in N\}.$$

Alors K contient L. On pose $E''=K/L$ et on contemple les homomorphismes

$$f'':\begin{pmatrix} N\to E''\\ n\mapsto (f(n),0)+L\end{pmatrix}\quad\text{et}\quad g'':\begin{pmatrix} E''\to M\\ (e,e')+L\mapsto g(e)\end{pmatrix}.$$

Alors la suite

$$\xi'':\ 0\to N\xrightarrow{f''} E''\xrightarrow{g''} M\to 0$$

est exacte et sa classe d'équivalence ne dépend que des classes d'équivalence de ξ et ξ'. Ceci nous autorise à définir $[\xi]+[\xi']=[\xi'']$. On montre aisément que cette opération $+$ (appelée somme de Baer) est associative et commutative. Il est clair par ailleurs que les suites exactes courtes scindées forment une classe d'équivalence dans $Ext^1_A(M,N)$, c'est-à-dire un élément de $\mathrm{Ext}^1_A(M,N)$; cet élément est en fait l'élément neutre pour la structure de groupe abélien sur $\mathrm{Ext}^1_A(M,N)$. Enfin l'opposé de $[\xi]$ est la classe de la suite exacte

$$0\to N\xrightarrow{-f} E\xrightarrow{g} M\to 0.$$

Prenons à présent des homomorphismes $f:M'\to M$ et $g:N\to N'$ de A-modules. À une classe $[\xi]\in\mathrm{Ext}^1_A(M,N)$ représentée par la suite exacte courte

$$\xi:\ 0\to N\to E\to M\to 0,$$

on associe les suites exactes $f^*\xi$ et $g_*\xi$ obtenues par des diagrammes pullback et pushout (voir les exercices (5) et (6) du paragraphe 1.1.3) :

$$\begin{array}{lccccccc}
f^*\xi: & 0 & \longrightarrow & N & \longrightarrow & P & \longrightarrow & M' & \longrightarrow & 0\\
 & & & \| & & \downarrow & & \downarrow f & & \\
\xi: & 0 & \longrightarrow & N & \longrightarrow & E & \longrightarrow & M & \longrightarrow & 0\\
 & & & \downarrow g & & \downarrow & & \| & & \\
g_*\xi: & 0 & \longrightarrow & N' & \longrightarrow & Q & \longrightarrow & M & \longrightarrow & 0.
\end{array}$$

Les classes d'équivalence de $f^*\xi$ et de $g_*\xi$ ne dépendent pas du choix de ξ dans sa classe. On obtient ainsi deux foncteurs $\mathrm{Ext}^1_A(?,N)$ et $\mathrm{Ext}^1_A(M,?)$ en posant $\mathrm{Ext}^1_A(f,N)[\xi]=[f^*\xi]$ et $\mathrm{Ext}^1_A(M,g)[\xi]=[g_*\xi]$; ces foncteurs vont de la catégorie des A-modules vers celle des groupes abéliens ; le premier est contravariant et le second covariant. (Il faut vérifier l'axiome concernant la composition des homomorphismes, mais cela n'est pas difficile.) Ces foncteurs sont additifs. On montre aussi l'égalité $\mathrm{Ext}^1_A(f,N')\circ\mathrm{Ext}^1_A(M,g)=\mathrm{Ext}^1_A(M',g)\circ\mathrm{Ext}^1_A(f,N)$, en tant qu'homomorphismes de groupes de $\mathrm{Ext}^1_A(M,N)$ dans $\mathrm{Ext}^1_A(M',N')$; l'application composée est généralement notée $\mathrm{Ext}^1(f,g)$.

Pour finir, considérons une suite exacte courte de A-modules

$$\xi : \ 0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$$

et un A-module X. Alors on a une suite exacte longue de groupes abéliens

$$\begin{aligned} 0 \longrightarrow \mathrm{Hom}_A(X,L) &\xrightarrow{\mathrm{Hom}_A(X,f)} \mathrm{Hom}_A(X,M) \xrightarrow{\mathrm{Hom}_A(X,g)} \mathrm{Hom}_A(X,N) \longrightarrow \\ &\longrightarrow \mathrm{Ext}^1_A(X,L) \xrightarrow{\mathrm{Ext}^1_A(X,f)} \mathrm{Ext}^1_A(X,M) \xrightarrow{\mathrm{Ext}^1_A(X,g)} \mathrm{Ext}^1_A(X,N) \end{aligned}$$

dans laquelle l'homomorphisme de $\mathrm{Hom}_A(X,N)$ dans $\mathrm{Ext}^1_A(X,L)$ (appelé « homomorphisme de liaison ») est $h \mapsto \mathrm{Ext}^1_A(h,L)[\xi]$.

Soit de même Y un A-module. Alors on a une suite exacte longue de groupes abéliens

$$\begin{aligned} 0 \longrightarrow \mathrm{Hom}_A(N,Y) &\xrightarrow{\mathrm{Hom}_A(g,Y)} \mathrm{Hom}_A(M,Y) \xrightarrow{\mathrm{Hom}_A(f,Y)} \mathrm{Hom}_A(L,Y) \longrightarrow \\ &\longrightarrow \mathrm{Ext}^1_A(N,Y) \xrightarrow{\mathrm{Ext}^1_A(g,Y)} \mathrm{Ext}^1_A(M,Y) \xrightarrow{\mathrm{Ext}^1_A(f,Y)} \mathrm{Ext}^1_A(L,Y) \end{aligned}$$

dans laquelle l'homomorphisme de $\mathrm{Hom}_A(L,Y)$ dans $\mathrm{Ext}^1_A(N,Y)$ est $k \mapsto \mathrm{Ext}^1_A(N,k)[\xi]$.

Il serait ici logique d'écrire Ext^0 au lieu de Hom. On pourrait alors poursuivre indéfiniment vers la droite les suites exactes ci-dessus en introduisant des foncteurs additifs $\mathrm{Ext}^i_A(X,?)$ et $\mathrm{Ext}^i_A(?,Y)$ de la catégorie des A-modules vers celle des $\mathbf{Z}$-modules pour $i > 1$. La construction la plus simple de ces foncteurs consiste à définir $\mathrm{Ext}^i_A(M,N)$ comme un ensemble de classes d'équivalence de suites exactes de la forme

$$0 \to N \to E_i \to E_{i-1} \to \cdots \to E_2 \to E_1 \to M \to 0\,;$$

la relation d'équivalence est toutefois un peu plus compliquée à décrire que dans le cas $i = 1$. Une seconde méthode, plus commune mais moins concrète, consiste à se placer dans le cadre général de l'algèbre homologique. On peut vérifier que toutes ces constructions donnent la même chose, mais c'est assez fastidieux.

Signalons enfin que si L, M et N sont trois A-modules et si i et j sont deux entiers naturels, alors on dispose d'un « produit de Yoneda » de $\mathrm{Ext}^j_A(M,N) \times \mathrm{Ext}^i_A(L,M)$ dans $\mathrm{Ext}^{i+j}_A(L,N)$. Concrètement, pour $i = j = 0$, ce produit est le produit de composition $\circ$ des homomorphismes. Si i et j sont strictement positifs, le produit des classes des deux suites exactes

$$0 \to M \to E_i \to \cdots \to E_1 \to L \to 0$$

$$0 \to N \to F_j \to \cdots \to F_1 \to M \to 0$$

est la classe de la suite exacte figurant en première ligne du diagramme

$$\begin{array}{ccccccccccccc} 0 & \to & N & \to & F_j & \to \cdots \to & F_1 & \longrightarrow & E_i & \to \cdots \to & E_1 & \to & L \to 0. \\ & & & & & & & \searrow & \uparrow & & & & \\ & & & & & & & & M & & & & \\ & & & & & & & \nearrow & \searrow & & & & \\ & & & & & & 0 & & & 0 & & & \end{array}$$

(En comparant cette définition avec le diagramme présenté à la fin du paragraphe 1.1.3, on voit ici que chaque élément de $\mathrm{Ext}^i_A(M,N)$ s'écrit comme produit d'éléments appartenant à des $\mathrm{Ext}^1_A(X,Y)$.) Si $i=0$ et $j>0$, le produit de $[\xi]\in\mathrm{Ext}^j_A(M,N)$ par $f\in\mathrm{Hom}_A(L,M)$ coïncide avec $\mathrm{Ext}^j_A(f,N)[\xi]$ et est donné par une construction de type pullback. Pour $i>0$ et $j=0$, le produit de $f\in\mathrm{Hom}_A(M,N)$ par $[\xi]\in\mathrm{Ext}^i_A(L,M)$ coïncide avec $\mathrm{Ext}^i_A(L,f)[\xi]$ et est donné par une construction de type pushout. Notons enfin que pour $L=M=N$, le produit de Yoneda munit le groupe additif $\mathrm{Ext}^\bullet_A(M,M)=\bigoplus_{i\in\mathbf{N}}\mathrm{Ext}^i_A(M,M)$ d'une structure d'anneau $\mathbf{N}$-gradué, le neutre multiplicatif étant id_M.

Exercice. On considère la situation donnée par le diagramme suivant dans la catégorie des A-modules.

$$\begin{array}{rccccccccc} & & & & & & & & X & \\ & & & & & & & & \downarrow{\scriptstyle h} & \\ \xi: & 0 & \longrightarrow & L & \xrightarrow{f} & M & \xrightarrow{g} & N & \longrightarrow & 0 \\ & & & \downarrow{\scriptstyle k} & & & & & & \\ & & & Y & & & & & & \end{array}$$

(i) Prouver que $\mathrm{Ext}^1_A(h,L)[\xi]=0$ dans $\mathrm{Ext}^1_A(X,L)$ si et seulement s'il existe un homomorphisme $s:X\to M$ tel que $h=gs$.

(ii) Prouver que $\mathrm{Ext}^1_A(N,k)[\xi]=0$ dans $\mathrm{Ext}^1_A(N,Y)$ si et seulement s'il existe un homomorphisme $t:M\to Y$ tel que $k=tf$.

(Cet exercice demande de vérifier que les suites longues indiquées plus haut sont exactes en $\mathrm{Hom}_A(X,N)$ et $\mathrm{Hom}_A(L,Y)$, respectivement.)

1.1.6 Modules injectifs et projectifs

L'intérêt premier de ces notions réside dans leur rôle en algèbre homologique. Je n'aborderai pas cet aspect des choses.

Modules projectifs : Un A-module P est dit projectif si le foncteur $\mathrm{Hom}_A(P,?)$ est exact.

1.1.6.1 Proposition. *Pour qu'un coproduit $\coprod_{i\in I}P_i$ de A-modules soit projectif, il faut et il suffit que chaque facteur P_i soit projectif.*

Preuve. Soit $L\xrightarrow{f}M\xrightarrow{g}N$ une suite exacte de A-modules. Son image par le foncteur

$$\mathrm{Hom}_A\left(\coprod_{i\in I}P_i,?\right)\cong\prod_{i\in I}\mathrm{Hom}_A(P_i,?)$$

est de la forme

$$\prod_{i\in I}\mathrm{Hom}_A(P_i,L)\xrightarrow{\prod_{i\in I}\mathrm{Hom}_A(P_i,f)}\prod_{i\in I}\mathrm{Hom}_A(P_i,M)\xrightarrow{\prod_{i\in I}\mathrm{Hom}_A(P_i,g)}\prod_{i\in I}\mathrm{Hom}_A(P_i,N).$$

Pour que cette suite de groupes abéliens soit exacte, il faut et il suffit que chacune des suites

$$\mathrm{Hom}_A(P_i, L) \xrightarrow{\mathrm{Hom}_A(P_i,f)} \mathrm{Hom}_A(P_i, M) \xrightarrow{\mathrm{Hom}_A(P_i,g)} \mathrm{Hom}_A(P_i, N)$$

soit exacte. Autrement dit, pour que le A-module $\coprod_{i\in I} P_i$ soit projectif, il faut et il suffit que chacun des A-modules P_i soit projectif. □

Scolie. Le A-module à gauche régulier ${}_AA$ est projectif, puisque qu'on a un isomorphisme $\mathrm{Hom}_A({}_AA, M) \cong M$ naturel en M. La proposition ci-dessus entraîne alors qu'un A-module libre est projectif. On en déduit qu'un module facteur direct d'un module libre est projectif : si deux modules P et P' sont tels que $P \oplus P'$ est libre, alors P et P' sont projectifs.

1.1.6.2 Proposition. *Soit P un A-module. Les cinq assertions suivantes sont équivalentes.*

(i) P est un A-module projectif.

(ii) Pour tout épimorphisme $g : M \to N$ de A-modules et tout homomorphisme $h : P \to N$, il existe $k \in \mathrm{Hom}_A(P, M)$ faisant commuter le diagramme

$$\begin{array}{ccccc} & & & & P \\ & & & \swarrow^{k} & \downarrow{\scriptstyle h} \\ M & \xrightarrow[g]{} & N & \longrightarrow & 0. \end{array}$$

(iii) Toute suite exacte courte $0 \to L \to M \to P \to 0$ est scindée.

(iv) Pour tout A-module L, $\mathrm{Ext}^1_A(P, L) = 0$.

(v) P est un facteur direct d'un A-module libre.

Preuve. Supposons (i) vraie. Dans la situation de (ii), la suite $M \xrightarrow{g} N \to 0$ est exacte. L'assertion (i) dit alors que la suite $\mathrm{Hom}_A(P, M) \xrightarrow{\mathrm{Hom}_A(P,g)} \mathrm{Hom}_A(P, N) \to 0$ est elle aussi exacte. Ainsi $\mathrm{Hom}_A(P, g)$ est surjectif. L'homomorphisme h est donc l'image par $\mathrm{Hom}_A(P, g)$ d'un certain homomorphisme k. Cela établit (ii).

Réciproquement, supposons (ii). Pour montrer que le foncteur $\mathrm{Hom}_A(P, ?)$ est exact, il suffit de montrer que l'image qu'il donne d'une suite exacte courte $0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$ est une suite exacte courte. On sait déjà que

$$0 \to \mathrm{Hom}_A(P, L) \xrightarrow{\mathrm{Hom}_A(P,f)} \mathrm{Hom}_A(P, M) \xrightarrow{\mathrm{Hom}_A(P,g)} \mathrm{Hom}_A(P, N)$$

est exacte. (ii) donne alors la surjectivité de $\mathrm{Hom}_A(P, g)$ et c'est gagné.

Supposons (ii) et considérons une suite exacte courte $0 \to L \to M \xrightarrow{g} P \to 0$. En prenant $N = P$ et $h = \mathrm{id}_P$, le (ii) donne $k : P \to M$ tel que $g \circ k = h = \mathrm{id}_P$. C'est une des conditions qui assure que notre suite exacte courte est scindée. Cela montre (iii).

Réciproquement, supposons (iii) vraie et prenons un épimorphisme $g : M \to N$ et un homomorphisme $h : P \to N$. Nous pouvons introduire le noyau de g et construire le pullback

$$\begin{array}{ccccc} & & L & \xrightarrow{g'} & P \\ & & {\scriptstyle h'}\downarrow & & \downarrow{\scriptstyle h} \\ 0 & \longrightarrow \ker g \longrightarrow & M & \xrightarrow[g]{} & N. \end{array}$$

On peut identifier le noyau de g' avec celui de g. La surjectivité de g entraîne celle de g'. On obtient ainsi une suite exacte courte $0 \to \ker g \to L \xrightarrow{g'} P \to 0$. L'assertion (iii), supposée vraie, dit que cette suite est scindée, d'où l'existence d'un homomorphisme $f : P \to L$ tel que $g' \circ f = \mathrm{id}_P$. L'homomorphisme $k = h' \circ f$ de P dans M vérifie $g \circ k = h$. (ii) est donc vérifiée.

L'équivalence des assertions (iii) et (iv) provient de la définition de Ext^1_A.

Nous avons déjà vu que (v) implique (i). Montrons que (iii) implique (v). Il existe un homomorphisme surjectif g d'un module libre, disons F, sur P. On dispose ainsi d'une suite exacte courte $0 \to \ker g \to F \xrightarrow{g} P \to 0$. D'après (iii), cette suite est scindée, de sorte qu'il existe un sous-module P' de F tel que $F = \ker g \oplus P'$. Ce module P', qui est isomorphe à P, est facteur direct du module libre F. Ceci établit (v). □

L'intérêt des modules projectifs est qu'ils offrent les mêmes facilités que les modules libres, avec en outre la propriété d'être stables par passage aux facteurs directs. La proposition suivante dit que dans un module projectif, il est parfois possible de raisonner comme s'il y avait un système de coordonnées.

1.1.6.3 Lemme de la base duale. *Un A-module à gauche est projectif si et seulement s'il existe deux familles d'éléments $(e_i) \in P^I$ et $(e^i) \in \mathrm{Hom}_A(P, A)^I$ telles que pour chaque $x \in P$, l'ensemble $\{i \in I \mid e^i(x) \neq 0\}$ soit fini et $x = \sum_{i \in I} e^i(x) e_i$. De plus, chaque famille génératrice peut être utilisée pour jouer le rôle de (e_i) ; réciproquement, chaque famille jouant le rôle de (e_i) est génératrice.*

Preuve. Supposons que P soit projectif. Soit $(e_i)_{i \in I}$ une famille génératrice du A-module P. L'homomorphisme $g : (a_i)_{i \in I} \mapsto \sum_{i \in I} a_i e_i$ de $A^{(I)}$ dans P est surjectif. La condition (iii) de la proposition 1.1.6.2 dit que la suite $0 \to \ker g \to A^{(I)} \xrightarrow{g} P \to 0$ est scindée, d'où un homomorphisme $k : P \to A^{(I)}$ tel que $g \circ k = \mathrm{id}_P$. Les homomorphismes $e^i : P \to A$ définis par l'égalité $k(x) = (e^i(x))_{i \in I}$ pour tout $x \in P$ vérifient les conditions requises.

Réciproquement, supposons avoir deux familles (e_i) et (e^i) comme dans l'énoncé. On définit deux homomorphismes $g : A^{(I)} \to P$ et $k : P \to A^{(I)}$ de la façon suivante : on pose $g\big((a_i)_{i \in I}\big) = \sum_{i \in I} a_i e_i$, de sorte que g envoie la base canonique du module libre $A^{(I)}$ sur la famille $(e_i)_{i \in I}$; on pose $k(x) = (e^i(x))_{i \in I}$ pour tout $x \in P$. Alors $g \circ k = \mathrm{id}_P$, ce qui implique que la suite $0 \to \ker g \to A^{(I)} \xrightarrow{g} P \to 0$ est exacte et scindée. Ainsi $A^{(I)} \cong P \oplus \ker g$, de sorte que la condition (v) de la proposition 1.1.6.2 est vérifiée. Le A-module P est donc projectif. □

Signalons enfin qu'il y a des anneaux sur lesquels tout module projectif de type fini est libre : c'est le cas des anneaux locaux (voir le paragraphe 2.3.1) ou des anneaux de polynômes en un nombre fini d'indéterminées à coefficients dans un corps (théorème de Quillen-Suslin).

Modules injectifs : Un A-module Q est dit injectif si le foncteur $\mathrm{Hom}_A(?, Q)$ est exact.

1.1.6.4 Proposition. *Pour qu'un produit $\prod_{i\in I} Q_i$ de A-modules soit injectif, il faut et il suffit que chaque facteur Q_i soit injectif.*

Preuve. La preuve est identique à celle de la proposition correspondante pour les modules projectifs, à ceci près qu'on remplace coproduit par produit et qu'on utilise l'isomorphisme de foncteurs

$$\mathrm{Hom}_A\left(?, \prod_{i\in I} Q_i\right) \cong \prod_{i\in I} \mathrm{Hom}_A(?, Q_i).$$

□

1.1.6.5 Proposition. *Soit Q un A-module. Les cinq assertions suivantes sont équivalentes.*

(i) Q est un A-module injectif.

(ii) Pour tout monomorphisme $f : L \to M$ de A-modules et tout homomorphisme $h : L \to Q$, il existe $k \in \mathrm{Hom}_A(M, Q)$ faisant commuter le diagramme

$$\begin{array}{ccccc} 0 & \longrightarrow & L & \xrightarrow{f} & M \\ & & {\scriptstyle h}\downarrow & \swarrow_{k} & \\ & & Q. & & \end{array}$$

(iii) Toute suite exacte courte $0 \to Q \to M \to N \to 0$ est scindée.

(iv) Pour tout A-module N, $\mathrm{Ext}^1_A(N, Q) = 0$.

(v) Pour chaque idéal à gauche I de A et chaque $h \in \mathrm{Hom}_A(I, Q)$, il existe $k \in \mathrm{Hom}_A(A, Q)$ tel que $h = k\,\big|_I$.

Preuve. La preuve de l'équivalence des assertions (i), (ii), (iii) et (iv) est semblable à ce qui a été vu plus haut pour les modules projectifs et est omise.

(v) est le cas particulier de (ii) quand f est l'injection de l'idéal à gauche I dans A ; donc (ii) implique (v). Réciproquement, supposons (v) et montrons (ii). Plaçons-nous dans la situation de (ii), à ceci près qu'on identifie L au sous-module $f(L)$ de M. Soit $\mathscr{M}$ l'ensemble des couples (N, k) où N est un sous-module de M contenant L et $k : N \to Q$ est un homomorphisme prolongeant h. On écrit $(N, k) \preccurlyeq (N', k')$ si $N \subseteq N'$ et si k' prolonge k ; ainsi $\preccurlyeq$ est un ordre partiel sur $\mathscr{M}$. Certainement $\mathscr{M}$ est non-vide car il contient (L, h).

L'ensemble ordonné $\mathscr{M}$ est inductif. De fait, si $\mathscr{N}$ est une partie non-vide totalement ordonnée de $\mathscr{M}$, on pose $P = \bigcup_{(N,k)\in\mathscr{N}} N$ et on définit $q : P \to Q$ en recollant les homomorphismes $k : N \to Q$. On vérifie sans difficulté que (P, q) est un majorant de $\mathscr{N}$ dans $\mathscr{M}$.

D'après le lemme de Zorn, $\mathscr{M}$ admet donc un élément maximal, disons (N, k). Soit $x \in M$. L'ensemble $I = \{a \in A \mid ax \in N\}$ est un idéal à gauche de A. L'homomorphisme de A-modules $\tilde{n} : a \mapsto k(ax)$ de I dans Q se prolonge en un homomorphisme $\tilde{k}$ de A dans Q. En combinant k et $\tilde{k}$, on obtient un prolongement k' de k au sous-module $N' = N + Ax$ de M. (Chaque élément $n' \in N'$ s'écrit $n + ax$ avec $n \in N$ et $a \in A$; l'élément $k'(n') = k(n) + \tilde{k}(a)$ est alors indépendant du choix de la décomposition $n' = n + ax$ utilisée.) L'inégalité $(N, k) \preccurlyeq (N', k')$ et la maximalité de (N, k) conduisent alors à $N = N'$, donc à $x \in N$. Ainsi $N = M$, ce qui établit (ii). □

Exemple. Soit A un anneau principal. Le (v) de la proposition dit qu'un A-module Q est injectif si et seulement si il est divisible, c'est-à-dire si et seulement si pour tout $a \in A$ et $x \in Q$, il existe $y \in Q$ tel que $x = ay$. Ainsi les $\mathbf{Z}$-modules $\mathbf{Q}$ et $\mathbf{Q}/\mathbf{Z}$ sont injectifs.

1.1.6.6 Proposition. *Tout A-module peut être plongé dans un A-module injectif.*

Preuve. Regardons d'abord le cas particulier $A = \mathbf{Z}$. Un $\mathbf{Z}$-module M quelconque est toujours isomorphe à un quotient $\mathbf{Z}^{(I)}/K$ d'un module libre. Maintenant $\mathbf{Z}^{(I)}/K$ est un sous-module de $\mathbf{Q}^{(I)}/K$, et ce dernier est un $\mathbf{Z}$-module divisible. L'exemple ci-dessus nous dit donc que nous avons réussi à plonger M dans un $\mathbf{Z}$-module injectif.

Venons-en au cas général. Soit M un A-module. Il existe un monomorphisme de $\mathbf{Z}$-modules i de M dans un $\mathbf{Z}$-module injectif E. On munit $\mathrm{Hom}_{\mathbf{Z}}(A, E)$ d'une structure de A-module en posant $af = (b \mapsto f(ba))$, pour $a \in A$ et $f \in \mathrm{Hom}_{\mathbf{Z}}(A, E)$. Les deux foncteurs $\mathrm{Hom}_{\mathbf{Z}}(?, E)$ et $\mathrm{Hom}_A(?, \mathrm{Hom}_{\mathbf{Z}}(A, E))$ de la catégorie des A-modules dans la catégorie des $\mathbf{Z}$-modules sont canoniquement isomorphes [4]. Le foncteur $\mathrm{Hom}_{\mathbf{Z}}(?, E)$ étant exact [5], il en est de même de $\mathrm{Hom}_A(?, \mathrm{Hom}_{\mathbf{Z}}(A, E))$. Ainsi $\mathrm{Hom}_{\mathbf{Z}}(A, E)$ est un A-module injectif. □

Exercice. (Lemme de Schanuel) Étant données deux suites exactes de A-modules

$$0 \to L \to P \to X \to 0 \quad \text{et} \quad 0 \to L' \to P' \to X \to 0$$

4. Au niveau des objets, l'isomorphisme s'obtient ainsi, pour tout A-module M : à f dans $\mathrm{Hom}_{\mathbf{Z}}(M, E)$, on associe $m \mapsto (a \mapsto f(am))$ dans $\mathrm{Hom}_A(M, \mathrm{Hom}_{\mathbf{Z}}(A, E))$; à g dans $\mathrm{Hom}_A(M, \mathrm{Hom}_{\mathbf{Z}}(A, E))$, on associe $m \mapsto g(m)(1)$ dans $\mathrm{Hom}_{\mathbf{Z}}(M, E)$. Cet isomorphisme se comprend mieux en termes de produit tensoriel :

$$\mathrm{Hom}_A(?, \mathrm{Hom}_{\mathbf{Z}}(A, E)) \cong \mathrm{Hom}_{\mathbf{Z}}(A \otimes_A ?, E) \cong \mathrm{Hom}_{\mathbf{Z}}(?, E),$$

voir à ce sujet le corollaire 1.4.1.2.

5. Le lecteur attentif aura remarqué un petit raccourci dans la preuve. Le foncteur $\mathrm{Hom}_{\mathbf{Z}}(?, E)$ va a priori de la catégorie des $\mathbf{Z}$-module dans elle-même. Ici, je regarde sa restriction à la catégorie des A-modules. La restriction est encore un foncteur exact, car toute suite exacte de A-modules est une suite exacte de $\mathbf{Z}$-modules. Le point est que le noyau et l'image d'un homomorphisme ne changent pas, qu'on le regarde comme un homomorphisme de A-modules ou de $\mathbf{Z}$-modules.

avec P et P' projectifs, il existe un isomorphisme $L' \oplus P \cong L \oplus P'$.
(Indication : introduire le diagramme pullback

$$\begin{array}{ccc} Y & \longrightarrow & P \\ \downarrow & & \downarrow \\ P' & \longrightarrow & X, \end{array}$$

et en utilisant l'exercice (4) du paragraphe 1.1.3, montrer l'existence de deux suites exactes $0 \to L' \to Y \to P \to 0$ et $0 \to L \to Y \to P' \to 0$.)

1.2 Dévissage des modules

1.2.1 Conditions de finitude

Module de type fini : un A-module est dit de type fini s'il est engendré par un nombre fini d'éléments.

Tout quotient d'un module de type fini est de type fini.

1.2.1.1 Proposition. *Soit M un A-module de type fini et $L \subsetneq M$ un sous-module strict de M. Alors il existe un sous-module N contenant L et maximal.*

Preuve. Soit $S \subseteq M$ une partie finie et génératrice. Certainement L ne contient pas S. Appelons $\mathscr{M}$ l'ensemble des sous-modules de M contenant L et ne contenant pas S, et ordonnons $\mathscr{M}$ par la relation usuelle d'inclusion. Alors $\mathscr{M}$ est non-vide (il contient L) et inductif.

En effet, soit $\mathscr{N}$ une partie non-vide totalement ordonnée de $\mathscr{M}$. On vérifie sans difficulté que $P = \bigcup_{N \in \mathscr{N}} N$ est un sous-module de M. Si S était inclus dans P, alors chaque élément de S appartiendrait à un $N \in \mathscr{N}$; puisque S est fini et $\mathscr{N}$ totalement ordonnée, on trouverait alors un $N \in \mathscr{N}$ contenant tous les éléments de S, en contradiction avec la définition de $\mathscr{M}$. Ainsi P appartient à $\mathscr{M}$, et il majore évidemment $\mathscr{N}$.

Ayant établi que $\mathscr{M}$ est un ensemble ordonné non-vide et inductif, nous pouvons appliquer le lemme de Zorn et obtenir l'existence d'un élément maximal dans $\mathscr{M}$, autrement dit l'existence d'un élément maximal parmi les sous-modules stricts de M contenant L. □

Module noethérien : un A-module M est dit noethérien si toute suite croissante de sous-modules de M stationne à partir d'un certain rang.

1.2.1.2 Proposition. *Soit A un anneau.*

(i) Étant donné un A-module M, les trois assertions suivantes sont équivalentes :

(a) M est noethérien.

(b) Tout ensemble non-vide de sous-modules de M possède un élément maximal pour l'inclusion.

(c) Tout sous-module de M est de type fini.

(ii) Soit N un sous-module d'un A-module M. Alors M est noethérien si et seulement si N et M/N sont noethériens.

(iii) Soit M un A-module et $n \in \mathbf{N}$. Si M est noethérien, alors M^n est noethérien.

Preuve. (i) Supposons que (b) soit fausse et montrons que (a) l'est aussi. Puisque (b) n'est pas vraie, il existe un ensemble non-vide $\mathscr{N}$ de sous-modules de M n'ayant pas d'élément maximal. Nous pouvons alors construire par récurrence une suite strictement croissante d'éléments de $\mathscr{N}$: on prend $N_0 \in \mathscr{N}$, et supposant N_0, ..., N_n construits, on choisit $N_{n+1} \in \mathscr{N}$ contenant strictement N_n (cela est possible car N_n n'est pas un élément maximal de $\mathscr{N}$). Ainsi (a) n'est pas vraie.

Montrons maintenant que (b) implique (c). Soit N un sous-module de M. Notons $\mathscr{N}$ l'ensemble des sous-modules de N qui sont de type fini. Certainement $\mathscr{N}$ est non-vide ; d'après l'hypothèse (b), il contient donc un élément maximal, disons L. Soit $x \in N$. Le module L étant de type fini, il en est de même du sous-module $L + Ax$; ainsi $L + Ax \in \mathscr{N}$. Comme $L + Ax$ contient L, la maximalité de L dans $\mathscr{N}$ force $L = L + Ax$, et donc $x \in L$. Ceci étant vrai pour tout $x \in N$, les sous-modules L et N sont égaux. Ainsi N est de type fini. L'assertion (c) est donc vraie.

Montrons maintenant que (c) entraîne (a). On suppose (c) vraie. Soit $(N_n)_{n\in\mathbf{N}}$ une suite croissante de sous-modules de M. Alors $N = \bigcup_{n\in\mathbf{N}} N_n$ est un sous-module de M. D'après (c), N est engendré par un ensemble fini S d'éléments. Chaque élément de S appartient à un N_n, et puisque la suite de sous-modules est croissante et que S est fini, il existe un rang n pour lequel tous les éléments de S appartiennent à N_n. Alors le sous-module N est inclus dans N_n. Pour $p \geq n$, on a alors $N \subseteq N_n \subseteq N_p \subseteq N$. La suite $(N_n)_{n\in\mathbf{N}}$ stationne donc à partir du rang n. L'assertion (a) est établie.

On aurait pu prouver que (b) impliquait (a) directement, sans passer par (c), de la façon suivante. Supposons (b). Soit $(N_n)_{n\in\mathbf{N}}$ une suite croissante de sous-modules de M. L'ensemble $\mathscr{N}$ des sous-modules N_n est non-vide ; il admet donc un élément maximal, disons N_n. Pour $p \geq n$, on a $N_n \subseteq N_p$ car la suite est croissante. Comme N_n est un élément maximal de $\mathscr{N}$, ceci force $N_n = N_p$. Ainsi la suite $(N_n)_{n\in\mathbf{N}}$ stationne à partir du rang n.

(ii) Soit N un sous-module d'un A-module M. Supposons que N et M/N soient noethériens et montrons que M est noethérien. Soit $(L_n)_{n\in\mathbf{N}}$ une suite croissante de sous-modules de M. Alors $(L_n \cap N)_{n\in\mathbf{N}}$ est une suite croissante de sous-modules de N, donc elle stationne à partir d'un certain rang. De même, $((L_n + N)/N)_{n\in\mathbf{N}}$ est une suite croissante de sous-modules de M/N, donc elle stationne à partir d'un certain rang. Pour n assez grand, on a donc $L_n \cap N = L_{n+1} \cap N$ et $L_n + N = L_{n+1} + N$. Cela entraîne que l'inclusion $L_n \subseteq L_{n+1}$ est une égalité. (C'est un exercice facile et standard : chaque $x \in L_{n+1}$ s'écrit $y+n$ avec $y \in L_n$ et $n \in N$; alors $n = x - y \in L_{n+1} \cap N$, donc $n \in L_n$ et finalement $x = y + n \in L_n$.) Bref $(L_n)_{n\in\mathbf{N}}$ stationne à partir d'un certain rang. Nous avons établi que M est noethérien. La preuve de l'implication inverse (si M est noethérien, alors N et M/N sont noethériens) découle presque directement des définitions ; la rédaction des détails est laissée au lecteur.

(iii) Pour chaque entier naturel n, on dispose d'une suite exacte courte (et même scindée) $0 \to M \xrightarrow{f} M^{n+1} \xrightarrow{g} M^n \to 0$, où $f(m) = (m, 0, \ldots, 0)$ et $g(m_0, m_1, \ldots, m_n) = (m_1, \ldots, m_n)$. Un raisonnement par récurrence basé sur l'assertion (ii) permet alors d'établir (iii). □

Module artinien : un A-module M est dit artinien si toute suite décroissante de sous-modules de M stationne à partir d'un certain rang.

1.2.1.3 Proposition. *Soit A un anneau.*

(i) Un A-module M est artinien si et seulement si tout ensemble non-vide de sous-modules de M possède un élément minimal pour l'inclusion.

(ii) Soit N un sous-module d'un A-module M. Alors M est artinien si et seulement si N et M/N sont artiniens.

(iii) Soit M un A-module et $n \in \mathbf{N}$. Si M est artinien, alors M^n est artinien.

Module de présentation finie : un A-module M est dit de présentation finie s'il existe une suite exacte de A-modules de la forme $A^m \to A^n \to M \to 0$. En d'autres termes, on demande l'existence d'un système fini de générateurs $(m_i)_{1 \leq i \leq n}$ de M pour lequel le sous-module des relations (c'est-à-dire le noyau de l'homomorphisme $A^n \to M$ qui envoie le i-ème élément de la base canonique de A^n sur m_i) est de type fini.

Exemples.

(1) Le $\mathbf{Z}$-module régulier est noethérien mais pas artinien.

(2) Si p est un nombre premier, alors le $\mathbf{Z}$-module $\mathbf{Z}[\frac{1}{p}]/\mathbf{Z}$ est artinien mais pas noethérien. (Les sous-modules propres de $\mathbf{Z}[\frac{1}{p}]/\mathbf{Z}$ sont les $\{a/p^n + \mathbf{Z} \mid a \in \mathbf{Z}\}$, pour $n \in \mathbf{N}$; ils forment une suite strictement croissante pour l'inclusion.)

Exercices.

(1) Si M est un A-module de type fini, une décomposition en somme directe $M = \bigoplus_{i \in I} M_i$ n'a qu'un nombre fini de termes non-nuls [6].

(2) Soient M un A-module et $f \in \mathrm{End}_A(M)$. Montrer que si M est noethérien et f est surjective, alors f est injective. Montrer que si M est artinien et f est injective, alors f est surjective. (Indication : mimer la preuve du lemme de Fitting ci-dessous.)

1.2.2 Théorème de Krull-Schmidt

1.2.2.1 Lemme de Fitting. *Soit f un endomorphisme d'un A-module M artinien et noethérien. Alors il existe une décomposition $M = f^\infty(M) \oplus f^{-\infty}(0)$ en somme directe de deux sous-modules stables par f, de sorte que la restriction de f à $f^\infty(M)$ soit un automorphisme et que la restriction de f à $f^{-\infty}(0)$ soit nilpotente.*

6. Cet exercice montre en particulier que si A est un anneau non réduit à $\{0\}$, alors un A-module libre $M \cong A^{(I)}$ est de type fini si et seulement si I est un ensemble fini.

Preuve. Puisque M est noethérien, la suite croissante de sous-modules $(\ker f^n)_{n\in\mathbf{N}}$ stationne à partir d'un certain rang. Puisque M est artinien, la suite décroissante de sous-modules $(\operatorname{im} f^n)_{n\in\mathbf{N}}$ stationne à partir d'un certain rang. Il existe donc deux sous-modules $f^{-\infty}(0)$ et $f^\infty(M)$ de M et un entier naturel n tels que $\ker f^p = f^{-\infty}(0)$ et $\operatorname{im} f^p = f^\infty(M)$ pour $p \geq n$. En particulier $f^{-\infty}(0) = \ker f^n = \ker f^{2n}$ et $f^\infty(M) = \operatorname{im} f^n = \operatorname{im} f^{2n}$.

Montrons que $f^{-\infty}(0) \cap f^\infty(M) = 0$: si x appartient à l'intersection, alors x s'écrit $f^n(y)$, et l'égalité $f^n(x) = 0$ entraîne que $y \in \ker f^{2n} = \ker f^n$. Il vient ainsi $x = 0$.

Montrons que $f^{-\infty}(0) + f^\infty(M) = M$: si x appartient à M, alors $f^n(x) \in \operatorname{im} f^n = \operatorname{im} f^{2n}$, d'où l'existence d'un y tel que $f^n(x) = f^{2n}(y)$. Ainsi x est la somme d'un élément de $\ker f^n = f^{-\infty}(0)$ et de $f^n(y) \in \operatorname{im} f^n = f^\infty(M)$.

La restriction de f à $f^{-\infty}(0)$ est nilpotente puisque $f^{-\infty}(0) = \ker f^n$. La restriction de f à $f^\infty(M)$ est injective puisque $\ker f \subseteq f^{-\infty}(0)$ intersecte trivialement $f^\infty(M)$; la restriction de f à $f^\infty(M)$ est surjective puisque $f^n\big(f^\infty(M)\big) = f^n\big(\ker f^n + f^\infty(M)\big) = f^n(M) = f^\infty(M)$. □

Module indécomposable : on dit qu'un A-module M est indécomposable si $M \neq 0$ et s'il n'existe pas de décomposition de M en somme directe $M' \oplus M''$ de deux sous-modules non-nuls.

1.2.2.2 Corollaire. *L'anneau des endomorphismes d'un module indécomposable artinien et noethérien est local.*

Preuve. Donnons-nous un module indécomposable artinien et noethérien, notons B son anneau d'endomorphismes, et posons $J = B \setminus B^\times$. D'après le lemme de Fitting, un élément de B est soit nilpotent, soit inversible (et il ne peut pas être les deux à la fois car B n'est pas le module nul) ; autrement dit, J est l'ensemble des éléments nilpotents de B. Nous voulons montrer que J est un idéal bilatère de B.

Soit $x \in J$. Puisque x est nilpotent, $\ker x \neq 0$ et $\operatorname{coker} x \neq 0$. Alors pour chaque $a \in B$, nous avons $\ker ax \neq 0$ et $\operatorname{coker} xa \neq 0$, ce qui interdit à ax et à xa d'être inversible, et impose donc $ax \in J$ et $xa \in J$. Ainsi J est stable par multiplication par les éléments de B.

Il nous reste à montrer que J est un sous-groupe additif de B. Soient $x, y \in J$. Si $x + y$ n'appartenait pas à J, il serait inversible, d'inverse disons b. Alors bx et by appartiendraient à J et $bx + by = 1$. La nilpotence de by entraînerait alors l'inversibilité de $bx = 1 - by$ (substituer by à z dans la série $(1-z)^{-1} = 1 + z + z^2 + \cdots$), ce qui est exclus. Bref $x + y$ doit appartenir à J. Ainsi J est stable par somme. D'après l'alinéa précédent, J contient 0 et est stable par passage à l'opposé : J est donc bien un sous-groupe. □

1.2.2.3 Proposition. *Soit M un A-module artinien ou noethérien. Alors M s'écrit comme somme directe finie $M = M_1 \oplus \cdots \oplus M_m$ de sous-modules indécomposables.*

Preuve. Pour cette preuve, convenons de dire qu'un module est complètement décomposable s'il peut s'écrire comme somme directe finie de sous-modules indécomposables.

Supposons d'abord M artinien et notons $\mathscr{M}$ l'ensemble des sous-modules de M qui ne sont pas complètement décomposables. Si $\mathscr{M}$ est non-vide, il possède un élément minimal N. Certainement N n'est ni nul, ni indécomposable : on peut donc écrire $N = N_1 \oplus N_2$, avec N_1 et N_2 non-nuls. Par minimalité de N dans $\mathscr{M}$, ni N_1 ni N_2 n'appartiennent à $\mathscr{M}$. Ainsi N_1 et N_2 sont complètement décomposables, de sorte que N l'est : contradiction. Ainsi $\mathscr{M}$ est vide. En particulier M est complètement décomposable.

La preuve du cas où M est noethérien est analogue, à ceci près qu'on introduit l'ensemble $\mathscr{M}$ des sous-modules N de M tels que M/N ne soit pas complètement décomposable et qu'on raisonne en supposant l'existence d'un élément maximal dans $\mathscr{M}$. □

1.2.2.4 Lemme. *Soient $M = M' \oplus M'' = N_1 \oplus N_2 \oplus \cdots \oplus N_n$ deux décompositions d'un A-module en somme directe de sous-modules. On suppose que l'anneau des endomorphismes de M' est local et que les N_i sont indécomposables. Alors il existe $s \in \{1, \ldots, n\}$ tel que $M' \cong N_s$ et $M = N_s \oplus M''$.*

Preuve. Notons

$$\varphi' : M' \to M, \quad \varphi'' : M'' \to M, \quad \psi' : M \to M', \quad \psi'' : M \to M''$$

les inclusions et projections définies par la somme directe $M = M' \oplus M''$; ainsi

$$\begin{pmatrix} \varphi' & \varphi'' \end{pmatrix} \begin{pmatrix} \psi' \\ \psi'' \end{pmatrix} = (\mathrm{id}_M) \quad \text{et} \quad \begin{pmatrix} \psi' \\ \psi'' \end{pmatrix} \begin{pmatrix} \varphi' & \varphi'' \end{pmatrix} = \begin{pmatrix} \mathrm{id}_{M'} & 0 \\ 0 & \mathrm{id}_{M''} \end{pmatrix}. \qquad (*)$$

Pour $t \in \{1, \ldots, n\}$, appelons $i_t : N_t \to N$ et $p_t : M \to N_t$ les inclusions et projections définies par la somme directe $M = N_1 \oplus N_2 \oplus \cdots \oplus N_n$.

Alors $\mathrm{id}_{M'} = \psi' \circ \varphi' = \sum_{t=1}^{n} \psi' \circ i_t \circ p_t \circ \varphi'$. Comme $\mathrm{End}_A(M')$ est un anneau local, un des termes de cette somme est inversible : disons $\psi' \circ i_s \circ p_s \circ \varphi'$. Ce fait entraîne certainement que $p_s \circ \varphi$ est une injection de M' dans N_s et que $\psi \circ i_s$ est une surjection de N_s sur M' ; il entraîne également que $N_s = \mathrm{im}(p_s \circ \varphi') \oplus \ker(\psi' \circ i_s)$. L'indécomposabilité de N_s nous dit alors que le premier terme est N_s et que le second est 0 ; autrement dit, $p_s \circ \varphi'$ est surjectif et $\psi' \circ i_s$ est injectif. Nous avons ainsi deux isomorphismes en sens opposés entre M' et N_s.

Appelons χ l'inverse de la composée $\psi' \circ i_s \circ p_s \circ \varphi'$; ainsi

$$\psi' \circ i_s \circ p_s \circ \varphi' \circ \chi = \mathrm{id}_M \quad \text{et} \quad p_s \circ \varphi' \circ \chi \circ \psi' \circ i_s = \mathrm{id}_{N_s}.$$

Définissons $\widetilde{p}_s : M \to N_s$ et $\widetilde{\psi}'' : M \to M''$ par

$$\widetilde{p}_s = p_s \circ \varphi' \circ \chi \circ \psi' \quad \text{et} \quad \widetilde{\psi}'' = \psi'' \circ (\mathrm{id}_M - i_s \circ p_s \circ \varphi' \circ \chi \circ \psi').$$

Utilisant les égalités précédentes et les relations $(*)$, on vérifie que

$$\begin{pmatrix} i_s & \varphi'' \end{pmatrix} \begin{pmatrix} \widetilde{p}_s \\ \widetilde{\psi}'' \end{pmatrix} = (\mathrm{id}_M) \quad \text{et} \quad \begin{pmatrix} \widetilde{p}_s \\ \widetilde{\psi}'' \end{pmatrix} \begin{pmatrix} i_s & \varphi'' \end{pmatrix} = \begin{pmatrix} \mathrm{id}_{N_s} & 0 \\ 0 & \mathrm{id}_{M''} \end{pmatrix}.$$

Ainsi $M = N_s \oplus M''$, les homomorphismes $\widetilde{p}_s$ et $\widetilde{\psi}''$ étant les projections définies par cette décomposition. □

1.2.2.5 Proposition. *Soient $M = M_1 \oplus \cdots \oplus M_m = N_1 \oplus \cdots \oplus N_n$ deux décompositions d'un A-module en somme directe de sous-modules. On suppose que l'anneau des endomorphismes de chaque M_i est local et que tous les N_i sont indécomposables. Alors $m = n$ et il existe une permutation σ de l'ensemble $\{1, \ldots, n\}$ telle que pour chaque $i \in \{1, \ldots, n\}$, on ait $M_i \cong N_{\sigma(i)}$ et*

$$M = N_{\sigma(1)} \oplus \cdots \oplus N_{\sigma(i)} \oplus M_{i+1} \oplus \cdots \oplus M_m.$$

Preuve. La preuve consiste à construire, par récurrence sur $\ell \in \{0, \ldots, m\}$, une application injective $\sigma : \{1, \ldots, \ell\} \to \{1, \ldots, n\}$ telle que pour chaque $i \in \{1, \ldots, \ell\}$ on ait $M_i \cong N_{\sigma(i)}$ et

$$M = N_{\sigma(1)} \oplus \cdots \oplus N_{\sigma(i)} \oplus M_{i+1} \oplus \cdots \oplus M_n.$$

L'initialisation de la récurrence est banale. Prenons $\ell \in \{1, \ldots, m\}$ et supposons les valeurs $\sigma(1)$, …, $\sigma(\ell - 1)$ construites. Appliquant le lemme 1.2.2.4 aux deux décompositions

$$M = M_\ell \oplus \big(N_{\sigma(1)} \oplus \cdots \oplus N_{\sigma(\ell-1)} \oplus M_{\ell+1} \oplus \cdots \oplus M_n\big) = N_1 \oplus \cdots \oplus N_n$$

on trouve $s \in \{1, \ldots n\}$ tel que $M_\ell \cong N_s$ et

$$M = N_s \oplus \big(N_{\sigma(1)} \oplus \cdots \oplus N_{\sigma(\ell-1)} \oplus M_\ell \oplus \cdots \oplus M_m\big).$$

Ceci implique que $s \notin \{\sigma(1), \ldots, \sigma(\ell - 1)\}$, et il suffit de définir $\sigma(\ell) = s$ pour pouvoir passer au cran suivant.

Une fois la construction achevée, on obtient

$$M = N_{\sigma(1)} \oplus \cdots \oplus N_{\sigma(m)} = N_1 \oplus \cdots \oplus N_n.$$

La comparaison prescrit la bijectivité de σ et l'égalité $m = n$. □

Compte tenu du corollaire 1.2.2.2 et de la proposition 1.2.2.3, nous obtenons finalement :

1.2.2.6 Théorème de Krull-Schmidt. *Soit M un A-module artinien et noethérien. Alors M peut être décomposé en somme directe finie de sous-modules indécomposables. Le nombre et les classes d'isomorphisme des sous-modules apparaissant dans une telle décomposition sont indépendants des choix opérés.*

Le théorème de Krull-Schmidt est rudimentaire : il affirme que les modules indécomposables sont les « blocs de base » des modules artiniens et noethériens, mais ne livre aucune information sur la manière de les trouver. Les anneaux pour lesquels on connaît les modules indécomposables sont peu nombreux : il y a essentiellement les anneaux semi-simples (voir le paragraphe 2.1.2), les anneaux de Dedekind (voir le paragraphe suivant), et les algèbres de type de représentation fini (l'exemple standard est l'algèbre des chemins d'un carquois de type Dynkin).

Exercices.

(1) Montrer qu'un A-module M dont l'anneau des endomorphismes est local est indécomposable. (Indication : supposons que M soit décomposable. L'anneau $B = \mathrm{End}_A(M)$ contient alors un idempotent $e \neq 1$. Comme e et $1-e$ sont tous deux non-nuls, l'équation $e(1-e) = 0$ exclut que e ou $1-e$ soit inversible dans B. Ainsi B possède deux éléments non-inversibles dont la somme est inversible.)

(2) Montrer que tout A-module noethérien peut s'écrire comme somme directe finie de sous-modules indécomposables. (Compléter la preuve de la proposition 1.2.2.3.)

(3) Soit $\mathbf{F}$ un corps fini, de cardinal disons q. On rappelle que pour chaque entier naturel n, le groupe $\mathbf{GL}_n(\mathbf{F})$ est d'ordre $\alpha_n = (q^n-1)(q^n-q)\cdots(q^n-q^{n-1})$.

(i) Soient $k \leq n$ deux entiers naturels. Montrer qu'il y a exactement $\alpha_n/\alpha_k\alpha_{n-k}$ paires (X, Y) formées de deux sous-espaces vectoriels supplémentaires de $\mathbf{F}^n$, tels que $\dim X = k$ et $\dim Y = n-k$.

(ii) Pour chaque entier naturel n, on note β_n le nombre de matrices nilpotentes dans $\mathbf{Mat}_n(\mathbf{F})$ (on convient que $\beta_0 = 1$). Montrer que

$$\sum_{k=0}^{n} \beta_k/\alpha_k = q^{n^2}/\alpha_n.$$

(Indication : regardons les éléments de $\mathbf{Mat}_n(\mathbf{F})$ comme des endomorphismes de l'espace vectoriel $V = \mathbf{F}^n$. D'après le lemme de Fitting, chaque élément $u \in \mathbf{Mat}_n(\mathbf{F})$ détermine une unique décomposition $V = u^\infty(V) \oplus u^{-\infty}(0)$ en somme directe de deux sous-espaces, sur lesquels u agit de façon respectivement inversible et nilpotente. Ainsi on atteint chaque élément $u \in \mathbf{Mat}_n(\mathbf{F})$ une et une seule fois en prenant une décomposition $V = X \oplus Y$, un endomorphisme nilpotent de X, et un élément de $\mathbf{GL}(Y)$.)

(iii) En déduire que $\beta_n = q^{n(n-1)}$.

1.2.3 Modules de type fini sur un anneau principal

Dans ce paragraphe, A est un anneau commutatif intègre principal. Soit M un A-module. Un élément x de M est dit de torsion s'il existe un élément $a \neq 0$ de A tel que $ax = 0$. On note $\mathrm{tor}\, M$ l'ensemble des éléments de torsion de M ; c'est un sous-module de M. On dit que M est de torsion si $M = \mathrm{tor}\, M$; on dit que M est sans torsion si $\mathrm{tor}\, M = 0$.

1.2.3.1 Proposition. *Un A-module de type fini est noethérien. Un A-module de type fini et de torsion est artinien et noethérien.*

Preuve. Le A-module régulier ${}_AA$ est noethérien, puisque ses sous-modules, autrement dit les idéaux de A, sont engendrés par un élément, donc sont de type fini. Il s'ensuit que si n est un entier naturel, le module libre A^n est noethérien. Un A-module M de type fini est un quotient d'un A^n ; c'est donc un module noethérien.

Soit a un élément non-nul de A. Les sous-modules du A-module $A/(a)$ sont en bijection avec les idéaux de A contenant (a), donc avec les diviseurs de a, à association près. L'anneau A

étant factoriel, a n'a qu'un nombre fini de diviseurs à association près. Ainsi le A-module $A/(a)$ n'a qu'un nombre fini de sous-modules, ce qui implique qu'il est artinien et noethérien. Pour tout entier naturel n, le A-module A^n/aA^n, égal au produit de n copies de $A/(a)$, est donc artinien et noethérien.

Soit M un A-module de type fini et de torsion. Soit $(m_1, \ldots, m_n)$ une famille génératrice finie de M. Pour chaque $i \in \{1, \ldots, n\}$ existe un élément non-nul $a_i \in A$ tel que $a_i m_i = 0$. Alors $a = a_1 \cdots a_n$ annule chaque m_i, donc annule tous les éléments de M. (Attention : on se sert ici de la commutativité de A.) L'épimorphisme de A-modules $f : A^n \to M$ qui envoie la base canonique de A^n sur $(m_1, \ldots, m_n)$ se factorise par A^n/aA^n. Ainsi M est un quotient du module artinien et noethérien A^n/aA^n ; c'est donc un module artinien et noethérien. □

1.2.3.2 Proposition. *Un A-module sans torsion de type fini est isomorphe à un sous-module d'un module libre de type fini.*

Preuve. Soit M un A-module de type fini sans torsion. Soit $(m_i)_{i \in I}$ une famille génératrice finie de M. Soit $(m_j)_{j \in J}$ avec $J \subseteq I$ une sous-famille libre maximale : on demande que cette sous-famille soit une base du sous-module N qu'elle engendre, et que pour chaque m_i avec $i \notin J$, il existe un élément non-nul $a_i \in A$ tel que $a_i m_i \in N$. Soit a le produit des a_i pour $i \in I \setminus J$. Alors l'application $m \mapsto am$ est un endomorphisme du A-module M (car A est commutatif), injectif (puisque M est sans torsion) et à valeurs dans N (par construction). Ainsi M se trouve réalisé comme sous-module du module libre N. □

Sur un anneau non-nul B, un module libre $M \cong B^{(I)}$ est de type fini si et seulement si I est un ensemble fini, d'après l'exercice (1) du paragraphe 1.2.1. Si en outre B est commutatif, alors l'exercice du paragraphe 1.1.2 montre que le cardinal de I ne dépend que de M, et même que de la classe d'isomorphisme de M. Ce cardinal s'appelle le rang de M. Deux B-modules libres sont donc isomorphes si et seulement si ils ont même rang, et un B-module libre est de type fini si et seulement si son rang est fini.

1.2.3.3 Proposition. *Un sous-module d'un A-module libre de rang fini n est libre de rang fini au plus égal à n* [7].

Preuve. Nous montrons par récurrence sur n que tout sous-module M de A^n est libre de rang au plus n. L'assertion est évidemment vraie pour $n = 0$. Admettons-la pour $n - 1$ et montrons-la pour n. Soit M un sous-module de A^n. Appelons $f : A^n \to A$ l'application n-ième coordonnée. Alors $\ker f$ est un module libre de rang $n-1$; par hypothèse de récurrence, $\ker f \cap M$ est donc un module libre de rang au plus $n - 1$. Par ailleurs, $f(M)$ est un sous-module de A, donc est de la forme Aa puisque A est principal ; selon que a est nul ou non, Aa est libre de rang 0 ou 1. Dans tous les cas, le troisième terme de la suite exacte courte $0 \to (M \cap \ker f) \to M \to f(M) \to 0$ est libre, donc projectif. Cette suite exacte est donc scindée, de sorte que $M = (M \cap \ker f) \oplus f(M)$ est somme directe de deux modules libres de rangs au plus $n - 1$ et 1 : il s'ensuit que M est libre de rang au plus n. □

7. On peut en fait montrer que si M est un A-module libre, alors chaque sous-module de M est libre, sans avoir besoin de l'hypothèse que M est de type fini. Voir par exemple le lemme 15 p. 44 du livre *Infinite abelian groups* par Irving Kaplansky, The University of Michigan Press, 1969.

Soit M un A-module de type fini. Le module $M/\operatorname{tor} M$ est sans torsion et de type fini. Les deux propositions précédentes montrent qu'il est libre ; il est donc projectif, ce qui impose à la suite exacte $0 \to \operatorname{tor} M \to M \to M/\operatorname{tor} M \to 0$ d'être scindée. Ainsi $M \cong \operatorname{tor} M \oplus (M/\operatorname{tor} M)$. Le problème de la classification des A-modules de type fini à isomorphisme près se subdivise ainsi en deux études : la classification à isomorphisme près des A-modules de type fini de torsion et celle des A-modules de type fini sans torsion.

Nous avons vu qu'un A-module de type fini sans torsion est libre ; un tel module est donc caractérisé à isomorphisme près par son rang. Il nous faut maintenant étudier les A-modules de type fini de torsion ; le résultat de classification est la proposition 1.2.3.6 à venir.

1.2.3.4 Lemme. *Soit I un idéal non-nul de A et B l'anneau A/I. Alors le B-module régulier ${}_BB$ est injectif.*

Preuve. Appelons a un générateur de l'idéal I et notons $x \mapsto \overline{x}$ l'application de A dans B (réduction modulo I). Soit J un idéal de B et $h \in \operatorname{Hom}_B(J, {}_BB)$. On écrit $J = (b)/(a)$, où (b) est un idéal de A contenant (a) ; ainsi b divise a, d'où c tel que $a = bc$. L'homomorphisme h est déterminé par l'élément $\overline{t} = h\big(\overline{b}\big)$ de B. De plus, $\overline{ct} = \overline{c}h\big(\overline{b}\big) = h\big(\overline{cb}\big) = h(\overline{a}) = h(0) = 0$. Cela signifie que a divise ct, d'où b divise t. Soit $u \in A$ tel que $t = bu$ et soit k l'endomorphisme $\overline{x} \mapsto \overline{xu}$ de B ; ainsi $h\big(\overline{b}\big) = \overline{t} = \overline{bu} = k\big(\overline{b}\big)$. Il s'ensuit que h et k coïncident sur le sous-B-module de B engendré par $\overline{b}$; en d'autres termes, h est la restriction de k à J. Vu le critère (v) de la proposition 1.1.6.5, nous avons démontré que ${}_BB$ était injectif. □

Dans un anneau principal A, les idéaux premiers non-nuls coïncident avec les idéaux maximaux ; un élément $p \in A$ est irréductible si et seulement si l'idéal (p) qu'il engendre est premier et non-nul.

1.2.3.5 Proposition. *Soit M un module de torsion, de type fini et indécomposable. Alors il existe un unique idéal premier non-nul $\mathfrak{p}$ de A et un unique entier $n \geq 1$ tels que $M \cong A/\mathfrak{p}^n$. Réciproquement, tout tel module $A/\mathfrak{p}^n$ est de torsion, de type fini et indécomposable.*

Preuve. Rappelons que l'annulateur d'un A-module M est l'idéal

$$\operatorname{ann} M = \{a \in A \mid \forall m \in M,\ am = 0\}$$

de A. Pour chaque $m \in M$, notons μ_m un générateur de l'idéal $\{a \in A \mid am = 0\}$.

À présent, soit M un A-module de type fini et de torsion. Notre premier souci est de trouver un élément $m \in M$ tel que $(\mu_m) = \operatorname{ann} M$.

Montrons d'abord que pour toute paire $\{m', m''\}$ d'éléments de M, il existe $m \in M$ tel que μ_m soit un PPCM de $\mu_{m'}$ et $\mu_{m''}$. Pour cela, on utilise la décomposition en produit d'éléments irréductibles de $\mu_{m'}$ et de $\mu_{m''}$ pour trouver des factorisations $\mu_{m'} = c'd'$ et $\mu_{m''} = c''d''$ de sorte que c' et c'' soient premiers entre eux et que leur produit soit un PPCM de $\mu_{m'}$ et $\mu_{m''}$. Écrivons une égalité de Bézout $b'c' + b''c'' = 1$ et posons $m = d'm' + d''m''$. Certainement,

tout multiple commun de $\mu_{m'}$ et de $\mu_{m''}$ annule m. Dans l'autre sens, si a annule m, alors $ad'm' = -ad''m''$, et donc

$$ad'm' = (b'c' + b''c'')ad'm' = b'c'ad'm' - b''c''ad''m'' = ab'\mu_{m'}m' - ab''\mu_{m''}m'' = 0,$$

ce qui montre que ad' est un multiple de $\mu_{m'}$ et que ad'' est un multiple de $\mu_{m''}$. Ainsi a est un multiple commun de c' et c'', donc est un multiple de leur produit, lequel est un PPCM de $\mu_{m'}$ et $\mu_{m''}$ par construction. Les éléments de A annulant m sont donc les multiples communs de $\mu_{m'}$ et de $\mu_{m''}$: nous avons bien $\mu_m = \text{PPCM}\,(\mu_{m'}, \mu_{m''})$.

Nous pouvons trouver une famille finie $(m_1, \ldots, m_n)$ de générateurs de M. Par une récurrence immédiate, la propriété que nous venons de prouver entraîne l'existence d'un $m \in M$ tel que $(\mu_m) = (\mu_{m_1}) \cap \cdots \cap (\mu_{m_n})$. Le membre de droite de cette égalité est l'ensemble des $a \in A$ qui annulent tous les m_i, donc qui annulent tous les éléments de M. Ainsi $(\mu_m) = \operatorname{ann} M$.

Regardons maintenant l'homomorphisme $a \mapsto am$ du A-module à gauche régulier dans M. Son image est le sous-module Am engendré par m, son noyau est $(\mu_m) = \operatorname{ann} M$. Nous disposons ainsi d'une suite exacte courte

$$0 \to {}_AA/\operatorname{ann} M \to M \to M/am \to 0.$$

Appelons B l'anneau quotient $A/\operatorname{ann} M$. Le A-module M peut être vu comme un B-module, car l'homomorphisme de A dans $\text{End}_{\mathbf{Z}}(M)$ définissant la structure de A-module de M se factorise à travers B ; le sous-module de M engendré par m est le même, qu'on regarde M comme un module sur A ou sur B. Notre suite exacte peut donc être vue comme une suite exacte de B-modules

$$0 \to {}_BB \to M \to M/Bm \to 0.$$

Le lemme 1.2.3.4 entraîne que cette suite est scindée. Donc en tant que B-module, $M \cong {}_BB \oplus (M/Bm)$, et en tant que A-module, $M \cong {}_AA/\operatorname{ann} M \oplus (M/Am)$. Cela montre que si M est un A-module indécomposable, alors $M \cong {}_AA/\operatorname{ann} M$.

Bref nous avons montré qu'un A-module M de type fini, de torsion et indécomposable est nécessairement isomorphe à un module A/I, où I est un idéal non-nul de A. De plus, la donnée de M détermine I, car $I = \operatorname{ann} M$. Il nous reste à vérifier que A/I est indécomposable si et seulement si I est une puissance strictement positive d'un idéal premier.

La condition est nécessaire. En effet, une variante du théorème des restes chinois dit que si $a = up_1^{\alpha_1} \cdots p_n^{\alpha_n}$ est la décomposition d'un élément non-nul $a \in A$ en produit d'un élément inversible u et de puissances $p_i^{\alpha_i}$ d'éléments irréductibles distincts, alors il y a un isomorphisme de A-modules

$$A/(a) \cong A/(p_1^{\alpha_1}) \oplus \cdots \oplus A/(p_n^{\alpha_n}).$$

Pour que $A/(a)$ soit un A-module indécomposable, il est donc nécessaire que la décomposition de a en produit de puissances d'éléments irréductibles fasse intervenir exactement un facteur.

La condition est suffisante. De fait, soit $\mathfrak{p}$ un idéal premier et $n \geq 1$ un entier. Soit B l'anneau $A/\mathfrak{p}^n$. C'est un anneau local, car il possède un unique idéal maximal, à savoir $\mathfrak{p}/\mathfrak{p}^n$ [8]. Identifiant le A-module $A/\mathfrak{p}^n$ au B-module régulier, nous obtenons l'égalité $\text{End}_A(A/\mathfrak{p}^n) = \text{End}_B({}_BB) \cong B$. L'anneau des endomorphismes du module $A/\mathfrak{p}^n$ est donc local : le module est indécomposable (voir au besoin l'exercice (1) du paragraphe 1.2.2). □

8. Un anneau commutatif B est local si et seulement s'il possède un unique idéal maximal. De fait, un élément $b \in B$ est inversible si et seulement si l'idéal (b) est B tout entier, c'est-à-dire n'est contenu dans

1.2.3.6 Proposition. *Pour chaque A-module M de type fini et de torsion, il existe une unique suite finie décroissante d'idéaux $A \neq I_1 \supseteq I_2 \supseteq \cdots \supseteq I_n \neq 0$ telle que*

$$M \cong A/I_1 \oplus A/I_2 \oplus \cdots \oplus A/I_n.$$

Preuve. Soit M un A-module de type fini et de torsion. On peut utiliser le théorème de Krull-Schmidt, car M est artinien et noethérien : M s'écrit comme somme de modules indécomposables, et les termes de la somme sont uniques à isomorphisme près. La proposition précédente dit que les modules indécomposables pouvant intervenir dans la décomposition de M sont isomorphes à des $A/(p^\alpha)$, où p est un élément irréductible de A et $\alpha \geq 1$ est un entier. Nous écrivons ainsi

$$M \cong \bigoplus_{i=1}^{m} \left(\bigoplus_{j=1}^{n_i} A \big/ \left(p_i^{\alpha_{ij}}\right) \right),$$

avec $p_1, \ldots, p_m$ des éléments irréductibles deux à deux non-associés et pour chaque i, $\alpha_{i1} \geq \alpha_{i2} \geq \cdots \geq \alpha_{in_i} > 0$. On convient d'écrire $\alpha_{ij} = 0$ pour $j > n_{ij}$. On pose $n = \max(n_1, \ldots, n_m)$ et $a_{n+1-j} = p_1^{\alpha_{1j}} \cdots p_m^{\alpha_{mj}}$ pour $1 \leq j \leq n$. Alors $a_1 \mid a_2 \mid \cdots \mid a_n$, et le théorème des restes chinois donne

$$M \cong \bigoplus_{j=1}^{n} \left(\bigoplus_{i=1}^{m} A \big/ \left(p^{\alpha_{ij}}\right) \right) \cong \bigoplus_{j=1}^{n} A/(a_{n+1-j}) = A/(a_1) \oplus A/(a_2) \oplus \cdots A/(a_n).$$

En reprenant ce raisonnement dans l'autre sens, on constate que l'unicité dans la décomposition de Krull-Schmidt impose l'unicité des idéaux (a_1), ..., (a_n). □

1.2.3.7 Exemple. Cette proposition, appliquée au cas $A = \mathbf{Z}$, entraîne aisément le théorème de classification des groupes abéliens finis :

Soit G un groupe abélien fini. Alors il existe une unique suite finie $(a_1, a_2, \ldots, a_n)$ d'entiers supérieurs à deux telle que $G \cong \mathbf{Z}/a_1\mathbf{Z} \times \mathbf{Z}/a_2\mathbf{Z} \times \cdots \times \mathbf{Z}/a_n\mathbf{Z}$ et $a_1 \mid a_2 \mid \cdots \mid a_n$.

1.2.3.8 Remarques.

(1) La voie habituelle pour prouver le théorème de classification des A-modules de type fini est de passer par l'étude des matrices équivalentes à coefficients dans A ; voir par exemple le chapitre 3 du livre *Basic Algebra I* de N. Jacobson. Outre sa simplicité conceptuelle, cette méthode présente l'avantage d'être algorithmique quand A est un anneau euclidien. La méthode exposée ci-dessus est inspirée des livres de Curtis et Reiner ([6], p. 403 ; [7], p. 39).

(2) Un anneau de Dedekind est un anneau commutatif intègre A tel que chaque idéal I de A est un A-module projectif (utiliser le lemme de la base duale 1.1.6.3 pour voir que cette condition est équivalente à la définition usuelle : tout idéal fractionnaire de A est

aucun idéal maximal de B. Ceci montre que $B^\times$ est le complémentaire de l'union des idéaux maximaux de B. Si B n'a qu'un seul idéal maximal, alors $B \setminus B^\times$ est précisément cet idéal maximal, de sorte que B est bien un anneau local. Réciproquement, supposons B local : alors $B \setminus B^\times$ est un idéal qui contient tous les idéaux maximaux de B ; c'est donc l'unique idéal maximal de B.

inversible). Tout anneau principal est un anneau de Dedekind. Les résultats exposés dans ce paragraphe quand A est un anneau principal restent encore valables quand A est un anneau de Dedekind, à l'exception de la proposition 1.2.3.3, qui doit être remplacée par : un sous-module d'un module projectif de type fini est projectif. En combinant cette assertion avec la proposition 1.2.3.2, on voit qu'un A-module de type fini est sans torsion si et seulement s'il est projectif. De plus, on montre sans grande difficulté que tout module projectif de type fini est isomorphe à une somme directe d'idéaux $I_1 \oplus \cdots \oplus I_m$ non-nuls de A, et qu'il existe un isomorphisme $I_1 \oplus \cdots \oplus I_m \cong J_1 \oplus \cdots \oplus J_n$ entre deux telles sommes si et seulement si $m = n$ et $I_1 \cdots I_m = J_1 \cdots J_n$. Ainsi les classes d'isomorphisme de A-modules projectifs de type fini sont classifiées par la donnée d'un entier naturel et d'une classe d'idéaux.

(3) Le théorème appelé parfois « décomposition de Frobenius » dans les cours sur la réduction des endomorphismes n'est autre que notre proposition 1.2.3.6 appliquée à l'anneau $A = k[X]$, où k est un corps. Outre la démonstration évoquée dans la remarque (1) ci-dessus, on trouve souvent dans les manuels une démonstration de l'assertion d'existence basée sur la dualité des k-espaces vectoriels. Cette approche est en fait équivalente à celle que nous avons suivie. De fait, prenons un polynôme $P \in k[X]$ de degré n et regardons la k-algèbre $B = k[X]/(P)$. Appelons λ la forme linéaire sur B qui, à un élément $\overline{Q}$ de B, associe le coefficient de X^{n-1} du reste de la division euclidienne de Q par P. Alors la forme bilinéaire $(f, g) \mapsto \lambda(fg)$ de $B \times B$ dans k est non-dégénérée (on s'en convainc aisément en examinant sa matrice dans la base $(\overline{1}, \overline{X}, \ldots, \overline{X}^{n-1})$). On peut ainsi identifier B à son dual. La forme particulière $(f, g) \mapsto \lambda(fg)$ de notre forme bilinéaire montre que la dualité D introduite dans la remarque 3.2.1.1 envoie le B-module à droite régulier sur le B-module à gauche régulier. Le premier étant projectif, le second est injectif : c'est notre lemme 1.2.3.4, prouvé ici sans utiliser le critère (v) de la proposition 1.1.6.5.

Exercice. Soit A un anneau commutatif intègre principal. Montrer qu'un A-module de type fini M est indécomposable si et seulement s'il est isomorphe au A-module régulier ou à un module de la forme $A/\mathfrak{p}^n$, où $\mathfrak{p}$ est un idéal premier et $n \geq 1$ est un entier. (Indication : M est soit de torsion, soit sans torsion, puisque $M \cong \operatorname{tor} M \oplus (M/\operatorname{tor} M)$. Pour montrer que le A-module régulier est indécomposable, on pourra observer que son anneau d'endomorphismes $\operatorname{End}_A({}_A A) \cong A$ ne contient pas d'idempotent autre que 1.)

1.2.4 Théorème de Jordan-Hölder

Nous allons maintenant casser un module en morceaux plus petits que dans le paragraphe 1.2.2, dans l'espoir que ceux-ci soient plus faciles à classifier que les modules indécomposables. L'inconvénient est que la connaissance de ces petits morceaux ne suffit en général pas à reconstruire le module de départ.

Module simple : M est dit simple s'il a exactement deux sous-modules : 0 et lui-même. Ainsi un sous-module N d'un module M est maximal si et seulement si le quotient M/N est simple. Un module simple est artinien et noethérien.

Soient M un A-module simple et $x \in M$ un élément non-nul. Alors l'homomorphisme $a \mapsto ax$ de A sur M est surjectif de noyau un idéal à gauche maximal $\mathfrak{m}$ de A. Ainsi $M \cong A/\mathfrak{m}$.

1.2.4.1 Exemples.

(1) Les $\mathbf{Z}$-modules simples sont les groupes abéliens isomorphes à $\mathbf{Z}/p\mathbf{Z}$, où p est un nombre premier.

(2) Plus généralement, si A est un anneau principal, alors les A-modules simples sont les modules isomorphes à $A/\mathfrak{p}$, où $\mathfrak{p}$ est un idéal premier non-nul de A. (Autrement dit, $\mathfrak{p}$ est l'idéal engendré par un élément irréductible de A.) Ces modules sont deux à deux non-isomorphes (même preuve que pour l'assertion d'unicité de la proposition 1.2.3.5 : l'idéal $\mathfrak{p}$ est l'idéal annulateur de tout module isomorphe à $A/\mathfrak{p}$).

(3) En particulier, prenons $A = k[X]$, avec k un corps algébriquement clos. Chaque $k[X]$-module simple est isomorphe à un module $k[X]/(X-a)$, avec a uniquement déterminé. Autrement dit, chaque $k[X]$-module simple est la donnée d'un k-espace vectoriel de dimension 1 muni d'une homothétie, et le rapport de cette homothétie détermine la classe d'isomorphisme du $k[X]$-module.

1.2.4.2 Lemme (Schur). *Un homomorphisme entre deux modules simples est soit nul, soit un isomorphisme. L'anneau des endomorphismes d'un module simple est un anneau à division.*

Preuve. Soit $f : M \to N$ un homomorphisme non-nul entre deux modules simples. Alors le noyau de f est un sous-module de M différent de M ; il est donc réduit à 0 puisque M est simple. L'image de f est un sous-module de N différent de 0 ; elle est égale à N tout entier puisque N est simple. Ainsi f est injective et surjective ; c'est donc un isomorphisme. Dans le cas $M = N$, ce que nous venons de montrer s'énonce ainsi : tout endomorphisme non-nul est un automorphisme. □

1.2.4.3 Lemme du papillon (ou de Zassenhaus). *Dans un A-module L, on se donne des sous-modules M, M', N, N' tels que $M' \subseteq M$ et $N' \subseteq N$. Alors*

$$\frac{(M \cap N) + M'}{(M \cap N') + M'} \cong \frac{(M \cap N) + N'}{(M' \cap N) + N'}.$$

Preuve. Soit f la restriction à $M \cap N$ de la surjection canonique de M sur $M/((M \cap N') + M')$. Le noyau de f est $(M \cap N) \cap ((M \cap N') + M') = (M \cap N') + (M' \cap N)$; l'image de f est

$$\frac{(M \cap N) + ((M \cap N') + M')}{(M \cap N') + M'} = \frac{(M \cap N) + M'}{(M \cap N') + M'}.$$

Ainsi f induit un isomorphisme entre ce dernier module et

$$\frac{M \cap N}{(M \cap N') + (M' \cap N)}.$$

Pour conclure, il suffit d'observer que la situation est symétrique en (M, M') et (N, N'). □

Filtration : une filtration croissante d'un module M est une suite croissante $(M_n)_{n\in\mathbf{Z}}$ de sous-modules de M. On demande que l'union $\bigcup_{n\in\mathbf{Z}} M_n$ soit M tout entier et que l'intersection $\bigcap_{n\in\mathbf{Z}} M_n$ soit réduite à 0. On demande parfois que la suite soit en fait finie. Les modules M_{n+1}/M_n sont appelés les facteurs ou les quotients successifs de la filtration.

Gradué associé : soit M un module muni d'une filtration $(M_n)_{n\in\mathbf{Z}}$. Le module gradué associé est $\operatorname{gr} M = \bigoplus_{n\in\mathbf{Z}} M_n/M_{n-1}$.

Soit N un sous-module d'un module M. Une filtration $(M_n)_{n\in\mathbf{Z}}$ de M induit une filtration $(N\cap M_n)_{n\in\mathbf{Z}}$ sur N et une filtration $((M_n+N)/N)_{n\in\mathbf{Z}}$ sur M/N. On a alors une suite exacte courte de modules gradués $0\to\operatorname{gr} N\to\operatorname{gr} M\to\operatorname{gr}(M/N)\to 0$ (la preuve de cette assertion est laissée en exercice).

Raffinement : on dit qu'une filtration $(M_n)_{n\in\mathbf{Z}}$ d'un module M raffine une autre filtration $(N_n)_{n\in\mathbf{Z}}$ du même module M s'il existe une application strictement croissante φ de $\mathbf{Z}$ dans lui-même telle que $N_n = M_{\varphi(n)}$ pour tout n.

1.2.4.4 Théorème de raffinement de Schreier. *On peut toujours raffiner deux filtrations finies d'un A-module de façon à avoir la même suite de facteurs, à permutation et à isomorphisme près.*

Preuve. Soient $(M_s)_{0\le s\le m}$ et $(N_t)_{0\le t\le n}$ deux filtrations finies d'un même module M. Posons $M_{s,t} = (M_s\cap N_t) + M_{s-1}$ et $N_{t,s} = (M_s\cap N_t) + N_{t-1}$. À s fixé, lorsque t croît de 0 à n, le sous-module $M_{s,t}$ croît de M_{s-1} à M_s. Ainsi

$$\begin{aligned}
0 &= M_{1,0} \subseteq M_{1,1} \subseteq M_{1,2} \subseteq \cdots \subseteq M_{1,n}\\
&= M_{2,0} \subseteq M_{2,1} \subseteq M_{2,2} \subseteq \cdots \subseteq M_{2,n}\\
&= M_{3,0} \subseteq M_{3,1} \subseteq M_{3,2} \subseteq \cdots\\
&\qquad\qquad\qquad\qquad\qquad \cdots \subseteq M_{m-1,n}\\
&= M_{m,0} \subseteq M_{m,1} \subseteq M_{m,2} \subseteq \cdots \subseteq M_{m,n} = M
\end{aligned}$$

est un filtration de M qui raffine

$$0 = M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots \subseteq M_{m-1} \subseteq M_m = M.$$

De même, les $N_{t,s}$, convenablement ordonnés, sont les termes d'une filtration de M qui raffine $(N_t)_{0\le t\le n}$.

Le lemme du papillon dit que pour $M_{s,t}/M_{s,t-1} \cong N_{t,s}/N_{t,s-1}$ pour tous entiers strictement positifs s et t. À réindexation près, nos deux filtrations ont donc même suite de quotients successifs. □

Série de composition : une filtration d'un module dont tous les quotients successifs sont simples (en particulier, non-nuls) est appelée une série de composition ; une série de composition n'admet pas de raffinement sans répétition.

1.2.4.5 Théorème de Jordan-Hölder. *Soit M un A-module artinien et noethérien. Alors M possède une série de composition. Deux séries de composition de M ont même suite de facteurs, à permutation et à isomorphisme près.*

Preuve. La seule chose qui nous reste à montrer est l'existence d'une série de composition dans M. Appelons $\mathscr{M}$ l'ensemble des sous-modules de M possédant une série de composition. Cet ensemble est non-vide puisque le sous-module nul appartient à $\mathscr{M}$. Il possède donc un élément maximal, disons N. Supposons que $N \neq M$. Alors l'ensemble $\mathscr{N}$ des sous-modules de M contenant strictement N est non-vide puisqu'il contient M. Il possède donc un élément minimal, disons L. Alors L/N est simple ; comme N possède une série de composition, L en possède une. Ainsi $L \in \mathscr{M}$, ce qui contredit la maximalité de N. Cette contradiction montre qu'on avait en fait $N = M$. □

Exemple. Soit k un corps algébriquement clos. Un $k[X]$-module artinien et noethérien est la même chose que la donnée d'un k-espace vectoriel E de dimension finie muni d'un endomorphisme u. D'après l'exemple 1.2.4.1 (3), une série de composition de ce $k[X]$-module est la même chose qu'une suite finie $0 = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_n = E$ de sous-espaces stables par u vérifiant $\dim E_i/E_{i-1} = 1$, autrement dit qu'un drapeau complet stable par u. Dans une base de E adaptée à un tel drapeau, la matrice de u est triangulaire. La suite des coefficients diagonaux de cette matrice indique la suite des classes d'isomorphismes des $k[X]$-modules E_i/E_{i-1}. À permutation près, elle ne dépend pas du choix du drapeau.

Soit M un A-module artinien et noethérien. On note $\ell(M)$ le nombre de quotients successifs d'une série de composition de M. Pour tout A-module simple S, on note $(M : S)$ le nombre de quotients isomorphes à S dans une série de composition de M. L'entier $\ell(M)$ s'appelle la longueur du module M ; les entiers $(M : S)$ s'appellent les multiplicités de Jordan-Hölder de M.

Remarque. Certains auteurs parlent de module de longueur finie au lieu de module artinien et noethérien. On trouvera une preuve du théorème de Jordan-Hölder assez différente de celle donnée ici dans le chapitre I.1 du livre d'Auslander, Reiten et Smalø [2].

Exercices.

(1) Montrer que les $\mathbf{Z}$-modules artiniens et noethériens sont les groupes abéliens finis. Montrer que quand k est un corps, les $k[X]$-modules artiniens et noethériens sont les k-espaces vectoriels de dimension finie munis d'un endomorphisme.

(2) On dit qu'un A-module artinien et noethérien est unisériel s'il possède une seule série de composition. Supposons que A soit un anneau principal. Montrer que chaque A-module artinien, noethérien et indécomposable est unisériel. (Indication : un A-module artinien et noethérien est de type fini et de torsion ; s'il est de surcroît indécomposable, il est isomorphe à un $A/\mathfrak{p}^n$, avec $\mathfrak{p}$ idéal premier non-nul de A et $n \geq 1$ entier. Les sous-modules de $A/\mathfrak{p}^n$ sont de la forme $\mathfrak{q}/\mathfrak{p}^n$, où $\mathfrak{q}$ est un idéal de A contenant $\mathfrak{p}^n$. La décomposition des idéaux de A en produit d'idéaux premiers montre que $\mathfrak{q}$ est

nécessairement de la forme $\mathfrak{p}^m$, avec $0 \leq m \leq n$. Ainsi les sous-modules de $A/\mathfrak{p}^n$ forment un ensemble totalement ordonné pour l'inclusion, ce qui montre que le module $A/\mathfrak{p}^n$ ne possède qu'une seule série de composition, à savoir

$$\mathfrak{p}^n/\mathfrak{p}^n \subseteq \mathfrak{p}^{n-1}/\mathfrak{p}^n \subseteq \mathfrak{p}^{n-2}/\mathfrak{p}^n \subseteq \cdots \subseteq \mathfrak{p}/\mathfrak{p}^n \subseteq A/\mathfrak{p}^n.$$

On pourra en outre observer que les quotients successifs de cette série de composition sont tous isomorphes à $A/\mathfrak{p}$, et que l'énoncé de l'exercice est encore vrai si A est un anneau de Dedekind.)

1.2.5 Groupe de Grothendieck

Les multiplicités de Jordan-Hölder d'un module M ne déterminent en général pas ce dernier, même à isomorphisme près. Le groupe de Grothendieck que nous introduisons dans ce paragraphe est le cadre abstrait adéquat pour étudier les propriétés qui ne dépendent que des multiplicités de Jordan-Hölder d'un module. Soit A un anneau.

1.2.5.1 Proposition. *Soit $0 \to L \to M \to N \to 0$ une suite exacte courte de A-modules. On suppose que M est artinien et noethérien, de sorte que L et N sont aussi artiniens et noethériens. Alors $\ell(M) = \ell(L) + \ell(N)$, et pour tout A-module simple S, on a $(M : S) = (L : S) + (N : S)$.*

Preuve. À isomorphisme près, on peut voir L comme un sous-module de M et N comme le quotient M/L. La proposition vient du théorème de Jordan-Hölder, une fois observé qu'on peut fabriquer une série de composition de M en raboutant une série de composition de L avec une série de composition de $N = M/L$. □

Il est licite de parler de l'ensemble $\mathscr{I}$ des classes d'isomorphisme de A-modules artiniens et noethériens. Le groupe abélien libre $\mathbf{Z}^{(\mathscr{I})}$ possède une base naturelle, en bijection avec $\mathscr{I}$: à la classe d'isomorphisme d'un A-module M correspond un élément (M) de la base de $\mathbf{Z}^{(\mathscr{I})}$. Les éléments de $\mathbf{Z}^{(\mathscr{I})}$ sont les combinaisons $\mathbf{Z}$-linéaires des symboles (M), où il y a un symbole par classe d'isomorphisme de A-module noethérien et artinien. On définit le groupe de Grothendieck $G_0(A)$ comme étant le quotient de $\mathbf{Z}^{(\mathscr{I})}$ par le sous-groupe engendré par tous les éléments de la forme $(M) - (L) - (N)$, chaque fois qu'existe une suite exacte courte $0 \to L \to M \to N \to 0$ [9]. On note $[M]$ l'image de (M) dans $G_0(A)$. Notons enfin $\mathscr{S}$ l'ensemble des classes d'isomorphisme de A-modules simples.

9. Le même procédé permet de définir le groupe de Grothendieck $K_0(\mathscr{C})$ d'une catégorie additive exacte $\mathscr{C}$, c'est-à-dire d'une catégorie additive pour laquelle les notions de monomorphisme, d'épimorphisme et de suite exacte courte sont définies. Étant donné un anneau A, les trois catégories fréquemment étudiées par cette approche sont la catégorie $A\text{-mod}_{\text{lf}}$ des A-modules artiniens et noethériens (l'indice « lf » signifie « de longueur finie »), la catégorie A-mod des A-modules de type fini, et la catégorie $\mathscr{P}(A)$ des A-modules projectifs de type fini. Signalons que notre définition $G_0(A) = K_0(A\text{-mod}_{\text{lf}})$ s'éloigne de la convention habituelle, qui est $G_0(A) = K_0(A\text{-mod})$; la différence s'estompe toutefois lorsque A est un anneau artinien.

1.2.5.2 Proposition. *Les éléments $[M]$, pour $M \in \mathscr{S}$, forment une base du $\mathbf{Z}$-module $G_0(A)$. Il existe un isomorphisme de groupes abéliens $d : G_0(A) \to \mathbf{Z}^{(\mathscr{S})}$ tel que $d\big([M]\big) = ((M : S))_{S\in\mathscr{S}}$ pour tout A-module artinien et noethérien M.*

Preuve. Désignons par $p : \mathbf{Z}^{(\mathscr{I})} \to G_0(A)$ la surjection canonique et par $i : \mathbf{Z}^{(\mathscr{S})} \to \mathbf{Z}^{(\mathscr{I})}$ l'homomorphisme injectif de groupes abéliens induit par l'inclusion $\mathscr{S} \subseteq \mathscr{I}$. D'après la proposition 1.2.5.1, l'homomorphisme de groupes abéliens de $\mathbf{Z}^{(\mathscr{I})}$ dans $\mathbf{Z}^{(\mathscr{S})}$ qui envoie (M) sur $((M : S))_{S\in\mathscr{S}}$ se factorise à travers p, définissant $d : G_0(A) \to \mathbf{Z}^{(\mathscr{S})}$. Nous obtenons ainsi un diagramme

$$\begin{array}{ccc} \mathbf{Z}^{(\mathscr{I})} & \xrightarrow{\quad p \quad} & G_0(A), \\ & {\scriptstyle i}\nwarrow \quad \swarrow{\scriptstyle d} & \\ & \mathbf{Z}^{(\mathscr{S})} & \end{array}$$

dans lequel $d \circ p \circ i = \mathrm{id}_{\mathbf{Z}^{(\mathscr{S})}}$.

Maintenant, un raisonnement par récurrence sur la longueur de M montre que le symbole $[M]$ appartient à l'image de $p \circ i$. C'est évidemment le cas quand $M = 0$ ou quand M est simple, c'est-à-dire quand $\ell(M) \leq 1$. Supposant $\ell(M) \geq 2$, il existe une suite exacte courte $0 \to L \to M \to N \to 0$, avec L et N de longueurs strictement inférieures à $\ell(M)$; alors les symboles $[L]$ et $[N]$ appartiennent à l'image de $p \circ i$, donc $[M] = [L] + [N]$ aussi. Ceci montre donc que $p \circ i$ est surjectif.

On déduit de ce qui précède que d et $p \circ i$ sont des isomorphismes de groupes abéliens, réciproques l'un de l'autre. Cela entraîne la proposition. □

Exercices.

(1) Montrer qu'il existe un homomorphisme de groupes abéliens de $G_0(A)$ dans $\mathbf{Z}$ envoyant $[M]$ sur $\ell(M)$ pour tout A-module artinien et noethérien.

(2) Soit $0 \to M_0 \to M_1 \to \cdots \to M_n \to 0$ une suite exacte d'homomorphismes entre des A-modules artiniens et noethériens. Montrer l'égalité $\sum_{i=0}^{n}(-1)^i[M_i] = 0$ dans $G_0(A)$. En déduire que $\sum_{i=0}^{n}(-1)^i\ell(M_i) = 0$.

(3) Soient M et N deux A-modules artiniens et noethériens. Montrer que pour tout homomorphisme $f \in \mathrm{Hom}_A(M, N)$, on a $\ell(\ker f) - \ell(\mathrm{coker}\, f) = \ell(M) - \ell(N)$. En déduire que dans le cas $\ell(M) = \ell(N)$, un tel homomorphisme f est injectif si et seulement s'il est surjectif. (Indication : utiliser l'exercice précédent et la suite exacte $0 \to \ker f \to M \to N \to \mathrm{coker}\, f \to 0$.)

1.3 Modules complètement réductibles, radical, socle

Nous nous donnons un anneau A quelconque pour toute cette section. Soit M un A-module artinien et noethérien. Le théorème de Krull-Schmidt dit que quand on casse M en somme directe de sous-modules indécomposables, les morceaux sont parfaitement déterminés, avec multiplicité, à l'ordre et à isomorphisme près ; la connaissance de ces morceaux permet de reconstituer M à isomorphisme près. Le théorème de Jordan-Hölder casse M en morceaux encore plus petits ; là encore les morceaux sont parfaitement déterminés, avec multiplicité ;

mais leur connaissance ne permet en général pas de reconstituer M. Le cas sympathique est quand ces deux décompositions coïncident, autrement dit, quand les termes indécomposables de la décomposition de Krull-Schmidt sont des modules simples. On dit alors que le module M est complètement réductible. Il se trouve qu'on peut faire une étude complète de cette situation sans même nos hypothèses de finitude habituelles.

1.3.1 Modules complètement réductibles

1.3.1.1 Théorème. *Pour un module M sur un anneau A, les trois conditions suivantes sont équivalentes :*

(i) Le module M est la somme de ses sous-modules simples.

(ii) Il existe une famille de sous-modules simples M_i de M dont M est la somme directe.

(iii) Tout sous-module N de M admet un supplémentaire : il existe un sous-module N' de M tel que $M = N \oplus N'$.

Preuve. Admettons (i). Soit N un sous-module de M, soit $\mathscr{L}$ l'ensemble des sous-modules simples de M, et soit $\mathscr{X}$ l'ensemble des parties X de $\mathscr{L}$ tel que la somme $N + \sum_{L\in X} L$ soit directe. Muni de l'ordre d'inclusion, l'ensemble $\mathscr{X}$ est inductif.

En effet, soit $\mathscr{Y} \subseteq \mathscr{X}$ une partie totalement ordonnée de $\mathscr{X}$ et posons $X = \bigcup_{Y\in\mathscr{Y}} Y$. Une relation de la forme $n + \sum_{L\in X} m_L = 0$, avec $n \in N$ et $m_L \in L$, ne peut comporter qu'un nombre fini de termes non-nuls ; les L pour lesquels $m_L \neq 0$ sont donc en nombre fini, ils appartiennent chacun à un $Y \in \mathscr{Y}$, et comme $\mathscr{Y}$ est totalement ordonné, ils appartiennent tous à un même Y. Notre relation peut donc se voir comme étant de la forme $n+\sum_{L\in Y} m_L = 0$ pour un certain $Y \in \mathscr{Y}$. En particulier $Y \in \mathscr{X}$, et donc n et tous les m_L sont nuls. Bref la somme $N + \sum_{L\in X} L$ est directe, donc $X \in \mathscr{X}$, et $\mathscr{Y}$ est bien majorée dans $\mathscr{X}$.

Ayant montré que $\mathscr{X}$ est inductif, nous pouvons en prendre un élément maximal, disons X. Soit $P = N \oplus \bigoplus_{L\in X} L$. Si L' est un sous-module simple de M, alors la somme $P + L'$ ne peut pas être directe, par maximalité de X. Donc $P \cap L' \neq 0$. Comme L' est simple, cela signifie $L' \subseteq P$. Le sous-module P contient donc tous les sous-modules simples de M. D'après (i), $P = M$. Nous avons ainsi fabriqué un supplémentaire de N dans M, à savoir $\bigoplus_{L\in X} L$: cela montre (iii). Par ailleurs, ce raisonnement appliqué au sous module $N = 0$ montre qu'on peut écrire M comme somme directe d'une famille de sous-modules simples : cela montre (ii).

Il nous reste à montrer que (iii) entraîne (i). Supposons donc (iii), et appelons N la somme des sous-modules simples de M. Supposons que $N \neq M$. On peut alors trouver un sous-module de type fini P de M tel que $N \cap P = 0$. (Prendre par exemple $P = Ax$, avec x non-nul appartenant à un supplémentaire de N dans M.) Soit Q un sous-module maximal de P, soit R un supplémentaire de Q dans M. Alors $P \cap R$ est un supplémentaire de Q dans P. Comme Q est maximal, $P \cap R \cong P/Q$ est simple. Par définition, $P \cap R \subseteq N$. Cela contredit $N \cap P = 0$. Bref $N = M$, ce qui établit (i). □

Un module est dit complètement réductible s'il vérifie les trois propriétés équivalentes de la proposition ci-dessus.

1.3.1.2 Remarque. Pour un module M complètement réductible, il est équivalent d'être artinien, d'être noethérien, ou d'avoir un nombre fini de termes dans une décomposition en somme directe de sous-modules simples. De fait, si l'écriture de M en somme directe de sous-modules simples fait apparaître un nombre infini de termes, alors M n'est ni noethérien, ni artinien ; si elle ne comporte qu'un nombre fini n de termes, alors une récurrence sur n montre que M est noethérien et artinien.

Nous verrons dans la section 2.1 des généralisations du résultat suivant.

1.3.1.3 Proposition. *Soit Δ un anneau à division. À isomorphisme près, il n'y a qu'un Δ-module simple, à savoir le module régulier. Tout Δ-module est libre et complètement réductible.*

Preuve. Observons d'abord que le module régulier ${}_\Delta\Delta$ est simple, car Δ n'a pas d'idéal à gauche non-banal. Soit M un Δ-module simple. Prenant un élément non-nul $x \in M$, l'homomorphisme $a \mapsto ax$ de ${}_\Delta\Delta$ dans M est un isomorphisme d'après le lemme de Schur. Ainsi tout Δ-module simple est isomorphe au module régulier.

Soit M un Δ-module. Pour tout élément non-nul $x \in M$, l'homomorphisme $a \mapsto ax$ de ${}_\Delta\Delta$ dans M est non-nul, donc est injectif (puisque ${}_\Delta\Delta$ est simple). Son image, qui est le sous-module Δx engendré par x, est donc un module simple. La somme des sous-modules simples de M est donc M tout entier. Ainsi M est complètement réductible.

Nous pouvons donc écrire M comme somme directe de sous-modules simples. Chacun d'entre eux étant isomorphe au module régulier, cela signifie que M est libre. □

1.3.1.4 Proposition. *Un sous-module ou un quotient d'un module complètement réductible est complètement réductible.*

Preuve. Soit M un module complètement réductible, soit N un sous-module de M.

Soit L un sous-module de N. Alors L possède un supplémentaire dans M, disons P, et $P \cap N$ est un supplémentaire de L dans N. Tout sous-module de N possède donc un supplémentaire dans N. Ainsi N est complètement réductible.

Par ailleurs, l'image dans M/N d'un sous-module simple de M est soit simple, soit réduite à 0. Le fait que M soit somme de ses sous-modules simples entraîne donc que M/N est somme de sous-modules simples. Ainsi M/N est complètement réductible. □

Étant donnés un A-module complètement réductible M et un A-module simple S, on note $M_{(S)}$ la somme dans M des sous-modules isomorphes à S. Les sous-modules $M_{(S)}$ s'appellent les composantes isotypiques de M. L'ensemble des composantes isotypiques de M est donc indexé par l'ensemble $\mathscr{S}$ des classes d'isomorphisme de A-modules simples, et chaque sous-module simple de M est inclus dans une composante isotypique.

1.3.1.5 Proposition. *Un module complètement réductible est la somme directe de ses composantes isotypiques.*

Preuve. Partons d'un module complètement réductible M et d'une écriture comme somme directe de sous-modules simples $M = \bigoplus_{L\in X} L$. Cette décomposition fournit une projection $p_L : M \to L$ pour chaque $L \in X$. D'après le lemme de Schur, la restriction de p_L à un sous-module simple T de M ne peut être non-nulle que si L et T sont isomorphes. Autrement dit, T est inclus dans la somme des $L \in X$ qui lui sont isomorphes. Ceci entraîne que pour chaque A-module simple S, la composante isotypique $M_{(S)}$ est la somme des $L \in X$ dans cette classe d'isomorphisme que S. Le résultat $M = \bigoplus_{(S)\in\mathscr{S}} M_{(S)}$ découle alors immédiatement de l'écriture $M = \bigoplus_{L\in X} L$. □

Exercices.

(1) Soit M un A-module complètement réductible et N un sous-module de M ; ainsi N et M/N sont complètement réductibles. Pour chaque A-module simple S, notons $M_{(S)}$, $N_{(S)}$ et $(M/N)_{(S)}$ les composantes S-isotypiques de M, N et M/N, respectivement. Montrer l'inclusion $N_{(S)} \subseteq N \cap M_{(S)}$. En comparant les décompositions

$$M = \bigoplus_{(S)\in\mathscr{S}} M_{(S)} \quad (*) \qquad \text{et} \qquad N = \bigoplus_{(S)\in\mathscr{S}} N_{(S)},$$

où $\mathscr{S}$ est l'ensemble des classes d'isomorphisme de A-modules simples, montrer qu'il y a en fait égalité $N_{(S)} = N \cap M_{(S)}$. Ainsi, N est compatible avec la décomposition $(*)$ de M, au sens où $N = \bigoplus_{(S)\in\mathscr{S}} \big(N \cap M_{(S)}\big)$. Montrer également que $(M/N)_{(S)} = \big(N + M_{(S)}\big)/N \cong M_{(S)}/N_{(S)}$.

(2) Soit $f : M \to N$ un homomorphisme entre deux A-modules complètement réductibles. Montrer l'inclusion $f(M_{(S)}) \subseteq N_{(S)}$, pour A-module simple S. (Indication : l'homomorphisme f envoie un sous-module simple de M soit sur 0, soit sur un sous-module qui lui est isomorphe.)

(3) Soient k un corps, E un k-espace vectoriel de dimension finie, u un endomorphisme de E, μ le polynôme minimal de u. On munit E de la structure de $k[X]$-module définie par u.

(i) Supposons que μ soit le produit $P_1 \cdots P_k$ de polynômes irréductibles unitaires distincts. Le lemme des noyaux dit qu'alors $E = \ker P_1(u) \oplus \cdots \oplus \ker P_k(u)$. Montrer que le $k[X]$-module E est complètement réductible et que ses composantes isotypiques sont les $\ker P_i(u)$.

(ii) Réciproquement, montrer que si le $k[X]$-module E est complètement réductible, alors μ est produit de polynômes irréductibles unitaires distincts.

(Note : cet exercice se généralise sans peine aux modules sur les anneaux principaux ; voir par exemple l'exercice (7) du paragraphe 2.2.2, ou bien [7], p. 72, exerc. 17.)

1.3.2 Théorème de densité

Un exemple de module complètement réductible est le suivant. On se donne un corps k (un anneau à division marcherait tout aussi bien) et deux entiers naturels m et n. On prend

$A = \mathbf{Mat}_m(k)$ et $M = \mathbf{Mat}_{m,n}(k)$. On fait agir A sur M par le produit usuel des matrices. Il y a un seul A-module simple à isomorphisme près, à savoir k^m (nous montrerons cela au chapitre 2), et M est somme directe de n copies de ce module simple ; la décomposition consiste évidemment à voir une matrice $m \times n$ comme une collection de n vecteurs colonnes. Dans ce contexte, $B = \mathrm{End}_A(M)$ s'identifie à l'anneau $\mathbf{Mat}_n(k)^{\mathrm{op}}$, agissant par multiplication matricielle à droite. Alors M est un B-module, et par symétrie, $\mathrm{End}_B(M)$ s'identifie à l'anneau A. Ainsi A et B sont le commutant l'un de l'autre dans l'anneau $\mathrm{End}_{\mathbf{Z}}(M)$. Ce phénomène est général dans le contexte des modules complètement réductibles.

1.3.2.1 Théorème (Jacobson, Chevalley). *Soit M un module complètement réductible sur un anneau A. Soit $f \in \mathrm{End}_{\mathbf{Z}}(M)$ qui commute à tous les endomorphismes du A-module M. Alors pour toute famille finie $(x_1, \ldots, x_n)$ d'éléments de M, il existe $a \in A$ tel que $(f(x_1), \ldots, f(x_n)) = (ax_1, \ldots, ax_n)$.*

Preuve. Considérons l'application $f^{(n)} : (y_1, \ldots, y_n) \mapsto (f(y_1), \ldots, f(y_n))$ de M^n dans M^n. Alors $f^{(n)}$ commute à tous les endomorphismes du A-module M^n. En effet, un endomorphisme g de M^n s'écrit sous forme d'une matrice $(g_{ij})_{1 \leq i,j \leq n}$ d'éléments de $\mathrm{End}_A(M)$, et pour tout élément $m = (m_i)_{1 \leq i \leq n}$ de M^n, on calcule

$$\begin{aligned}
\big(f^{(n)} \circ g\big)(m) &= f^{(n)}\left(\left(\textstyle\sum_{j=1}^n g_{ij} m_j\right)_{1 \leq i \leq n}\right) \\
&= \left(f\left(\textstyle\sum_{j=1}^n g_{ij} m_j\right)\right)_{1 \leq i \leq n} \\
&= \left(\textstyle\sum_{j=1}^n g_{ij} f(m_j)\right)_{1 \leq i \leq n} \\
&= \big(g \circ f^{(n)}\big)(m),
\end{aligned}$$

en utilisant que $f^{(n)}(m)$ est le n-uplet $\big(f(m_i)\big)_{1 \leq i \leq n}$ et que f commute à tout élément de $\mathrm{End}_A(M)$.

Considérons à présent le n-uplet $(x_1, \ldots, x_n)$ de l'énoncé et le sous-module

$$A(x_1, \ldots, x_n) = \{(ax_1, \ldots, ax_n) \mid a \in A\}$$

qu'il engendre dans M^n. Comme M^n est un A-module complètement réductible, on peut trouver un supplémentaire de $A(x_1, \ldots, x_n)$ dans M^n, d'où un projecteur $p \in \mathrm{End}_A(M^n)$ d'image $A(x_1, \ldots, x_n)$. Il s'ensuit que le n-uplet $(f(x_1), \ldots, f(x_n)) = \big(f^{(n)} \circ p\big)(x_1, \ldots, x_n)$ appartient à

$$\mathrm{im}\big(f^{(n)} \circ p\big) = \mathrm{im}\big(p \circ f^{(n)}\big) \subseteq \mathrm{im}\, p = \{(ax_1, \ldots, ax_n) \mid a \in A\}.$$

□

Remarque. Soit k un corps, E un k-espace vectoriel de dimension finie et u un endomorphisme de E. Ainsi E est muni d'une structure de $k[X]$-module. Il est bien connu qu'un endomorphisme $v \in \mathrm{End}_k(E)$ est un polynôme en u si et seulement s'il commute avec tous

les endomorphismes qui commutent avec u (c'est un résultat dû à Wedderburn). Ceci signifie que l'image de $k[X]$ dans $\mathrm{End}_k(E)$ (ou dans $\mathrm{End}_{\mathbf{Z}}(E)$) est égale à son bicommutant. Il n'y a ici pas besoin de supposer que le $k[X]$-module E est complètement réductible. On voit ainsi que la réciproque naïve du théorème de densité serait fausse.

1.3.3 Radical, tête et socle d'un module

Soit M un A-module.

Le radical de M est l'intersection des sous-modules maximaux de M ; c'est un sous-module de M noté $\operatorname{rad} M$.

La tête de M est le quotient $\operatorname{hd} M = M/\operatorname{rad} M$ (parfois notée $\operatorname{top} M$).

Le socle de M est la somme des sous-modules simples de M ; c'est un sous-module de M noté $\operatorname{soc} M$.

1.3.3.1 Propriétés.

(i) La tête d'un module est le plus grand de ses quotients de radical 0.

(ii) Le socle d'un module est le plus grand de ses sous-modules complètement réductibles.

(iii) Un module est complètement réductible si et seulement s'il est égal à son socle ; son radical est alors réduit à 0.

Preuve. Ces propriétés sont faciles à vérifier. À titre d'exemple, donnons la preuve détaillée de (i). Soit M un A-module. Les sous-modules maximaux de $\operatorname{hd} M$ sont les modules de la forme $L/\operatorname{rad} M$, où L est un sous-module maximal de M contenant $\operatorname{rad} M$. La dernière condition est en fait redondante, chaque sous-module maximal de M contenant $\operatorname{rad} M$. Le radical de $\operatorname{hd} M$ est l'intersection de ces sous-modules $L/\operatorname{rad} M$; c'est donc 0, puisque l'intersection des modules L est $\operatorname{rad} M$. Ainsi la tête de M est bien un quotient de M de radical 0.

Soit maintenant M/N un quotient de M. Si M/N est de radical 0, alors l'intersection des sous-modules maximaux de M contenant N est égale à N. L'intersection $\operatorname{rad} M$ de tous les sous-modules maximaux de M est donc incluse dans N. Ainsi M/N apparaît comme le quotient de $\operatorname{hd} M$ par $N/\operatorname{rad} M$. Tout quotient de M de radical 0 est donc un quotient de $\operatorname{hd} M$: ce dernier est donc le plus grand des quotients de M de radical 0. □

La proposition suivante est plus substantielle.

1.3.3.2 Proposition.

(i) Si M est un A-module de type fini, alors $M = \operatorname{rad} M$ si et seulement si $M = 0$.

(ii) Si M est un module artinien, alors $\operatorname{soc} M = 0$ si et seulement si $M = 0$.

(iii) Un module artinien est complètement réductible si et seulement si son radical est 0.

Preuve. Soit M un A-module non-réduit à 0. La proposition 1.2.1.1 affirme que si M est de type fini, alors il existe au moins un sous-module maximal de M, et donc $\operatorname{rad} M \subsetneq M$. Cela prouve (i). La proposition 1.2.1.3 (i) entraîne que si M est artinien non-nul, alors M contient un sous-module minimal non-nul, lequel est alors simple ; et ainsi $\operatorname{soc} M \neq 0$. Cela prouve (ii).

Il nous reste à prouver (iii). Soit M un module artinien de radical 0. Appelons $\mathscr{M}$ l'ensemble des sous-modules N qui s'écrivent comme intersection finie de sous-modules maximaux de M. Alors $\mathscr{M}$ possède un élément minimal, disons N. Par minimalité, l'intersection de N avec tout sous-module maximal de M ne peut être strictement incluse dans N. Donc N est inclus dans chaque sous-module maximal, d'où $N \subseteq \operatorname{rad} M = 0$. Conclusion : il existe un ensemble fini X de sous-modules maximaux de M tel que $\bigcap_{L\in X} L = 0$.

L'homomorphisme canonique de M dans $\prod_{L\in X} M/L$ est alors injectif. Puisque X est fini, $\prod_{L\in X} M/L = \bigoplus_{L\in X} M/L$ est complètement réductible. Ainsi M est isomorphe à un sous-module d'un module complètement réductible : il est donc complètement réductible. Réciproquement, un module complètement réductible est de radical 0 : c'est la dernière des propriétés 1.3.3.1. L'assertion (iii) est prouvée. □

Contre-exemple. Le $\mathbf{Z}$-module $\mathbf{Z}$ est de radical nul mais n'est pas complètement réductible.

1.3.3.3 Exemple. Soit $f : M \to N$ est un homomorphisme de modules. Si N est complètement réductible, alors $M/\ker f \cong \operatorname{im} f$ est complètement réductible, donc est de radical 0, et par conséquent $\ker f \supseteq \operatorname{rad} M$. Si M est complètement réductible, alors $\operatorname{im} f \cong M/\ker f$ est complètement réductible, ce qui implique que $\operatorname{im} f \subseteq \operatorname{soc} N$.

Exercices.

(1) Soient M et N deux modules sur un anneau A. Montrer les égalités $\operatorname{rad}(M \oplus N) = (\operatorname{rad} M) \oplus (\operatorname{rad} N)$ et $\operatorname{soc}(M \oplus N) = (\operatorname{soc} M) \oplus (\operatorname{soc} N)$.

(2) Soit M un module artinien. Pour tout sous-module N de M, le quotient M/N est complètement réductible si et seulement si $\operatorname{rad} M \subseteq N$. Ainsi $\operatorname{hd} M$ est le plus grand quotient complètement réductible de M. (Indication : une des implications est facile ; pour l'autre, utiliser qu'un quotient d'un module complètement réductible est complètement réductible.)

1.3.4 Sous-modules superflus et essentiels

Un sous-module N de M est dit superflu (ou petit) si pour tout sous-module $X \subsetneq M$, on a $N + X \subsetneq M$.

On dit qu'un épimorphisme de A-modules $f : M \to N$ est essentiel (certains auteurs, non des moindres, préfèrent dire « superflu ») si tout homomorphisme $g : L \to M$ tel que $f \circ g$ soit surjectif est surjectif ; cela équivaut à demander que $\ker f$ soit superflu.

Un sous-module N de M est dit essentiel (ou grand) si pour tout sous-module $X \neq 0$, on a $N \cap X \neq 0$.

On dit qu'un monomorphisme de A-modules $f : N \to M$ est essentiel si tout homomorphisme $g : M \to L$ tel que $g \circ f$ est injectif est injectif ; cela équivaut à demander que $\operatorname{im} f$ soit essentiel.

1.3.4.1 Proposition. *Soient A un anneau et M un A-module.*

(i) Un sous-module superflu de M est nécessairement inclus dans le radical de M.

(ii) Un sous-module essentiel de M contient nécessairement le socle de M.

Preuve. Soit N un sous-module superflu de M. Si L est un sous-module maximal de M, alors $L \subsetneq X$, donc $L \subseteq L + N \subsetneq X$. Par maximalité de L, cela impose $L = L + N$, donc $N \subseteq L$. Ceci étant vrai pour tout L maximal, N est inclus dans le radical de M.

Soit N un sous-module essentiel de M. Si L est un sous-module simple de M, alors $L \supseteq L \cap N \neq 0$. Par minimalité de L, cela impose $L = L \cap N$, donc $L \subseteq N$. Ceci étant vrai pour tout L simple, N contient le socle de M. □

Dans certaines circonstances, les conditions nécessaires données dans la proposition sont suffisantes.

Exercice. Soient A un anneau et M un A-module. Montrer les deux énoncés suivants :

(i) Si M est de type fini, alors un sous-module N de M est superflu si et seulement s'il est inclus dans $\operatorname{rad} M$.

(ii) Si M est artinien, alors un sous-module N de M est essentiel si et seulement s'il contient $\operatorname{soc} M$.

(Indication pour le premier énoncé : supposons $N \subseteq \operatorname{rad} M$. Chaque sous-module $X \subsetneq M$ est inclus dans un sous-module maximal L de M d'après la proposition 1.2.1.1 ; de $\operatorname{rad} M \subseteq L$ découle alors $N + X \subseteq L \subsetneq M$.)

1.4 Produit tensoriel

1.4.1 Produit tensoriel de modules

Motivation : soient k un corps, E, F et G trois k-espaces vectoriels. L'espace $\operatorname{Bil}_k(E \times F, G)$ des applications bilinéaires de $E \times F$ dans G est isomorphe à $\operatorname{Hom}_k(E, \operatorname{Hom}_k(F, G))$: à une application bilinéaire $B : E \times F \to G$, on associe l'application linéaire $x \mapsto B(x, ?)$ de E dans $\operatorname{Hom}_k(F, G)$. On sait qu'on peut construire de façon canonique un espace vectoriel noté $E \otimes_k F$ tel qu'il existe des isomorphismes naturels

$$\operatorname{Bil}_k(E \times F, G) \cong \operatorname{Hom}_k(E, \operatorname{Hom}_k(F, G)) \cong \operatorname{Hom}_k(E \otimes_k F, G).$$

De plus, il y a des isomorphismes naturels

$$(E \otimes_k F) \otimes_k G \cong E \otimes_k (F \otimes_k G),$$
$$(E \oplus F) \otimes_k G \cong (E \otimes_k G) \oplus (F \otimes_k G),$$
$$E \otimes_k (F \oplus G) \cong (E \otimes_k F) \oplus (E \otimes_k G).$$

Enfin si E' et F' sont deux autres k-espace vectoriels et si $f : E \to E'$ et $g : F \to F'$ sont deux applications linéaires, on dispose d'une application linéaire $f \otimes g$ de $E \otimes_k F$ dans $E' \otimes_k F'$.

Nous allons étendre ces résultats au cadre des modules sur un anneau A, fixé pour tout ce paragraphe. Pour cela, il est agréable d'introduire une dissymétrie.

Module à droite : un A-module à droite est la donnée d'un groupe abélien M et d'un homomorphisme d'anneaux de A^{op} dans $\mathrm{End}(M)$. On dispose alors d'une opération de A sur M, qu'on note comme un produit ma, avec $m \in M$ et $a \in A$; pour le produit dans A, on a alors $m(ab) = (ma)b$. Un homomorphisme entre deux A-modules à droite M et N est un homomorphisme de groupes abéliens $f : M \to N$ tel que $f(ma) = f(m)a$ pour tout $m \in M$ et tout $a \in A$. Un exemple de A-module à droite est le module régulier A_A : c'est le groupe abélien $(A, +)$ sur lequel les éléments de A agissent par multiplication à droite.

Soit L un A-module à droite et M un A-module à gauche. Soit F le groupe abélien libre $\mathbf{Z}^{(L\times M)}$. Pour abréger, l'élément $e_{(l,m)}$ de la base naturelle de F correspondant à un couple $(l, m) \in L \times M$ sera noté simplement (l, m). Soit F_0 le sous-groupe de F engendré par les éléments de la forme

$$\begin{cases} (l + l', m) - (l, m) - (l', m), \\ (l, m + m') - (l, m) - (l, m'), \\ (la, m) - (l, am), \end{cases}$$

pour $(l, l') \in L^2$, $(m, m') \in M^2$, $a \in A$. Le $\mathbf{Z}$-module quotient F/F_0 est appelé produit tensoriel de L et M au dessus de A et est noté $L \otimes_A M$. Il vient avec une application $(l, m) \mapsto l \otimes m$ de $L \times M$ dans $L \otimes_A M$, où $l \otimes m$ est l'image de $(l, m) \in F$ dans le quotient $F/F_0 = L \otimes_A M$. Par construction, la famille $(l \otimes m)_{(l,m)\in L\times M}$ d'éléments de $L \otimes_A M$ est génératrice.

1.4.1.1 Proposition (propriété universelle du produit tensoriel). *Soient L un A-module à droite, M un A-module à gauche, G un $\mathbf{Z}$-module, $f : L \times M \to G$ une application vérifiant*

$$\begin{cases} f(l + l', m) = f(l, m) + f(l', m), \\ f(l, m + m') = f(l, m) + f(l, m'), \\ f(la, m) = f(l, am), \end{cases}$$

pour tous $(l, l') \in L^2$, $(m, m') \in M^2$, $a \in A$. Alors il existe un unique morphisme de $\mathbf{Z}$-modules $\tilde{f} : L \otimes_A M \to G$ tel que

$$\tilde{f}(l \otimes m) = f(l, m)$$

pour tout $(l, m) \in L \times M$.

Preuve. Contemplons la suite exacte courte $0 \to F_0 \xrightarrow{i} F \xrightarrow{p} L \otimes_A M \to 0$ de $\mathbf{Z}$-modules. Appliquant le foncteur $\mathrm{Hom}_{\mathbf{Z}}(?, G)$, nous obtenons la suite exacte

$$0 \to \mathrm{Hom}_{\mathbf{Z}}(L \otimes_A M, G) \xrightarrow{\mathrm{Hom}_{\mathbf{Z}}(p,G)} \mathrm{Hom}_{\mathbf{Z}}(F, G) \xrightarrow{\mathrm{Hom}_{\mathbf{Z}}(i,G)} \mathrm{Hom}_{\mathbf{Z}}(F_0, G).$$

Ainsi le groupe des homomorphismes de $L \otimes_A M$ dans G est le noyau de $\mathrm{Hom}_{\mathbf{Z}}(i, G)$. En termes plus terre-à-terre, ce verbiage signifie qu'un homomorphisme de F/F_0 dans G est la même chose qu'un homomorphisme $h : F \to G$ qui s'annule sur F_0. Dire alors que h s'annule sur F_0, c'est dire que le noyau de h contient tous les éléments engendrant F_0.

Le $\mathbf{Z}$-module F étant libre, la donnée d'un homomorphisme $h : F \to G$ est équivalente à la donnée de l'image par h de chaque vecteur de la base naturelle de F : l'application $h \mapsto (h(l, m))_{(l,m)\in L\times M}$ est un isomorphisme de groupes de $\mathrm{Hom}_{\mathbf{Z}}(F, G)$ sur $G^{L\times M}$. Par ailleurs, le groupe $G^{L\times M}$ est l'ensemble des applications de $L \times M$ dans G.

À une application $f : L \times M \to G$ donnée comme dans l'énoncé de la proposition correspond donc un homomorphisme $h : F \to G$. Les conditions imposées à f font que h s'annule sur F_0, donc se factorise en $h = \tilde{f} \circ p$. Cela montre l'existence de $\tilde{f}$. L'unicité de $\tilde{f}$ provient de ce que les éléments de la forme $l \otimes m$ engendrent le $\mathbf{Z}$-module $L \otimes_A M$. □

Exemples.

(1) Soit M un A-module à gauche. Alors le produit tensoriel $A \otimes_A M$ du A-module à droite régulier A_A par M s'identifie naturellement au groupe additif sous-jacent à M. De fait, la propriété universelle du produit tensoriel (proposition 1.4.1.1), utilisée avec l'application $f : (a, m) \mapsto am$ de $A \times M$ dans M, montre l'existence d'un homomorphisme de groupes abéliens $\tilde{f} : A \otimes_A M \to M$ tel que $\tilde{f}(a \otimes m) = am$ pour tout $(a, m) \in A \times M$. Dans l'autre sens, soit $g : M \to A \otimes_A M$ l'application $m \mapsto 1 \otimes m$. Cette application g est un homomorphisme de groupes, car en vertu des relations définissant le produit tensoriel, nous avons $g(m+m') = 1 \otimes (m+m') = 1 \otimes m+1 \otimes m' = g(m)+g(m')$, pour tout $(m, m') \in M^2$. Il est manifeste que $\tilde{f} \circ g$ est l'identité de M. Par ailleurs, $g \circ \tilde{f}$ est un endomorphisme du groupe abélien $A \otimes_A M$ qui fixe chaque générateur $a \otimes m$, puisque $1 \otimes am = a \otimes m$ dans $A \otimes_A M$. Ainsi $\tilde{f}$ et g sont des isomorphismes réciproques.

(2) Soient m et n deux entiers naturels. On note A_c^m la puissance m-ième du A-module à droite régulier, que l'on voit comme l'ensemble des vecteurs colonnes de hauteur m à coefficients dans A. On note A_l^n la puissance n-ième du A-module à gauche régulier, que l'on voit comme l'ensemble des vecteurs lignes de longueur n à coefficients dans A. Par la propriété universelle du produit tensoriel, le produit matriciel $f : A_c^m \times A_l^n \to \mathbf{Mat}_{m,n}(A)$ induit un homomorphisme de groupes abéliens $\tilde{f} : A_c^m \otimes_A A_l^n \to \mathbf{Mat}_{m,n}(A)$. En fait, $\tilde{f}$ est un isomorphisme. Pour le montrer, on définit une application $g : \mathbf{Mat}_{m,n}(A) \to A_c^m \otimes_A A_l^n$ en posant $g(M) = \sum_{i=1}^m e_i \otimes m_i$, où e_i est le i-ème élément de la base canonique de A_c^m et où m_i est la i-ème ligne de M. On vérifie alors que g est un homomorphisme de groupes abéliens, puis que $\tilde{f} \circ g$ et $g \circ \tilde{f}$ sont les identités de $\mathbf{Mat}_{m,n}(A)$ et $A_c^m \otimes_A A_l^n$, respectivement. Ces vérifications se font en utilisant les relations dans le produit tensoriel, comme dans l'exemple précédent.

(3) Soit n un entier naturel. Notons A_c^n l'ensemble des vecteurs colonnes de hauteur n à coefficients dans A ; c'est un $\mathbf{Mat}_n(A)$-module à gauche. Notons A_l^n l'ensemble des vecteurs lignes de longueur n à coefficients dans A ; c'est un $\mathbf{Mat}_n(A)$-module à droite. Le produit matriciel $g : A_l^n \times A_c^n \to A$ vérifie les hypothèses de la proposition 1.4.1.1 ; le point le plus important à vérifier est l'égalité $g(xM, y) = g(x, My)$ pour $(x, M, y) \in A_l^n \times \mathbf{Mat}_n(A) \times A_c^n$, qui n'est autre que l'associativité du produit matriciel. Nous obtenons ainsi un homomorphisme de groupes abéliens $\tilde{g} : A_l^n \otimes_{\mathbf{Mat}_n(A)} A_c^n \to A$. On

prouve alors comme précédemment que $\tilde{g}$ est un isomorphisme. Plus précisément, pour $i, j \in \{1, \ldots, n\}$ et $a, b \in A$, notons $e_i(a)$ l'élément de A_l^n ayant des zéros partout sauf a à la position i, notons $f_j(b)$ l'élément de A_c^n ayant des zéros partout sauf b à la position j, et notons $E_{1i}(a)$ la matrice $n \times n$ avec des zéros partout sauf un a à la position $(1, i)$. Soit h l'application $a \mapsto e_1(1) \otimes f_1(a)$ de A dans $A_l^n \otimes_{\mathbf{Mat}_n(A)} A_c^n$. On vérifie aisément que h est un homomorphisme de groupes et que $\tilde{g} \circ h = \mathrm{id}_A$. Dans l'autre sens, l'égalité

$$e_i(a) \otimes f_j(b) = e_1(1)E_{1i}(a) \otimes f_j(b) = e_1(1) \otimes E_{1i}(a)f_j(b) = \begin{cases} e_1(1) \otimes f_1(ab) & \text{si } i = j, \\ 0 & \text{si } i \neq j, \end{cases}$$

dans $A_l^n \otimes_{\mathbf{Mat}_n(A)} A_c^n$ montre que $h \circ \tilde{g}$ est l'identité du produit tensoriel.

Remarque. Soient A un anneau, M un A-module à droite, N un A-module à gauche. On peut alors former les produits tensoriels $M \otimes_A N$ et $M \otimes_{\mathbf{Z}} N$. On voit immédiatement que le premier est le quotient du second par le sous-groupe engendré par les éléments $ma \otimes n - m \otimes an$, pour $(m, a, n) \in M \times A \times N$. Ceci est à rapprocher du fait que si L et N sont deux A-modules à gauche, $\mathrm{Hom}_A(L, N)$ est un sous-groupe de $\mathrm{Hom}_{\mathbf{Z}}(L, N)$: les propriétés du bifoncteur $\otimes$ sont souvent duales des propriétés du bifoncteur Hom.

1.4.1.2 Corollaire. *Soient L un A-module à droite, M un A-module à gauche, G un $\mathbf{Z}$-module. On munit le groupe abélien $\mathrm{Hom}_{\mathbf{Z}}(L, G)$ d'une structure de A-module à gauche en posant $ah = (l \mapsto h(la))$ pour $h \in \mathrm{Hom}_{\mathbf{Z}}(L, G)$ et $a \in A$. Pour $f \in \mathrm{Hom}_{\mathbf{Z}}(L \otimes_A M, G)$ et $m \in M$, notons $f(? \otimes m)$ l'élément $l \mapsto f(l \otimes m)$ de $\mathrm{Hom}_{\mathbf{Z}}(L, G)$. Alors l'application qui à f associe $m \mapsto f(? \otimes m)$ est un isomorphisme de groupes abéliens de $\mathrm{Hom}_{\mathbf{Z}}(L \otimes_A M, G)$ sur $\mathrm{Hom}_A(M, \mathrm{Hom}_{\mathbf{Z}}(L, G))$.*

Preuve. Soit $f \in \mathrm{Hom}_{\mathbf{Z}}(L \otimes_A M, G)$. Pour chaque $m \in M$, l'application $f(? \otimes m)$ de L dans G est un homomorphisme de groupes abéliens, car les relations dans le produit tensoriel et l'additivité de f font que

$$f((l + l') \otimes m) = f(l \otimes m + l' \otimes m) = f(l \otimes m) + f(l' \otimes m).$$

L'application $g : m \mapsto f(? \otimes m)$ de M dans $\mathrm{Hom}_{\mathbf{Z}}(L, G)$ est donc bien définie. Cette application g est un homomorphisme de A-modules. En effet, pour tous $m, m' \in M$ et $a \in A$, on calcule

$$f(l \otimes (m + m')) = f(l \otimes m + l \otimes m') = f(l \otimes m) + f(l \otimes m'),$$

d'où

$$g(m + m') = f(? \otimes (m + m')) = f(? \otimes m) + f(? \otimes m') = g(m) + g(m').$$

De même

$$g(am) = f(? \otimes am) = (l \mapsto f(la \otimes m)) = af(? \otimes m) = ag(m).$$

On définit alors une application F de $\mathrm{Hom}_{\mathbf{Z}}(L \otimes_A M, G)$ dans $\mathrm{Hom}_A(M, \mathrm{Hom}_{\mathbf{Z}}(L, G))$ en posant $g = F(f)$, et on vérifie que F est un homomorphisme de groupes.

Inversement, soit g un homomorphisme de A-modules de M dans $\mathrm{Hom}_{\mathbf{Z}}(L,G)$. Alors l'application $h : (l,m) \mapsto g(m)(l)$ de $L \times M$ dans G vérifie les hypothèses de la proposition 1.4.1.1. Posant $f = \tilde{h}$, on obtient un homomorphisme de groupes abéliens de $L \otimes_A M$ dans G tel que $f(l \otimes m) = g(m)(l)$. Posant alors $f = G(g)$, on définit une application G de $\mathrm{Hom}_A(M, \mathrm{Hom}_{\mathbf{Z}}(L,G))$ dans $\mathrm{Hom}_{\mathbf{Z}}(L \otimes_A M, G)$.

On vérifie que pour tout $f \in \mathrm{Hom}_{\mathbf{Z}}(L \otimes_A M, G)$, $G \circ F(f)$ et f coïncident sur tout élément de la forme $l \otimes m$, donc coïncident sur $L \otimes_A M$. Ainsi $G \circ F = \mathrm{id}$. On vérifie de même que $F \circ G = \mathrm{id}$. □

1.4.1.3 Corollaire. *Soient L et L' deux A-modules à droite, M et M' deux A-modules à gauche, $f : L \to L'$ et $g : M \to M'$ deux homomorphismes de A-modules. Alors il existe un unique homomorphisme de $\mathbf{Z}$-module $f \otimes g : L \otimes_A M \to L' \otimes_A M'$ tel que $(f \otimes g)(l \otimes m) = f(l) \otimes g(m)$ pour tous $l \in L$ et $m \in M$.*

Preuve. L'application $h : (l,m) \mapsto f(l) \otimes g(m)$ de $L \times M$ dans $L' \otimes_A M'$ vérifie les hypothèses de la proposition précédente. Par exemple, la relation $h(l+l',m) = h(l,m) + h(l',m)$ provient de ce que f est un homomorphisme de groupes additifs et de la relation

$$(f(l) + f(l')) \otimes g(m) = f(l) \otimes g(m) + f(l') \otimes g(m)$$

dans $L' \otimes_A M'$. Dès lors, l'application $f \otimes g$ cherchée est l'application $\tilde{h}$ de la proposition précédente. □

En présence de suites d'homomorphismes de A-modules à droite $L \xrightarrow{f} L' \xrightarrow{f'} L''$ et à gauche $M \xrightarrow{g} M' \xrightarrow{g'} M''$, on a l'égalité $(f' \otimes g') \circ (f \otimes g) = (f' \circ f) \otimes (g' \circ g)$ entre homomorphismes de $L \otimes_A M$ et $L'' \otimes_A M''$. De fait, les deux homomorphismes situés de part et d'autre dans cette égalité prennent la même valeur sur chaque élément de la forme $l \otimes m$, pour $(l,m) \in L \times M$; ces éléments engendrant $L \otimes_A M$, les deux homomorphismes sont égaux. Par ailleurs, $\mathrm{id}_L \otimes \mathrm{id}_M$ est l'identité de $L \otimes_A M$.

Ceci nous dit en particulier que chaque A-module à gauche Y définit un foncteur covariant $? \otimes_A Y$ de la catégorie des A-modules à droite dans la catégorie des $\mathbf{Z}$-modules. À un A-module à droite L, ce foncteur associe le $\mathbf{Z}$-module $L \otimes_A Y$; à un homomorphisme f de A-modules à droite, ce foncteur associe l'homomorphisme $f \otimes \mathrm{id}_Y$ de $\mathbf{Z}$-modules. On peut ainsi noter $f \otimes_A Y$ au lieu de $f \otimes \mathrm{id}_Y$.

Le foncteur $? \otimes_A Y$ est additif. Il en résulte qu'il commute aux sommes directes finies. En fait, il commute aussi aux sommes directes infinies.

1.4.1.4 Proposition. *Soient $(L_t)_{t \in T}$ une famille de A-modules à droite et M un A-module à gauche. Alors il existe un unique isomorphisme canonique entre les groupes abéliens*

$$\left(\bigoplus_{t \in T} L_t \right) \otimes_A M \quad \text{et} \quad \bigoplus_{t \in T} (L_t \otimes_A M)$$

qui envoie $(l_t)_{t \in T} \otimes m$ sur $(l_t \otimes m)_{t \in T}$ pour chaque $\left((l_t)_{t \in T}, m\right) \in \left(\bigoplus_{t \in T} L_t \right) \times M$.

Preuve. Posons $L = \bigoplus_{t\in T} L_t$. En vertu de la propriété universelle du produit tensoriel, l'application $\big((l_t)_{t\in T}, m\big) \mapsto (l_t \otimes m)_{t\in T}$ de $L\times M$ dans $\bigoplus_{t\in T}\big(L_t \otimes_A M\big)$ induit un homomorphisme de groupes abéliens $f : L \otimes_A M \to \bigoplus_{t\in T}\big(L_t \otimes_A M\big)$. Il s'agit maintenant de démontrer que f est un isomorphisme.

Pour chaque $t \in T$, notons $i_t : L_t \to L$ l'homomorphisme canonique. La famille des homomorphismes $i_t \otimes \mathrm{id}_M : L_t \otimes_A M \to L \otimes_A M$ définit un homomorphisme $g : \bigoplus_{t\in T}\big(L_t \otimes_A M\big) \to L \otimes_A M$. On vérifie que $g \circ f$ et $f \circ g$ sont les identités de $L \otimes_A M$ et $\bigoplus_{t\in T}\big(L_t \otimes_A M\big)$, respectivement, en vérifiant qu'ils fixent des générateurs de ces modules. □

1.4.1.5 Proposition.

(i) Pour chaque A-module à gauche Y, le foncteur $? \otimes_A Y$ est exact à droite : si $L \xrightarrow{f} M \xrightarrow{g} N \to 0$ est une suite exacte de A-modules à droite, alors

$$L \otimes_A Y \xrightarrow{f\otimes \mathrm{id}_Y} M \otimes_A Y \xrightarrow{g\otimes \mathrm{id}_Y} N \otimes_A Y \to 0$$

est une suite exacte de $\mathbf{Z}$-modules.

(ii) Si Y est un A-module à gauche projectif, alors le foncteur $? \otimes_A Y$ est exact : si $L \xrightarrow{f} M \xrightarrow{g} N$ est une suite exacte de A-modules à droite, alors

$$L \otimes_A Y \xrightarrow{f\otimes \mathrm{id}_Y} M \otimes_A Y \xrightarrow{g\otimes \mathrm{id}_Y} N \otimes_A Y$$

est une suite exacte de $\mathbf{Z}$-modules.

(iii) Si la suite exacte courte de A-modules à droite $0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$ est scindée, alors pour tout A-module à gauche Y, la suite de $\mathbf{Z}$-modules

$$0 \to L \otimes_A Y \xrightarrow{f\otimes \mathrm{id}_Y} M \otimes_A Y \xrightarrow{g\otimes \mathrm{id}_Y} N \otimes_A Y \to 0$$

est exacte et scindée.

Preuve. Plaçons-nous dans les hypothèses de l'assertion (i). L'homomorphisme g étant surjectif, chaque élément de la forme $n \otimes y$ dans $N \otimes_A Y$ est dans l'image de $g \otimes \mathrm{id}_Y$. Ces éléments engendrant $N \otimes_A Y$, nous voyons que $g \otimes \mathrm{id}_Y$ est surjectif. Par ailleurs, l'égalité $g \circ f = 0$ entraîne que $(g \otimes \mathrm{id}_Y) \circ (f \otimes \mathrm{id}_Y) = (g \circ f) \otimes \mathrm{id}_Y = 0$, ce qui montre l'inclusion $\mathrm{im}(f \otimes \mathrm{id}_Y) \subseteq \ker(g \otimes \mathrm{id}_Y)$.

On définit une application k de $N \times Y$ dans $\mathrm{coker}(f \otimes \mathrm{id}_Y)$ de la façon suivante : étant donné $(n, y) \in N \times Y$, on peut trouver $m \in M$ tel que $g(m) = n$, et on pose $k(n, y) = m \otimes y + \mathrm{im}(f \otimes \mathrm{id}_Y)$. Le point ici est que $k(n, y)$ ne dépend que de n et pas du choix de m : un autre choix m' diffère de m par un élément de $\ker g = \mathrm{im}\, f$, de sorte que $m' \otimes y$ diffère de $m \otimes y$ par un élément de $\mathrm{im}(f \otimes \mathrm{id}_Y)$. L'application k satisfait aux hypothèses de la proposition 1.4.1.1, d'où un homomorphisme $\tilde{k}$ de $N \otimes_A Y$ dans $\mathrm{coker}(f \otimes \mathrm{id}_Y)$ tel que $\tilde{k}(n \otimes y) = k(n, y)$ pour $n \in N$ et $y \in Y$. Notons $\tilde{g}$ l'application de $\mathrm{coker}(f \otimes \mathrm{id}_Y) = (M \otimes_A Y)/\,\mathrm{im}(f \otimes \mathrm{id}_Y)$ dans $N \otimes_A Y$ obtenue en factorisant $g \otimes \mathrm{id}_Y$. Alors $\tilde{k} \circ \tilde{g} = \mathrm{id}$. Ainsi $\tilde{g}$ est injectif ; autrement dit, le noyau $\ker(g \otimes \mathrm{id}_Y)/\,\mathrm{im}(f \otimes \mathrm{id}_Y)$ de $\ker \tilde{g}$ est réduit à 0. Cela achève la preuve de l'exactitude de la suite donnée dans l'énoncé (i).

Considérons une suite exacte courte $L \xrightarrow{f} M \xrightarrow{g} N$ de A-modules à droite. La distributivité du produit tensoriel par rapport à la somme implique que la classe $\mathscr{Y}$ des A-modules à gauche Y pour lesquels la suite

$$L \otimes_A Y \xrightarrow{f\otimes \mathrm{id}_Y} M \otimes_A Y \xrightarrow{g\otimes \mathrm{id}_Y} N \otimes_A Y$$

est exacte, est stable par somme directe et par passage aux facteurs directs. En outre, le A-module à gauche régulier appartient à $\mathscr{Y}$, car pour $Y = {}_AA$, la seconde des suites ci-dessus s'identifie naturellement à la première. Tout A-module libre est somme directe de modules isomorphes à ${}_AA$, donc appartient à $\mathscr{Y}$. Tout A-module projectif est facteur direct d'un module libre, donc appartient à $\mathscr{Y}$. Ceci établit (ii).

Sous les hypothèses de (iii), il existe une décomposition $M = M' \oplus M''$ du terme central de la suite exacte telle que les applications f et g s'écrivent sous forme de matrices par blocs

$$0 \to L \xrightarrow{\begin{pmatrix} f' \\ 0 \end{pmatrix}} M' \oplus M'' \xrightarrow{\begin{pmatrix} 0 & g'' \end{pmatrix}} N \to 0,$$

$f' : L \to M'$ et $g'' : M'' \to N$ étant des isomorphismes de A-modules à droite. Le résultat découle alors de la distributivité du produit tensoriel par rapport à la somme directe. □

De même, chaque A-module à droite X donne lieu à un foncteur covariant $X \otimes_A ?$ de la catégorie des A-modules à gauche dans la catégorie des groupes abéliens. Ce foncteur commute aux sommes directes, finies ou infinies ; il est exact à droite, et est exact dès que X est projectif.

Remarque. Soit p un entier strictement positif et contemplons la suite exacte courte $0 \to \mathbf{Z} \xrightarrow{f} \mathbf{Z} \xrightarrow{g} \mathbf{Z}/p\mathbf{Z} \to 0$, où f est la multiplication par p et g est l'application canonique. L'application du foncteur $? \otimes_{\mathbf{Z}} \mathbf{Z}/p\mathbf{Z}$ conduit à la suite $\mathbf{Z}/p\mathbf{Z} \to \mathbf{Z}/p\mathbf{Z} \to \mathbf{Z}/p\mathbf{Z} \to 0$, dans laquelle la première flèche est nulle. Le foncteur $? \otimes_{\mathbf{Z}} \mathbf{Z}/p\mathbf{Z}$ n'est donc pas exact.

Un A-module à gauche Y (respectivement, un A-module à droite X) est dit plat si le foncteur $? \otimes_A Y$ (respectivement, $X \otimes_A ?$) est exact. L'exemple ci-dessus montre que le $\mathbf{Z}$-module $\mathbf{Z}/p\mathbf{Z}$ n'est pas plat. L'exercice (2) ci-dessous montre qu'un module sur un anneau principal est plat si et seulement s'il est sans torsion.

Le défaut d'exactitude des foncteurs $\mathrm{Hom}_A(?, Y)$ et $\mathrm{Hom}_A(X, ?)$ étaient mesurés par les foncteurs $\mathrm{Ext}^1_A(?, Y)$ et $\mathrm{Ext}^1_A(X, ?)$, grâce auxquels on pouvait compléter les suites exactes courtes tronquées en des suites exactes longues (voir le paragraphe 1.1.5). De même, le défaut d'exactitude des foncteurs $? \otimes_A Y$ et $X \otimes_A ?$ est mesuré par des foncteurs $\mathrm{Tor}^A_1(?, Y)$ et $\mathrm{Tor}^A_1(X, ?)$. Pour des détails et une construction explicite du bifoncteur $\mathrm{Tor}^A_1(?, ?)$, je renvoie au chapitre V, §7 (et en particulier à l'exercice 1) du livre *Homology* de Saunders Mac Lane, Die Grundlehren der mathematischen Wissenschaften, Band 114, Springer-Verlag, 1963.

Exercices.

(1) Soient L un A-module à droite et M un A-module à gauche. Soient $L' \subseteq L$ et $M' \subseteq M$ des sous-modules. On dispose alors des suites exactes courtes

$$0 \to L' \xrightarrow{i} L \xrightarrow{p} L/L' \to 0 \qquad \text{et} \qquad 0 \to M' \xrightarrow{j} M \xrightarrow{q} M/M' \to 0.$$

Montrer que le noyau de $p \otimes q : L \otimes_A M \to (L/L') \otimes_A (M/M')$ est la somme des images de $i \otimes \mathrm{id}_M$ et de $\mathrm{id}_L \otimes j$. Ainsi quand $i \otimes \mathrm{id}_M$ et $\mathrm{id}_L \otimes j$ sont injectifs, on peut écrire

$$(L/L') \otimes_A (M/M') \cong \frac{L \otimes_A M}{L' \otimes_A M + L \otimes_A M'}.$$

(2) Soit A un anneau commutatif intègre principal. Montrer qu'un A-module Y est sans torsion si et seulement si le foncteur $? \otimes_A Y$ est exact. (Indication : commencer par traiter le cas où Y est de type fini, en utilisant qu'un module de type fini sans torsion sur un anneau principal est libre, puis se ramener à ce cas-là en travaillant avec la construction du produit tensoriel. Note : le résultat vaut aussi quand A est un anneau de Dedekind.)

1.4.2 Produit tensoriel d'anneaux

1.4.2.1 Proposition. *Soient A et B deux anneaux, dont les neutres multiplicatifs sont notés 1_A et 1_B. Soit $C = A \otimes_{\mathbf{Z}} B$ le produit tensoriel de leurs sous-groupes additifs sous-jacents. Il existe une et une seule structure d'anneau sur C pour laquelle le produit de deux éléments $a \otimes b$ et $a' \otimes b'$ est $aa' \otimes bb'$. L'élement neutre pour la multiplication est $1_A \otimes 1_B$. Les applications $a \mapsto (a \otimes 1_B)$ et $b \mapsto (1_A \otimes b)$ sont des homomorphismes d'anneaux de A dans C et de B dans C.*

Preuve. La seule difficulté ici est de montrer l'existence d'une application $m : C \times C \to C$ telle que

$$m\left(\sum_{i=1}^{p} a_i \otimes b_i, \sum_{j=1}^{q} a'_j \otimes b'_j\right) = \sum_{i=1}^{p} \sum_{j=1}^{q} a_i a'_j \otimes b_i b'_j,$$

pour tous $(p, q) \in \mathbf{N}^2$, $(a_i, b_i) \in (A \times B)^p$ et $(a'_j, b'_j) \in (A \times B)^q$. On pourra alors définir la multiplication sur C comme étant cette application. L'associativité, la distributivité, et le fait que $1_A \otimes 1_B$ soit un élément neutre pour cette multiplication découleront de calculs immédiats, de sorte que la proposition sera établie. La difficulté est que pour $(s, t) \in C^2$, il y a plusieurs écritures possibles $s = \sum_{i=1}^{p} a_i \otimes b_i$ et $t = \sum_{j=1}^{q} a'_j \otimes b'_j$.

Pour $a \in A$, on note $L_a : A \to A$ la multiplication à gauche par a. Pour $b \in B$, on note $M_b : B \to B$ la multiplication à gauche par b. Ces applications sont des homomorphismes de $\mathbf{Z}$-modules. Leur produit tensoriel $L_a \otimes M_b$ est un endomorphisme du produit tensoriel $C = A \otimes_{\mathbf{Z}} B$. En formules, $(L_a \otimes M_b)\left(\sum_{j=1}^{q} a'_j \otimes b'_j\right) = \sum_{j=1}^{q} aa'_j \otimes bb'_j$.

Soit t un élément de C. L'application $(a, b) \mapsto (L_a \otimes M_b)(t)$ de $A \times B$ dans C vérifie les hypothèses de la proposition 1.4.1.1. Il existe donc un endomorphisme R_t du groupe abélien

$A \otimes_{\mathbf{Z}} B$ tel que $R_t(a \otimes b) = (L_a \otimes M_b)(t)$ pour tout $(a,b) \in A \times B$. En formules, pour $s = \sum_{i=1}^{p} a_i \otimes b_i$ et $t = \sum_{j=1}^{q} a'_j \otimes b'_j$, nous avons

$$R_t(s) = \sum_{i=1}^{p} R_t(a_i \otimes b_i) = \sum_{i=1}^{p} \sum_{j=1}^{q} a_i a'_j \otimes b_i b'_j.$$

Le membre de droite de cette égalité ne dépend donc que de $(s,t) \in C^2$ et pas des écritures particulières de s et t utilisées. □

Ainsi, étant donnés deux anneaux A et B, on peut construire un anneau $A \otimes_{\mathbf{Z}} B$ « contenant » [10] A et B et où chaque élément de A commute avec chaque élément de B. Remarquons ici que le produit ordinaire $A \times B$ ne convient pas : l'application $a \mapsto (a,0)$ de A dans $A \times B$ n'est pas un homomorphisme d'anneaux.

1.4.2.2 Corollaire. *Soient A, B et C des anneaux, et soient $f : A \to C$ et $g : B \to C$ des homomorphismes d'anneaux. On suppose que pour chaque $(a,b) \in A \times B$, on a $f(a)g(b) = g(b)f(a)$. Alors il existe un unique homomorphisme d'anneaux $h : A \otimes_{\mathbf{Z}} B \to C$ tel que $h(a \otimes b) = f(a)g(b)$ pour chaque $(a,b) \in A \times B$.*

Preuve. Par la propriété universelle du produit tensoriel, l'application $(a,b) \mapsto f(a)g(b)$ de $A \times B$ dans C définit un homomorphisme de groupes abéliens $h : A \otimes_{\mathbf{Z}} B \to C$ tel que $h(a \otimes b) = f(a)g(b)$ pour chaque $(a,b) \in A \times B$. Munissons $A \otimes_{\mathbf{Z}} B$ de la structure d'anneau décrite dans la proposition 1.4.2.1. Il est manifeste que h préserve le neutre multiplicatif. Que h préserve aussi la multiplication résulte d'un calcul direct, dans lequel on se sert de l'hypothèse que $f(a)g(b) = g(b)f(a)$ pour chaque $(a,b) \in A \times B$. □

1.4.2.3 Exemples.

(1) Soient A un anneau, L un A-module à droite, M un A-module à gauche. Pour chaque $(f,g) \in \mathrm{End}_A(L) \times \mathrm{End}_A(M)$, on a l'égalité entre endomorphismes de $L \otimes_A M$

$$(f \otimes \mathrm{id}_M) \circ (\mathrm{id}_L \otimes g) = f \otimes g = (\mathrm{id}_L \otimes g) \circ (f \otimes \mathrm{id}_M).$$

Cette égalité montre l'existence d'un homomorphisme d'anneaux naturel de $\mathrm{End}_A(L) \otimes_{\mathbf{Z}} \mathrm{End}_A(M)$ dans $\mathrm{End}_{\mathbf{Z}}(L \otimes_A M)$ qui envoie $f \otimes g$ sur $f \otimes g$, pour chaque $(f,g) \in \mathrm{End}_A(L) \times \mathrm{End}_A(M)$. (Il est ici malencontreux que la même notation désigne deux objets différents ; cette ambiguïté n'a toutefois que peu d'impact.)

(2) Soient A un anneau, L et M deux A-modules à gauche. Pour $(f,g) \in \mathrm{End}_A(L) \times \mathrm{End}_A(M)$, on a l'égalité entre endomorphismes de $\mathrm{Hom}_A(L,M)$

$$\mathrm{Hom}_A(f,M) \circ \mathrm{Hom}_A(L,g) = \mathrm{Hom}_A(f,g) = \mathrm{Hom}_A(L,g) \circ \mathrm{Hom}_A(f,M),$$

d'après l'exercice (3) du paragraphe 1.1.4. (Concrètement, l'image par $\mathrm{Hom}_A(f,g)$ d'un élément $h \in \mathrm{Hom}_A(L,M)$ est la composée $g \circ h \circ f$.) Nous obtenons ainsi l'existence d'un homomorphisme d'anneaux de $\mathrm{End}_A(L)^{\mathrm{op}} \otimes_{\mathbf{Z}} \mathrm{End}_A(M)$ dans $\mathrm{End}_{\mathbf{Z}}(\mathrm{Hom}_A(L,M))$ qui envoie $f \otimes g$ sur $\mathrm{Hom}_A(f,g)$, pour chaque $(f,g) \in \mathrm{End}_A(L) \times \mathrm{End}_A(M)$.

10. Les homomorphismes de A et B dans $A \otimes_{\mathbf{Z}} B$ ne sont pas nécessairement injectifs (voir l'exercice (1) ci-après pour un exemple), d'où les guillemets autour du mot contenant.

Exercices.

(1) Soient m et n deux entiers naturels. Notons d leur plus grand diviseur commun. Montrer l'existence d'un isomorphisme d'anneaux $\mathbf{Z}/m\mathbf{Z} \otimes_{\mathbf{Z}} \mathbf{Z}/n\mathbf{Z} \cong \mathbf{Z}/d\mathbf{Z}$.

(2) Soient B et C deux anneaux, soit L un B-module à gauche et soit M un C-module à droite. Montrer que $L \otimes_{\mathbf{Z}} M$ est naturellement muni d'une structure de $B \otimes C$-module à gauche. (Indication : utiliser l'exemple 1.4.2.3 (1) avec $A = \mathbf{Z}$.)

(3) Soient A et B deux anneaux et m et n deux entiers strictement positifs. Montrer l'existence d'un isomorphisme $\mathbf{Mat}_m(A) \otimes_{\mathbf{Z}} \mathbf{Mat}_n(B) \cong \mathbf{Mat}_{mn}(A \otimes_{\mathbf{Z}} B)$.

1.4.3 Bimodules

Dans ce paragraphe, on se donne quatre anneaux A, B, C et D.

Bimodules : un A-B-bimodule est un $A \otimes_{\mathbf{Z}} B^{\mathrm{op}}$-module à gauche. Autrement dit, c'est un groupe abélien M muni d'une structure de A-module à gauche et d'une structure de B-module à droite, avec la contrainte que les actions de A et de B commutent l'une avec l'autre : $a(mb) = (am)b$ pour tous $a \in A$, $b \in B$, $m \in M$. On explicite cette situation dans la notation en écrivant ${}_AM_B$ pour signifier que A agit à gauche et B agit à droite sur M.

1.4.3.1 Exemples.

(1) Soit A un anneau. Le groupe additif $(A, +)$ peut être muni d'une structure de A-A-bimodule, l'action à gauche et à droite de A étant donnée par la multiplication de A. Le A-A-bimodule ainsi obtenu est appelé le bimodule régulier et est parfois noté ${}_AA_A$. Son anneau d'endomorphismes s'identifie avec le centre de A : à un endomorphisme f du bimodule régulier, on associe $f(1)$, qui appartient au centre de A puisque $af(1) = f(a \cdot 1) = f(a) = f(1 \cdot a) = f(1)a$ pour tout $a \in A$.

(2) Un B-module à droite M est un $\mathrm{End}_B(M)$-B-bimodule. Observant que l'anneau des endomorphismes du A-module régulier à droite A_A est isomorphe à A lui-même (l'isomorphisme est $a \mapsto (b \mapsto ab)$), nous voyons que l'exemple (1) est un cas particulier de celui-ci.

(3) Soient L un A-B-bimodule et M un A-C-bimodule. Ainsi L et M sont des A-modules à gauche et l'on a des homomorphismes d'anneaux de B^{op} dans $\mathrm{End}_A(L)$ et de C^{op} dans $\mathrm{End}_A(M)$, d'où un homomorphisme d'anneaux de $B \otimes_{\mathbf{Z}} C^{\mathrm{op}}$ dans $\mathrm{End}_A(L)^{\mathrm{op}} \otimes_{\mathbf{Z}} \mathrm{End}_A(M)$. Par composition avec l'homomorphisme naturel de ce dernier anneau dans $\mathrm{End}_{\mathbf{Z}}(\mathrm{Hom}_A(L, M))$ présenté dans l'exemple 1.4.2.3 (2), on voit que le groupe abélien $\mathrm{Hom}_A(L, M)$ est muni d'une structure de B-C-bimodule. Concrètement, cette structure est donnée par $bfc = (l \mapsto f(lb)c)$ pour $b \in B$, $c \in C$ et $f \in \mathrm{Hom}_A(L, M)$.

(4) Soient L un A-B-bimodule et M un B-C-bimodule. Autrement dit, L est un B-module à droite, M est un B-module à gauche, et on dispose d'homomorphismes d'anneaux de A dans $\mathrm{End}_B(L)$ et de C^{op} dans $\mathrm{End}_B(M)$. On a alors un homomorphisme d'anneaux de $A \otimes C^{\mathrm{op}}$ dans $\mathrm{End}_B(L) \otimes_{\mathbf{Z}} \mathrm{End}_B(M)$. Par composition avec l'homomorphisme d'anneaux de $\mathrm{End}_B(L) \otimes_{\mathbf{Z}} \mathrm{End}_B(M)$ dans $\mathrm{End}_{\mathbf{Z}}(L \otimes_B M)$ présenté dans l'exemple 1.4.2.3 (1), on obtient une structure de A-C-bimodule sur $L \otimes_B M$. L'action de A et C sur $L \otimes_B M$ est telle que $a(l \otimes m)c = (al) \otimes (mc)$ pour $a \in A$, $c \in C$, $l \in L$, $m \in M$.

1.4.3.2 Proposition. *Soient A, B, C et D quatre anneaux, et soient L un B-module à droite, M un B-C-bimodule et N un C-module à gauche. Il existe un unique homomorphisme de groupes abéliens de $(L \otimes_B M) \otimes_C N$ dans $L \otimes_B (M \otimes_C N)$ qui envoie $(l \otimes m) \otimes n$ sur $l \otimes (m \otimes n)$ pour tous $l \in L$, $m \in M$, $n \in N$. Cet homomorphisme est un isomorphisme. Si L est un A-B-bimodule et N est un C-D-bimodule, alors on a en fait affaire à un isomorphisme de A-D-bimodules.*

Preuve. Fixons $n \in N$. Par la propriété universelle du produit tensoriel, l'application $(l, m) \mapsto l \otimes (m \otimes n)$ de $L \times M$ dans $L \otimes_B (M \otimes_C N)$ définit un homomorphisme de $\mathbf{Z}$-modules de $L \otimes_B M$ dans $L \otimes_B (M \otimes_C N)$. On munit $L \otimes_B M$ de sa structure de C-module à droite. Utilisant à nouveau la propriété universelle du produit tensoriel, nous voyons que l'application $\left(\sum_{i=1}^p l_i \otimes m_i, n\right) \mapsto \sum_{i=1}^p l_i \otimes (m_i \otimes n)$ de $(L \otimes_B M) \times N$ dans $L \otimes_B (M \otimes_C N)$, dont nous venons de prouver l'existence, définit un homomorphisme de $\mathbf{Z}$-modules $\alpha : (L \otimes_B M) \otimes_C N \to L \otimes_B (M \otimes_C N)$. Le cas échéant, on vérifie que α est compatible avec les actions de A et D sur les deux produits de trois facteurs.

De la même manière, on montre l'existence et l'unicité d'un homomorphisme de $\mathbf{Z}$-modules $\beta : L \otimes_B (M \otimes_C N) \to (L \otimes_B M) \otimes_C N$ tel que $\beta(l \otimes (m \otimes n)) = (l \otimes m) \otimes n$. La composée $\beta \circ \alpha$ est un endomorphisme du $\mathbf{Z}$-module $(L \otimes_B M) \otimes_C N$ qui fixe les éléments de la forme $(l \otimes m) \otimes n$. Ces derniers engendrent $(L \otimes_B M) \otimes_C N$, donc $\beta \circ \alpha = \mathrm{id}$. On montre de même que $\alpha \circ \beta = \mathrm{id}$, ce qui établit que α et β sont des isomorphismes réciproques. □

Le résultat suivant nous dit que la donnée d'un A-B-bimodule permet de relier la catégorie des A-modules à la catégorie des B-modules. Sa preuve est laissée en exercice.

1.4.3.3 Proposition. *Soient A et B deux anneaux, et soient L un A-B-bimodule, M un B-module et N un A-module. On munit $L \otimes_B M$ de sa structure de A-module naturelle et on munit $\mathrm{Hom}_A(L, N)$ de sa structure de B-module naturelle. Alors l'isomorphisme de groupes abéliens $f \mapsto (m \mapsto f(? \otimes m))$ de $\mathrm{Hom}_{\mathbf{Z}}(L \otimes_B M, N)$ sur $\mathrm{Hom}_B(M, \mathrm{Hom}_{\mathbf{Z}}(L, N))$ induit par restriction un isomorphisme $\mathrm{Hom}_A(L \otimes_B M, N) \cong \mathrm{Hom}_B(M, \mathrm{Hom}_A(L, N))$.*

Plus précisément, on dispose du foncteur $L \otimes_B ?$ de la catégorie des B-modules dans la catégorie des A-modules et du foncteur $\mathrm{Hom}_A(L, ?)$ qui va dans l'autre sens. La terminologie pour exprimer l'existence de l'isomorphisme $\mathrm{Hom}_A(L \otimes_B M, N) \cong \mathrm{Hom}_B(M, \mathrm{Hom}_A(L, N))$ est de dire que le premier foncteur est l'adjoint à gauche du second, ou que le second est l'adjoint à droite du premier.

Quand L est un module projectif de type fini et générateur (en un sens à définir) et $B = \mathrm{End}_A(L)^{\mathrm{op}}$, les deux foncteurs ci-dessus sont des équivalences de catégories. On dit alors avoir affaire à un contexte de Morita, voir par exemple [7], §3D pour plus davantage de détails sur cette situation.

Exercices.

(1) Soient A un anneau, M un A-module à gauche, I un idéal bilatère de A. L'anneau A et le quotient A/I peuvent être vus comme des A-A-bimodules, de sorte qu'on peut former

les produits tensoriels $A \otimes_A M$ et $(A/I) \otimes_A M$. Montrer l'existence d'un isomorphisme de A-modules de $A \otimes_A M$ sur M envoyant $a \otimes m$ sur am, pour tout $(a, m) \in A \times M$. Montrer l'existence d'un isomorphisme de A-modules $(A/I) \otimes_A M \cong M/IM$.

(2) Démontrer la proposition 1.4.3.3.

1.4.4 Changement de base

Soit $\chi : B \to A$ un homomorphisme d'anneaux ; on peut alors munir A d'une action de B à gauche ou à droite en posant $ba = \chi(b)a$ et $ab = a\chi(b)$, respectivement, pour tous $(a, b) \in A \times B$. Ainsi A peut être muni d'une structure de A-B-bimodule ou de B-A-bimodule. Soit V un A-module à gauche. On munit le groupe additif $(V, +)$ de l'action de B obtenue en composant l'homomorphisme d'anneaux de A dans $\mathrm{End}_{\mathbf{Z}}(M)$ avec χ ; le B-module ainsi obtenu est noté $\mathrm{res}^A_B V$. Ce module $\mathrm{res}^A_B V$ peut se retrouver de deux manières : soit en utilisant la structure de A-B-bimodule sur A pour obtenir une structure de B-module sur $V \cong \mathrm{Hom}_A(A, V)$, soit en utilisant la structure de B-A-bimodule sur A pour obtenir une structure de B-module sur $V \cong A \otimes_A V$. Par ailleurs, soit W un B-module à gauche. La structure de A-B-bimodule sur A munit $\mathrm{ind}^A_B W = A \otimes_B W$ d'une structure de A-module à gauche ; la structure de B-A-bimodule sur A munit $\mathrm{coind}^A_B W = \mathrm{Hom}_B(A, W)$ d'une structure de A-module à gauche. La proposition 1.4.3.3 montre qu'on a alors des isomorphismes naturels

$$\mathrm{Hom}_B(W, \mathrm{res}^A_B V) \cong \mathrm{Hom}_A(\mathrm{ind}^A_B W, V) \quad \text{et} \quad \mathrm{Hom}_B(\mathrm{res}^A_B V, W) \cong \mathrm{Hom}_A(V, \mathrm{coind}^A_B W).$$

Ainsi le foncteur res^A_B admet un adjoint à gauche, à savoir ind^A_B, et un adjoint à droite, à savoir coind^A_B.

Nous verrons ultérieurement qu'il est parfois possible d'identifier les foncteurs ind^A_B et coind^A_B ; ce sera notamment le cas dans le cadre des représentations des groupes finis.

1.4.5 Structure des modules complètement réductibles

1.4.5.1 Proposition. *Soient A et B des anneaux, S un A-module simple, $\Delta = \mathrm{End}_A(S)^{\mathrm{op}}$, et T un Δ-B-bimodule. On suppose que T est un B-module simple et on munit $S \otimes_\Delta T$ de sa structure de A-B-bimodule.*

(i) En tant que A-module, $S \otimes_\Delta T$ est complètement réductible, et est isotypique de type S.

(ii) En tant que B-module à droite, $S \otimes_\Delta T$ est complètement réductible, et est isotypique de type T.

(iii) Le A-B-bimodule $S \otimes_\Delta T$ est simple.

Preuve. D'après le lemme de Schur, Δ est un anneau à division. Le Δ-module à droite est donc libre, d'après la proposition 1.3.1.3. Choisissons une base $(e_i)_{i \in I}$ du Δ-module à droite S. Alors

$$S \otimes_\Delta T = \left(\bigoplus_{i \in I} e_i \Delta \right) \otimes_\Delta T = \bigoplus_{i \in I} \Big(e_i \Delta \otimes_\Delta T \Big),$$

et chaque terme $e_i \Delta \otimes_\Delta T$ de cette somme directe est un B-module isomorphe à $\Delta \otimes_\Delta T$, donc à T. Cela prouve (ii). La preuve de (i) s'obtient de façon analogue, en exploitant le fait que

le Δ-module T est libre, somme directe de sous-modules isomorphes au Δ-module à gauche régulier.

Soit U un sous-bimodule non-nul du A-B-bimodule $S \otimes_\Delta T$. Soit u un élément non-nul de U. On peut écrire $u = \sum_i e_i \otimes t'_i$ avec $t'_i \in T$, de façon unique ; cette somme ne comporte qu'un nombre fini de termes non-nuls. Fixons un indice j tel que $t'_j \neq 0$. Soit $k \in I$ et $t \in T$. Le B-module T étant simple, il existe $b \in B$ tel que $t = t'_j b$. Soit $f \in \mathrm{End}_\Delta(S)$ défini par : $f(e_i) = 0$ si $i \neq j$, $f(e_j) = e_k$. D'après le théorème de densité, il existe $a \in A$ tel que $ae_i = f(e_i)$ pour tous les indices $i \in I$ pour lesquels $t'_i \neq 0$. Alors $aub = e_k \otimes t$. Ainsi $e_k \otimes t \in U$. Tout élément de $S \otimes_\Delta T$ étant somme d'éléments de la forme $e_k \otimes t$, nous avons donc $U = S \otimes_\Delta T$. Ainsi $S \otimes_\Delta T$ n'a que deux sous-modules, 0 et lui-même. Cela établit (iii). □

Soient A un anneau, M un A-module complètement réductible et $B = \mathrm{End}_A(M)^{\mathrm{op}}$. Alors M est un A-B-bimodule. Comme les homomorphismes entre modules complètement réductibles respectent les composantes isotypiques (voir l'exercice (2) du paragraphe 1.3.1), chaque composante isotypique du A-module M est un sous-A-B-bimodule de M.

1.4.5.2 Proposition. *Dans ce contexte, soient S un A-module simple et $\Delta = \mathrm{End}_A(S)^{\mathrm{op}}$; ainsi $T = \mathrm{Hom}_A(S, M)$ est un Δ-B-bimodule*[11]*. Alors le B-module T est soit nul, soit simple, et l'application d'évaluation $(x, f) \mapsto f(x)$ de $S \times T$ dans M induit un isomorphisme de $S \otimes_\Delta T$ sur la composante S-isotypique de M.*

Preuve. Soit U un sous-B-module de T différent de 0. Soit $f \in U$ un élément non-nul. Alors f induit un isomorphisme $\tilde{f}$ de S sur l'image de f. Comme M est complètement réductible, cette dernière admet un supplémentaire dans M : on écrit $M = \mathrm{im}\, f \oplus X$. Soit $g \in T$. On définit un endomorphisme b de M de la façon suivante

$$M = \mathrm{im}\, f \oplus X \xrightarrow{\begin{pmatrix} g \circ \tilde{f}^{-1} & 0 \end{pmatrix}} M,$$

en adoptant une écriture par blocs reflétant la décomposition en somme directe de M. Alors dans le B-module à droite T, on a $fb = b \circ f = g$, ce qui montre que $g \in U$. Ainsi U contient tous les éléments de T. Nous avons montré que T est un B-module simple.

L'application d'évaluation remplit les conditions pour se factoriser par le produit tensoriel $S \otimes_\Delta T$, puisque l'action de Δ sur T est donnée par $\delta f = f \circ \delta$. On vérifie sans peine que l'homomorphisme de groupes abéliens $\mathrm{ev} : S \otimes_\Delta T \to M$ qui en résulte est un homomorphisme de A-B-bimodules. Comme le A-module $S \otimes_\Delta T$ est complètement réductible et isotypique de type S, l'image de ev est incluse dans la composante S-isotypique de M. Par ailleurs, ev est injectif car il est non-nul et le A-B-bimodule $S \otimes_\Delta T$ est simple. Enfin, chaque élément y de la composante S-isotypique du A-module M appartient à une somme finie $\sum_{i \in I} N_i$ de sous-modules de M isomorphes à S ; écrivant $N_i = \mathrm{im}\, f_i$ pour des $f_i \in T$ et $y = \sum_{i \in I} n_i$ pour des $n_i \in N_i$, disons $n_i = f_i(x_i)$, on arrive à $y = \mathrm{ev}\Big(\sum_{i \in I} x_i \otimes f_i\Big)$. Cela montre que l'image de ev est la composante S-isotypique de M. □

11. Concrètement, l'action de Δ et de B sur T est donnée par le produit de composition des applications.

Reprenons le contexte présenté avant l'énoncé de la proposition 1.4.5.2. Le théorème de densité montre que l'on a presque $A = \mathrm{End}_B(M)$. (Plus précisément, l'homomorphisme d'anneaux de A dans $\mathrm{End}_B(M)$ est presque surjectif ; le théorème de densité ne dit rien sur l'injectivité.) Ainsi il y a une certaine symétrie entre A et B. La proposition suivante va plus loin, puisqu'elle dit que M est complètement réductible non seulement en tant que A-module, mais aussi en tant que B-module. Mieux : les composantes isotypiques de M sont les mêmes, et cela permet d'établir une bijection entre l'ensemble des classes d'isomorphisme de A-modules simples et l'ensemble des classes d'isomorphisme de B-modules simples pouvant être réalisées comme sous-modules de M. Ainsi M met en relation la théorie des A-modules et celle des B-modules.

1.4.5.3 Proposition. *Soit M un A-module. Notons $B = \mathrm{End}_A(M)^{\mathrm{op}}$, de sorte que M est un A-B-bimodule. Si M est complètement réductible en tant que A-module, alors :*

(i) En tant que B-module ou que A-B-bimodule, M est complètement réductible.

(ii) Les composantes isotypiques du A-module M sont les sous-A-B-bimodules simples de M.

(iii) Pour tout A-module simple S, la composante S-isotypique du A-module M est égale à la composante $\mathrm{Hom}_A(S, M)$-isotypique du B-module M.

(iv) La correspondance $S \mapsto \mathrm{Hom}_A(S, M)$ induit une bijection φ de l'ensemble des classes d'isomorphismes de A-modules simples apparaissant dans M sur l'ensemble des classes d'isomorphisme de B-modules simples apparaissant dans M.

Preuve. Écrivons la décomposition du A-module M en somme directe de ses composantes isotypiques $M = \bigoplus_{(S)\in\mathscr{S}} M_{(S)}$, où $\mathscr{S}$ est l'ensemble des classes d'isomorphisme de A-modules simples. Par les deux propositions précédentes, nous savons que $M_{(S)} = S \otimes_\Delta T$, avec $\Delta = \mathrm{End}_A(S)^{\mathrm{op}}$ et $T = \mathrm{Hom}_A(S, M)$. Nous savons notamment que T est un B-module simple et que chaque $M_{(S)}$ est un A-B-bimodule simple et un B-module complètement réductible isotypique de type T. Cela montre (i), à savoir que M est complètement réductible comme B-module et comme A-B-bimodule.

Les $M_{(S)}$ ne sont pas isomorphes en tant que A-modules, donc ne le sont pas en tant que A-B-bimodules. La décomposition $M = \bigoplus_{(S)\in\mathscr{S}} M_{(S)}$ est donc une décomposition du A-B-bimodule M en somme directe de sous-bimodules simples deux-à-deux non-isomorphes. C'est donc la décomposition du A-B-bimodule M en ses composantes isotypiques. Nous obtenons ainsi (ii) : en effet un sous-A-B-bimodule simple de M est inclus dans la composante isotypique correspondante, et cette dernière étant simple, il y a égalité.

Soit S un A-module simple. La projection sur $M_{(S)}$ parallèlement à la somme des autres composantes isotypiques du A-module M est un idempotent $b \in B$. Il agit par l'identité sur $T = \mathrm{Hom}_A(S, M)$ et agit par zéro sur chaque espace $T' = \mathrm{Hom}_A(S', M)$ correspondant à un A-module simple S' non-isomorphe à S. On voit ainsi que si S' n'est pas isomorphe à S, alors les B-modules simples T et T' ne sont pas isomorphes. Ainsi les termes de la décomposition $M = \bigoplus_{(S)\in\mathscr{S}} M_{(S)}$ sont un B-modules complètement réductibles isotypiques de types différents : les $M_{(S)}$ sont donc les composantes isotypiques du B-module M, d'où (iii).

Enfin l'assertion (iv) découle de l'assertion (iii). □

EXERCICE. Soit M un module complètement réductible sur un anneau A. On pose $B = \mathrm{End}_A(M)^{\mathrm{op}}$; ainsi M est un B-module à droite complètement réductible. Soient S un A-module simple, $\Delta = \mathrm{End}_A(S)^{\mathrm{op}}$ et $T = \mathrm{Hom}_A(S, M)$. Ainsi Δ est un anneau à division, S est un A-Δ-bimodule, T est un Δ-B-bimodule, et la composante S-isotypique de M est isomorphe à $S \otimes_\Delta T$. On suppose que $T \neq 0$; on sait qu'alors T est un B-module à droite simple.

(i) Montrer que $\tilde{S} = \mathrm{Hom}_B(T, M)$ est un A-module simple. (Indication : procéder comme dans la preuve de la proposition 1.4.5.2, en faisant appel au théorème de densité pour justifier de pouvoir échanger les rôles de A et B.)

Chaque $s \in S$ définit un homomorphisme de B-modules $\mathrm{ev}_s : f \mapsto f(s)$ de T dans M. On en déduit une application $\mathrm{ev} : S \to \tilde{S}$.

(ii) Montrer que l'application $\mathrm{ev} : S \to \tilde{S}$ est un isomorphisme de A-modules.

(iii) Montrer que la structure de Δ-B-bimodule sur T définit un isomorphisme d'anneaux $\Delta \cong \mathrm{End}_B(T)$. (Indication : posons $\Delta' = \mathrm{End}_B(T)$. Comme T est un B-module simple, Δ' est un anneau à division. La structure de Δ-B-bimodule sur T définit un homomorphisme d'anneaux $\lambda : \Delta \to \Delta'$. Comme Δ est un anneau à division, λ est nécessairement injectif. De même, $\tilde{S}$ est un A-Δ'-bimodule, d'où un homomorphisme injectif d'anneaux $\mu : \Delta' \to \mathrm{End}_A\big(\tilde{S}\big)$. L'isomorphisme $\mathrm{ev} : S \to \tilde{S}$ induit un isomorphisme $\Delta \cong \mathrm{End}_A\big(\tilde{S}\big)$, lequel n'est autre que $\mu \circ \lambda$. On voit ainsi que λ et μ sont des isomorphismes.)

2 Théorie élémentaire des anneaux

Introduction

L'objet de la théorie des représentations est l'étude des modules sur un anneau A donné, lequel est souvent une algèbre sur un corps (voir le chapitre 3). Il s'agit d'obtenir une classification à isomorphisme près des modules sur un anneau A, voire une description explicite de ceux-ci. En général, les modules et les anneaux sont soumis à des conditions de finitude afin d'éviter des cas trop sauvages. Le théorème de Krull-Schmidt permet de se restreindre à l'étude des modules indécomposables, mais ceci reste encore souvent un problème très délicat. C'est pourquoi on commence toujours par essayer d'étudier les modules simples le plus précisément possible.

Nous commençons ce chapitre en étudiant le cas des anneaux jouissant de la propriété a priori favorable que tous leurs modules à gauche sont complètement réductibles. Un tel anneau est dit semi-simple. Nous présentons plusieurs caractérisations des anneaux semi-simples et prouvons le théorème de structure de Wedderburn : un anneau semi-simple est le produit d'un nombre fini d'anneaux de matrices à coefficients dans un anneau à division.

Le cas des anneaux semi-simples est suffisamment bien compris pour qu'on essaie d'y ramener d'autres situations. Ainsi pour tout anneau A, on définit un idéal bilatère $J(A)$ appelé le radical de Jacobson (dit parfois de Perlis-Jacobson) de A. Les A-modules complètement réductibles sont alors automatiquement des modules sur l'anneau $A/J(A)$. Dans le cas où A est un anneau artinien à gauche (cette condition signifie que le A-module à gauche régulier est artinien), la réciproque est vraie, et de plus $A/J(A)$ est semi-simple. La connaissance des A-modules simples est alors équivalente à l'explicitation de la structure de $A/J(A)$.

Un autre phénomène remarquable se produit quand A est artinien à gauche : l'idéal $J(A)$ est nilpotent, c'est-à-dire qu'il existe un entier positif n tel que tout produit de n éléments de $J(A)$ est nul. Ce fait, qui paraît anecdotique, permet d'étudier plus en détail les A-modules projectifs. Plus précisément, il permet de montrer que tout A-module projectif est somme directe (éventuellement infinie) de A-modules projectifs indécomposables, que tout A-module projectif indécomposable est isomorphe à un facteur direct du A-module régulier ${}_AA$, et qu'il y a une bijection canonique entre les A-modules simples et les A-modules projectifs indécomposables. Des résultats analogues sont vrais concernant les A-modules injectifs. Ces faits invitent à élucider la structure des A-modules projectifs ou injectifs indécomposables, par exemple à déterminer leurs multiplicités de Jordan-Hölder.

Tout ceci n'apporte toutefois que peu de renseignements sur les modules indécomposables. Les méthodes récentes pour aborder cette question (théorie du basculement, carquois d'Auslander-Reiten, équivalence de catégories dérivées) sont au-delà du niveau de ce cours. Nous nous bornerons à expliquer la notion de bloc d'un anneau artinien à gauche A. Il s'agit ici d'écrire A comme un produit d'anneaux $\prod_{i\in I} B_i$ de la façon la plus fine possible. Il y a unicité d'une telle décomposition et le produit est fini. Chaque A-module M se décompose alors en une somme directe $\bigoplus_{i\in I} M_i$, où M_i est un B_i-module annulé par les autres blocs B_j de la décomposition. L'étude des A-modules est ainsi découplée en l'étude des B_i-modules, séparément pour chaque $i \in I$.

2.1 Anneaux simples et semi-simples artiniens

2.1.1 Théorème de Wedderburn-Artin

Rappelons une conséquence de la proposition 1.3.1.3 : un anneau à division Δ n'a qu'un seul module simple à isomorphisme près, et tout Δ-module est complètement réductible. Les anneaux simples artiniens ont eux aussi ces deux propriétés.

Anneau simple : un anneau est dit simple s'il n'est pas réduit à $\{0\}$ et s'il n'a pas d'idéal bilatère non-banal.

Anneau artinien : un anneau A est dit artinien à gauche si le A-module à gauche régulier ${}_AA$ est artinien. Un anneau A est dit artinien à droite si l'anneau A^{op} est artinien à gauche.

Annulateur d'un module : rappelons que l'annulateur d'un A-module M est l'idéal bilatère $\operatorname{ann} M = \{a \in A \mid \forall m \in M,\ am = 0\}$.

Module fidèle : un A-module est dit fidèle si son annulateur est réduit à $\{0\}$.

2.1.1.1 Théorème de Wedderburn-Artin. *Pour un anneau A, les quatre assertions suivantes sont équivalentes :*

(i) A est un anneau simple, artinien à gauche.

(ii) A est un anneau simple, artinien à droite.

(iii) A est un anneau artinien à gauche et possède un module simple et fidèle.

(iv) Il existe un entier $n \geq 1$ et un anneau à division Δ tels que A soit isomorphe à $\mathbf{Mat}_n(\Delta)$.

Si ces assertions sont vraies, alors il y a exactement une classe d'isomorphisme de A-modules simples. Si S est un A-module simple et si $A \cong \mathbf{Mat}_n(\Delta)$, comme dans l'assertion (iv), alors $\Delta \cong \mathrm{End}_A(S)^{\mathrm{op}}$ et n est la longueur du Δ-module S. Ainsi la classe d'isomorphisme de Δ et l'entier n sont entièrement déterminés par A. Enfin, le A-module régulier est complètement réductible de longueur n.

Preuve. Supposons (i). Soit S un A-module simple (prendre par exemple $A = A/\mathfrak{m}$, où $\mathfrak{m}$ est un idéal à gauche maximal). L'annulateur de S est un idéal bilatère de A, distinct de A : c'est donc $\{0\}$ puisque S est simple. Ainsi S est fidèle et (iii) est vrai.

Supposons (iii). Soit S un A-module simple et fidèle. Soit $\Delta = \mathrm{End}_A(S)^{\mathrm{op}}$; ainsi S est un A-Δ-bimodule. Comme S est un A-module simple, c'est un A-module complètement réductible : nous pouvons lui appliquer le théorème de densité. Par ailleurs, le lemme de Schur affirme que Δ est un anneau à division ; la proposition 1.3.1.3 dit alors que S est un Δ-module libre. Soit donc $(e_i)_{i\in I}$ une base du Δ-module S.

Si I était infini, nous pourrions trouver une partie dénombrable dans I, et donc nous pourrions considérer que $I \supseteq \mathbf{N}$. Pour chaque $n \in \mathbf{N}$ existerait alors $f \in \mathrm{End}_\Delta(S)$ tel que $f(e_0) = f(e_1) = \cdots = f(e_{n-1}) = 0$ et $f(e_n) = e_n$. Le théorème de densité nous donnerait alors

l'existence d'un élément $a \in A$ tel que $ae_0 = ae_1 = \cdots = ae_{n-1} = 0$ et $ae_n = e_n$. La suite $(J_n)_{n\in\mathbf{N}}$ d'idéaux à gauche dans A définie par

$$J_n = \{a \in A \mid ae_0 = ae_1 = \cdots = ae_{n-1} = 0\}$$

serait alors strictement décroissante, en contradiction avec l'hypothèse que A est artinien à gauche. Ainsi I est fini.

Nous pouvons supposer que $I = \{1, \ldots, n\}$. Le lemme de densité nous dit alors que l'homomorphisme d'anneaux de A dans $\mathrm{End}_\Delta(S)$ est surjectif. Il est par ailleurs injectif, car son noyau doit être un idéal bilatère de A, qui est simple. Ainsi $A \cong \mathrm{End}_\Delta(S) \cong \mathbf{Mat}_n(\Delta)$. (Il faut ici faire attention que Δ n'est pas commutatif : l'isomorphisme $\mathrm{End}_\Delta(S) \cong \mathbf{Mat}_n(\Delta)$ provient de l'isomorphisme $S \cong \Delta^n$ de Δ-modules à droite.) Bref (iv) est vrai.

Nous avons vu dans l'exercice (2) du paragraphe 1.1.1 que les idéaux bilatères d'un anneau $\mathbf{Mat}_n(B)$ étaient de la forme $\mathbf{Mat}_n(I)$, pour I un idéal bilatère de B. Ainsi $\mathbf{Mat}_n(\Delta)$ est simple dès que Δ est un anneau à division. Par ailleurs, le produit matriciel munit $S = \Delta^n$, vu comme l'ensemble des vecteurs colonnes de taille n, d'une structure de module sur l'anneau $\mathbf{Mat}_n(\Delta)$. On vérifie directement que S est engendré par n'importe lequel de ses éléments non-nul, donc qu'il est simple. Regardant une matrice $n\times n$ comme la suite de ses vecteurs colonnes, nous constatons que le $\mathbf{Mat}_n(\Delta)$-module à gauche régulier est isomorphe à S^n. Comme S est simple, il est artinien, donc S^n est artinien : l'anneau $\mathbf{Mat}_n(\Delta)$ est donc artinien à gauche. Un anneau $\mathbf{Mat}_n(\Delta)$ vérifie donc la condition (i). Nous voyons ainsi que (iv) entraîne (i).

Pour tout anneau B, la transposition des matrices fournit un isomorphisme d'anneaux entre $\mathbf{Mat}_n(B^{\mathrm{op}})$ et $\mathbf{Mat}_n(B)^{\mathrm{op}}$. Ainsi un anneau A vérifie la condition (iv) si et seulement si A^{op} la vérifie. L'équivalence entre (i) et (iv) précédemment obtenue implique donc l'équivalence entre (ii) et (iv). Ceci achève la preuve de l'équivalence des quatre assertions.

Supposons que A vérifie les quatre assertions. Soit I un idéal à gauche minimal de A et S un A-module à gauche simple. L'annulateur de S est un idéal bilatère de A différent de A, c'est donc $\{0\}$. Ainsi I n'annule pas S : il existe $x \in S$ tel que l'homomorphisme $a \mapsto ax$ de I dans S soit non-nul. D'après le lemme de Schur, c'est un isomorphisme. Ainsi S est nécessairement isomorphe à I : il n'y a qu'une seule classe d'isomorphisme de A-module simple.

Si $A = \mathbf{Mat}_n(\Delta)$, comme dans l'assertion (iv), alors le A-module simple est $S = \Delta^n$, vu comme ensemble de vecteurs colonnes. L'anneau $\mathrm{End}_A(S)^{\mathrm{op}}$ est alors Δ, agissant par multiplication à droite coordonnée par coordonnée. L'anneau à division Δ et l'entier positif n apparaissant dans (iv) sont donc uniques, à isomorphisme près pour le premier. Enfin, le A-module régulier est isomorphe à S^n, l'isomorphisme consistant à voir une matrice $n \times n$ comme la suite de ses n vecteurs colonnes. Le A-module régulier est donc complètement réductible de longueur n. □

Un anneau A vérifiant les quatre assertions de la proposition ci-dessus est appelé anneau simple artinien (il n'est pas besoin de préciser à gauche ou à droite).

Exercices.

(1) Soit A un anneau. Montrer que l'application $f \mapsto f(1)$ est un isomorphisme de l'anneau des endomorphismes du A-bimodule régulier sur le centre $Z(A)$ de A. En déduire que le centre d'un anneau simple est un corps. (Indication : si f est un endomorphisme du bimodule régulier, alors $af(1) = f(a1) = f(a) = f(1a) = f(1)a$ pour chaque $a \in A$ et donc $f(1) \in Z(A)$. Dans l'autre sens, si $b \in Z(A)$, alors l'application $a \mapsto ab$ est un endomorphisme du A-bimodule régulier. On vérifie que ces deux applications sont des bijections réciproques et que ce sont des homomorphismes d'anneaux. La dernière question de l'exercice est alors conséquence du lemme de Schur 1.2.4.2.)

(2) Soit Δ un anneau à division et $n \geq 1$ un entier. Montrer que les automorphismes de $\mathbf{Mat}_n(\Delta)$ sont les applications $A \mapsto S\sigma(A)S^{-1}$, où $\sigma \in \mathrm{Aut}(\Delta)$ et $S \in \mathbf{Mat}_n(\Delta)$ avec S inversible.

2.1.2 Anneaux semi-simples artiniens

Le théorème suivant inclut comme cas particulier le fait que tout module sur un anneau simple artinien est complètement réductible.

2.1.2.1 Théorème. *Les propriétés suivantes concernant un anneau A sont équivalentes :*

(i) Le A-module régulier ${}_AA$ est complètement réductible.

(ii) Tout A-module est complètement réductible.

(iii) A est un anneau artinien à gauche et possède un module complètement réductible et fidèle.

(iv) A est produit fini d'anneaux simples artiniens.

Preuve. Supposons (i). Soit M un A-module. Étant donné $m \in M$, le sous-module Am engendré par m est l'image de l'homomorphisme $a \mapsto am$ de ${}_AA$ dans M. Isomorphe à un quotient du module complètement réductible ${}_AA$, le module Am est lui-même complètement réductible, donc est inclus dans le socle de M. Ceci étant vrai pour tout $m \in M$, nous voyons que $M = \operatorname{soc} M$, donc que M est complètement réductible. Cela montre (ii). La réciproque (ii) $\Rightarrow$ (i) est banale.

Supposons (i). D'après l'exercice (1) du paragraphe 1.2.1 et la remarque 1.3.1.2, le A-module à gauche régulier est artinien. L'anneau A est donc artinien à gauche. Par ailleurs, le A-module à gauche régulier est un A-module complètement réductible et fidèle. Ainsi (iii) est vraie.

Réciproquement, supposons (iii), c'est-à-dire supposons l'existence d'un A-module M fidèle et complètement réductible. Pour $m \in M$, posons $I_m = \{a \in A \mid am = 0\}$. Soit $\mathscr{I}$ l'ensemble des idéaux à gauche de A de la forme $I_{m_1} \cap \cdots \cap I_{m_n}$, pour $n \in \mathbf{N}$ et $(m_1, \ldots, m_n) \in M^n$. Comme A est artinien à gauche, $\mathscr{I}$ possède un élément minimal, disons J. Pour chaque $m \in M$, $J \cap I_m$ appartient à $\mathscr{I}$ et est inclus dans J, d'où $J \subseteq I_m$ par minimalité de J. Ainsi $J \subseteq \bigcap_{m \in M} I_m = \operatorname{ann} M = \{0\}$. Écrivant $J = I_{m_1} \cap \cdots \cap I_{m_n}$, ceci signifie que l'homomorphisme $a \mapsto (am_1, \ldots, am_n)$ de ${}_AA$ dans M^n est injectif. Ainsi le A-module à gauche régulier est réalisé

comme un sous-module d'un module complètement réductible. D'après la proposition 1.3.1.4, cela entraîne (i).

Supposons à nouveau (i). L'opposé $\mathrm{End}_A({}_AA)^{\mathrm{op}}$ de l'anneau des endomorphismes du A-module à gauche régulier est isomorphe à A, agissant sur ${}_AA$ par multiplication à droite. D'après le corollaire 1.4.5.3, chaque composante S-isotypique du A-module à gauche régulier est un sous-bimodule simple du A-A-bimodule régulier A. Simplifions la notation en écrivant $A = \bigoplus_{i\in I} B_i$ pour la décomposition du A-module à gauche régulier en somme directe de ses composantes isotypiques. Ici les B_i sont des idéaux bilatères minimaux non-nuls et la somme est finie (à nouveau on utilise l'exercice (1) du paragraphe 1.2.1).

Si $i \neq j$, alors le produit d'un élément de B_i par un élément de B_j est nul, car il appartient à $B_i \cap B_j = 0$. Dans la décomposition $A = \bigoplus_{i\in I} B_i$, le produit s'effectue donc composante par composante. Décomposons l'unité multiplicative de A dans cette somme directe : $1 = \sum_{i\in I} \varepsilon_i$. Fixons $i \in I$. Alors pour chaque $x \in B_i$, on a $x\varepsilon_j = \varepsilon_j x = 0$ pour tout $j \neq i$, et par différence avec $x1 = 1x = x$, on arrive à $\varepsilon_i x = x\varepsilon_i = x$. Nous concluons que B_i est un anneau, de neutre multiplicatif ε_i. La décomposition de ${}_AA$ en ses composantes isotypiques est ainsi un isomorphisme d'anneaux $A = \prod_{i\in I} B_i$ (le produit se fait composante par composante puisque le produit d'un élément de B_i par un élément de B_j est nul dès que $i \neq j$).

Chaque anneau B_i est simple : soit I un idéal bilatère de B_i ; puisque $B_jI = IB_j = 0$ pour tout $j \neq i$, l'égalité $A = \sum_{j\in I} B_j$ montre que I est un idéal bilatère de A ; la minimalité de l'idéal bilatère B_i entraîne alors que $I = 0$ ou $I = B_i$. Par ailleurs (iii) est vraie, donc le A-module à gauche régulier ${}_AA$ est artinien. Chaque sous-module B_i de ${}_AA$ est donc artinien. Compte-tenu de la structure de produit $A = \prod_{i\in I} B_i$, cela signifie que pour chaque i, le B_i-module à gauche régulier est artinien. Ainsi chaque anneau B_i est simple artinien. Cela montre (iv).

Il nous reste à établir que (iv) entraîne (i). Supposons (iv). On écrit $A = \prod_{i\in I}$, où I est un ensemble fini et où chaque B_i est un anneau simple artinien. Ainsi on a une décomposition ${}_AA = \bigoplus_{i\in I} B_i$, où chaque B_i peut être vu comme un module sur lui-même ou sur A. Pour chaque $i \in I$, le B_i-module à gauche régulier est complètement réductible d'après le théorème 2.1.1.1. Alors B_i est encore un module complètement réductible quand on le regarde comme un A-module. En tant que somme directe de modules complètement réductibles, ${}_AA$ est complètement réductible. L'assertion (i) est vraie. □

Un anneau A vérifiant les quatre assertions du théorème 2.1.2.1 est appelé anneau semi-simple artinien. Au vu de l'assertion (iv), A est semi-simple artinien si et seulement si A^{op} l'est, ce qui rend inutile toute précision du genre anneau semi-simple artinien à gauche.

Notons enfin que la preuve du théorème 2.1.2.1 montre que quand on écrit un anneau semi-simple artinien comme un produit $\prod_{i\in I} B_i$ d'anneaux simples artiniens, les B_i sont les idéaux bilatères minimaux de A ; ils sont donc uniques à réindexation près. Les B_i sont aussi les composantes isotypiques du A-module à gauche régulier. On les appelle les composantes simples ou composantes de Wedderburn de A.

2.1.2.2 Proposition. *Sur un anneau semi-simple artinien A, les classes d'isomorphisme de modules simples sont en bijection canonique avec les composantes simples de l'anneau. Plus précisément :*

(i) Tout A-module simple est isomorphe à un idéal à gauche minimal de A.

(ii) Tout idéal à gauche minimal de A est inclus dans une composante simple de A.

(iii) Deux idéaux à gauche minimaux de A sont isomorphes en tant que A-modules si et seulement s'ils sont inclus dans la même composante simple de A.

Preuve. Soit S un A-module simple. Choisissant $x \in S$ non-nul, on construit un homomorphisme surjectif $f : a \mapsto ax$ du A-module à gauche régulier sur S. Soit L un supplémentaire du noyau de f dans ${}_AA$. Alors f induit un isomorphisme de L sur S ; de plus, L est un sous-module simple de ${}_AA$, c'est-à-dire un idéal à gauche minimal de A. Tout ceci prouve (i). Les assertions (ii) et (iii) viennent ensuite de ce que les composantes simples de A sont les composantes isotypiques du A-module à gauche régulier. □

2.1.2.3 Proposition. *Tout quotient d'un anneau semi-simple artinien est un anneau semi-simple artinien. Plus précisément, soient A un anneau semi-simple artinien et $A = \prod_{i\in I} B_i$ sa décomposition en composantes simples ; alors chaque idéal bilatère de A est une somme $\bigoplus_{i\in J} B_i$, où J est une partie de I.*

Preuve. Soit $A = \bigoplus_{i\in I} B_i$ la décomposition en composantes simples d'un anneau semi-simple artinien. Ainsi A est un A-A-bimodule complètement réductible, les B_i sont les composantes isotypiques de A, et ce sont des sous-bimodules simples. Soit K un idéal bilatère de A, autrement dit un sous-bimodule. Alors K est complètement réductible, en tant que A-A-bimodule. Il est donc somme de ses composantes isotypiques, lesquelles sont les intersections de K avec les composantes isotypiques de A (voir l'exercice (1) du paragraphe 1.3.1). Ainsi $K = \bigoplus_{i\in I}(K \cap B_i)$. Comme les A-A-bimodules B_i sont simples, $K \cap B_i$ est soit 0, soit B_i. Ainsi $K = \bigoplus_{i\in J} B_j$, pour une partie $J \subseteq I$. Le quotient A/K est alors isomorphe au produit des B_i pour $i \notin J$; il est donc semi-simple artinien. □

2.1.2.4 Remarque. Soit $A = \prod_{i\in I} B_i$ la décomposition en composantes simples d'un anneau semi-simple artinien. Pour chaque $i \in I$, choisissons un idéal à gauche minimal S_i de la composante B_i. Alors la famille $(S_i)_{i\in I}$ contient un représentant de chaque classe d'isomorphisme de A-module simple. Si $j \neq i$, alors B_j annule S_i, puisque le produit B_jB_i est réduit à $\{0\}$ dans A. L'annulateur de S_i contient donc $\bigoplus_{j\neq i} B_j$, et lui est donc égal. Ainsi S_i est le B_i-module simple que l'on voit comme un A-module à travers l'homomorphisme d'anneaux de A sur $B_i \cong A \,/\, \bigoplus_{j\neq i} B_j$. Le théorème de Wedderburn-Artin nous dit alors que $B_i \cong \mathbf{Mat}_{n_i}(\Delta_i)$, où $\Delta_i = \mathrm{End}_A(S_i)^{\mathrm{op}}$ et n_i est la longueur du Δ_i-module S_i.

2.2 Radical de Jacobson

2.2.1 Définition du radical de Jacobson

2.2.1.1 Proposition. *Soit A un anneau. L'ensemble des idéaux bilatères inclus dans*

$$1 - A^\times = \{a \in A \mid 1 - a \text{ est inversible}\}$$

possède un plus grand élément pour l'inclusion.

Preuve. Soit $\mathscr{I}$ l'ensemble des idéaux bilatères I inclus dans $1 - A^\times$. L'idéal $\{0\}$ appartient à $\mathscr{I}$. Commençons par montrer que $\mathscr{I}$ est stable par somme.

À cet effet, prenons deux éléments I et J de $\mathscr{I}$ et montrons que $I+J$ est dans $\mathscr{I}$. Un élément a de $I+J$ s'écrit $b+c$, avec $b \in I$ et $c \in J$. Comme $I \subseteq 1 - A^\times$, l'élement $1-b$ est inversible. Comme J est un idéal, $(1-b)^{-1}c$ appartient à J ; et puisque $J \subseteq 1-A^\times$, l'élement $1-(1-b)^{-1}c$ est inversible. Ainsi $1 - a = (1 - b)(1 - (1 - b)^{-1}c)$ est inversible.

Notons J la somme de tous les éléments de $\mathscr{I}$. C'est un idéal de A. Ensuite, chaque élément a de J appartient en fait à une somme finie $I_1 + \cdots + I_n$ d'idéaux appartenant à $\mathscr{I}$, et puisque $I_1 + \cdots + I_n$ appartient lui-même à $\mathscr{I}$, l'élément $1 - a$ est inversible. Cela montre que $J \in \mathscr{I}$. Ainsi $\mathscr{I}$ a un plus grand élément, à savoir J. □

Radical de Jacobson d'un anneau : le radical de Jacobson d'un anneau A est le plus grand des idéaux I tels que $1 - a$ soit inversible pour chaque $a \in I$. On le note $J(A)$. Il est manifeste que $J(A^{\mathrm{op}}) = J(A)$.

Traditionnellement, on définit $J(A)$ au moyen de la caractérisation concrète suivante.

2.2.1.2 Proposition. *Pour tout anneau A,*

$$J(A) = \{x \in A \mid \forall a \in A,\ 1 - ax \text{ a un inverse à gauche}\}.$$

Preuve. Appelons I le membre de droite de l'égalité ci-dessus. Il est clairement stable par multiplication à gauche par les éléments de A : $(b, x) \in A \times I \ \Rightarrow\ bx \in I$.

Soit $(b, x) \in A \times I$. Pour tout $a \in A$, l'élément $1 - bax$ admet un inverse à gauche dans A, disons c ; de l'égalité $c(1 - bax) = 1$ vient alors

$$(1 + axcb)(1 - axb) = 1 - ax(1 - c + cbax)b = 1,$$

et donc $1 - axb$ admet un inverse à gauche. On voit ainsi que $xb \in I$. Bref I est stable par multiplication à droite par les éléments de A.

Soit $(x, y) \in I^2$. Pour tout $a \in A$, l'élément $1 - ax$ admet un inverse à gauche, disons b, et puisque $yb \in I$, l'élément $1-ayb$ admet un inverse à gauche, disons c ; des égalités $b(1-ax) = 1$ et $c(1 - ayb) = 1$ vient alors

$$bc(1 - a(x + y)) = bc(1 - ayb)(1 - ax) = b(1 - ax) = 1,$$

et donc $1 - a(x + y)$ admet un inverse à gauche. On voit ainsi que $x + y \in I$. Bref I est stable par addition.

Les deux alinéas précédents établissent que I est un idéal bilatère. Soit $x \in I$. Alors $1 - x$ admet un inverse à gauche, disons a, et $1+ax$ admet un inverse à gauche, disons b. Des égalités $a(1 - x) = 1$ et $b(1 + ax) = 1$, on déduit que $ba = 1$ puis que

$$(1 - x)a = ba(1 - x)a = b(a(1 - x))a = ba = 1$$

et donc $1 - x$ est inversible. Ainsi I est un idéal bilatère inclus dans $1 - A^\times$; par conséquent $I \subset J(A)$.

L'inclusion opposée étant évidente, l'égalité annoncée a lieu. □

Voyons à présent le lien entre le radical de Jacobson d'un anneau A et les A-modules.

Module régulier (rappels) : le A-module régulier ${}_AA$ est le groupe abélien $(A,+)$, muni de l'opération à gauche de A par multiplication. Les sous-modules de ${}_AA$ sont les idéaux à gauche de l'anneau A. Un endomorphisme de ${}_AA$ est de la forme $a \mapsto ab$, où $b \in A$.

La première assertion du théorème suivant montre que $J(A)$ est le radical du A-module régulier : $J(A) = \operatorname{rad}{}_AA$. Puisque A et A^{op} ont même radical de Jacobson, $J(A)$ est aussi le radical du A-module à droite régulier : $J(A) = \operatorname{rad} A_A$.

Rappelons que l'annulateur d'un A-module M est le noyau de l'homomorphisme d'anneaux de A dans $\mathrm{End}_{\mathbf{Z}}(M)$ définissant la structure de A-module.

2.2.1.3 Théorème. *Soit A un anneau.*

(i) $J(A)$ coïncide avec les deux ensembles suivants :
- *le radical $\operatorname{rad}{}_AA$ du A-module à gauche régulier, c'est-à-dire l'intersection des idéaux à gauche maximaux de A ;*
- *l'intersection des idéaux annulateurs des A-modules simples.*

(ii) Si M est un A-module, alors $J(A)M \subseteq \operatorname{rad} M$.

(iii) (Lemme de Nakayama) Soit M est un A-module de type fini. Si $J(A)M = M$, alors $M = 0$.

Preuve. Soit $z \in A$. Si $z \notin \operatorname{rad}{}_AA$, alors il existe un idéal à gauche maximal $\mathfrak{m}$ tel que $z \notin \mathfrak{m}$. Alors $z + \mathfrak{m}$ engendre le A-module simple $A/\mathfrak{m}$, donc il existe $a \in A$ tel que $1 - az \in \mathfrak{m}$. Cela interdit $1 - az$ inversible à gauche, et ainsi $z \notin J(A)$. Réciproquement si $z \notin J(A)$, alors il existe $a \in A$ tel que $1 - az$ n'est pas inversible à gauche. L'idéal à gauche $A(1 - az)$ est alors propre, donc contenu dans un idéal à gauche maximal $\mathfrak{m}$. Alors $1 - az \in \mathfrak{m}$, d'où $z \notin \mathfrak{m}$, puis $z \notin \operatorname{rad}{}_AA$. Ces raisonnements prouvent l'égalité $J(A) = \operatorname{rad}{}_AA$.

Notons $\mathfrak{r}$ l'intersection des annulateurs des A-modules simples. Chaque idéal à gauche maximal $\mathfrak{m}$ contient l'annulateur d'un A-module simple S (prendre $S = A/\mathfrak{m}$), donc contient $\mathfrak{r}$. On en déduit $\operatorname{rad}{}_AA \supseteq \mathfrak{r}$. Soit S un A-module simple. Chaque élément non-nul x de S détermine un homomorphisme surjectif $a \mapsto ax$ du A-module régulier ${}_AA$ sur S. Comme S est simple, le noyau $\mathfrak{m}_x$ de cet homomorphisme est un idéal à gauche maximal. On voit ainsi que l'annulateur de S, qui est l'intersection des $\mathfrak{m}_x$ pour $x \in S \setminus \{0\}$, contient $\operatorname{rad}{}_AA$. Le radical $\operatorname{rad}{}_AA$ est donc inclus dans l'annulateur de n'importe quel A-module simple, c'est-à-dire $\operatorname{rad}{}_AA \subset \mathfrak{r}$. L'égalité $\mathfrak{r} = \operatorname{rad}{}_AA$ a donc bien lieu, ce qui conclut la preuve de (i).

Soit M un A-module. Pour chaque sous-module maximal $L \subseteq M$, le A-module M/L est simple, donc est annulé par $J(A)$. Ainsi $J(A)M \subseteq L$. Le sous-module $J(A)M$ est donc inclus dans tous les sous-modules maximaux de M, d'où (ii).

Enfin soit M un A-module de type fini tel que $J(A)M = M$. L'assertion (ii) implique alors que $\operatorname{rad} M = M$. D'après la proposition 1.3.3.2 (i), cela entraîne que $M = 0$. Nous avons démontré (iii). □

Remarque. Un idéal d'un anneau A est dit primitif s'il est l'annulateur d'un A-module simple ; quand A est commutatif, un idéal est primitif si et seulement s'il est maximal. La proposition précédente entraîne que $J(A)$ est l'intersection des idéaux primitifs de A.

Les premières définitions du radical d'un anneau A étaient limitées au cas d'un anneau artinien ; quand A est artinien à gauche ou à droite, $J(A)$ est le plus grand idéal nilpotent. L'apport de Jacobson fut de trouver la définition adaptée au cas général : il a compris qu'un anneau A s'étudiait avec ses modules, et a défini le radical de A comme l'intersection des idéaux primitifs de A. L'inconvénient de cette définition est que l'égalité $J(A) = J(A^{\mathrm{op}})$ n'est pas évidente : la notion d'idéal primitif n'est pas stable par passage à l'anneau opposé.

Enfin, de nombreux auteurs définissent $J(A)$ comme étant le radical du A-module à gauche régulier. Avec cette approche, l'égalité $J(A) = J(A^{\mathrm{op}})$ ne coule pas de source : elle exprime que les radicaux des A-modules réguliers, à gauche et à droite, sont égaux. Notons en revanche qu'en l'absence d'hypothèse sur l'anneau A, les socles des A-modules réguliers, à gauche et à droite, sont généralement différents.

2.2.1.4 Corollaire. *Soit A un anneau. Regarder un $A/J(A)$-module comme un A-module fournit une bijection de l'ensemble des classes d'isomorphisme de $A/J(A)$-modules simples sur l'ensemble des classes d'isomorphisme de A-modules simples.*

Preuve. Soit I un idéal bilatère de A. Un A/I-module M peut-être vu comme un A-module en composant l'homomorphisme d'anneaux de A/I dans $\mathrm{End}_{\mathbf{Z}}(M)$ avec l'épimorphisme canonique de A sur A/I. Les sous-modules de M sont les mêmes qu'on regarde M comme un module sur A ou sur A/I ; ainsi M est simple en tant que A-module si et seulement s'il l'est en tant que A/I-module. Si N est un second A/I-module, alors les groupes d'homomorphismes entre M et N sont les mêmes que l'on regarde M et N comme des modules sur A ou sur A/I ; ainsi M et N sont isomorphes en tant que A-modules si et seulement s'ils le sont en tant que A/I-modules. Enfin, un A-module provient par cette construction d'un A/I-module si et seulement si $I \subseteq \mathrm{ann}\, M$.

Le corollaire provient de toutes ces remarques et du fait que $J(A)$ est contenu dans l'annulateur de chaque A-module simple. □

Exercices.

(1) Soit A un anneau. Montrer que tout idéal bilatère maximal de A contient $J(A)$.

(2) Soit A un anneau. Montrer qu'un élément $x \in A$ est inversible si et seulement si $x + J(A)$ est inversible dans $A/J(A)$.

(3) On dit qu'un idéal I d'un anneau A est nilpotent s'il existe un entier naturel n tel que $I^n = \{0\}$; autrement dit, si le produit de n éléments de I (pas nécessairement distincts) est toujours nul. Montrer que tout idéal bilatère nilpotent I de A est inclus dans le radical de Jacobson $J(A)$. (Indication : I est inclus dans $1 - A^{\times}$, car pour chaque $x \in I$, $1 - x$ est inversible, d'inverse $1 + x + x^2 + \cdots$.)

(4) Soit A un anneau. Montrer l'existence d'un A-module complètement réductible d'annulateur $J(A)$.

(5) Soit e un idempotent d'un anneau A ; ainsi eAe est un anneau de neutre multiplicatif e. Montrer que $J(eAe) = eJ(A)e$. (Indication : un élément $x \in eJ(A)e$ vérifie $x = exe$ et $x \in J(A)$; $1 - x$ possède donc un inverse dans A, disons y, et on vérifie que eye est un inverse de $e - x$ dans eAe. Ainsi $eJ(A)e$ est un idéal bilatère de eAe contenu dans $e - (eAe)^\times$, d'où $eJ(A)e \subseteq J(eAe)$. Dans l'autre sens, soit $z \in J(eAe)$. Prenons $a \in A$. Alors $eaz = eaez \in J(eAe)$, donc $e - eaz$ possède un inverse à gauche y dans eAe, c'est-à-dire $y = ye$ et $ye(1 - az) = e$. On calcule ensuite $(1 - e + y)(1 - az) = (1-e+ye)(1-az) = (1-e)(1-az)+e = 1-t$, avec $t = (1-e)az$. Maintenant $z \in eAe$ entraîne $t^2 = 0$, et donc $1 - t$ est inversible. Il s'ensuit que $1 - az$ possède un inverse à gauche dans A. Ceci étant vrai pour tout $a \in A$, on a $z \in J(A)$. Ce raisonnement montre l'inclusion $J(eAe) \subseteq J(A) \cap eAe = eJ(A)e$.)

(6) Montrer l'égalité $\mathbf{Mat}_n(J(A)) = J(\mathbf{Mat}_n(A))$ pour tout anneau A et tout entier $n \geq 1$.

(7) Soient A un anneau et I un idéal bilatère de A inclus dans le radical de Jacobson $J(A)$. Montrer que le radical de Jacobson de A/I est $J(A)/I$.

(8) On définit le socle à gauche d'un anneau A comme étant le socle $\operatorname{soc}{}_A A$ du A-module régulier. De même, on définit le socle à droite de A comme étant le socle $\operatorname{soc} A_A$ du module à droite régulier ; ainsi le socle à droite de A est le socle à gauche de A^{op}. Montrer que ces socles sont des idéaux bilatères de A.

2.2.2 Cas d'un anneau artinien

2.2.2.1 Théorème. *Soit A un anneau artinien à gauche ou à droite.*

(i) A est un anneau semi-simple si et seulement si $J(A) = \{0\}$.

(ii) L'anneau $A/J(A)$ est semi-simple artinien.

Preuve. Quitte à remplacer A par A^{op}, nous pouvons supposer que A est artinien à gauche.

(i) Le A-module à gauche régulier est artinien. D'après la proposition 1.3.3.2 (iii), il est complètement réductible si et seulement si son radical est réduit à 0. Or ce radical est $J(A)$, d'après le théorème 2.2.1.3.

(ii) Le quotient $B = A/J(A)$ du A-module à gauche régulier est ce que nous avions appelé la tête de ${}_A A$ au paragraphe 1.3.3. D'après la propriété 1.3.3.1 (i), le radical de B est $\{0\}$. En tant que quotient d'un module artinien, B est un A-module artinien. Il est donc complètement réductible d'après la proposition 1.3.3.2 (iii). Maintenant, B est en fait un anneau, et sa structure de A-module à gauche s'identifie à sa structure de B-module à gauche régulier à travers l'homomorphisme d'anneaux de A sur B. On voit ainsi que le B-module à gauche régulier est complètement réductible, c'est-à-dire que B est un anneau semi-simple artinien.

On peut formuler l'argument prouvant (ii) d'une manière un peu différente. D'abord, $A/J(A)$ est un anneau artinien à gauche, parce que c'est un quotient de l'anneau artinien à gauche A. Ensuite, le radical de Jacobson de $A/J(A)$ est $\{0\}$, d'après l'exercice (7) ci-dessus. On peut ainsi utiliser (i). □

2.2.2.2 Corollaire. *Soit A un anneau artinien à gauche ou à droite.*

(i) Un A-module M est complètement réductible si et seulement si $J(A)M = 0$.

(ii) Pour tout A-module M, on a les égalités

$$\operatorname{rad} M = J(A)M \quad et \quad \operatorname{soc} M = \{x \in M \mid J(A)x = 0\}.$$

(iii) Un A-module M est complètement réductible si et seulement si son radical est 0. En particulier, la tête d'un A-module est toujours complètement réductible.

Preuve. L'annulateur d'un A-module simple contient $J(A)$, donc $J(A)$ annule tout A-module simple. Il s'ensuit que $J(A)$ annule tout A-module complètement réductible. Dans l'autre sens, si l'annulateur d'un A-module M contient $J(A)$, alors M peut être vu comme un $A/J(A)$-module. Or tout $A/J(A)$-module est complètement réductible, puisque l'anneau $A/J(A)$ est semi-simple artinien. Ainsi M est somme de ses sous-modules simples, et ceci est vrai qu'on regarde M comme un module sur $A/J(A)$ ou sur A. Nous avons prouvé (i).

Soit M un A-module. L'assertion (i) nous dit que $M/J(A)M$ est un A-module complètement réductible. Son radical est donc nul, ce qui implique que $\operatorname{rad} M \subseteq J(A)M$. Compte-tenu du théorème 2.2.1.3 (ii), cette inclusion est une égalité. Par ailleurs, le socle de M est le plus grand sous-module complètement réductible de M. Vu l'assertion (i), le socle de M est le plus grand sous-module de M annulé par $J(A)$. Cela montre l'égalité $\operatorname{soc} M = \{x \in M \mid J(A)x = 0\}$. Nous avons donc prouvé (ii).

L'assertion (iii) est une conséquence immédiate de (i) et (ii). □

On définit le produit de deux idéaux bilatères I et J d'un anneau A par

$$IJ = \{a_1b_1 + \cdots + a_kb_k \mid k \in \mathbf{N},\ (a_i, b_i) \in (I \times J)^k\}\,;$$

c'est un idéal bilatère de I. On définit alors la puissance n-ième I^n comme étant le produit itéré de I avec lui-même, n fois.

Idéal nilpotent : un idéal I d'un anneau A est dit nilpotent s'il existe un entier naturel n tel que $I^n = \{0\}$, autrement dit, tel que le produit de n éléments de I est toujours nul.

L'exercice (3) du paragraphe précédent nous dit que tout idéal bilatère nilpotent d'un anneau A est inclus dans le radical de Jacobson $J(A)$. Le (i) du théorème ci-dessous affirme que la réciproque est vraie quand A est artinien à gauche ou à droite ; dans ce cas, $J(A)$ est le plus grand idéal nilpotent de A.

2.2.2.3 Théorème. *Soit A un anneau artinien à gauche.*

(i) L'idéal $J(A)$ est nilpotent.

(ii) (Théorème de Hopkins) L'anneau A est noethérien à gauche.

Preuve. (i) Nous avons $J(A) \supseteq J(A)^2 \supseteq J(A)^3 \supseteq \cdots$, et comme A est artinien, il existe un entier naturel n tel que $J(A)^n = J(A)^{n+1}$. Supposons que $J(A)^n \neq 0$. Alors il existe un idéal

à gauche I, minimal parmi les idéaux tels que $J(A)^n I \neq 0$. Soit $x \in I$ tel que $J(A)^n x \neq 0$. Alors $J(A)x$ est un idéal à gauche inclus dans I et $J(A)^n(J(A)x) = J(A)^{n+1}x = J(A)^n x \neq 0$, donc $I = J(A)x$ par minimalité de I. Ainsi il existe $z \in J(A)$ tel que $x = zx$. Puisque $1 - z$ est inversible, cela entraîne $x = 0$, ce qui est absurde.

(ii) On munit le A-module régulier ${}_AA$ de la filtration décroissante finie $M_n = J(A)^n$. Le n-ième facteur de la filtration M_n/M_{n+1} est annulé par $J(A)$. D'après le corollaire 2.2.2.2 (i), il est complètement réductible. Or il est artinien, donc il est noethérien (remarque 1.3.1.2). Utilisant de façon répétée la proposition 1.2.1.2 (ii), on en déduit que le A-module régulier est noethérien. □

Remarque. Bien évidemment, la conclusion de l'énoncé (i) est également valide si l'anneau A est supposé artinien à droite. Notons cependant qu'il existe des anneaux artiniens (et donc noethériens) à gauche, qui ne sont pas noethériens (et donc pas artiniens) à droite. Un exemple est l'anneau des matrices de la forme $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ avec $a, b \in \mathbf{R}$ et $c \in \mathbf{Q}$; voir [1], p. 130.

2.2.2.4 Corollaire. *Soit A un anneau artinien à gauche. Alors tout A-module de type fini est artinien et noethérien.*

Preuve. C'est une conséquence immédiate du théorème de Hopkins ci-dessus et des propositions 1.2.1.2 et 1.2.1.3. □

Rappelons qu'on dit qu'un sous-module N d'un module M est superflu si pour tout sous-module $X \subsetneq M$, on a $N + X \subsetneq M$, et qu'on dit que N est essentiel si pour tout sous-module $X \neq 0$, on a $N \cap X \neq 0$.

2.2.2.5 Corollaire. *Soit A un anneau artinien à gauche ou à droite.*

(i) Soit M un A-module. Les trois propriétés suivantes sont équivalentes : $M = \operatorname{rad} M$, $\operatorname{soc} M = 0$, $M = 0$.

(ii) Soit M un A-module et $N \subseteq M$ un sous-module. Alors N est superflu si et seulement s'il est inclus dans $\operatorname{rad} M$.

(iii) Soit M un A-module et $N \subseteq M$ un sous-module. Alors N est essentiel si et seulement s'il contient $\operatorname{soc} M$.

Preuve. Soit M un A-module. Nous allons montrer les deux implications

$$M \neq 0 \;\Rightarrow\; \operatorname{soc} M \neq 0 \qquad \text{et} \qquad M = \operatorname{rad} M \;\Rightarrow\; M = 0.$$

Notons $J = J(A)$; c'est un idéal nilpotent d'après le théorème 2.2.2.3 (i). Supposons $M \neq 0$. Alors il existe n tel que $J^n M \neq 0$ et $J^{n+1} M = 0$. D'après le corollaire 2.2.2.2 (i), on a alors $J^n M \subseteq \operatorname{soc} M$, ce qui assure $\operatorname{soc} M \neq 0$. Supposons maintenant $M = \operatorname{rad} M$. Le corollaire 2.2.2.2 (ii) nous dit alors que $M = JM$. De là, $M = JM = J^2M = J^3M = \cdots$, et la

nilpotence de J conduit à $M = 0$. Nos deux implications sont établies, et elles démontrent l'assertion (i).

Soit N un sous-module d'un A-module M. Supposons que N soit inclus dans $\operatorname{rad} M$. Soit X un sous-module de M tel que $X \subsetneq M$. Alors $M/X \neq 0$, et (i) nous dit qu'alors $M/X \neq \operatorname{rad}(M/X)$. Cela entraîne $X + \operatorname{rad} M \subsetneq M$. À fortiori, $X + N \subsetneq M$. Nous avons ainsi montré que N était superflu. L'assertion (ii) découle maintenant de la proposition 1.3.4.1.

Soit N un sous-module d'un A-module M. Supposons que N contienne $\operatorname{soc} M$. Soit X un sous-module non-nul de M. Des inclusions $N \supseteq \operatorname{soc} M \supseteq \operatorname{soc} X$, nous déduisons que $N \cap X \supseteq \operatorname{soc} X$. Mais d'après l'assertion (i), le fait que X soit non-nul implique que $\operatorname{soc} X \neq 0$, d'où $N \cap X \neq 0$. Nous avons ainsi montré que N était essentiel. L'assertion (iii) découle maintenant de la proposition 1.3.4.1. □

Exercices.

(1) Soit A un anneau artinien à gauche, $e \in A$ un élément idempotent. Montrer que l'anneau eAe est artinien à gauche.

(2) Soit A un anneau artinien à gauche, soient m et n deux entiers naturels. Montrer que si les A-modules à gauche A^m et A^n sont isomorphes, alors $m = n$.

(3) Soit A un anneau artinien à gauche ou à droite. Alors le nombre de classes d'isomorphisme de A-modules à gauche simples est fini et égal au nombre de composantes simples de l'anneau semi-simple artinien $A/J(A)$. Montrer que c'est aussi le nombre de classes d'isomorphisme de A-modules à droite simples. (Note : une famille de A-modules simples $(S_1, \ldots, S_k)$ est dite basique si elle comporte un et un seul représentant de chaque classe d'isomorphisme de A-modules simples.)

(4) Soit A un anneau artinien à gauche ou à droite et soit $(M_\lambda)_{\lambda \in \Lambda}$ une famille de A-modules. Posons $M = \bigoplus_{\lambda \in \Lambda} M_\lambda$. Montrer les égalités $\operatorname{rad} M = \bigoplus_{\lambda \in \Lambda} \operatorname{rad} M_\lambda$ et $\operatorname{soc} M = \bigoplus_{\lambda \in \Lambda} \operatorname{soc} M_\lambda$. (Indication : utiliser le corollaire 2.2.2.2 (ii).)

(5) Soit A un anneau artinien à gauche ou à droite et soit M un A-module. On appelle longueur de Loewy de M le plus petit entier naturel ℓ pour lequel il existe une filtration finie $0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_{\ell-1} \subseteq M_\ell = M$ de M dont tous les quotients successifs M_n/M_{n-1} sont complètement réductibles. Montrer que la longueur de Loewy de M est bien définie et est le plus petit entier naturel ℓ tel que $J(A)^\ell M = 0$.

(6) Soit A un anneau commutatif. L'ensemble des éléments nilpotents de A est un idéal, qu'on appelle le nilradical de A et qu'on note $\sqrt{(0)}$ (on sait même que $\sqrt{(0)}$ est l'intersection des idéaux premiers de A). Montrer que si A est artinien, alors $J(A) = \sqrt{(0)}$.

(7) Soit A un anneau commutatif intègre principal, soit $a \in A$ non-nul. Calculer le radical de Jacobson de l'anneau $A/(a)$. Montrer que $A/(a)$ est semi-simple artinien si et seulement si a est sans facteur carré (c'est-à-dire n'est pas divisible par le carré d'un élément irréductible). Retrouver le résultat de l'exercice (3) du paragraphe 1.3.1.

2.3 Quelques résultats concernant les modules projectifs et injectifs

2.3.1 Cas d'un anneau local

Rappel : un anneau A est dit local si l'ensemble des éléments non-inversibles de A est un idéal de A.

2.3.1.1 Proposition. *Étant donné un anneau A, les quatre assertions suivantes sont équivalentes :*

(i) *A est local.*

(ii) *$J(A)$ est l'ensemble des éléments non-inversibles de A.*

(iii) *$A/J(A)$ est un anneau à division.*

(iv) *$A \neq \{0\}$ et pour chaque $x \in A$, x ou $1-x$ est inversible.*

(v) *A possède exactement un idéal à gauche maximal.*

Preuve. Nous allons montrer les implications (i) $\Rightarrow$ (iv) $\Rightarrow$ (ii) et (ii) $\Rightarrow$ (v) $\Rightarrow$ (iii) $\Rightarrow$ (ii). Cela établira notre proposition, car visiblement (ii) entraîne (i).

Supposons (i). Alors $I = A \setminus A^\times$ est un idéal de A. Soit $x \in A$. Alors x ou $1-x$ ne peuvent appartenir tous deux à I, car leur somme n'appartient pas à I. Donc soit x, soit $1-x$ est inversible. L'assertion (iv) est donc vraie.

Supposons (iv). Soit x un élément de A n'appartenant pas à $J(A)$. Alors il existe $a \in A$ tel que $1-ax$ ne soit pas inversible à gauche. Il s'ensuit que ax est inversible, d'où $b \in A$ tel que $bax = 1$. Ainsi x est inversible à gauche. De même, x est inversible à droite, et donc inversible tout court. Ainsi $J(A)$ contient l'ensemble $A \setminus A^\times$ des éléments non-inversibles de A. L'inclusion opposée étant évidente (A est supposé non-nul), cela entraîne que (ii) est vraie.

Supposons (ii). L'élément 0 appartient à $J(A)$ donc n'est pas inversible, donc $A \neq \{0\}$, donc A possède au moins un idéal à gauche maximal. Soit $\mathfrak{m}$ un idéal à gauche maximal. Chaque élément de $\mathfrak{m}$ est non-inversible à gauche, donc est non-inversible tout court, donc appartient à $J(A)$; ainsi $\mathfrak{m} \subseteq J(A)$. Le théorème 2.2.1.3 (i) permet de conclure à l'égalité $\mathfrak{m} = J(A)$, assurant l'unicité affirmée dans (v).

Supposons (v). Le théorème 2.2.1.3 (i) entraîne que $J(A)$ est l'unique idéal maximal à gauche de A. L'anneau quotient $B = A/J(A)$ possède alors exactement deux idéaux à gauche, à savoir $\{0\}$ et A. Ainsi le B-module régulier à gauche ${}_BB$ est simple, donc son anneau d'endomorphisme B^{op} est un anneau à division (lemme de Schur), et l'énoncé (iii) est satisfait.

Supposons (iii). Soit x un élément de A n'appartenant pas à $J(A)$. L'élément $x + J(A)$ du quotient $A/J(A)$ est alors non-nul, donc est inversible puisque nous supposons que (iii) est vraie. Il existe donc $y \in A$ tel que $yx \equiv xy \equiv 1$ modulo $J(A)$. Ainsi $1-yx$ et $1-xy$ appartiennent à $J(A)$, et donc yx et xy sont inversibles. Cela entraîne que x est inversible à gauche et à droite, donc inversible. Nous avons donc montré que $J(A) \supseteq A \setminus A^\times$. L'inclusion opposée étant évidente ((iii) interdit à A d'être l'anneau nul), cela entraîne (ii). □

Il est bien sûr possible de remplacer « gauche » par « droite » dans l'énoncé (v). En contemplant l'exemple de $\mathbf{Mat}_n(k)$, où k est un corps, on observera qu'on ne peut en revanche pas remplacer « gauche » par « bilatère ».

2.3.1.2 Proposition.

Tout module projectif de type fini sur un anneau local est libre.

Preuve. Soit A un anneau local. On pose $\overline{A} = A/J(A)$. Pour tout A-module M, on pose $\overline{M} = M/J(A)M$; c'est un A-module qu'on peut aussi regarder comme un $\overline{A}$-module.

Soit P un A-module projectif de type fini. D'après la proposition 1.3.1.3, $\overline{P}$ est un $\overline{A}$-module libre. Il existe donc un A-module libre de type fini F et un isomorphisme $g : \overline{F} \to \overline{P}$ de $\overline{A}$-modules, ou de A-modules, c'est ici pareil. Comme F est un A-module projectif et que l'homomorphisme canonique $p : P \to \overline{P}$ est surjectif, on peut compléter le diagramme ci-dessous par un homomorphisme h :

$$\begin{array}{ccc} F & \overset{h}{\twoheadrightarrow} & P \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle p} \\ \overline{F} & \underset{g}{\longrightarrow} & \overline{P}. \end{array}$$

L'application $p \circ h = g \circ f$ étant surjective, on a $(\operatorname{im} h) + J(A)P = P$. Ainsi $J(A)(\operatorname{coker} h) = \operatorname{coker} h$. Or $\operatorname{coker} h$ est un A-module de type fini puisque P est de type fini. Le lemme de Nakayama nous dit alors que $\operatorname{coker} h = 0$, c'est-à-dire que h est surjectif.

Du coup, P étant projectif, on peut trouver un homomorphisme $k : P \to F$ tel que $h \circ k = \mathrm{id}_P$. Alors $g \circ f \circ k = p \circ h \circ k = p$ est surjectif, et comme g est un isomorphisme, $f \circ k$ est surjectif. Ainsi $(\operatorname{im} k) + J(A)F = F$, c'est-à-dire $J(A)(\operatorname{coker} k) = \operatorname{coker} k$. Comme F est de type fini, $\operatorname{coker} k$ est de type fini, et le lemme de Nakayama nous dit que $\operatorname{coker} k = 0$. Bref k est surjectif. Combiné à $h \circ k = \mathrm{id}_P$, cela nous donne que k est un isomorphisme. □

Kaplansky a démontré que l'hypothèse « de type fini » était en fait inutile dans l'énoncé ci-dessus (Ann. of Math. **68** (1958), pp. 372–377).

2.3.2 Idempotents

Rappel : un idempotent d'un anneau A est un élément $e \in A$ non-nul tel que $e^2 = e$. Je ne suis pas un fanatique de la condition $e \neq 0$, mais elle est traditionnelle.

De façons peut-être surprenante de prime abord, l'étude des modules projectifs sur un anneau passe par une étude des idempotents de cet anneau. (À dire vrai, il existe d'autres méthodes, mais celle-ci conserve son attrait malgré son âge vénérable.) Commençons par une introduction sur la signification des idempotents.

Soit M un groupe abélien et appelons B l'anneau de ses endomorphismes. Considérons une décomposition en somme directe $M = \bigoplus_{i \in I} M_i$, avec I fini et $M_i \neq 0$ pour tout $i \in I$. Pour chaque $i \in I$, la projection e_i sur M_i parallèlement à $\sum_{j \neq i} M_j$ est un élément de B ; concrètement si $x \in M$ s'écrit $\sum_{i \in I} x_i$ dans la décomposition, alors $e_i(x) = x_i$. Ces éléments

e_i sont des idempotents de l'anneau B et vérifient les relations $e_i \circ e_j = 0$ si $i \neq j$, et $\sum_{i\in I} e_i = \mathrm{id}_M$. Réciproquement, toute famille finie $(e_i)_{i\in I}$ d'idempotents de B vérifiant ces relations détermine une décomposition en somme directe $M = \bigoplus_{i\in I} M_i$, avec $M_i = \operatorname{im} e_i$. Bien évidemment, ce résultat se généralise aux décompositions d'un module sur un anneau.

Au début du cours, nous avions déclaré qu'un moyen d'étudier un anneau A était de regarder ses modules, c'est-à-dire ses actions sur des groupes abéliens. Autrement dit, nous essayons de tirer des informations sur A à partir de nos connaissances sur les anneaux $\mathrm{End}_{\mathbf{Z}}(M)$, ces derniers étant censés être bien connus, ou du moins assez concrets. Nous allons donc copier dans un anneau A quelconque la construction précédente. Voici les définitions pertinentes.

Soit A un anneau. Deux idempotents e et f sont dits orthogonaux si $ef = fe = 0$. Alors si $(e_i)_{i\in I}$ est une famille finie d'idempotents deux à deux orthogonaux, $e = \sum_{i\in I} e_i$ est un idempotent. Réciproquement, une décomposition idempotente d'un idempotent e est une écriture de e comme une somme finie $\sum_{i\in I} e_i$ d'idempotents deux à deux orthogonaux. Un idempotent est dit primitif s'il ne s'écrit pas comme somme de deux idempotents orthogonaux, autrement dit si sa seule décomposition idempotente est la décomposition banale, réduite à un seul terme.

Exemples.

(1) Soit e un idempotent d'un anneau A. Si $e \neq 1$, alors e et $1 - e$ sont des idempotents orthogonaux et $1 = e + (1 - e)$ est une décomposition idempotente de l'unité.

(2) Soient A un anneau non-nul et n un entier strictement positif. Pour $i \in \{1, \ldots, n\}$, notons E_{ii} la matrice à coefficients dans A avec zéro partout sauf un à la position (i, i). Alors dans l'anneau $\mathbf{Mat}_n(A)$, $1 = \sum_{i=1}^{n} E_{ii}$ est une décomposition idempotente de l'unité.

(3) Soit A un anneau et e un idempotent de A. Si $e = \sum_{i\in I} e_i$ une décomposition idempotente de e, alors chaque e_i appartient à l'anneau eAe, et $e = \sum_{i\in I} e_i$ est une décomposition idempotente de l'unité dans eAe. Réciproquement, chaque décomposition idempotente de l'unité dans eAe est une décomposition idempotente de e dans A.

Deux idempotents e et f de A sont dits équivalents s'il existe $a \in eAf$ et $b \in fAe$ tels que $ab = e$ et $ba = f$; on écrit alors $e \simeq f$. Nous noterons $\mathrm{pi}(A)$ l'ensemble des idempotents primitifs de A et $\mathrm{pi}(A)/\simeq$ l'ensemble des classes d'équivalence d'idempotents primitifs.

Nous concluons ce paragraphe avec deux résultats qui comparent les idempotents d'un anneau A avec ceux du quotient A/I, où I est un idéal bilatère de A contenu dans le radical de Jacobson $J(A)$. Le premier résultat dit en particulier qu'un idempotent de A n'appartient jamais à $J(A)$, et que si deux idempotents e et f sont congrus modulo $J(A)$, alors ils sont équivalents.

2.3.2.1 Proposition. *Soient A un anneau et I un idéal bilatère de A contenu dans le radical de Jacobson $J(A)$.*

(i) L'image d'un idempotent e de A par l'homomorphisme canonique de A sur A/I est un idempotent $\overline{e}$ de A/I.

(ii) Deux idempotents e et f de A sont équivalents si et seulement si leurs images $\overline{e}$ et $\overline{f}$ dans A/I sont équivalentes.

Preuve. (i) Soit e un idempotent de A et soit $\overline{e}$ son image dans A/I. Certainement $\overline{e}^2 = \overline{e}$. Par ailleurs, $1 - e$ n'est pas inversible car $e \neq 0$ et $e(1-e) = 0$. Ceci implique que $e \notin J(A)$, et par voie de conséquence $\overline{e} \neq 0$.

(ii) Il est clair que si e et f sont équivalents, alors $\overline{e}$ et $\overline{f}$ le sont. Réciproquement, supposons que $\overline{e} \simeq \overline{f}$. Il existe $\overline{a} \in \overline{eAf}$ et $\overline{b} \in \overline{fAe}$ tels que $\overline{ab} = \overline{e}$ et $\overline{ba} = \overline{f}$. Remontons $\overline{a}$ et $\overline{b}$ en des éléments a et b de A. Quitte à remplacer a par eaf et b par fbe, on peut supposer que $a \in eAf$ et $b \in fAe$. Maintenant $e - ab \in I \cap eAe$, et l'exercice (5) du paragraphe 2.2.1 donne

$$I \cap eAe = eIe \subseteq eJ(A)e = J(eAe).$$

Ceci garantit que ab est un élément inversible de eAe. De même, ba est un élément inversible de fAf. Il existe donc des éléments $c \in eAe$ et $d \in fAf$ tels que $abc = e$ et $dba = f$. Mais alors $db = dbe = dbabc = fbc = bc$, et donc $e \simeq f$. □

L'exercice (3) du paragraphe 2.2.1 montre que chaque idéal nilpotent de A est inclus dans $J(A)$, donc convient dans le rôle de I.

2.3.2.2 Théorème (relèvement des idempotents). *Soit I un idéal bilatère nilpotent d'un anneau A. On note $a \mapsto \overline{a}$ l'homomorphisme canonique de A sur A/I.*

(i) Pour chaque idempotent $\overline{c}$ de l'anneau A/I, il existe un idempotent e de A tel que $\overline{e} = \overline{c}$. De plus, e peut être choisi comme un polynôme en c à coefficients entiers sans terme constant.

(ii) Soit e un idempotent de A. Pour chaque décomposition idempotente $\overline{e} = \overline{c_1} + \cdots + \overline{c_n}$ dans A/I, il existe une décomposition idempotente $e = e_1 + \cdots + e_n$ dans A telle que $\overline{e_i} = \overline{c_i}$. En particulier, e est primitif si et seulement si $\overline{e}$ est primitif.

Preuve. (i) Soit $c \in A$ un relevé de $\overline{c}$. Soit $\mathscr{E}$ l'ensemble des $a \in A$ s'écrivant comme polynôme sans terme constant en c et tels que $\overline{a} = \overline{c}$. Si $a \in \mathscr{E}$, alors $a^2 - a$ appartient à I donc est nilpotent : on peut ainsi noter $n(a)$ le plus petit entier naturel n tel que $(a^2 - a)^n = 0$. Soit $e \in \mathscr{E}$ choisi de sorte que $n(e)$ est minimal. Posons $t = e^2 - e$ et $e' = e - 2et + t$. Certainement $t \in I$ et $e' \in \mathscr{E}$; un calcul facile fournit $(e')^2 - e' = 4t^3 - 3t^2$. Si $t \neq 0$, alors $n(e) > 1$, d'où $n(e') < n(e)$, ce qui contredit le choix de e. Bref $t = 0$ et e est le relèvement cherché de c.

(ii) On procède par récurrence sur n, le cas $n = 1$ étant évident. Admettons le résultat pour $n - 1$. Puisque $\overline{ec_1e} = \overline{c_1}$ est un idempotent de A/I, nous pouvons trouver un idempotent e_1 de A s'écrivant comme un polynôme sans terme constant en ec_1e et tel que $\overline{e_1} = \overline{c_1}$. Alors $e_1 \in eAe$ et $e' = e - e_1$ est un idempotent orthogonal à e_1. Notre hypothèse de récurrence nous autorise à remonter la décomposition idempotente à $n-1$ termes $\overline{e'} = \overline{c_2} + \cdots + \overline{c_n}$ dans A/I en une décomposition idempotente $e' = e_2 + \cdots + e_n$ dans A, avec donc $\overline{e_i} = \overline{c_i}$. Pour $i \geq 2$, nous avons $e_i \in e'Ae'$, ce qui implique $e_1e_i = e_ie_1 = 0$. L'écriture $e = e_1 + \cdots + e_n$ est ainsi une décomposition idempotente dans A qui relève $\overline{e} = \overline{c_1} + \cdots + \overline{c_n}$. □

EXERCICE. Soient e et f deux idempotents équivalents d'un anneau A. Montrer que e et f sont simultanément primitifs ou non-primitifs. (Indication : il existe $a \in eAf$ et $b \in fAe$ tels que $ab = e$ et $ba = f$. Supposons l'existence d'une décomposition idempotente $e = e' + e''$ de e ; posons $f' = be'a$ et $f'' = be''a$. Alors $f = f' + f''$ est une décomposition idempotente de f.)

2.3.3 Modules principaux indécomposables

Voyons à présent le lien entre idempotents et modules projectifs. Pour cela, souvenons-nous de l'isomorphisme d'anneaux $\varphi : a \mapsto (b \mapsto ba)$ de l'anneau opposé A^{op} sur l'anneau des endomorphismes du A-module à gauche régulier. Chaque décomposition idempotente de l'unité dans A^{op} donne donc une décomposition idempotente de l'unité dans $\mathrm{End}_A({}_AA)$, qui fournit une décomposition de ${}_AA$ en somme directe de sous-modules. De façon explicite, la décomposition idempotente $1 = \sum_{i\in I} e_i$ dans A se traduit par l'écriture $A = \bigoplus_{i\in I} Ae_i$, puisque Ae_i est l'image de l'endomorphisme $\varphi(e_i) : b \mapsto be_i$ de ${}_AA$.

Nous nous trouvons donc conduits à associer à chaque idempotent $e \in A$ le sous-module Ae de ${}_AA$. Ce module est projectif : à la décomposition idempotente $1 = e + (1 - e)$ de l'unité dans A correspond la décomposition ${}_AA = Ae \oplus A(1 - e)$ du A-module à gauche régulier, qui fait apparaître Ae comme facteur direct d'un A-module libre. Ainsi le foncteur $\mathrm{Hom}_A(Ae, ?)$ est exact ; le résultat suivant en donne une description concrète.

2.3.3.1 Proposition. *Soient A un anneau, e un idempotent de A et M un A-module. Alors l'application $f \mapsto f(e)$ est un isomorphisme de groupes de $\mathrm{Hom}_A(Ae, M)$ sur eM. Dans le cas $M = Ae$, l'application est un isomorphisme d'anneaux $\mathrm{End}_A(Ae) \cong (eAe)^{\mathrm{op}}$.*

Preuve. Plaçons-nous dans les hypothèses de la proposition. Si $f \in \mathrm{Hom}_A(Ae, M)$, alors $f(e) = f(e^2) = ef(e)$ appartient bien à eM. Ainsi notre application $\varphi : f \mapsto f(e)$ va bien de $\mathrm{Hom}_A(Ae, M)$ dans eM. Dans l'autre sens, considérons l'application ψ qui à $em \in eM$ associe l'homomorphisme $ae \mapsto aem$ de Ae dans M. On vérifie sans difficulté que φ et ψ sont des homomorphismes de groupes inverses l'un de l'autre. Dans le cas où $M = Ae$, nous avons $\varphi(\mathrm{id}_{Ae}) = e$ et $\varphi(g \circ f) = g(f(e)) = g(f(e)e) = f(e)g(e) = \varphi(f)\varphi(g)$, ce qui montre que φ est un homomorphisme d'anneaux de $\mathrm{End}_A(Ae)$ dans $(eAe)^{\mathrm{op}}$. □

Soient e et f deux idempotents de A. À travers les isomorphismes

$$\begin{aligned} \mathrm{Hom}_A(Ae, Af) &\cong eAf, & \mathrm{End}_A(Ae) &= (eAe)^{\mathrm{op}}, \\ \mathrm{Hom}_A(Af, Ae) &\cong fAe, & \mathrm{End}_A(Af) &= (fAf)^{\mathrm{op}}, \end{aligned}$$

l'existence de deux isomorphismes réciproques entre les modules Ae et Af se traduit par l'existence de $a \in eAf$ et $b \in fAe$ tels que $ab = e$ et $ba = f$. Ainsi $Ae \cong Af$ si et seulement si $e \simeq f$.

On appelle module principal indécomposable un facteur direct indécomposable du A-module à gauche régulier. Autrement dit, un module principal indécomposable est un sous-module indécomposable de ${}_AA$ de la forme Ae, avec e idempotent ; en particulier, c'est un module projectif

indécomposable. Pour chaque idempotent e de A, les décompositions de Ae correspondent aux décompositions idempotentes de e ; notamment Ae est indécomposable si et seulement si e est primitif. Ainsi l'application $e \mapsto Ae$ est une bijection de l'ensemble $\mathrm{pi}(A)$ des idempotents primitifs de A sur l'ensemble des modules principaux indécomposables.

La proposition 1.2.2.3 affirme que si le A-module régulier à gauche est artinien ou noethérien, alors il peut être décomposé comme somme directe finie de sous-modules indécomposables. Ces derniers sont alors des modules principaux indécomposables. Il en existe donc ! Nous verrons dans le prochain paragraphe un résultat plus intéressant : si A est un anneau artinien à gauche, alors tout A-module projectif est somme directe de modules projectifs indécomposables, et tout A-module projectif indécomposable est isomorphe à un module principal indécomposable. Ainsi il existe une bijection entre $\mathrm{pi}(A)/\simeq$ et l'ensemble des classes d'isomorphisme de A-modules projectifs indécomposables.

2.3.3.2 Remarque. Les idempotents de A déterminent aussi des A-modules à droite : il suffit de considérer le A-module à droite régulier A_A et les idéaux à droite eA. À nouveau, deux idempotents e et f sont équivalents si et seulement si les A-modules eA et fA sont isomorphes, et un idempotent e est primitif si et seulement si le A-module eA est indécomposable.

Une manière de systématiser cette observation consiste à introduire une dualité. Utilisant la structure de A-A-bimodule régulier sur A, on peut munir le groupe abélien $T(M) = \mathrm{Hom}_A(M, A)$ d'une structure de A-module à droite, pour chaque A-module à gauche M. Inversement quand N est un A-module à droite, on munit $T(N) = \mathrm{Hom}_A(N, A)$ d'une structure de A-module à gauche. On dispose ainsi d'une paire de foncteurs additifs entre la catégorie des A-modules à gauche et la catégorie des A-modules à droite. Cette dualité échange le A-module régulier à gauche avec le A-module régulier à droite. Étant additive, elle échange les sommes directes $({}_AA)^n$ et $(A_A)^n$ de ces modules. Un module projectif de type fini étant facteur direct d'un module libre de type fini, notre dualité consiste en deux bijections inverses l'une de l'autre quand on la restreint aux A-modules projectifs de type fini. La proposition 2.3.3.1 montre par ailleurs que pour tout idempotent e, la dualité T échange entre eux les A-modules projectifs Ae et eA.

Signalons pour finir que la dualité T permet de construire une opération appelée « transposition » et notée Tr. Cette dernière échange elle aussi A-modules à gauche et A-modules à droite ; toutefois, alors que T se comporte de façon bijective avec les modules indécomposables projectifs, Tr se comporte de façon bijective avec les modules indécomposables non-projectifs. La théorie d'Auslander-Reiten, qui vise à organiser l'étude des modules indécomposables, utilise cette opération Tr. Pour des détails, le lecteur est renvoyé au chapitre IV du livre d'Auslander, Reiten et Smalø [2].

2.3.3.3 Proposition. *Soit A un anneau semi-simple artinien. Alors les sous-modules principaux indécomposables de A sont les idéaux à gauche minimaux de A. La bijection $e \mapsto Ae$ de* $\mathrm{pi}(A)$ *sur l'ensemble des modules principaux indécomposables induit une bijection de* $\mathrm{pi}(A)/\simeq$ *sur l'ensemble des classes d'isomorphisme de A-modules simples.*

Preuve. À cause de la complète réductibilité des A-modules, tout sous-module de ${}_AA$ est facteur direct. Pour la même raison, un A-module est indécomposable si et seulement s'il est simple. Ainsi les facteurs directs indécomposables de de ${}_AA$ sont les sous-modules simples de ${}_AA$. Cela montre la première assertion. La seconde provient de la proposition 2.1.2.2 (i). □

2.3.3.4 Proposition. *Soit A un anneau artinien à gauche ou à droite et soit $J = J(A)$ son radical de Jacobson. Alors l'application $e \mapsto Ae/Je$ induit une bijection de* $\mathrm{pi}(A)/\simeq$ *sur l'ensemble des classes d'isomorphisme de A-modules simples.*

Preuve. D'après la proposition 2.3.2.1 et le théorème 2.3.2.2, l'application qui à un idempotent e de A associe son image $\overline{e}$ dans A/J, induit une bijection de $\mathrm{pi}(A)/\simeq$ sur $\mathrm{pi}(A/J)/\simeq$. La proposition 2.3.3.3 affirme pour sa part que l'application $\overline{e} \mapsto (A/J)\overline{e}$ induit une bijection de $\mathrm{pi}(A/J)/\simeq$ sur l'ensemble des classes d'isomorphisme de A/J-modules simples. Enfin le corollaire A/J-modules simples s'identifie à l'ensemble des classes d'isomorphisme de A-modules simples. La proposition s'obtient en composant ces trois bijections. □

Exercices.

(1) Soit e un idempotent d'un anneau A. Pour chaque A-module M, l'anneau eAe agit de façon naturelle sur le groupe abélien eM. (Cette action correspond à la structure de $\mathrm{End}_A(Ae)$-module à droite sur $\mathrm{Hom}_A(Ae, M)$.) Montrer que si $0 \to L \to M \to N \to 0$ est une suite exacte courte de A-modules à gauche, alors $0 \to eL \to eM \to eN \to 0$ est une suite exacte courte de eAe-modules à gauche.

(2) Soit e un idempotent d'un anneau A et M un A-module artinien et noethérien. On suppose que $eN = 0$ pour tout facteur de composition N de M. Montrer que $eM = 0$. (Indication : prendre une série de composition $0 = M_0 \subset M_1 \subset M_2 \subset \cdots \subset M_n = M$ de M. Alors $eM_i \subseteq M_{i-1}$, d'où $eM = e^nM = 0$. Une autre façon de rédiger cela est d'observer que Ae est projectif et d'écrire que par conséquent, $0 \to eM_{i-1} \to eM_i \to e(M_i/M_{i-1}) \to 0$ est exact, avec $e(M_i/M_{i-1}) = 0$, d'où $eM = eM_n = eM_{n-1} = \cdots = eM_1 = eM_0 = 0$.)

(3) Soit A un anneau artinien à gauche et soient e et f deux idempotents de A. Montrer que e et f sont équivalents si et seulement s'il existe $u \in A^\times$ tel que $fu = ue$. (Indication : si u existe, on pose $a = eu^{-1}f$ et $b = fue$ et on a $ab = e$ et $ba = f$. Réciproquement, si $e \simeq f$, alors $Ae \cong Af$, donc par Krull-Schmidt, $A(1-e) \cong A(1-f)$, d'où $1-e \simeq 1-f$; on trouve alors $a \in eAf$ et $b \in fAe$ tels que $ab = e$ et $ba = f$, puis $a' \in (1-e)A(1-f)$ et $b' \in (1-f)A(1-e)$ tels que $a'b' = 1-e$ et $b'a' = 1-f$; on vérifie que $ab' = b'a = a'b = ba' = 0$ et on prend $u = b + b'$, avec $u^{-1} = a + a'$.)

(4) Soit A un anneau artinien à gauche ou à droite et soit J son radical de Jacobson. Soit $e \in A$ un idempotent. Montrer que les propriétés suivantes sont équivalentes : (i) e est primitif ; (ii) Ae est un A-module indécomposable ; (iii) Ae/Je est un A-module simple ; (iv) eAe est un anneau local ; (v) eAe/eJe est un anneau à division. (Indication : on pourra montrer les implications (i) ⇒ (iii) ⇒ (v) ⇒ (iv) ⇒ (ii) ⇒ (i). Pour (iii) ⇒ (v), établir que $\mathrm{End}_A(Ae/Je) \cong (eAe/eJa)^{\mathrm{op}}$ et utiliser le lemme de Schur.)

2.3.4 Couvertures projectives et enveloppes injectives

Rappels du paragraphe 1.3.4 : un épimorphisme essentiel $p : M \to N$ est un homomorphisme surjectif dont le noyau est un sous-module superflu de M. Un monomorphisme essentiel $i : M \to N$ est un homomorphisme injectif dont l'image est un sous-module essentiel de N.

Couverture projective : soit M un A-module. Une couverture projective de M est un couple (P, p) où P est un A-module projectif et $p : P \to M$ est un épimorphisme essentiel. On dit parfois que P ou que $p : P \to M$ est une couverture projective de M.

Exemple : si P est un module projectif, alors $\mathrm{id}_P : P \to P$ est une couverture projective de P.

La proposition suivante entraîne en particulier l'unicité à isomorphisme près de la couverture projective d'un module.

2.3.4.1 Proposition. *Soit $p : P \to M$ une couverture projective de M, Q un A-module projectif et $q : Q \to M$ un épimorphisme. Alors il existe une décomposition $Q = Q' \oplus Q''$ et un isomorphisme $\varphi : Q' \to P$ tels que $q\,\big|_{Q'} = p \circ \varphi$ et $q\,\big|_{Q''} = 0$. Si (Q, q) est une couverture projective de M, alors $Q'' = 0$.*

Preuve. Le module Q étant projectif, il existe un homomorphisme $h : Q \to P$ faisant commuter le diagramme

$$\begin{array}{ccccc} & & Q & & \\ & \overset{h}{\swarrow} & \big\downarrow{\scriptstyle q} & & \\ P & \xrightarrow[p]{} & M & \longrightarrow & 0. \end{array}$$

La surjectivité de $q = p \circ h$ entraîne que $\operatorname{im} h + \ker p = P$; comme $\ker p$ est superflu, cela donne que h est surjectif. La suite exacte courte $0 \to \ker h \to Q \xrightarrow{h} P \to 0$ est scindée, puisque P est projectif. On peut donc l'écrire

$$0 \to \ker h \to Q' \oplus Q'' \xrightarrow{\begin{pmatrix} \varphi & 0 \end{pmatrix}} P \to 0,$$

avec $\varphi : Q' \to P$ un isomorphisme et $Q'' = \ker h$. Si (Q, q) est une couverture projective de M, alors $\ker q$ est superflu. Comme $\ker q \supseteq Q''$, cela donne Q'' superflu ; et comme $Q' + Q'' = Q$, on a $Q' = Q$, et donc $Q'' = 0$. □

2.3.4.2 Théorème. *Soit A un anneau artinien à gauche ou à droite.*

(i) Tout A-module M admet une unique couverture projective, notée $C(M)$.

(ii) Pour toute famille $(M_\lambda)_{\lambda\in\Lambda}$ de A-modules, $C\Big(\bigoplus_{\lambda\in\Lambda} M_\lambda\Big) \cong \bigoplus_{\lambda\in\Lambda} C(M_\lambda)$.

(iii) Pour tout module M, $C(M) = C(\operatorname{hd} M)$.

(iv) La couverture projective d'un module de type fini est un module de type fini.

Preuve. On commence par prouver l'assertion (ii) sous l'hypothèse supplémentaire que chacun des M_λ a une couverture projective $C(M_\lambda)$. Par définition, le noyau de cette couverture projective est superflu ; d'après le corollaire 2.2.2.5 (ii), il est inclus dans le radical de $C(M_\lambda)$. L'exercice (4) du paragraphe 2.2.2 dit alors que la somme directe des noyaux $\ker(C(M_\lambda) \to M_\lambda)$ est incluse dans le radical du module $\bigoplus_{\lambda\in\Lambda} C(M_\lambda)$. Ainsi le noyau de l'homomorphisme $\left(\bigoplus_{\lambda\in\Lambda} C(M_\lambda)\right) \to \left(\bigoplus_{\lambda\in\Lambda} M_\lambda\right)$ est superflu, à nouveau d'après le corollaire 2.2.2.5 (ii). Comme le module $\bigoplus_{\lambda\in\Lambda} C(M_\lambda)$ est projectif (proposition 1.1.6.1), il est une couverture projective de $\bigoplus_{\lambda\in\Lambda} M_\lambda$.

Puis on prouve l'assertion (iii) sous l'hypothèse supplémentaire que $\operatorname{hd} M$ a une couverture projective (P, p). Par projectivité existe alors une flèche q de P dans M rendant commutatif le diagramme

$$\begin{array}{ccc} & & P \\ & \overset{q}{\swarrow} & \downarrow p \\ M & \xrightarrow{c} & \operatorname{hd} M. \end{array}$$

La composée p de q avec l'homomorphisme canonique c de M sur $\operatorname{hd} M$ étant surjective, on a $q(P) + \operatorname{rad} M = M$, ce qui nécessite $q(P) = M$ puisque $\operatorname{rad} M$ est superflu. Par ailleurs, le noyau de q est superflu, car il est inclus dans $\ker(c \circ q) = \ker p$, lequel est lui-même superflu. Ainsi (P, q) est une couverture projective de M.

Il nous reste à établir (i) et (iv). Grâce au cas particulier de (iii) que nous avons établi et au corollaire 2.2.2.2 (iii), il nous suffit de traiter le cas d'un module complètement réductible, et grâce à (ii), nous pouvons nous borner au cas d'un module simple. Tout module simple est isomorphe au quotient $Ae/J(A)e$, où e est un idempotent primitif. Le A-module Ae est projectif et l'homomorphisme canonique $Ae \to Ae/J(A)e$ est un épimorphisme essentiel, puisque son noyau est égal au radical du module Ae. Ainsi Ae est la couverture projective de $Ae/J(A)e$. □

Remarque. On trouvera une preuve du théorème d'existence des couvertures projectives basées sur d'autres idées que les idempotents dans le paragraphe I.4 de [2]. La preuve basée sur les idempotents a toutefois l'avantage d'être généralisable à la classe des anneaux dits semi-parfaits, qui englobe les algèbres de type fini sur un anneau de valuation complet.

2.3.4.3 Proposition. *Soit A un anneau artinien à gauche ou à droite.*

(i) La couverture projective d'un A-module simple est indécomposable ; la tête d'un module projectif indécomposable est simple.

(ii) Tout A-module projectif est somme directe de modules indécomposables.

Preuve. Soit (P, p) la couverture projective d'un module simple et écrivons P comme somme directe $M \oplus N$ de deux sous-modules. Certainement $K = \ker p$ est un sous-module maximal, puisque $\operatorname{im} p \cong P/K$ est simple. Ensuite K ne peut pas contenir à la fois M et N. S'il ne contient pas M, alors $M + K = P$ par maximalité de K, et donc $M = P$ puisque K est

superflu. De manière analogue, si K ne contient pas N, alors $N = P$. Dans tous les cas, la décomposition $P = M \oplus N$ est banale. Cela démontre la première assertion de (i).

Soit P un A-module projectif. Alors P est sa propre couverture projective, donc est la couverture projective de sa tête d'après le théorème 2.3.4.2 (iii). Écrivons cette tête comme une somme de sous-modules simples : $\operatorname{hd} P = \bigoplus_{\lambda\in\Lambda} S_\lambda$. Alors $P = C(\operatorname{hd} P) = \bigoplus_{\lambda\in\Lambda} C(S_\lambda)$ d'après le théorème 2.3.4.2 (ii). Ainsi P est somme directe de modules indécomposables. Si P est indécomposable, alors la somme comporte exactement un terme, donc la tête de P est simple. Cela finit la preuve de (i) et démontre (ii). □

Un des intérêts de la notion de couverture projective est donné par la proposition suivante.

2.3.4.4 Proposition. *Soient A un anneau artinien à gauche, S un A-module simple, et $p : P \to S$ la couverture projective de S. La structure de A-$\operatorname{End}_A(P)^{\mathrm{op}}$-bimodule sur P permet de munir $\operatorname{Hom}_A(P, M)$ d'une structure de $\operatorname{End}_A(P)^{\mathrm{op}}$-module, pour tout A-module M.*

(i) Le A-module P est artinien et noethérien, l'anneau $\operatorname{End}_A(P)$ est local, et $\operatorname{Hom}_A(P, S)$ est l'unique $\operatorname{End}_A(P)^{\mathrm{op}}$-module simple, à isomorphisme près.

(ii) Pour tout A-module M de longueur finie, le module $\operatorname{Hom}_A(P, M)$ sur $\operatorname{End}_A(P)^{\mathrm{op}}$ est de longueur finie, égale à la multiplicité de Jordan-Hölder du module S dans M.

Preuve. Le théorème 2.3.4.2 (iv) montre que P est de type fini. Il est donc artinien et noethérien, d'après le corollaire 2.2.2.4. Le corollaire 1.2.2.2 dit alors que $\operatorname{End}_A(P)$ est un anneau local. Par ailleurs, soit h un élément non-nul de $\operatorname{Hom}_A(P, S)$. Alors h se factorise à travers la tête de P et induit un isomorphisme $\operatorname{hd} P \cong S$. Ainsi $h : P \to S$ est un épimorphisme essentiel, donc est une couverture projective. La proposition 2.3.4.1 montre alors l'existence d'un automorphisme φ de P tel que $h = p \circ \varphi$. Par transitivité, deux éléments non-nuls de $\operatorname{Hom}_A(P, S)$ sont donc reliés l'un à l'autre par l'action d'un élément de $\operatorname{End}_A(P)^{\mathrm{op}}$. Cela implique que $\operatorname{Hom}_A(P, S)$ est un $\operatorname{End}_A(P)^{\mathrm{op}}$-module simple et finit la preuve de (i).

L'assertion (ii) est vraie si M est un module simple isomorphe à S, grâce à (i). Si M est un module simple non-isomorphe à S, alors tout homomorphisme de P dans M se factorise à travers $\operatorname{hd} P \cong S$ d'après l'exemple 1.3.3.3, ce qui implique que $\operatorname{Hom}_A(P, M) \cong \operatorname{Hom}_A(S, M) = 0$ et montre (ii) dans ce cas également. Bref (ii) est vraie quand M est simple, et bien sûr aussi quand $M = 0$. De là, le cas général se démontre par récurrence sur la longueur de M, en utilisant la proposition 1.2.5.1 et l'exactitude du foncteur $\operatorname{Hom}_A(P, ?)$. □

Remarques.

(1) Reprenons la situation présentée dans l'énoncé de la proposition 2.3.4.4. Notons J le radical de Jacobson de A. Il existe un idempotent primitif $e \in A$ tel que $S = Ae/Je$. Alors $P = Ae$, $\operatorname{Hom}_A(P, M) = eM$ et $\operatorname{End}_A(P)^{\mathrm{op}} = eAe$. La proposition dit que le eAe-module eM est de longueur finie égale à la multiplicité de Jordan-Hölder du module simple Ae/Je dans M. (Incidemment, le eAe-module simple est $\operatorname{Hom}_A(P, S) \cong eS \cong eAe/eJe$. En tant qu'anneau, eAe/eJe peut être identifié à l'anneau à division $\operatorname{End}_A(S)^{\mathrm{op}}$. Par ailleurs, eAe/eJe est le quotient de l'anneau local eAe par son radical de Jacobson.)

(2) Toujours dans cette situation, supposons maintenant que A est une algèbre de dimension finie sur un corps k. Alors S, P, M, $\mathrm{Hom}_A(P,M)$ et $\mathrm{Hom}_A(P,S)$ sont des espaces vectoriels de dimension finie sur k. De plus, on peut identifier les espaces vectoriels $\mathrm{Hom}_A(P,S)$, $\mathrm{Hom}_A(\mathrm{hd}\,P,S)$ et $\mathrm{End}_A(S)$, car tout homomorphisme de P dans S se factorise à travers la tête de P, laquelle est isomorphe à S. La longueur du $\mathrm{End}_A(P)^{\mathrm{op}}$-module $\mathrm{Hom}_A(P,M)$ est alors égale à $\dim_k \mathrm{Hom}_A(P,M)/\dim_k \mathrm{End}_A(S)$.

Enveloppe injective : soit M un A-module. Une enveloppe injective de M est un couple (E,i) où E est un A-module injectif et $i : M \to E$ est un monomorphisme essentiel. On dit parfois que E ou que $i : M \to E$ est une enveloppe injective de M.

Exemple : si Q est un module injectif, alors $\mathrm{id}_Q : Q \to Q$ est une enveloppe injective de Q.

La proposition suivante entraîne en particulier l'unicité à isomorphisme près de l'enveloppe injective d'un module.

2.3.4.5 Proposition. *Soit $i : M \to E$ une enveloppe injective de M, Q un A-module injectif et $j : M \to Q$ un monomorphisme. Alors il existe une décomposition $Q = Q' \oplus Q''$ et un isomorphisme $\varphi : E \to Q'$ tels que $j = \varphi \circ i$. Si (Q,j) est une enveloppe injective de M, alors $Q'' = 0$.*

Preuve. La preuve est semblable à celle de la proposition 2.3.4.1. □

2.3.4.6 Théorème. *Soit A un anneau artinien à gauche.*

(i) Tout A-module M admet une unique enveloppe injective, notée $E(M)$.

(ii) Pour toute famille $(M_\lambda)_{\lambda\in\Lambda}$ de A-modules, $E\Big(\bigoplus_{\lambda\in\Lambda} M_\lambda\Big) \cong \bigoplus_{\lambda\in\Lambda} E(M_\lambda)$.

(iii) Pour tout module M, $E(M) = E(\mathrm{soc}\,M)$.

Preuve. L'assertion (i) de ce théorème est valable pour n'importe quel anneau A : c'est le théorème de Eckmann-Schöpf, voir [6], §57 pour une preuve.

La preuve de l'assertion (ii) comprend deux étapes. On montre d'abord que si $(Q_\lambda)_{\lambda\in\Lambda}$ est une famille de modules injectifs, alors $\bigoplus_{\lambda\in\Lambda} Q_\lambda$ est injectif. La comparaison avec la proposition 1.1.6.4 montre que c'est le cas quand l'ensemble d'indice Λ est fini ; pour ramener le cas général à cette situation, on utilise le critère d'injectivité de la proposition 1.1.6.5 (v) et le fait que dans un anneau artinien à gauche, tous les idéaux à gauche sont de type fini (théorème de Hopkins 2.2.2.3 (ii)). Ensuite, on considère une famille $(M_\lambda)_{\lambda\in\Lambda}$ de A-modules. On dispose alors des enveloppes injectives $i_\lambda : M_\lambda \hookrightarrow E(M_\lambda)$, d'où un monomorphisme $i = \bigoplus_{\lambda\in\Lambda} i_\lambda$ de $\bigoplus_{\lambda\in\Lambda} M_\lambda$ dans $\bigoplus_{\lambda\in\Lambda} E(M_\lambda)$. D'après la première étape, le codomaine est un module injectif. En outre, le fait que chaque i_λ soit un monomorphisme essentiel implique que i en est un. (Ce n'est pas difficile à voir ; dans le cas qui nous occupe d'un anneau A artinien, on peut même aller très rapidement en utilisant le corollaire 2.2.2.5 (iii) et l'exercice (4) du paragraphe 2.2.2). Ainsi i est une enveloppe injective, ce qui démontre l'assertion (ii).

Enfin l'assertion (iii) est conséquence du fait que l'inclusion $\operatorname{soc} M \hookrightarrow M$ est un monomorphisme essentiel (corollaire 2.2.2.5 (iii)) : la composée $\operatorname{soc} M \hookrightarrow M \hookrightarrow E(M)$ est alors elle aussi un monomorphisme essentiel, et est donc une enveloppe injective de $\operatorname{soc} M$. □

2.3.4.7 Proposition. *Soit A un anneau artinien à gauche.*

(i) L'enveloppe injective d'un A-module simple est indécomposable ; le socle d'un module injectif indécomposable est simple.

(ii) Tout A-module injectif est somme directe de modules indécomposables.

Preuve. La preuve suit les mêmes lignes que celle de la proposition 2.3.4.3. □

Remarques. Comme indiqué dans la preuve, l'assertion (i) du théorème 2.3.4.6 vaut pour n'importe quel anneau A ; en revanche, il n'est pas garanti que $E(M)$ soit de type fini quand M l'est, même si A est artinien. L'assertion (ii) de ce même théorème 2.3.4.6 est elle aussi vraie sans hypothèse sur A quand la somme (indexée sur l'ensemble Λ) est finie ; sa validité dans le cas général est équivalente au fait que l'anneau A est noethérien à gauche (voir [1], Proposition 18.13). Enfin les assertions 2.3.4.6 (iii) et 2.3.4.7 (i) sont vraies si on suppose A artinien à droite.

Dans le cas d'un anneau A artinien à gauche ou à droite, nous avons ainsi des bijections entre trois ensembles :

$$\left\{\begin{array}{c}\text{classes d'isom. de}\\ \text{projectifs indécomp.}\end{array}\right\} \underset{C(?)}{\overset{\mathrm{hd}}{\rightleftarrows}} \left\{\begin{array}{c}\text{classes d'isom. de}\\ \text{modules simples}\end{array}\right\} \underset{\mathrm{soc}}{\overset{E(?)}{\rightleftarrows}} \left\{\begin{array}{c}\text{classes d'isom. de}\\ \text{injectifs indécomp.}\end{array}\right\}.$$

Exercices.

(1) Soit A un anneau artinien à gauche ou à droite. Montrer que tout A-module projectif indécomposable est isomorphe à un A-module principal indécomposable.

(2) Soient A un anneau artinien à gauche ou à droite et P un A-module projectif indécomposable. Montrer que tout quotient de P est indécomposable. (Indication : soit X un quotient de P. Alors $\operatorname{hd} X \cong \operatorname{hd} P$ est simple. Le corollaire 2.2.2.5 (i) et l'exercice (4) du paragraphe 2.2.2 interdisent alors à X d'être décomposable.)

(3) Soit A un anneau artinien à gauche ou à droite et soit Q un A-module injectif indécomposable. Montrer que l'anneau $\operatorname{End}_A(Q)$ est local. (Indication : commencer par observer qu'un endomorphisme injectif h de Q est nécessairement inversible ; de fait, $h(Q)$ est un sous-module injectif de Q, donc est un facteur direct de Q, ce qui entraîne $h(Q) = Q$ puisque Q est indécomposable. Observer également que le socle de Q est un sous-module essentiel et simple, donc est inclus dans tout sous-module non-nul de Q. Maintenant, soit $f \in \operatorname{End}_A(Q)$. Les deux sous-modules $\ker f$ et $\ker(\mathrm{id} - f)$ s'intersectent trivialement, donc ils ne peuvent contenir tous les deux le socle de Q, donc l'un des deux est nul. Ainsi, f ou $\mathrm{id} - f$ est un monomorphisme, et est donc inversible. Utiliser la proposition 2.3.1.1 (iv) pour conclure.)

2.4 Blocs d'un anneau artinien

2.4.1 Idempotents centraux

Dans un anneau commutatif, les idempotents sont isolés et il n'existe au plus qu'une décomposition idempotente primitive de l'unité. Plus précisément :

2.4.1.1 Proposition. *Soit A un anneau commutatif. Supposons que $1 = \sum_{i\in I} e_i$ soit une décomposition idempotente de l'unité dans A et que chaque e_i soit un idempotent primitif. Alors chaque idempotent de A est une somme $\sum_{i\in J} e_i$, où J est une partie de I. En particulier, $\{e_i \mid i \in I\}$ est l'ensemble de tous les idempotents primitifs de A.*

Preuve. L'anneau A étant commutatif, le produit de deux idempotents de A, si non-nul, est encore un idempotent. Ceci vu, soit e un idempotent de A. Chaque e_i étant primitif, $e_i = ee_i + (1-e)e_i$ ne peut pas être une décomposition idempotente de e_i, et donc $ee_i = 0$ ou $(1-e)e_i = 0$. Posons $J = \{i \in I \mid ee_i = e_i\}$; ainsi $I \setminus J = \{i \in I \mid ee_i = 0\}$. Alors $e = e\Big(\sum_{i\in I} e_i\Big) = \sum_{i\in J} e_i$. □

Soit $(B_i)_{i\in I}$ une famille finie d'anneaux et soit $A = \prod_{i\in I} B_i$ l'anneau produit. En tant que groupe abélien, nous pouvons donc écrire $A = \bigoplus_{i\in I} B_i$; chaque B_i apparaît ici comme un idéal bilatère de A. Appelons ε_i l'unité de B_i, vue comme élément de B. Alors les ε_i sont des idempotents appartenant au centre de A et $1 = \sum_{i\in I} \varepsilon_i$ est une décomposition idempotente de l'unité dans A. Enfin B_i est l'idéal bilatère engendré par ε_i, il s'identifie à l'anneau $\varepsilon_i A \varepsilon_i$, et la surjection canonique de A sur $B_i \cong A \,/\, \bigoplus_{j\neq i} B_j$ est donnée par $x \mapsto \varepsilon_i x$.

Réciproquement, soit A un anneau, et soit $A = \bigoplus_{i\in I} B_i$ une décomposition en somme directe d'idéaux bilatères de A. Chaque B_i est stable par multiplication, et le produit d'un élément de B_i par un élément de B_j est nul quand $i \neq j$, car il appartient à $B_i \cap B_j = \{0\}$. Ainsi dans la décomposition $A = \bigoplus_{i\in I} B_i$, le produit de A se calcule composante par composante. Écrivons $1 = \sum_{i\in I} \varepsilon_i$ selon cette décomposition. Alors pour chaque $x \in B_i$, on a $\varepsilon_j x = x\varepsilon_j = 0$ pour tout $j \neq i$, et par comparaison avec $1x = x1 = x$, on arrive à $\varepsilon_i x = x\varepsilon_i = x$; autrement dit ε_i est un élément neutre pour la multiplication de B_i. Ainsi chaque B_i est un anneau et A s'identifie à l'anneau produit $\prod_{i\in I} B_i$.

Ces considérations montrent que décomposer un anneau A en produit est un problème équivalent à décomposer A en somme directe d'idéaux bilatères, c'est-à-dire à décomposer le bimodule régulier ${}_AA_A$ en somme directe de sous-bimodules. D'après l'introduction au paragraphe 2.3.2, ce problème est équivalent à la recherche d'une décomposition idempotente de l'unité dans l'anneau des endomorphismes du bimodule régulier ${}_AA_A$, anneau qui est isomorphe au centre de A au vu de l'exemple 1.4.3.1 (1).

2.4.1.2 Proposition. *Soit A un anneau artinien à gauche ou à droite. Alors A est la somme directe d'une famille finie $(B_i)_{i\in I}$ d'idéaux bilatères indécomposables, et cette famille est unique à indexation près. Décomposons l'élément unité de A dans la somme directe $A = \bigoplus_{i\in I} B_i$ en écrivant $1 = \sum_{i\in I} \varepsilon_i$. Alors chaque B_i est un anneau pour la multiplication induite*

par celle de A, avec ε_i comme élément neutre. En tant qu'anneau, A s'identifie au produit $\prod_{i\in I} B_i$. On a $B_i = A\varepsilon_i = \varepsilon_i A$. La somme $1 = \sum_{i\in I} \varepsilon_i$ est une décomposition idempotente de l'unité, et les ε_i sont les idempotents primitifs du centre de A. Chaque idéal bilatère D de A supplémenté en tant qu'idéal bilatère est une somme $\bigoplus_{i\in J} B_i$, où J est une partie de I.

Preuve. Les hypothèses faites sur A font que le A-bimodule régulier est artinien. D'après la proposition 1.2.2.3, il s'écrit donc comme la somme directe d'une famille finie $(B_i)_{i\in I}$ de sous-bimodules indécomposables [12]. Décomposons l'élément unité de A dans la somme directe $A = \bigoplus_{i\in I} B_i$ en écrivant $1 = \sum_{i\in I} \varepsilon_i$. Nous avons vu ci-dessus que B_i est un anneau pour la multiplication induite par celle de A, avec ε_i comme élément neutre, et qu'en tant qu'anneau, A s'identifie au produit $\prod_{i\in I} B_i$. Comme $B_i \neq \{0\}$, cela entraîne que ε_i est un idempotent, qu'il est central, que $B_i = A\varepsilon_i = \varepsilon_i A$, et que la somme $1 = \sum_{i\in I} \varepsilon_i$ est une décomposition idempotente de l'unité.

Si l'on pourrait écrire $\varepsilon_i = \eta + \eta'$, avec η, η' deux idempotents centraux et orthogonaux, alors B_i se casserait en somme directe $\eta B_i \oplus \eta' B_i$, chaque terme étant un idéal bilatère (car par exemple, $\eta B_i = \eta\varepsilon_i A = \eta A = A\eta$). Cette impossibilité montre que ε_i est un idempotent primitif du centre de A.

Appliquant la proposition 2.4.1.1 au centre de A et à la décomposition unipotente $1 = \sum_{i\in I} \varepsilon_i$, on voit que $\{\varepsilon_i \mid i \in I\}$ est l'ensemble de tous les idempotents primitifs du centre de A. Ce fait montre l'unicité à indexation près de la famille $(B_i)_{i\in I}$.

Enfin soit D un idéal bilatère de A (disons non-nul pour éviter un cas trivial) supplémenté en tant qu'idéal bilatère. On écrit ainsi $A = D \oplus D'$ et on décompose l'unité de A selon les termes de cette somme : $1 = \eta + \eta'$. Alors D et D' sont des anneaux pour la multiplication induite par celle de A, avec η et η' comme éléments neutres. Cela entraîne que η est un idempotent central de A et que $D = \eta A = A\eta$. Appliquant à nouveau la proposition 2.4.1.1, on écrit $\eta = \sum_{i\in J} \varepsilon_i$ pour une partie $J \subseteq I$. Il vient alors $D = \eta A = \bigoplus_{i\in J} \varepsilon_i A = \bigoplus_{i\in J} B_i$. □

Les idéaux B_i apparaissant dans l'énoncé de la proposition 2.4.1.2 sont appelés les blocs de A. Les idempotents centraux ε_i sont appelés les idempotents de bloc.

Exemple. Les blocs d'un anneau semi-simple artinien sont ses composantes simples. (C'est une conséquence immédiate de la proposition 2.1.2.3.)

Exercice. Soit $(B_i)_{i\in I}$ une famille finie d'anneaux et soit $A = \prod_{i\in I} B_i$ l'anneau produit. Montrer que tout A-module M se décompose en somme directe $M = \bigoplus_{i\in I} M_i$, avec $M_i = B_i M$. Montrer que si $N = \bigoplus_{i\in I} N_i$ est la décomposition d'un second A-module, alors le groupe $\mathrm{Hom}_A(M, N)$ est canoniquement isomorphe au produit $\prod_{i\in I} \mathrm{Hom}_{B_i}(M_i, N_i)$.

12. C'est le seul endroit dans la preuve où l'on utilise que l'anneau A est artinien. La proposition 2.4.1.2 est tout aussi vraie si l'on suppose que le A-bimodule régulier est noethérien, ce qui est par exemple le cas quand A est noethérien à gauche.

2.4.2 Classes de liaison

2.4.2.1 Proposition. *Soit A un anneau artinien à gauche. Pour chaque A-module indécomposable M, il existe un unique bloc B de A tel que $BM = M$. L'idempotent de bloc correspondant agit sur M par l'identité. Tout autre bloc de A annule M.*

Preuve. Soit ε un idempotent de bloc. La multiplication par ε est un endomorphisme du A-module M, et on a une décomposition $M = \varepsilon M \oplus (1-\varepsilon)M$. Comme M est indécomposable, l'un des termes est M et l'autre est 0. Ainsi εM est M ou 0, et dans le premier cas, ε agit par l'identité sur M.

La somme des idempotents de bloc valant 1, il n'est pas possible que εM soit 0 pour tout idempotent de bloc ε. Par ailleurs, le produit de deux idempotents de bloc distincts étant nul, εM ne peut être égal à M que pour un seul idempotent de bloc. □

Dans le contexte de la proposition, le module M est dit appartenir au bloc B. L'idempotent du bloc B agit sur M par l'identité, les autres idempotents de blocs agissent sur M par 0.

Si un module indécomposable M appartient au bloc B, alors tout facteur de composition de M appartient aussi à B. Notre but à présent est d'obtenir une réciproque partielle à cette dernière assertion : nous allons montrer que deux modules principaux indécomposables P et P' appartiennent au même bloc si et seulement s'il existe une suite finie de modules principaux indécomposables $P = P_0$, P_1, ..., $P_n = P'$ telle que P_{j-1} et P_j ont un facteur de composition commun pour chaque j. Pour cela, il nous faut voir une autre méthode pour définir les blocs d'un anneau.

Supposons d'abord A semi-simple artinien. La proposition 2.1.2.3 indique que les blocs de A sont ses composantes simples. De plus, chaque composante simple de A est une composante isotypique du A-module à gauche régulier, donc est la somme des idéaux à gauche minimaux dans une classe d'isomorphisme de A-modules simples. Enfin, les idéaux à gauche minimaux de A sont les modules principaux indécomposables. Ainsi chaque module principal indécomposable est inclus dans un bloc de A, et chaque bloc est la somme des modules principaux indécomposables qu'il contient.

Il se trouve que la phrase précédente est également vraie quand A est un anneau artinien à gauche général. Une définition supplémentaire est toutefois nécessaire pour énoncer cela avec précision : on dit que deux idempotents primitifs e et e' de A sont liés, et on écrit $e \sim e'$, s'il existe une suite $e = f_0, f_1, \ldots, f_n = e'$ d'idempotents primitifs telle que les modules principaux indécomposables Af_{j-1} et Af_j ont un facteur de composition commun pour tout j. Ainsi $\sim$ est une relation d'équivalence, appelée liaison, et qui est plus grossière que $\simeq$. Il n'y a qu'un nombre fini de classes de liaison dans $\mathrm{pi}(A)$, puisqu'il n'y a qu'un nombre fini de classes d'équivalence pour $\simeq$ (proposition 2.3.3.4 et exercice (3) du paragraphe 2.2.2).

2.4.2.2 Proposition. *Soit A un anneau artinien à gauche.*

(i) Soient e un idempotent primitif de A et B un bloc de A. Le module principal indécomposable Ae appartient au bloc B si et seulement si $Ae \subseteq B$.

(ii) Si $E \subseteq \mathrm{pi}(A)$ est une classe de liaison, alors $\sum_{e\in E} Ae$ est un bloc de A. Chaque bloc de A s'obtient de cette façon, et la classe de liaison est déterminée par le bloc.

Preuve. Soit $e \in \mathrm{pi}(A)$. Si B est le bloc de A auquel appartient le module principal indécomposable Ae, alors $Ae = B(Ae) \subseteq B$, puisque B est un idéal bilatère. La réciproque est vraie, car Ae ne peut être inclus que dans un seul bloc. L'assertion (i) est prouvée.

Tout facteur de composition d'un module indécomposable appartient au même bloc que ce dernier. Ceci implique que si deux modules principaux indécomposables Ae et Af ont un facteur de composition commun, alors ils appartiennent au même bloc. Par transitivité, deux modules principaux indécomposables Ae et Af appartiennent au même bloc dès que les idempotents primitifs e et f sont liés. Le (i) montre ainsi que si E est une classe de liaison dans $\mathrm{pi}(A)$, alors $\sum_{e\in E} Ae$ est inclus dans un bloc de A.

Soit $(E_i)_{i\in I}$ une indexation des classes de liaison dans $\mathrm{pi}(A)$; ainsi $\mathrm{pi}(A) = \bigsqcup_{i\in I} E_i$. Pour $i \in I$, posons $D_i = \sum_{e\in E_i} Ae$. Ainsi qu'il a été remarqué au paragraphe 2.3.3, le A-module à gauche régulier peut être décomposé comme somme directe finie de sous-modules principaux indécomposables. Nous en déduisons que $\sum_{i\in I} D_i = A$, d'où l'existence d'élements $\eta_i \in D_i$ tels que $\sum_{i\in I} \eta_i = 1$.

Si deux idempotents primitifs e et f ne sont pas liés, alors Ae n'a pas de facteur de composition commun avec Af ; au vu de la proposition 2.3.4.4 (ii), on a donc $fAe = \mathrm{Hom}_A(Af, Ae) = 0$. On voit ainsi que $D_iD_j = 0$ si $i \neq j$. Cela entraîne que chaque D_i est un idéal bilatère : en effet, D_i est un idéal à gauche par définition et $D_iA = D_i\Big(\sum_{j\in I} D_j\Big) = D_iD_i \subseteq D_i$. Supposons avoir une somme nulle $\sum_{i\in I} x_i = 0$, avec $x_i \in D_i$ pour chaque $i \in I$. En utilisant à nouveau l'égalité $D_iD_j = 0$ si $i \neq j$, nous calculons

$$x_i = \left(\sum_{j\in I} \eta_j\right) x_i = \eta_i x_i = \eta_i \left(\sum_{j\in I} x_j\right) = 0$$

pour chaque $i \in I$. Ainsi nous avons une décomposition comme somme directe d'idéaux bilatères $A = \bigoplus_{i\in I} D_i$.

Nous avons par ailleurs montré que chaque D_i est inclus dans un bloc de A. Appliquant la proposition 2.4.1.2, nous concluons que les D_i sont les blocs de A. L'assertion (ii) est prouvée. □

Ainsi un anneau artinien à gauche A a autant de blocs qu'il y a autant de classes de liaison dans $\mathrm{pi}(A)$, et deux idempotents primitifs e et f de A sont liés si et seulement si les A-modules principaux indécomposables Ae et Af appartiennent au même bloc.

Pour conclure, tentons de relier les blocs d'un anneau artinien à gauche A à ceux de son quotient semi-simple $\overline{A} = A/J(A)$. La décomposition $A = \prod_{i\in I} B_i$ de A en blocs induit une décomposition $\overline{A} = \prod_{i\in I} \overline{B_i}$, où $\overline{B_i}$ est l'image de B_i dans $\overline{A}$. Il y a plusieurs façons de voir cela : on peut utiliser l'exercice (4) du paragraphe 2.2.2 pour montrer que $J(A) = \prod_{i\in I}\big(J(A)\cap B_i\big) = \prod_{i\in I} J(B_i)$; on peut aussi étudier l'image dans $\overline{A}$ des idempotents de blocs de A. Cela étant, la proposition 2.1.2.3 montre que chaque $\overline{B_i}$ est la somme de composantes simples de $\overline{A}$.

L'ensemble des composantes simples de $\overline{A}$ est en bijection avec l'ensemble des classes d'isomorphisme de $\overline{A}$-modules simples, donc avec $\mathrm{pi}(\overline{A})/\simeq$, donc avec $\mathrm{pi}(A)/\simeq$. L'ensemble des blocs de A est pour sa part en bijection avec $\mathrm{pi}(A)/\sim$. Le regroupement par paquets des composantes simples de $\overline{A}$ donné par la décomposition $\overline{A} = \prod_{i\in I} \overline{B_i}$ consiste à voir chaque classe de liaison dans $\mathrm{pi}(A)$ comme union de classes d'équivalence pour $\simeq$.

Exercices.

(1) Soit A un anneau artinien à gauche et soient e et e' deux idempotents primitifs de A. Montrer que les A-modules principaux indécomposables Ae et Ae' ont un facteur de composition commun si et seulement s'il existe un idempotent primitif f de A tel que $fAe \neq 0 \neq fAe'$. (Indication : utiliser la proposition 2.3.4.4.)

(2) Soit A un anneau artinien à gauche. Montrer que deux A-modules indécomposables M et M' appartiennent au même bloc si et seulement s'il existe une suite finie de modules indécomposables $M = M_0$, M_1, ..., $M_n = M'$ telle que M_{j-1} et M_j ont un facteur de composition commun pour chaque j.

(3) Montrer qu'un anneau commutatif artinien est isomorphe à un produit d'anneaux locaux. (Indication : soit B un bloc d'un anneau commutatif artinien. Alors B est lui-même commutatif artinien. L'anneau $B/J(B)$ est donc semi-simple artinien commutatif, donc est un produit de corps. Ce produit est réduit à un seul facteur, car à l'instar de B, l'anneau $B/J(B)$ ne possède pas d'idempotent autre que 1. Ainsi $B/J(B)$ est un corps, et on conclut en utilisant la proposition 2.3.1.1.)

3 Algèbres

Introduction

Il est bien connu que la réduction des endomorphismes est plus simple quand le corps de base est algébriquement clos. Il est donc important de savoir se ramener à ce cas. La méthode conceptuellement la plus simple est de travailler en coordonnées avec des matrices. Il est toutefois aussi possible de conserver le langage des modules : si K/k est une extension de corps et si V est un $k[X]$-module, alors on peut munir le produit tensoriel $V_{(K)} = K \otimes_k V$ d'une structure de $K[X]$-module.

Les deux premiers chapitres de cours étudiaient des objets définis « au-dessus de $\mathbf{Z}$ », sans référence à un corps de base k. Nous voulons maintenant avoir un contrôle sur ce corps et pouvoir le faire varier. Pour cela, nous devons remplacer la notion d'anneau par celle de k-algèbre : une k-algèbre est un anneau A muni d'une structure de k-espace vectoriel compatible. La théorie est ainsi faite que tout A-module est automatiquement un k-espace vectoriel sur lequel A agit par applications k-linéaires. Tout ce qui a été vu dans les chapitres précédents reste vrai, à condition de remplacer l'additivité (c'est-à-dire la $\mathbf{Z}$-linéarité) par la k-linéarité.

Un exemple est la théorie des représentations des groupes. Soient G un groupe, k un corps et n un entier naturel. Une représentation de degré n de G sur k est la donnée d'un homomorphisme de groupes de G dans $\mathbf{GL}_n(k)$. Le corps k est donné séparément de G et il est important de pouvoir le traiter comme une variable. En définissant la k-algèbre kG du groupe, on ramène l'étude des représentations de G sur k à l'étude des kG-modules de type fini.

Considérons une k-algèbre A et un A-module M. Pour toute extension de corps K/k, on peut munir $A_{(K)} = K \otimes_k A$ d'une structure de K-algèbre et $M_{(K)} = K \otimes_k M$ d'une structure de $A_{(K)}$-module. Des questions intéressantes sont : qu'est-ce que le passage de k à K rend plus simple quand K est algébriquement clos ? Le $A_{(K)}$-module $M_{(K)}$ détermine-t-il le A-module M à isomorphisme près ? À quelle condition la simplicité de M entraîne-t-elle celle de $M_{(K)}$? Tout $A_{(K)}$-module simple est-il de la forme $M_{(K)}$? À quelle condition sur A l'algèbre $A_{(K)}$ est-elle semi-simple pour toute extension K/k ?

L'examen de la dernière question est particulièrement intéressant, car il conduit au théorème principal de Wedderburn, qui est l'analogue pour les algèbres de la décomposition de Jordan-Dunford pour les endomorphismes d'un espace vectoriel de dimension finie.

Dans tout ce chapitre, k sera un anneau commutatif différent de $\{0\}$.
Ce sera un corps à partir du paragraphe 3.2.2.

3.1 k-linéarité

3.1.1 Préliminaires

Donnons-nous un anneau commutatif k. Dans ce chapitre, les objets que nous regarderons seront tous des k-modules. Nous les regarderons même comme des k-k-bimodules, k agissant à droite de la même façon qu'il agit à gauche (il faut impérativement que k soit commutatif

pour pouvoir faire cela). Cela permet d'utiliser les constructions péniblement mises au point dans le paragraphe 1.4.3.

Soient donc M et N des k-modules. Alors ce sont des k-k-bimodules. Une application $f : M \to N$ est un homomorphisme de k-modules si et seulement si c'est un homomorphisme de k-k-bimodules. De plus, le groupe $\mathrm{Hom}_k(M, N)$ se trouve alors muni d'une structure de k-k-bimodule, l'action étant donnée par

$$(\lambda f)(m) = f(m\lambda) = f(\lambda m) = \lambda f(m) = f(m)\lambda = (f\lambda)(m)$$

pour $f \in \mathrm{Hom}_k(M, N)$, $\lambda \in k$, $m \in M$. Le produit de composition des homomorphismes est alors une opération k-bilinéaire entre les espaces Hom_k.

Tout aussi passionnant est le comportement du produit tensoriel : $M \otimes_k N$ est un k-k-bimodule, l'action de $\lambda \in k$ sur un tenseur pur $m \otimes n$ étant donnée par

$$\lambda(m \otimes n) = (\lambda m) \otimes n = (m\lambda) \otimes n = m \otimes (\lambda n) = m \otimes (n\lambda) = (m \otimes n)\lambda$$

pour $(m, n) \in M \times N$, l'action sur un tenseur général $\sum_{i \in I} m_i \otimes n_i$ se déduisant de cette formule par additivité. Ce calcul présente deux intérêts mineurs. Il montre d'une part que l'action à gauche de k sur $M \otimes N$ coïncide avec l'action à droite ; et d'autre part, qu'il existe un isomorphisme canonique $M \otimes_k N \cong N \otimes_k M$ qui envoie $m \otimes n$ sur $n \otimes m$ pour chaque $(m, n) \in M \times N$. Ici encore, il faut pouvoir regarder M et N à la fois comme des k-modules à gauche et à droite, d'où l'importance que k soit commutatif.

Exercice. Soit k un anneau commutatif et soient M et N deux k-modules. Construire une application naturelle $\gamma : N \otimes_k \mathrm{Hom}_k(M, k) \to \mathrm{Hom}_k(M, N)$ telle que $\gamma(n \otimes f) = \big(m \mapsto f(m)n\big)$ pour chaque tenseur pur $n \otimes f$ dans le domaine de γ. Montrer que γ est un isomorphisme si M ou N est un k-module projectif de type fini.

3.1.2 Algèbres

k-algèbre : une k-algèbre est un anneau A muni d'un homomorphisme d'anneaux de k dans le centre $Z(A)$ de A.

Notons $\psi_A : k \to Z(A)$ l'homomorphisme d'anneaux donné avec A. Alors A est un k-module, l'action de $\lambda \in k$ étant donné par la multiplication à gauche ou à droite par $\psi_A(\lambda)$. Ainsi $\lambda(ab) = (\lambda a)b = (a\lambda)b = a(\lambda b) = a(b\lambda) = (ab)\lambda$ pour tout $(\lambda, a, b) \in k \times A^2$; on a donc une compatibilité entre la structure de k-module et la structure d'anneau de A.

Un homomorphisme de k-algèbres $f : A \to B$ est un homomorphisme d'anneaux et de k-modules. Il revient au même d'exiger que le diagramme suivant commute :

$$\begin{array}{ccccc} & \overset{\psi_A}{\nearrow} & Z(A) & \hookrightarrow & A \\ k & & & & \downarrow f \\ & \underset{\psi_B}{\searrow} & Z(B) & \hookrightarrow & B. \end{array}$$

3.1.2.1 Exemples.

(1) Un anneau est une $\mathbf{Z}$-algèbre.

(2) L'anneau k est une k-algèbre.

(3) Si M est un k-module, alors $\mathrm{End}_k(M)$ est une k-algèbre.

(4) Si A est une k-algèbre, alors A^{op} est aussi une k-algèbre : on garde la structure de k-module (ou de k-k-bimodule) et on prend la structure d'anneau de A^{op}.

(5) Si A est une k-algèbre et n un entier strictement positif, alors $\mathbf{Mat}_n(A)$ est une k-algèbre.

(6) Soient A et B deux k-algèbres. Alors le produit tensoriel $A \otimes_k B$ est un k-module (voir le paragraphe 3.1.1). Par ailleurs, $A \otimes_k B$ hérite d'une structure d'anneau quand on le regarde comme un quotient de $A \otimes_{\mathbf{Z}} B$ (le sous-groupe de $A \otimes_{\mathbf{Z}} B$ engendré par

$$\{a\psi_A(\lambda) \otimes b - a \otimes \psi_B(\lambda)b \mid (a, \lambda, b) \in A \times k \times B\}$$

est un idéal). On obtient ainsi une structure d'algèbre sur $A \otimes_k B$. On peut alors énoncer des résultats à ceux du paragraphe 1.4.2. Notamment, il existe des homomorphismes canoniques de k-algèbres de A et B dans $A \otimes_k B$, et pour tout A-module M et tout B-module N, on peut munir $M \otimes_k N$ d'une structure de $A \otimes_k B$-module.

(7) Soient A et B deux k-algèbres et m et n deux entiers strictement positifs. Il existe alors un isomorphisme $\mathbf{Mat}_m(A) \otimes_k \mathbf{Mat}_n(B) \cong \mathbf{Mat}_{mn}(A \otimes_k B)$.

Soit A une k-algèbre. Chaque A-module M est alors automatiquement un k-module, l'action de $\lambda \in k$ étant donnée par celle de $\psi_A(\lambda) \in A$. L'action de k commute alors à l'action de A, et il n'y a pas d'inconvénient à regarder M comme un k-k-bimodule. Tout homomorphisme de A-modules est automatiquement un homomorphisme de k-modules.

De façon équivalente, on peut définir un A-module à gauche comme la donnée d'un k-module M et d'un homomorphisme de k-algèbres de A dans $\mathrm{End}_k(M)$. On définit alors un A-module à droite comme étant un A^{op}-module à gauche.

Prenons à présent deux k-algèbres A et B. Au paragraphe 1.4.3, nous avions appelé A-B-bimodule un $A \otimes_{\mathbf{Z}} B^{\mathrm{op}}$-module à gauche. Dans le contexte actuel, cette définition présente l'inconvénient que la structure de k-module définie via l'action de A ne coïncide a priori pas avec le structure de k-module définie via l'action de B. Pour pallier ce problème, nous appellerons A-B-bimodule un $A \otimes_k B^{\mathrm{op}}$-module à gauche. Tout fonctionne alors de façon sympathique : on a une action à gauche de A, une action à droite de B, une action de k pouvant être vue comme une action à gauche ou à droite, et toutes ces actions commutent joyeusement.

Soient A une k-algèbre, L un A-module à droite, et M et N des A-modules à gauche. Alors $\mathrm{Hom}_A(M, N)$ est non seulement un sous-groupe abélien de $\mathrm{Hom}_{\mathbf{Z}}(M, N)$, mais aussi un sous-module du k-module $\mathrm{Hom}_k(M, N)$. Cela signifie d'une part que tout homomorphisme de A-modules de M dans N est automatiquement k-linéaire, et d'autre part que l'ensemble des homomorphismes A-linéaires de M dans N est stable par multiplication par les éléments de k. De la même façon, $L \otimes_A M$ est non seulement un quotient du $\mathbf{Z}$-module $L \otimes_{\mathbf{Z}} M$, mais

aussi un quotient du k-module $L \otimes_k M$ (dans les deux cas, on quotiente par le sous-module engendré par

$$\{(la) \otimes m - l \otimes (am) \mid (l, a, m) \in L \times A \times M\}).$$

On peut alors reprendre toutes les constructions des paragraphes 1.4.3 et 1.4.4 et les cuisiner à la sauce k-linéaire.

Signalons pour conclure deux points de terminologie. Nous avions évoqué la notion de catégorie additive au paragraphe 1.1.4 : c'est une catégorie dont les ensembles d'homomorphismes sont des groupes abéliens, dont les produits de composition sont des opérations $\mathbf{Z}$-bilinéaires, et dans laquelle on peut toujours faire des sommes directes finies. De la même manière, on parle de catégorie k-linéaire quand les ensembles d'homomorphismes sont des k-modules et les produits de composition sont des opérations k-bilinéaires, k étant toujours ici commutatif. Un foncteur $F : \mathscr{A} \to \mathscr{B}$ entre deux catégories k-linéaires est dit k-linéaire si pour chaque couple (M, N) d'objets de $\mathscr{A}$, l'application $F : \mathrm{Hom}_{\mathscr{A}}(M, N) \to \mathrm{Hom}_{\mathscr{B}}(F(M), F(N))$ induite au niveau des groupes est k-linéaire.

Exemples. Soit A une k-algèbre.

(1) La catégorie des A-modules à gauche est une catégorie k-linéaire.

(2) Pour chaque A-module à gauche X, le foncteur $\mathrm{Hom}_A(X, ?)$ est un foncteur k-linéaire covariant exact à gauche de la catégorie des A-modules à gauche vers la catégorie des k-modules. Pour chaque A-module à gauche Y, le foncteur $\mathrm{Hom}_A(?, Y)$ est un foncteur k-linéaire contravariant exact à gauche de la catégorie des A-modules à gauche vers la catégorie des k-modules.

(3) Pour chaque A-module à gauche X, le foncteur $\mathrm{Ext}^1_A(X, ?)$ est un foncteur k-linéaire covariant de la catégorie des A-modules à gauche vers la catégorie des k-modules. Pour chaque A-module à gauche Y, le foncteur $\mathrm{Ext}^1_A(?, Y)$ est un foncteur k-linéaire contravariant de la catégorie des A-modules à gauche vers la catégorie des k-modules.

(4) Pour chaque A-module à droite X, le foncteur $X \otimes_A ?$ est un foncteur k-linéaire covariant exact à droite de la catégorie des A-modules à gauche vers la catégorie des k-modules. Pour chaque A-module à gauche Y, le foncteur $? \otimes_A Y$ est un foncteur k-linéaire covariant exact à droite de la catégorie des A-modules à droite vers la catégorie des k-modules.

3.1.3 Changement de base

On choisit un anneau de base commutatif k. Soit K une k-algèbre commutative, autrement dit un anneau commutatif muni d'un homomorphisme de k dans K. À tout k-module W, on associe le K-module $W_{(K)} = K \otimes_k W$. On dispose alors d'un homomorphisme de k-modules $\iota_W : m \to 1 \otimes m$ de W dans $W_{(K)}$. Dans l'autre sens, chaque K-module V peut être vu comme un k-module via l'homomorphisme d'anneaux de k dans K. Étant donnés V et W comme ci-dessus, le paragraphe 1.4.4 affirme que l'application $f \mapsto f \circ \iota_W$ est un isomorphisme de $\mathrm{Hom}_K(W_{(K)}, V)$ sur $\mathrm{Hom}_k(W, V)$. (Nous devrions noter $\mathrm{ind}_k^K W$ plutôt que $W_{(K)}$ pour suivre les notations du paragraphe 1.4.4.)

Soient M et N deux k-modules. L'application $f \mapsto \iota_N \circ f$ est un homomorphisme de k-modules de $\mathrm{Hom}_k(M,N)$ dans $\mathrm{Hom}_k\big(M, N_{(K)}\big)$. Par ailleurs, $\mathrm{Hom}_k\big(M, N_{(K)}\big) \cong \mathrm{Hom}_K\big(M_{(K)}, N_{(K)}\big)$ est muni d'une structure de K-module. Nous voyons ainsi qu'il existe un homomorphisme naturel de K-modules

$$\alpha : \big(\mathrm{Hom}_k(M,N)\big)_{(K)} \to \mathrm{Hom}_K\big(M_{(K)}, N_{(K)}\big)$$

tel que $\alpha\big(\iota_{\mathrm{Hom}_k(M,N)}(f)\big) \circ \iota_M = \iota_N \circ f$ pour chaque $f \in \mathrm{Hom}_k(M,N)$.

3.1.3.1 Proposition. *Partons du contexte ci-dessus. Supposons que K soit un k-module plat et que M soit un k-module de présentation finie. Alors α est un isomorphisme.*

Preuve. Considérant k, K et N comme étant fixés, nous écrirons α_M pour indiquer que α dépend de M.

On commence par examiner le cas où M est libre de type fini, disons $M = k^n$. La distributivité du produit tensoriel sur la somme directe donne alors $M_{(K)} \cong K^n$, d'où

$$\mathrm{Hom}_K\big(M_{(K)}, N_{(K)}\big) \cong \mathrm{Hom}_K\big(K^n, N_{(K)}\big) \cong \big(N_{(K)}\big)^n \cong (N^n)_{(K)} \cong \big(\mathrm{Hom}_k(M,N)\big)_{(K)}.$$

C'est cette identification que réalise α_M, qui est donc bien un isomorphisme ici.

Quand M est de présentation finie, on dispose d'une suite exacte $F_1 \to F_0 \to M \to 0$, où F_0 et F_1 sont des k-modules libres de type fini. La naturalité de α fait qu'on dispose alors d'un diagramme commutatif

$$\begin{array}{ccccccc}
0 & \longrightarrow & \big(\mathrm{Hom}_k(M,N)\big)_{(K)} & \longrightarrow & \big(\mathrm{Hom}_k(F_0,N)\big)_{(K)} & \longrightarrow & \big(\mathrm{Hom}_k(F_1,N)\big)_{(K)} \\
 & & \downarrow{\scriptstyle \alpha_M} & & \downarrow{\scriptstyle \alpha_{F_0}} & & \downarrow{\scriptstyle \alpha_{F_1}} \\
0 & \longrightarrow & \mathrm{Hom}_K\big(M_{(K)}, N_{(K)}\big) & \longrightarrow & \mathrm{Hom}_K\big((F_0)_{(K)}, N_{(K)}\big) & \longrightarrow & \mathrm{Hom}_K\big((F_1)_{(K)}, N_{(K)}\big).
\end{array}$$

L'exactitude à gauche des foncteurs $\mathrm{Hom}_k(?,N)$ et $\mathrm{Hom}_K\big(?, N_{(K)}\big)$ et l'exactitude du foncteur $K \otimes_k ?$ implique que les lignes de ce diagramme sont exactes. Les deux applications α_{F_0} et α_{F_1} sont des isomorphismes. Une variante du lemme des cinq (exercice (3) du paragraphe 1.1.3) nous dit alors que α_M est un isomorphisme. □

Reprenons notre k-algèbre commutative K. Le foncteur $?_{(K)}$ d'extension des scalaires agit aussi sur une algèbre et ses modules. De fait, si A est une k-algèbre, alors $A_{(K)} = K \otimes_k A$ est une k-algèbre, $\iota_A : A \to A_{(K)}$ est un homomorphisme de k-algèbres, et l'homomorphisme $\lambda \mapsto \lambda \otimes 1$ de K dans $A_{(K)}$ munit cette dernière d'une structure de K-algèbre. Si en outre M est un A-module, alors $M_{(K)} = K \otimes_k M$ est un $K \otimes_k A = A_{(K)}$-module.

Dans cette situation, prenons un second A-module N. Alors l'homomorphisme α construit précédemment se restreint en un homomorphisme de K-modules

$$\beta : \big(\mathrm{Hom}_A(M,N)\big)_{(K)} \to \mathrm{Hom}_{A_{(K)}}\big(M_{(K)}, N_{(K)}\big),$$

et on peut énoncer un résultat analogue à la proposition précédente.

3.1.3.2 Proposition. *Partons du contexte ci-dessus. Supposons que K soit un k-module plat et que M soit un A-module de présentation finie. Alors β est un isomorphisme.*

Concluons ce paragraphe par quelques remarques. Nous nous sommes ici principalement attachés à décrire le changement de base quand K est une k-algèbre commutative. Ce cadre couvre deux situations courantes. La première est quand k est un corps et K est une extension de k ; alors le k-module K est automatiquement libre, donc plat. Prendre pour K la clôture algébrique de k permet alors de rendre les choses plus simples, mais demande de savoir ensuite redescendre sur k. La seconde situation est celle où k est un anneau intègre, par exemple $\mathbf{Z}$ ou $\mathbf{Z}_p$, et où K est soit un quotient par un idéal maximal, soit le corps des fractions de k. L'idée ici est de se ramener à un corps, mais K peut ne pas être toujours plat, ce qui empêche d'utiliser la proposition 3.1.3.2.

On peut également examiner ces constructions quand K n'est pas commutatif. On perd alors la possibilité de dire qu'on regarde des K-algèbres, mais la proposition de changement de base reste valable dans ce cas, avec la même preuve (voir [7], (2.38) par exemple). L'exploration de cette situation peut s'avérer payante ; voir par exemple le théorème 3.3.1.3.

Exercice. Soit k un anneau commutatif, soit K une k-algèbre commutative, et soient M et N deux k-modules. Définir un isomorphisme naturel de K-modules

$$\big(M \otimes_k N\big)_{(K)} \cong M_{(K)} \otimes_K N_{(K)}.$$

3.1.4 Algèbres symétriques et extérieures

Soient k un corps et V un k-espace vectoriel.

On pose $\mathsf{T}^0 V = k$ et $\mathsf{T}^1 V = V$. Pour chaque entier $n \geq 2$, on pose $\mathsf{T}^n V = \mathsf{T}^{n-1} V \otimes_k V$. Grâce à l'associativité du produit tensoriel (proposition 1.4.3.2), nous pouvons oublier le parenthésage et écrire plus simplement

$$\mathsf{T}^n V = \underbrace{V \otimes_k \cdots \otimes_k V}_{n \text{ facteurs}}.$$

Un élément de $\mathsf{T}^n V$ de la forme $v_1 \otimes \cdots \otimes v_n$, où $(v_1, \ldots, v_n) \in V^n$, est appelé tenseur pur. Chaque élément de $\mathsf{T}^n V$ peut s'écrire comme une somme finie de tenseurs purs.

Pour tout $(m, n) \in \mathbf{N}^2$, l'isomorphisme naturel $\mathsf{T}^m V \otimes_k \mathsf{T}^n V \cong \mathsf{T}^{m+n} V$ correspond à une application bilinéaire de $\mathsf{T}^m V \times \mathsf{T}^n V$ dans $\mathsf{T}^{m+n} V$, qui se comporte de la façon suivante sur les tenseurs purs :

$$(v_1 \otimes \cdots \otimes v_m, w_1 \otimes \cdots \otimes w_n) \mapsto v_1 \otimes \cdots \otimes v_m \otimes w_1 \otimes \cdots \otimes w_n.$$

Enfin, on pose $\mathsf{T} V = \bigoplus_{n \in \mathbf{N}} \mathsf{T}^n V$. Les applications $\mathsf{T}^m V \times \mathsf{T}^n V \to \mathsf{T}^{m+n} V$ peuvent être combinées pour définir une application bilinéaire de $\mathsf{T} V \times \mathsf{T} V$ dans $\mathsf{T} V$. Ainsi $\mathsf{T} V$ devient

une k-algèbre. L'élément neutre pour la multiplication est $1 \in k = \mathsf{T}^0 V$. L'algèbre $\mathsf{T} V$ est $\mathbf{N}$-graduée[13]. Enfin $\mathsf{T} V$ est engendrée par $V = \mathsf{T}^1 V$.

Soit I l'idéal de $\mathsf{T} V$ engendré par les éléments de la forme $v \otimes w - w \otimes v$, avec $(v, w) \in V^2$. Étant engendré par des éléments homogènes de degré 2, l'idéal I est homogène, ce qui signifie que $I = \bigoplus_{n \in \mathbf{N}} (I \cap \mathsf{T}^n V)$; en fait, $I = \bigoplus_{n \geq 2} (I \cap \mathsf{T}^n V)$. L'algèbre quotient $\mathsf{S} V = (\mathsf{T} V)/I$ est donc graduée : $\mathsf{S} V = \bigoplus_{n \in \mathbf{N}} \mathsf{S}^n V$, avec $\mathsf{S}^n V = (\mathsf{T}^n V + I)/I \cong \mathsf{T}^n V/(\mathsf{T}^n V \cap I)$. Le produit dans $\mathsf{S} V$ est désigné par la juxtaposition des opérandes. On a $\mathsf{S}^0 V = k$ et $\mathsf{S}^1 V = V$. L'algèbre $\mathsf{S} V$ est engendrée par $\mathsf{S}^1 V = V$; comme ces générateurs commutent entre eux, $\mathsf{S} V$ est commutative.

Soit J l'idéal de $\mathsf{T} V$ engendré par les éléments de la forme $v \otimes v$, avec $v \in V$. Étant engendré par des éléments homogènes de degré 2, l'idéal J vérifie $J = \bigoplus_{n \geq 2} (J \cap \mathsf{T}^n V)$. L'algèbre quotient $\bigwedge V = (\mathsf{T} V)/J$ est donc graduée : $\bigwedge V = \bigoplus_{n \in \mathbf{N}} \bigwedge^n V$, avec $\bigwedge^n V = (\mathsf{T}^n V + J)/J \cong \mathsf{T}^n V/(\mathsf{T}^n V \cap J)$. Le produit dans $\bigwedge V$ est désigné par le symbole $\wedge$. On a $\bigwedge^0 V = k$ et $\bigwedge^1 V = V$. L'algèbre $\bigwedge V$ est engendrée par $\bigwedge^1 V = V$. Pour $(v, w) \in V^2$, nous avons $v \wedge v = 0$ et $v \wedge w = -w \wedge v$. Si x et y sont deux éléments homogènes de $\bigwedge V$, de degrés respectifs $|x|$ et $|y|$, alors $x \wedge y = (-1)^{|x||y|} y \wedge x$.

Ces constructions sont fonctorielles : une application linéaire $f : V \to W$ induit des homomorphismes d'algèbres graduées $\mathsf{T}(f) : \mathsf{T} V \to \mathsf{T} W$, $\mathsf{S}(f) : \mathsf{S} V \to \mathsf{S} W$ et $\bigwedge(f) : \bigwedge V \to \bigwedge W$. Concrètement, l'application $\bigwedge(f)$ par exemple envoie un p-vecteur pur $v_1 \wedge \cdots \wedge v_p$ sur le p-vecteur $f(v_1) \wedge \cdots \wedge f(v_p)$.

3.1.4.1 Proposition. *Soient k un corps, V et W deux k-espaces vectoriels, $n \geq 1$ un entier.*

(i) Pour toute application n-linéaire $f : V^n \to W$, il existe une unique application linéaire $\tilde{f} : \mathsf{T}^n V \to W$ telle que $\tilde{f}(v_1 \otimes \cdots \otimes v_n) = f(v_1, \ldots, v_n)$ pour chaque $(v_1, \ldots, v_n) \in V^n$.

(ii) Pour toute application n-linéaire symétrique $f : V^n \to W$, il existe une unique application linéaire $\hat{f} : \mathsf{S}^n V \to W$ telle que $\hat{f}(v_1 \cdots v_n) = f(v_1, \ldots, v_n)$ pour chaque $(v_1, \ldots, v_n) \in V^n$.

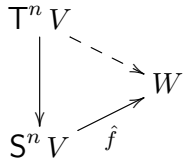
(iii) Pour toute application n-linéaire alternée $f : V^n \to W$, il existe une unique application linéaire $\hat{f} : \bigwedge^n V \to W$ telle que $\hat{f}(v_1 \wedge \cdots \wedge v_n) = f(v_1, \ldots, v_n)$ pour chaque $(v_1, \ldots, v_n) \in V^n$.

Preuve. L'assertion (i) se démontre par récurrence sur n à partir de la propriété universelle du produit tensoriel. Les détails de la preuve sont vraisemblablement pénibles à écrire...

Plaçons-nous dans les hypothèses de (ii). Montrons d'abord l'unicité de $\hat{f}$. Si $\hat{f}$ satisfait aux

13. Un anneau A est dit $\mathbf{N}$-gradué s'il s'écrit comme une somme directe $A = \bigoplus_{n \in \mathbf{N}} A_n$ de sorte que chaque A_n est un sous-groupe additif de A, que $1 \in A_0$, et que $A_m A_n \subseteq A_{m+n}$. Les éléments de A_n sont dits homogènes de degré n. La dernière condition signifie donc que le produit de deux éléments homogènes est homogène, le degré du produit étant la somme des degrés des facteurs.

conditions requises, alors l'application de $\mathsf{T}^n V$ dans W obtenue par composition



doit coïncider avec l'application $\tilde{f}$ de l'assertion (i). Ainsi si $\hat{f}$ existe, elle doit s'obtenir par factorisation de $\tilde{f}$. Réciproquement pour montrer l'existence de $\hat{f}$, il suffit de montrer que $\tilde{f}$ se factorise à travers la surjection canonique de $\mathsf{T}^n V$ sur $\mathsf{S}^n V$.

Tout élément de I est somme d'éléments de la forme $x \otimes (u \otimes v - v \otimes u) \otimes y$, avec $(u, v) \in V^2$ et $(x, y) \in (\mathsf{T} V)^2$. Utilisant la décomposition $\mathsf{T} V = \bigoplus_{p \in \mathbf{N}} \mathsf{T}^p V$, on constate que tout élément de $I \cap \mathsf{T}^n V$ est somme d'éléments de la forme $x \otimes (u \otimes v - v \otimes u) \otimes y$, avec $(u, v) \in V^2$, $(x, y) \in \mathsf{T}^p V \times \mathsf{T}^q V$ et $p + q = n - 2$; on peut en outre exiger ici que x et y soient des tenseurs purs. La symétrie de f fait que $\tilde{f}$ s'annule sur chaque tel élément. Ainsi $\tilde{f}$ s'annule sur $I \cap \mathsf{T}^n V$. On obtient alors $\hat{f}$ par passage au quotient. Ceci achève la preuve de l'assertion (ii).

La preuve de (iii) est analogue à la preuve de (ii). La seule différence consiste à se souvenir qu'une application n-linéaire alternée (c'est-à-dire qui est nulle chaque fois que deux des arguments sont égaux) est automatiquement antisymétrique ; c'est là un argument classiquement utilisé dans la construction du déterminant. □

3.1.4.2 Théorème. *Soient k un corps, $n \geq 1$ un entier, V un k-espace vectoriel, $(e_i)_{i \in I}$ une base de V, $\leq$ un ordre total sur I.*

(i) $\{e_{i_1} \otimes \cdots \otimes e_{i_n} \mid (i_1, \ldots, i_n) \in I^n\}$ *est une base de* $\mathsf{T}^n V$.

(ii) $\{e_{i_1} \cdots e_{i_n} \mid i_1 \leq \cdots \leq i_n$ *dans* $I\}$ *est une base de* $\mathsf{S}^n V$.

(iii) $\{e_{i_1} \wedge \cdots \wedge e_{i_n} \mid i_1 < \cdots < i_n$ *dans* $I\}$ *est une base de* $\bigwedge^n V$.

Preuve. Une remarque pour commencer : une base est une famille, et non pas un ensemble. L'énoncé de ce théorème est donc légèrement incorrect ; l'abus d'écriture commis n'a d'autre but que de permettre l'usage de la notation $\{\cdots \mid \cdots\}$ si commode...

L'assertion (i) se montre par récurrence sur n, en utilisant la distributivité du produit tensoriel sur la somme directe (proposition 1.4.1.4).

L'image d'une famille génératrice par une application linéaire surjective étant génératrice, l'assertion (i) implique que

$$\{e_{i_1} \cdots e_{i_n} \mid (i_1, \ldots, i_n) \in I^n\}$$

engendre $\mathsf{S}^n V$. Comme $\mathsf{S} V$ est une algèbre commutative, l'élément $e_{i_1} \cdots e_{i_n}$ est laissé stable par permutation des indices. On peut ainsi se restreindre aux suites $(i_1, \ldots, i_n)$ croissantes sans perdre le caractère générateur de notre famille de vecteurs. Considérons maintenant l'algèbre $\mathscr{A}$ des polynômes à coefficients dans k en la famille d'indéterminées $(\mathscr{E}_i)_{i \in I}$. À $v = \sum_{i \in I} a_i e_i$, associons le polynôme $\mathscr{V} = \sum_{i \in I} a_i \mathscr{E}_i$. La proposition 3.1.4.1 (ii) montre l'existence d'une

application linéaire $\hat{f} : \mathsf{S}^n V \to \mathscr{A}$ telle que $\hat{f}(v_1 \cdots v_n) = \mathscr{V}_1 \cdots \mathscr{V}_n$ pour chaque $(v_1, \ldots, v_n) \in V^n$. En particulier, $\hat{f}(e_{i_1} \cdots e_{i_n}) = \mathscr{E}_{i_1} \cdots \mathscr{E}_{i_n}$. La famille des monômes

$$\left\{ \mathscr{E}_{i_1} \cdots \mathscr{E}_{i_n} \;\middle|\; i_1 \leq \cdots \leq i_n \text{ dans } I \right\}$$

étant libre dans $\mathscr{A}$, notre famille de vecteurs de $\mathsf{S}^n V$ est libre. Nous avons ainsi prouvé (ii).

La preuve de (iii) commence comme la preuve de (ii) : on utilise l'égalité $e_{i_{\sigma(1)}} \wedge \cdots \wedge e_{i_{\sigma(n)}} = \operatorname{sgn}(\sigma) e_{i_1} \wedge \cdots \wedge e_{i_n}$, valable pour chaque suite $(i_1, \ldots, i_n) \in I^n$ et chaque permutation $\sigma \in \mathfrak{S}_n$, pour réordonner les indices et conclure que la famille

$$\left\{ e_{i_1} \wedge \cdots \wedge e_{i_n} \;\middle|\; i_1 \leq \cdots \leq i_n \text{ dans } I \right\}$$

engendre $\bigwedge^n V$. La sous-famille obtenue en se restreignant aux suites $(i_1, \ldots, i_n)$ strictement croissantes est encore génératrice, car les vecteurs éliminés sont nuls. Maintenant, soit $e^i \in V^*$ la forme linéaire qui vaut 1 en e_i et 0 en e_j pour $j \neq i$. Soit $\mathbf{i} = (i_1, \ldots, i_n)$ une suite strictement croissante d'indices. La proposition 3.1.4.1 (iii) montre l'existence d'une forme linéaire $e^{\mathbf{i}} : \bigwedge^n V \to k$ telle que

$$e^{\mathbf{i}}(v_1 \wedge \cdots \wedge v_n) = \sum_{\sigma \in \mathfrak{S}_n} e^{i_1}(v_{\sigma(1)}) \cdots e^{i_n}(v_{\sigma(n)})$$

pour chaque $(v_1, \ldots, v_n) \in V^n$. Pour chaque suite strictement croissante $\mathbf{j} = (j_1, \ldots, j_n)$ d'indices, $e^{\mathbf{i}}(e_{j_1} \wedge \cdots \wedge e_{j_n})$ vaut 1 si $\mathbf{j} = \mathbf{i}$ et 0 sinon. L'existence de toutes ces formes linéaires $e^{\mathbf{i}}$ impose à la famille

$$\left\{ e_{i_1} \wedge \cdots \wedge e_{i_n} \;\middle|\; i_1 < \cdots < i_n \text{ dans } I \right\}$$

d'être libre. Ceci termine la preuve de (iii). □

3.1.4.3 Corollaire. *Soient k un corps et V et W deux k-espaces vectoriels. Il existe des isomorphismes canoniques d'espaces vectoriels gradués*

$$\mathsf{S}(V \oplus W) \cong \mathsf{S}\, V \otimes_k \mathsf{S}\, W \quad \textit{et} \quad \textstyle\bigwedge(V \oplus W) \cong \bigwedge V \otimes_k \bigwedge W.$$

En particulier, pour chaque $n \in \mathbf{N}$, on a

$$\mathsf{S}^n(V \oplus W) \cong \bigoplus_{p+q=n} \mathsf{S}^p V \otimes_k \mathsf{S}^q W \quad \textit{et} \quad \textstyle\bigwedge^n(V \oplus W) \cong \bigoplus_{p+q=n} \bigwedge^p V \otimes_k \bigwedge^q W.$$

Preuve. Les injections de V et W dans $V \oplus W$ fournissent par fonctorialité des homomorphismes d'algèbres $f : \mathsf{S}\, V \to \mathsf{S}(V \oplus W)$ et $g : \mathsf{S}\, W \to \mathsf{S}(V \oplus W)$. En prenant des bases de V et W et en utilisant le théorème précédent, on vérifie sans difficulté que l'application $\sum_{i \in I} x_i \otimes y_i \mapsto f(x)g(y)$ de $\mathsf{S}\, V \otimes_k \mathsf{S}\, W$ dans $\mathsf{S}(V \oplus W)$ est un isomorphisme d'espaces vectoriels. Un raisonnement analogue fournit le résultat pour les algèbres extérieures. □

Remarque. L'isomorphisme $\mathsf{S}(V \oplus W) \cong \mathsf{S}\, V \otimes_k \mathsf{S}\, W$ contruit dans la preuve du corollaire 3.1.4.3 est un isomorphisme de k-algèbres ; cela se voit par exemple en utilisant (l'analogue pour les algèbres de) le corollaire 1.4.2.2. Le cas des algèbres extérieures est plus subtil : pour avoir un isomorphisme d'algèbres, il faut munir l'espace $\bigwedge V \otimes_k \bigwedge W$ du produit $(x \otimes y)(z \otimes t) = (-1)^{|y||z|} xz \otimes yt$, où y et z sont des éléments homogènes de degrés $|y|$ et $|z|$, respectivement.

3.1.4.4 Applications des algèbres symétriques et extérieures.

(1) Soit V un k-espace vectoriel de dimension n. Alors $\bigwedge^n V$ est une droite vectorielle. Chaque endomorphisme $f \in \mathrm{End}_k(V)$ induit un endomorphisme $\bigwedge^n(f)$ de la droite vectorielle $\bigwedge^n V$; le rapport de cet homomorphisme n'est autre que le déterminant de f. En effet, prenant une base $(e_1, \dots, e_n)$ de V et la base duale $(e^1, \dots, e^n)$ de V^*, on calcule

$$\begin{aligned}
\textstyle\bigwedge^n(f)(e_1 \wedge \cdots \wedge e_n) &= f(e_1) \wedge \cdots \wedge f(e_n) \\
&= \sum_{i_1,\dots,i_n=1}^{n} \left(\prod_{p=1}^{n} \langle e^{i_p}, f(e_p) \rangle \right) e_{i_1} \wedge \cdots \wedge e_{i_n} \\
&= \sum_{\sigma \in \mathfrak{S}_n} \left(\prod_{p=1}^{n} \langle e^{\sigma(p)}, f(e_p) \rangle \right) e_{\sigma(1)} \wedge \cdots \wedge e_{\sigma(n)} \\
&= \left(\sum_{\sigma \in \mathfrak{S}_n} \mathrm{sgn}(\sigma) \prod_{p=1}^{n} \langle e^{\sigma(p)}, f(e_p) \rangle \right) e_1 \wedge \cdots \wedge e_n \\
&= \det(f)\; e_1 \wedge \cdots \wedge e_n.
\end{aligned}$$

La formule $\det(f \circ g) = \det(f)\det(g)$ s'obtient alors gratuitement en utilisant la fonctorialité de la construction. Les formules de Binet-Cauchy trouvent également une interprétation naturelle dans ce cadre. Ainsi l'algèbre extérieure est une manière intrinsèque de définir les déterminants, sans utiliser de coordonnées ou de base.

(2) Soit V un espace vectoriel de dimension finie n. Soit $(e_1, \dots, e_n)$ une base de V, soit $(e^1, \dots, e^n)$ la base duale de V^*. Alors l'application $P(X_1, \dots, X_n) \mapsto P(e^1, \dots, e^n)$ de l'algèbre des polynômes $k[X_1, \dots, X_n]$ dans $\mathsf{S}\, V^*$ est un isomorphisme de k-algèbres graduées. Ainsi $\mathsf{S}\, V^*$ peut être regardée comme la version sans coordonnée d'une algèbre de polynômes. En outre quand k est infini, $\mathsf{S}\, V^*$ s'identifie à l'algèbre des fonctions polynomiales sur V (à cet égard, on observera que les éléments de V^* sont bien des fonctions sur V).

Soit k un corps et V un k-espace vectoriel. Pour simplifier les notations, nous écrirons $\otimes$ au lieu de $\otimes_k$, S^p au lieu de $\mathsf{S}^p V$, et $\bigwedge^p$ au lieu de $\bigwedge^p V$ pour chaque entier naturel p. Fixons un entier $n \geq 1$. Pour $0 \leq p \leq n-1$, définissons des applications linéaires

$$d_p : \mathsf{S}^{n-p-1} \otimes \textstyle\bigwedge^{p+1} \to \mathsf{S}^{n-p} \otimes \bigwedge^p \quad \text{et} \quad \delta_p : \mathsf{S}^{n-p} \otimes \bigwedge^p \to \mathsf{S}^{n-p-1} \otimes \bigwedge^{p+1}$$

par les formules

$$d_p(v_1 \cdots v_{n-p-1} \otimes w_1 \wedge \cdots \wedge w_{p+1}) = \sum_{i=1}^{p+1} (-1)^{i+1} v_1 \cdots v_{n-p-1} w_i \otimes w_1 \wedge \cdots \wedge \widehat{w_i} \wedge \cdots \wedge w_{p+1}$$

$$\delta_p(v_1 \cdots v_{n-p} \otimes w_1 \wedge \cdots \wedge w_p) = \sum_{i=1}^{n-p} v_1 \cdots \widehat{v_i} \cdots v_p \otimes v_i \wedge w_1 \wedge \cdots \wedge w_p,$$

où le chapeau signifie que le facteur est omis.

3.1.4.5 Lemme. *Les applications d_p et δ_p sont bien définies par les formules ci-dessus. Elles vérifient les équations*

$$d_{p-1}\circ d_p = \delta_{p+1}\circ\delta_p = 0 \quad et \quad d_p\circ\delta_p + \delta_{p-1}\circ d_{p-1} = n\,\mathrm{id}_{\mathsf{S}^{n-p}\otimes\bigwedge^p}.$$

Preuve. L'expression

$$\sum_{i=1}^{p+1}(-1)^{i+1}v_1\cdots v_{n-p-1}w_i\otimes w_1\wedge\cdots\wedge\widehat{w_i}\wedge\cdots\wedge w_{p+1}$$

est multilinéaire en $(v_1,\dots,v_{n-p-1},w_1,\dots,w_{p+1})$, symétrique en $(v_1,\dots,v_{n-p-1})$ et alternée en $(w_1,\dots,w_{p+1})$. Les propriétés universelles des différents avatars du produit tensoriel entraînent alors l'existence et l'unicité de d_p. On montre de même l'existence et l'unicité de δ_p.

Quand on applique $\delta_{p+1}\circ\delta_p$ à $v_1\cdots v_{n-p}\otimes w_1\wedge\cdots\wedge w_p$, on obtient

$$\sum_{\substack{i,j=1\\ i\neq j}}^{n-p} v_1\cdots\widehat{v_i}\cdots\widehat{v_j}\cdots v_{n-p}\otimes v_i\wedge v_j\wedge w_1\wedge\cdots\wedge w_p$$
$$= \sum_{1\le i<j\le n-p} v_1\cdots\widehat{v_i}\cdots\widehat{v_j}\cdots v_{n-p}\otimes\underbrace{(v_i\wedge v_j+v_j\wedge v_i)}_{0}\wedge w_1\wedge\cdots\wedge w_p;$$

ainsi $\delta_{p+1}\circ\delta_p = 0$. La preuve de $d_{p-1}\circ d_p = 0$ est du même genre.

Enfin on calcule l'image de $v_1\cdots v_{n-p}\otimes w_1\wedge\cdots\wedge w_p$ par $d_p\circ\delta_p$:

$$\sum_{i=1}^{n-p} v_1\cdots\widehat{v_i}\cdots v_{n-p}v_i\otimes w_1\wedge\cdots\wedge w_p+\sum_{i=1}^{n-p}\sum_{j=1}^{p}(-1)^j v_1\cdots\widehat{v_i}\cdots v_{n-p}w_j\otimes v_i\wedge w_1\wedge\cdots\wedge\widehat{w_j}\wedge\cdots\wedge w_p$$

et par $\delta_{p-1}\circ d_{p-1}$:

$$\sum_{i=1}^{n-p}\sum_{j=1}^{p}(-1)^{j+1}v_1\cdots\widehat{v_i}\cdots v_{n-p}w_j\otimes v_i\wedge w_1\wedge\cdots\wedge\widehat{w_j}\wedge\cdots\wedge w_p$$
$$+\sum_{j=1}^{p}(-1)^{j+1}v_1\cdots v_{n-p}\otimes\underbrace{w_j\wedge w_1\wedge\cdots\wedge\widehat{w_j}\wedge\cdots\wedge w_p}_{(-1)^{j+1}w_1\wedge\cdots\wedge w_p}.$$

De là, on obtient facilement la dernière équation. □

3.1.4.6 Théorème (complexes de Koszul). *Si k est de caractéristique zéro, alors pour tout $n>0$ les deux suites*

$$0\to\mathsf{S}^0\otimes\bigwedge^n\xrightarrow{d_{n-1}}\mathsf{S}^1\otimes\bigwedge^{n-1}\xrightarrow{d_{n-2}}\cdots\xrightarrow{d_1}\mathsf{S}^{n-1}\otimes\bigwedge^1\xrightarrow{d_0}\mathsf{S}^n\otimes\bigwedge^0\to 0$$
$$0\to\mathsf{S}^n\otimes\bigwedge^0\xrightarrow{\delta_0}\mathsf{S}^{n-1}\otimes\bigwedge^1\xrightarrow{\delta_1}\cdots\xrightarrow{\delta_{n-2}}\mathsf{S}^1\otimes\bigwedge^{n-1}\xrightarrow{\delta_{n-1}}\mathsf{S}^0\otimes\bigwedge^n\to 0$$

sont exactes.

Preuve. L'équation $d_{p-1}\circ d_p = 0$ donne immédiatement $\operatorname{im} d_p\subseteq\ker d_{p-1}$. Dans l'autre sens, prenons $x\in\ker d_{p-1}$. L'équation $d_p\circ\delta_p+\delta_{p-1}\circ d_{p-1} = n\,\mathrm{id}_{\mathsf{S}^{n-p}\otimes\bigwedge^p}$ nous dit qu'alors $nx = (d_p\circ\delta_p)(x)\in\operatorname{im} d_p$. Ainsi $x\in\operatorname{im} d_p$. □

3.1.4.7 Remarque. Une suite de modules et d'homomorphismes

$$\cdots \to A_{p+1} \xrightarrow{d_p} A_p \xrightarrow{d_{p-1}} A_{p-1} \to \cdots$$

est appelée complexe si $d_{p-1} \circ d_p = 0$; dans ce cas, $\operatorname{im} d_p \subseteq \ker d_{p-1}$. Un tel complexe est dit acyclique si on a $\operatorname{im} d_p = \ker d_{p-1}$ pour tout p (autrement dit, si la suite est exacte). Il est dit homotope à zéro s'il existe une suite d'applications $s_{p+1} : A_p \to A_{p+1}$ telle que $d_p \circ s_{p+1} + s_p \circ d_{p-1} = \mathrm{id}_{A_p}$. On vérifie facilement qu'un complexe homotope à zéro est acyclique.

Ce qu'on appelle complexe de Koszul est en fait le premier complexe du théorème 3.1.4.6. Il est homotope à zéro même quand la caractéristique de k est non-nulle. De fait, choisissons une base $(e_i)_{i\in I}$ de V et munissons I d'un ordre total $\leq$. Les vecteurs $e_{j_1} \cdots e_{j_{n-p}} \otimes e_{k_1} \wedge \cdots \wedge e_{k_p}$ forment une base de $\mathsf{S}^{n-p} \otimes \bigwedge^p$, les suites d'indices $(j_1, \ldots, j_{n-p})$ et $(k_1, \ldots, k_p)$ étant croissantes, la première au sens large et la seconde strictement. On définit une application linéaire $s_{p+1} : \mathsf{S}^{n-p} \otimes \bigwedge^p \to \mathsf{S}^{n-p-1} \otimes \bigwedge^{p+1}$ sur cette base en décrétant que

$$s_{p+1}(e_{j_1} \cdots e_{j_{n-p}} \otimes e_{k_1} \wedge \cdots \wedge e_{k_p}) = \begin{cases} e_{j_2} \cdots e_{j_{n-p}} \otimes e_{j_1} \wedge e_{k_1} \wedge \cdots \wedge e_{k_p} & \text{si } j_1 < k_1, \\ 0 & \text{sinon.} \end{cases}$$

On vérifie alors sans difficulté que $d_p \circ s_{p+1} + s_p \circ d_{p-1} = \mathrm{id}_{\mathsf{S}^{n-p} \otimes \bigwedge^p}$.

Exercices.

(1) Soit V un espace vectoriel sur un corps k (de caractéristique quelconque, éventuellement égale à 2). Il existe une application linéaire de $V^* \otimes V^*$ dans l'espace k^V des fonctions sur V à valeurs dans k, qui envoie un tenseur de la forme $f \otimes g$ sur la fonction $v \mapsto f(v)g(v)$. Décrire l'image et le noyau de cette application linéaire. (Indication : par définition, l'image est l'ensemble des formes quadratiques sur V. La remarque 3.1.4.4 (2) explique que notre application linéaire s'identifie à l'homomorphisme canonique de $\mathsf{T}^2 V^*$ sur $\mathsf{S}^2 V^*$; son noyau est donc le sous-espace vectoriel engendré par les éléments de la forme $f \otimes g - g \otimes f$. On pourra aussi comparer avec le complexe de Koszul

$$0 \to \bigwedge^2 V^* \xrightarrow{d_1} V^* \otimes V^* \xrightarrow{d_0} \mathsf{S}^2 V^* \to 0,$$

qui est exact d'après la remarque 3.1.4.7).

(2) Soit V un espace vectoriel de dimension p, soit n un entier naturel. Calculer la dimension de $\mathsf{S}^n V$ et de $\bigwedge^n V$. Les égalités (a priori douteuses) $(-1)^n \bigwedge^n V = \mathsf{S}^n(-V)$ et $(-1)^n \mathsf{S}^n V = \bigwedge^n(-V)$ ont-elles une chance d'être vraies au niveau des dimensions ?

3.2 Résultats classiques

3.2.1 Représentations d'une algèbre

Représentation matricielle : soit A une k-algèbre et $n \geq 1$ un entier. Une représentation matricielle de A de degré n est un homomorphisme de k-algèbres de A dans l'algèbre $\mathbf{Mat}_n(k)$ des matrices $n \times n$ à coefficients dans k.

Exemple. Une représentation matricielle de degré n de l'algèbre $k[T]$ est la donnée d'une matrice $X \in \mathbf{Mat}_n(k)$. De fait, la donnée de X équivaut à celle de l'homomorphisme d'algèbres $P(T) \mapsto P(X)$ de $k[T]$ dans $\mathbf{Mat}_n(k)$.

L'algèbre $\mathbf{Mat}_n(k)$ agit par multiplication à gauche sur l'ensemble k_c^n des vecteurs colonnes de taille n à coefficients dans k ; nous avons ainsi un isomorphisme d'algèbres $\mathbf{Mat}_n(k) \cong \mathrm{End}_k(k_c^n)$. De même, l'algèbre $\mathbf{Mat}_n(k)$ agit par multiplication à droite sur l'ensemble k_l^n des vecteurs lignes ; d'où un isomorphisme d'algèbres $\mathbf{Mat}_n(k)^{\mathrm{op}} \cong \mathrm{End}_k(k_l^n)$.

Soit A une k-algèbre et $n \geq 1$ un entier. La donnée d'une représentation matricielle de A de degré n permet de munir k_c^n d'une structure de A-module à gauche et de munir k_l^n d'une structure de A-module à droite. Réciproquement, la donnée d'un A-module à gauche M fournit une représentation matricielle de A dès que le k-module sous-jacent à M est libre de rang fini ; cette représentation dépend du choix d'une base du k-module M. De même, la donnée d'un A-module à droite N fournit une représentation matricielle de A dès que le k-module sous-jacent à N est libre de rang fini ; cette représentation matricielle dépend du choix d'une base du k-espace vectoriel N. Ceci nous amène à la définition suivante.

Représentation : soit A une k-algèbre. Une représentation de A est un A-module M (à gauche ou à droite) tel que le k-module sous-jacent à M soit un k-module projectif de type fini.

Quand k est un anneau principal ou un anneau local, tout k-module projectif de type fini est libre (propositions 1.2.3.3 et 2.3.1.2). La différence entre représentation et représentation matricielle se résume alors au fait d'avoir fixé une base. L'avantage d'utiliser des matrices est que les calculs sont très explicites et que le changement de base s'effectue de manière transparente.

Il y a quelques différences entre le langage des représentations et celui des modules : à la notion d'isomorphisme entre deux modules correspond la notion d'équivalence : deux représentations matricielles X et Y de même degré n d'une k-algèbre A sont dites équivalentes s'il existe une matrice inversible $P \in \mathbf{GL}_n(k)$ telle que $PX(a) = Y(a)P$ pour tout $a \in A$. Ainsi deux représentations matricielles provenant d'un même module mais correspondant à deux choix de bases différents sont équivalentes ; réciproquement, deux représentations matricielles équivalentes fournissent des modules isomorphes. Ainsi on peut identifier une classe d'équivalence de représentations matricielles de A avec une classe d'isomorphisme de A-modules.

Seconde différence de langage : considérons une représentation M de A, vue disons comme A-module à gauche. Une sous-représentation N de M est un sous-module tel que N et M/N soient des k-modules projectifs de type fini. (Cette condition supplémentaire est automatiquement satisfaite quand k est un corps.) Cette petite distinction entre les notions de sous-module et de sous-représentation se retrouve dans la notion de simplicité : une représentation irréductible est une représentation qui n'a pas de sous-représentation non-banale, quand bien même le module correspondant n'est pas simple (je ne sais pas si cet usage est général, car on entend parfois dire module irréductible au lieu de module simple).

Dernière définition : soit M une représentation de A, vue comme A-module. Le rang du k-module sous-jacent à M est appelé le degré de la représentation [14].

14. Quand le k-module sous-jacent à M est projectif mais n'est pas libre, le rang n'est plus un entier, mais

3.2.1.1 Remarque. Soit A une algèbre sur un anneau commutatif k. Dans la discussion précédente, quand nous regardions les représentations de A comme des A-modules, nous avions besoin de distinguer entre A-modules à gauche et A-modules à droite. En revanche, il n'y avait pas ce problème en ce qui concernait les représentations matricielles. Ainsi en passant par ces dernières, on peut associer un A-module à droite à un A-module à gauche et réciproquement, sous l'hypothèse que les k-modules sous-jacents soient libres de type fini.

Cette situation rappelle celle examinée dans la remarque 2.3.3.2. Un moyen de la formaliser est d'introduire une dualité. Quand M est un A-module à gauche, le k-dual $N = \mathrm{Hom}_k(M, k)$ de M est muni d'une structure de A-module à droite : pour $f \in N$ et $a \in A$, l'application $fa = (m \mapsto f(am))$ de M dans k est un élément de N. Réciproquement, le k-dual $M = \mathrm{Hom}_k(N, k)$ d'un A-module à droite N est un A-module à gauche (voir l'exemple 1.4.3.1 (3)).

La dualité que nous cherchons est donnée par le foncteur $D = \mathrm{Hom}_k(?, k)$. L'isomorphisme canonique de bidualité rend D involutif quand on le restreint aux A-modules dont le k-module sous-jacent est projectif de type fini. Par ailleurs D est un foncteur contravariant : à chaque homomorphisme de A-modules à gauche $f : M \to M'$ correspond un homomorphisme dans l'autre sens $D(f) : D(M') \to D(M)$ de A-modules à droite ($D(f)$ est la transposée de f). Quand k est un corps (cette hypothèse rend sans objet les petites subtilités liées à la notion de sous-représentation), la dualité D échange les notions de sous-module et de module quotient, préserve les modules simples et les modules complètement réductibles, échange le socle avec la tête, échange les notions de monomorphisme et d'épimorphisme, et même de monomorphisme essentiel et d'épimorphisme essentiel, etc.

Dans la suite de ce chapitre, nous supposerons que k est un corps.

3.2.2 Quelques faits sur les algèbres de dimension finie

3.2.2.1 Proposition. *Soit k un corps algébriquement clos et soit Δ une k-algèbre à division de dimension finie sur k. Alors $\Delta = k1$.*

Preuve. Soit $\delta \in \Delta$. L'homomorphisme d'algèbres $P \mapsto P(\delta)$ de $k[X]$ dans Δ ne peut pas être injectif, pour des raisons de dimension. Son noyau est donc un idéal non-nul de $k[X]$. Soit P un élément non-nul de degré minimal dans $\ker \varphi$. Supposons que P ne soit pas irréductible. On écrit alors $P = QR$, avec Q et R de degré strictement inférieur au degré de P. Alors $Q(\delta)$ et $R(\delta)$ ne sont pas nuls. Ils sont donc inversibles dans Δ, et donc leur produit $Q(\delta)R(\delta)$ est donc aussi inversible, en contradiction avec $P(\delta) = 0$. Bref P est nécessairement irréductible. Comme k est algébriquement clos, P est de la forme $X - a$, avec $a \in k$, et donc δ est a fois l'unité de Δ. L'homomorphisme d'anneaux $a \mapsto a1$ de k dans Δ est donc surjectif. Il est aussi injectif car k n'a pas d'idéal non-banal. □

Remarque. À isomorphisme près, il y a exactement trois algèbres à division de dimension finie sur le corps $\mathbf{R}$ des nombres réels : $\mathbf{R}$ lui-même, le corps $\mathbf{C}$ des nombres complexes, et l'algèbre $\mathbf{H}$ des quaternions de Hamilton.

une fonction localement constante à valeurs entières sur le spectre de k. Si k est intègre, le spectre de k est un espace topologique connexe, de sorte qu'aucune ambiguïté ne survient. Pour des détails, voir par exemple [11], section 7.7.

Une k-algèbre de dimension finie est un anneau artinien à gauche et à droite. Si A est une k-algèbre de dimension finie, alors chaque A-module de type fini est de dimension finie sur k (puisqu'il est quotient d'un module libre de type fini A^n). En particulier, un A-module simple ou un A-module projectif indécomposable est de dimension finie sur k. La proposition suivante montre que chaque A-module injectif indécomposable est aussi de dimension finie sur k. Un phénomène amusant est que si A est de dimension finie, tout module simple, projectif ou injectif est de k-dimension inférieure à celle de A ; en revanche, rien n'exclut l'existence de modules indécomposables de dimension arbitrairement grande.

3.2.2.2 Proposition. *Soient k un corps et A une k-algèbre de dimension finie.*

(i) Soit M un A-module de dimension finie sur k. Alors M est un A-module injectif si et seulement si son dual $D(M)$ est un A^{op}-module projectif.

(ii) L'enveloppe injective d'un A-module de type fini est de type fini.

Preuve. (i) Essentiellement, il s'agit de reprendre les assertions (ii) des propositions 1.1.6.2 et 1.1.6.5 et de voir que le foncteur de dualité D, qui consiste à prendre la transposée des homomorphismes, renverse les flèches et permet de passer de la caractérisation des modules projectifs à celle des modules injectifs. Il y a toutefois un problème : les modules L, M et N intervenant là sont quelconques alors que notre dualité D ne s'applique correctement qu'aux modules de dimension finie sur k. Faisons donc les choses proprement.

Supposons que M est injectif. Prenons un homomorphisme surjectif de A-modules à droite $f : A^n \to D(M)$. En dualisant, on obtient une suite exacte courte $0 \to M \xrightarrow{D(f)} D(A)^n \to \operatorname{coker} D(f) \to 0$ de A-modules à gauche. L'injectivité de M nous dit que cette suite est scindée : M est un facteur direct de $D(A)^n$. Dualisant à nouveau, nous voyons que $D(M)$ est un facteur direct de A^n, et est par conséquent projectif.

Dans l'autre sens, supposons que $D(M)$ est projectif. Soient I un idéal à gauche de A et $h \in \operatorname{Hom}_A(I, M)$. La projectivité de $D(M)$ fait qu'on peut compléter le diagramme

$$\begin{array}{ccccc} & & & & D(M) \\ & & \overset{f}{\swarrow} & & \downarrow{\scriptstyle D(h)} \\ D(A) & \longrightarrow & D(I) & \longrightarrow & 0. \end{array}$$

Alors h est la restriction à I de l'homomorphisme $D(f) \in \operatorname{Hom}_A(A, M)$. Le critère (v) de la proposition 1.1.6.5 dit alors que M est injectif.

(ii) Soit M un A-module de type fini. Alors on peut regarder $D(M)$ et sa couverture projective $p : C(D(M)) \to D(M)$. Comme $D(M)$ est de type fini, il en est de même de $C(D(M))$ d'après la proposition 2.3.4.2 (iv), et on peut à nouveau appliquer le foncteur de dualité. On arrive à $D(p) : D(C(D(M))) \to M$. Ici $D(C(D(M)))$ est injectif grâce à (i) et $D(p)$ est un monomorphisme essentiel car p est un épimorphisme essentiel. Bref $D(C(D(M)))$ coïncide avec l'enveloppe injective $E(M)$ de M. Cette dernière est donc de dimension finie sur k. □

3.2.3 Représentations et changement de base

Soient A une k-algèbre et K une extension de k.

K-représentation : prenons un entier $n \geq 1$. Un homomorphisme de k-algèbres $X : A \to \mathbf{Mat}_n(K)$ est appelé représentation de A sur K de degré n (ou K-représentation de A).

Posons $A_{(K)} = K \otimes_k A$, comme au paragraphe 3.1.3. L'isomorphisme de K-espaces vectoriels $f \mapsto f \circ \iota_A$ de $\mathrm{Hom}_K\big(A_{(K)}, \mathbf{Mat}_n(K)\big)$ sur $\mathrm{Hom}_k(A, \mathbf{Mat}_n(K))$ se restreint en un isomorphisme de l'ensemble des représentations matricielles de $A_{(K)}$ de degré n sur l'ensemble des K-représentations de A de degré n. Concrètement, la représentation de $A_{(K)}$ correspondant à une K-représentation $X : A \to \mathbf{Mat}_n(K)$ de A est son prolongement K-linéaire

$$\sum_{i \in I} \lambda_i \otimes a_i \mapsto \sum_{i \in I} \lambda_i X(a_i), \qquad \text{où } I \text{ est fini, } \lambda_i \in K \text{ et } a_i \in A.$$

Chaque représentation X de A est une K-représentation de A, vu que $\mathbf{Mat}_n(k) \subseteq \mathbf{Mat}_n(K)$. En termes de modules, cette évidence s'écrit de la façon suivante : si le A-module M fournit la représentation X, alors la K-représentation X est fournie par le $A_{(K)}$-module $M_{(K)}$. Pour s'en convaincre, il faut revenir aux définitions du paragraphe 3.1.3. Plus précisément, prenons M un k-espace vectoriel de dimension finie n et muni d'une base $(m_1, \ldots, m_n)$. Ainsi le K-espace vectoriel $M_{(K)}$ est de dimension n et est muni de la base $(1 \otimes m_1, \ldots, 1 \otimes m_n)$. Le point est de vérifier que le diagramme

$$\begin{array}{ccc} \mathbf{Mat}_n(k) & \longrightarrow & \mathbf{Mat}_n(K) \\ \downarrow & & \downarrow \\ \mathrm{End}_k(M) & \longrightarrow & \mathrm{End}_K\big(M_{(K)}\big) \end{array}$$

est commutatif, où les flèches verticales sont les isomorphismes définis par le choix des bases, où la flèche du haut est l'inclusion, et où la flèche du bas est l'application $f \mapsto \mathrm{id}_K \otimes f$.

3.2.3.1 Théorème (Noether, Deuring). *Soient k un corps, A une k-algèbre, K une extension de k, et X et Y deux représentations matricielles de A de même degré n. Alors X et Y sont des représentations équivalentes si et seulement s'il existe une matrice inversible $P \in \mathbf{GL}_n(K)$ telle que $PX(a) = Y(a)P$ pour tout $a \in A$.*

Preuve. Si X et Y sont équivalentes, alors il existe une matrice $P \in \mathbf{GL}_n(k)$ qui entrelace X et Y. En particulier P appartient à $\mathbf{GL}_n(K)$ et vérifie $PX(a) = Y(a)P$ pour tout $a \in A$. La difficulté est dans la réciproque, où il faut montrer que l'existence d'une matrice P adéquate à coefficients dans K entraîne celle d'une matrice à coefficients dans k.

Le sous-espace vectoriel $\{(X(a), Y(a)) \mid a \in A\}$ de $\mathbf{Mat}_n(k)^2$ étant de dimension finie, il est engendré par une partie finie $\{(X(a_i), Y(a_i)) \mid 1 \leq i \leq s\}$, où $(a_1, \ldots, a_s)$ est une suite finie d'éléments de A. Pour toute extension L du corps k, regardons le système linéaire homogène

$$PX(a_i) = Y(a_i)P \quad \text{pour chaque } i \in \{1, \ldots, s\}$$

portant sur (les coefficients d') une matrice $P \in \mathbf{Mat}_n(L)$. Les coefficients de ce système appartiennent à k. D'après les théorèmes classiques sur les systèmes d'équations linéaires (mise sous forme échelonnée, par exemple), on peut trouver une base $(P_1, \dots, P_r)$ de l'espace des solutions, indépendante de L et formée de matrices à coefficients dans k.

Notre hypothèse est qu'il existe $(t_1, \dots, t_r) \in K^r$ tel que $t_1P_1 + \cdots + t_rP_r \in \mathbf{GL}_n(K)$. Nous voulons montrer qu'il existe $(u_1, \dots, u_r) \in k^r$ tel que $u_1P_1 + \cdots + u_rP_r \in \mathbf{GL}_n(k)$.

Regardons le polynôme $Q(T_1, \dots, T_r) = \det(T_1P_1 + \cdots + T_rP_r)$. Notre hypothèse assure qu'il n'est pas identiquement nul. Par ailleurs, il est homogène de degré n. Si k est infini, alors il existe $(u_1, \dots, u_r) \in k^r$ n'annulant pas Q et c'est gagné. Sinon, k possède une extension finie L de cardinal plus grand que $n+1$. Il existe alors $(v_1, \dots, v_r) \in L^r$ n'annulant pas Q. La matrice $v_1P_1 + \cdots + v_rP_r$ appartient alors à $\mathbf{GL}_n(L)$ et entrelace X et Y.

Appelons M et N les A-modules fournis par les représentations X et Y. En tant que A-modules, $M_{(L)} = L \otimes_k M$ est isomorphe à la somme directe de $[L:k]$ copies de M. De même pour N. Notre matrice $v_1P_1 + \cdots + v_rP_r$ fournit un isomorphisme de $A_{(L)}$-modules entre $M_{(L)}$ et $N_{(L)}$, donc fournit a fortiori un isomorphisme de A-modules. En appliquant le théorème de Krull-Schmidt à la situation

$$\underbrace{M \oplus \cdots \oplus M}_{[L:k] \text{ termes}} \cong \underbrace{N \oplus \cdots \oplus N}_{[L:k] \text{ termes}},$$

on conclut que $M \cong N$. Les représentations X et Y sont donc équivalentes. □

Appliqué à l'algèbre $k[T]$, ce théorème affirme que deux matrices $n \times n$ à coefficients dans k sont semblables si et seulement si elles sont semblables sur K. Dans le langage des modules, ce théorème dit la chose suivante.

3.2.3.2 Corollaire. *Soient k un corps, A une k-algèbre, K une extension de k, et M et N deux A-modules de dimension finie sur k. Alors M et N sont isomorphes si et seulement si les $A_{(K)}$-modules $M_{(K)}$ et $N_{(K)}$ sont isomorphes.*

3.2.4 Théorèmes de Burnside et de Frobenius-Schur

La théorie des représentations des algèbres est plus simple quand le corps de base k est algébriquement clos. La principale raison pour cela est que k est alors la seule algèbre à division de dimension finie sur k (proposition 3.2.2.1).

3.2.4.1 Lemme (Schur). *Soit k un corps algébriquement clos, soit A une k-algèbre, soient M et N deux A-modules simples de dimension finie sur k. Si $M \cong N$, alors* $\mathrm{Hom}_A(M,N)$ *est de dimension* 1 *sur k ; si $M \ncong N$, alors* $\mathrm{Hom}_A(M,N) = 0$. *En particulier,* $\mathrm{End}_A(M) = k\,\mathrm{id}_M$.

Preuve. Il suffit de combiner le lemme de Schur 1.2.4.2 du chapitre 1 avec la proposition 3.2.2.1. La seule chose à dire en plus peut-être est que le k-espace vectoriel $\mathrm{Hom}_A(M,N)$ est de dimension finie, puisque c'est un sous-espace vectoriel de $\mathrm{Hom}_k(M,N)$. □

3.2.4.2 Théorème (Burnside). *Soient k un corps, A une k-algèbre, et M un A-module simple de dimension finie sur k. Si $\mathrm{End}_A(M) = k\ \mathrm{id}_M$, alors l'homomorphisme de A dans $\mathrm{End}_k(M)$ est surjectif.*

Preuve. Il s'agit d'un corollaire immédiat du théorème de densité 1.3.2.1. □

Soient A une k-algèbre, M un A-module de k-dimension finie n, et $T : A \to \mathbf{Mat}_n(k)$ une représentation matricielle de A qui fournit M. L'application qui à $a \in A$ associe la coordonnée (i, j) de $T(a)$ est une forme linéaire X_{ij} sur A, appelé coefficient matriciel de M. L'ensemble des coefficients matriciels X_{ij} dépend du choix de la k-base de M utilisée pour obtenir T, mais le sous-espace qu'il engendre dans A^* n'en dépend pas. Dans les hypothèses du théorème de Burnside (à savoir quand M simple et $\mathrm{End}_A(M) = k\ \mathrm{id}_M$), l'ensemble des n^2 coefficients matriciels X_{ij} est k-linéairement indépendant.

3.2.4.3 Théorème (Frobenius, Schur). *Soit k un corps algébriquement clos, soit A une k-algèbre, et soient M_1, ..., M_r des A-modules simples de dimension finie sur k et deux à deux non-isomorphes. Pour chaque $s \in \{1, \ldots, r\}$, soit $n_s = \dim_k(M_s)$ et soit $\{X_{ij}^{(s)} \mid 1 \leq i, j \leq n_s\}$ un ensemble de coefficients matriciels pour M_s. Alors le sous-ensemble*

$$\bigsqcup_{s=1}^{r} \{X_{ij}^{(s)} \mid 1 \leq i, j \leq n_s\}$$

de A^* est linéairement indépendant sur k.

Preuve. Considérons le A-module $M = M_1 \oplus \cdots \oplus M_r$. Appelons B l'image de A dans $\mathrm{End}_k(M)$. Alors M_1, ..., M_r sont des B-modules simples deux à deux non-isomorphes. De plus, B est une k-algèbre de dimension finie ayant un module complètement réductible fidèle, à savoir M. D'après le théorème 2.1.2.1 (iii) et sa preuve, B est semi-simple et le B-module régulier ${}_BB$ peut être plongé dans M^n pour un entier n assez grand. Tout B-module simple est isomorphe à un sous-module de ${}_BB$, donc à un sous-module de M. Ainsi B a exactement r classes d'équivalence de modules simples, fournies par M_1, ..., M_r.

Pour $s \in \{1, \ldots, r\}$, appelons C_s la composante simple de B correspondant au module M_s : ainsi C_s est la composante M_s-isotypique du B-module à gauche régulier. La structure d'anneau produit $B = C_1 \times \cdots \times C_r$ fait que $C_t C_s = 0$ dès que $t \neq s$; dans ce cas, C_t est inclus dans l'annulateur du sous-module C_s de ${}_BB$, et donc C_t annule M_s.

Pour chaque $s \in \{1, \ldots, r\}$, l'homomorphisme de B dans $\mathrm{End}_k(M_s)$ est surjectif, d'après le lemme de Schur et le théorème de Burnside ci-dessus. L'alinéa précédent dit que son noyau contient les C_t pour $t \neq s$. Cet homomorphisme induit donc un isomorphisme $C_s \cong \mathrm{End}_k(M_s)$. Ainsi pour chaque (i, j) avec $1 \leq i, j \leq n_s$, on peut trouver $a \in A$ tel que $X_{ij}^{(s)}(a) = 1$ et que $X_{lm}^{(t)}(a) = 0$ pour $(l, m, t) \neq (i, j, s)$. À ce stade, si l'on évalue au point a une combinaison k-linéaire

$$\sum_{t=1}^{r} \sum_{l,m=1}^{n_t} \alpha_{lm}^{(t)} X_{lm}^{(t)} = 0,$$

on trouve $\alpha_{ij}^{(s)} = 0$. □

Un peu de numérologie pour conclure ce paragraphe. Prenons une algèbre semi-simple A de dimension finie n sur un corps k pas forcément algébriquement clos. On peut alors décomposer A en produit de ses composantes simples $A \cong \mathbf{Mat}_{n_1}(\Delta_1) \times \cdots \times \mathbf{Mat}_{n_r}(\Delta_r)$. Ici, il y a r (classes d'isomorphisme de) A-modules simples M_1, ... M_r, l'algèbre à division Δ_i est l'opposée de l'anneau d'endomorphismes $\mathrm{End}_A(M_i)$, et n_i est la longueur du Δ_i-module à droite M_i (voir la remarque 2.1.2.4). Enfin le centre $Z(A)$ de A est isomorphe au produit des centres $Z(\Delta_i)$ des algèbres à division Δ_i. On voit ainsi que

$$\dim_k M_i = n_i \dim_k \Delta_i, \quad \dim_k A = \sum_{i=1}^{r} n_i^2 \dim_k \Delta_i \quad \text{et} \quad \dim_k Z(A) = \sum_{i=1}^{r} \dim_k Z(\Delta_i).$$

Si en outre k est algébriquement clos, alors $\Delta_i = k$ pour chaque $i \in \{1, \ldots, r\}$ d'après la proposition 3.2.2.1, d'où

$$\dim_k A = \sum_{i=1}^{r} (\dim_k M_i)^2 \quad \text{et} \quad \dim_k Z(A) = r.$$

3.2.5 Caractère d'une représentation

Soit A une k-algèbre. Notons A^* l'espace vectoriel dual $\mathrm{Hom}_k(A, k)$.

Le caractère d'une représentation matricielle $X : A \to \mathbf{Mat}_n(k)$ de A est la forme linéaire $\chi_X : a \mapsto \operatorname{tr} X(a)$ sur A. Deux représentations équivalentes ont même caractère : si X et $Y : A \to \mathbf{Mat}_n(k)$ sont équivalentes, alors il existe une matrice inversible $P \in \mathbf{GL}_n(k)$ telle que $Y(a) = PX(a)P^{-1}$ pour tout $a \in A$, ce qui implique que $X(a)$ et $Y(a)$ aient même trace.

De même, le caractère d'un A-module M de dimension finie sur k est la forme linéaire $\chi_M : a \mapsto \operatorname{tr} \rho(a)$, où $\rho : A \to \mathrm{End}_k(M)$ est l'homomorphisme d'algèbres définissant la structure de A-module sur M. Évidemment $\chi_M = \chi_X$ si le module M fournit la représentation matricielle X.

3.2.5.1 Proposition. *Soit $0 \to L \to M \to N \to 0$ une suite exacte courte de A-modules de dimension finie sur k. Alors $\chi_M = \chi_L + \chi_N$.*

Preuve. Choisissons une base de L et une base de N. En envoyant la première et en remontant la seconde dans M, on obtient par concaténation une base de M. Appelons X, Y et Z les représentations matricielles de A apportées par les modules L, M et N dans ces bases. Alors pour chaque $a \in A$, $Y(a)$ se décompose par blocs de la façon suivante

$$Y(a) = \begin{pmatrix} X(a) & * \\ 0 & Z(a) \end{pmatrix}.$$

La proposition traduit l'égalité $\operatorname{tr} Y(a) = \operatorname{tr} X(a) + \operatorname{tr} Z(a)$. □

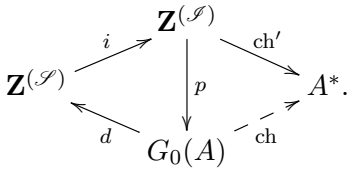
À partir de maintenant et jusqu'à la fin de ce paragraphe, nous supposerons que k est algébriquement clos. La proposition suivante est une conséquence immédiate du théorème de Frobenius-Schur.

3.2.5.2 Proposition. *Soit A une algèbre sur un corps k algébriquement clos. Si M_1, ..., M_r sont des A-modules simples de dimension finie sur k et deux à deux non-isomorphes, alors les formes linéaires χ_{M_1}, ..., χ_{M_r} sont linéairement indépendantes dans A^*.*

Supposons que A soit de dimension finie. Jointe à la proposition 1.2.5.2, le résultat suivant nous dit que deux A-modules de dimension finie sur k ont même caractère si et seulement s'ils ont mêmes facteurs de composition, avec les mêmes multiplicités de Jordan-Hölder.

3.2.5.3 Proposition. *Soit A une algèbre de dimension finie sur un corps k algébriquement clos. Alors il existe un unique homomorphisme de groupes abéliens* $\mathrm{ch} : G_0(A) \to A^*$ *tel que* $\mathrm{ch}[M] = \chi_M$ *pour chaque A-module de type fini. Cet homomorphisme est injectif.*

Preuve. Reprenons les notations du paragraphe 1.2.5. Dans notre contexte où A est une algèbre de dimension finie sur k, $\mathscr{I}$ est l'ensemble des classes d'isomorphismes de A-modules de dimension finie sur k. Soit $\mathrm{ch}' : \mathbf{Z}^{(\mathscr{I})} \to A^*$ l'homomorphisme de groupes abéliens qui envoie (M) sur χ_M. Le diagramme de la preuve de la proposition 1.2.5.2 peut alors être complété :



Pour mémoire, l'application d ici envoie l'élément $[M]$ du groupe de Grothendieck sur l'élément $((M : S))_{S \in \mathscr{I}}$. La proposition 3.2.5.1 dit que ch' se factorise à travers p, donnant ainsi lieu à l'homomorphisme ch. La proposition 3.2.5.2 implique que l'homomorphisme $\mathrm{ch}' \circ i$ est injectif. (Cette proposition dit en fait davantage, à savoir que l'homomorphisme de k-espaces vectoriels de $k^{(\mathscr{I})}$ dans A^* déduit par changement de base de $\mathrm{ch}' \circ i$ est injectif.) Puisque d est un isomorphisme, nous obtenons l'injectivité de $\mathrm{ch}' \circ i \circ d = \mathrm{ch} \circ p \circ i \circ d = \mathrm{ch}$. □

Exercice. Soit k un corps de caractéristique 0, pas nécessairement algébriquement clos, et soit A une k-algèbre. Montrer que si M_1, ..., M_r sont des A-modules simples de dimension finie sur k et deux à deux non-isomorphes, alors χ_{M_1}, ..., χ_{M_r} sont linéairement indépendantes dans A^*. (Indication : se ramener au cas où A est une algèbre semi-simple de dimension finie en utilisant le même procédé que dans la preuve du théorème de Frobenius-Schur. À ce stade, évaluer les caractères χ_{M_1}, ..., χ_{M_r} sur les éléments neutres des composantes simples de A.)

3.2.6 Représentations absolument irréducibles

Dans tout ce paragraphe, on se donne une algèbre A sur un corps k. Les modules considérés sont toujours de dimension finie sur k.

Module absolument simple : un A-module M est dit absolument simple si pour toute extension K de k, le $A_{(K)}$-module $M_{(K)}$ est simple.

On définit de manière analogue la notion de représentation absolument irréductible.

3.2.6.1 Théorème. *Pour un A-module M simple de dimension finie, les conditions suivantes sont équivalentes :*

(i) *M est absolument simple.*

(ii) *Pour toute extension finie K de k, le $A_{(K)}$-module $M_{(K)}$ est simple.*

(iii) *Il existe une extension algébriquement close Ω de k telle que le $A_{(\Omega)}$-module $M_{(\Omega)}$ est simple.*

(iv) $\mathrm{End}_A(M) = k\,\mathrm{id}_M$.

(v) *Pour toute k-algèbre B et tout B-module simple N, le $A \otimes_k B$-module $M \otimes_k N$ est simple.*

Preuve. Supposons (iii). Le lemme de Schur 3.2.4.1 dit que $\mathrm{End}_{A_{(\Omega)}}\big(M_{(\Omega)}\big)$ est de dimension 1 sur Ω. L'isomorphisme de Ω-espaces vectoriels $\mathrm{End}_{A_{(\Omega)}}\big(M_{(\Omega)}\big) \cong \big(\mathrm{End}_A(M)\big)_{(\Omega)}$ de la proposition 3.1.3.2 nous dit alors que $\mathrm{End}_A(M)$ est de dimension 1 sur k. (Note : cet isomorphisme peut être prouvé sans l'arsenal déployé au paragraphe 3.1.3 ; examiner à ce sujet la preuve du théorème 3.2.3.1.) Cela prouve (iv).

Supposons (iv). Le théorème de Burnside 3.2.4.2 affirme que l'homomorphisme de A dans $\mathrm{End}_k(M)$ est surjectif. Prenons une extension K de k. L'homomorphisme de $A_{(K)}$ dans $\big(\mathrm{End}_k(M)\big)_{(K)} \cong \mathrm{End}_K\big(M_{(K)}\big)$ est donc surjectif. On en déduit que $M_{(K)}$ est un $A_{(K)}$-module simple. Ceci étant valable quel que soit K, nous avons montré (i).

Supposons (ii). Soit Ω une clôture algébrique de k. Prenons une base $(e_i)_{i\in I}$ du k-espace vectoriel sous-jacent à M. Soit m un élément non-nul de $M_{(\Omega)}$. Alors m s'écrit $\sum_{i\in I} \omega_i \otimes e_i$, pour une famille de scalaires $(\omega_i) \in \Omega^I$. Soit K la sous-extension de Ω/k engendrée par les éléments de cette famille ; ainsi K est une extension finie de k. Nous pouvons regarder $M_{(K)}$ comme un sous-K-espace vectoriel de $M_{(\Omega)}$ et $A_{(K)}$ comme une sous-K-algèbre de $A_{(\Omega)}$, et nous avons $m \in M_{(K)}$. Puisque nous supposons (ii), le $A_{(K)}$-module $M_{(K)}$ est simple, donc est engendré par m. Alors $A_{(\Omega)}m = \Omega \otimes_K A_{(K)}m = \Omega \otimes_K M_{(K)} = M_{(\Omega)}$. Ainsi le $A_{(\Omega)}$-module $M_{(\Omega)}$ est engendré par m. Ceci étant vrai pour tout élement m non-nul, $M_{(\Omega)}$ est un $A_{(\Omega)}$-module simple. (iii) est donc vérifiée.

L'implication (iv) $\Rightarrow$ (v) est un cas particulier de la proposition 1.4.5.1 (iii). L'assertion (ii) est un cas particulier de l'assertion (v). Enfin l'implication (i) $\Rightarrow$ (iii) est une conséquence immédiate de la définition. □

Soit A une k-algèbre de dimension finie. On dit que A est décomposée si tout A-module simple est absolument simple. On dit qu'une extension K de k décompose A si la K-algèbre $A_{(K)}$ est décomposée.

3.2.6.2 Proposition. *Soient k un corps, K une extension de A, et A une k-algèbre de dimension finie.*

(i) *L'extension K décompose A si et seulement si l'algèbre semi-simple $A_{(K)}/J\big(A_{(K)}\big)$ est produit d'algèbres de matrices $\mathbf{Mat}_n(K)$ à coefficients dans K.*

(ii) *Si K décompose A, alors toute extension E de K décompose A.*

(iii) Si le corps K est algébriquement clos, alors il décompose A.

(iv) Il existe une extension finie de k qui décompose A.

Preuve. Soit K une extension de k. On peut décomposer l'algèbre semi-simple $A_{(K)}/J\big(A_{(K)}\big)$ en produit de composantes simples $\prod_{i\in I}\mathbf{Mat}_{n_i}(\Delta_i)$. Chacune de ces composantes simples correspond à un module simple M_i et l'algèbre à division Δ_i est l'opposée de l'anneau d'endomorphismes $\mathrm{End}_A(M_i)$. D'après le théorème 3.2.6.1, le $A_{(K)}$-module M_i est absolument simple si et seulement si $\Delta_i = K$. Cela donne l'équivalence annoncée dans (i).

Supposons que K décompose A. Avec (i), on peut donc écrire $A_{(K)}/J\big(A_{(K)}\big)$ comme un produit $\prod_{i\in I}\mathbf{Mat}_{n_i}(K)$. Soit E une extension de K. Par extension des scalaires, nous avons alors $A_{(E)}/J\big(A_{(K)}\big)_{(E)} \cong \prod_{i\in I}\mathbf{Mat}_{n_i}(E)$. Cet anneau est semi-simple, donc son radical de Jacobson est réduit à $\{0\}$. Comme $J\big(A_{(K)}\big)_{(E)}$ est un idéal nilpotent de $A_{(E)}$, il est inclus dans le radical de Jacobson $J\big(A_{(E)}\big)$. D'après l'exercice (7) du paragraphe 2.2.1, le radical de Jacobson du quotient $A_{(E)}/J\big(A_{(K)}\big)_{(E)}$ est $J\big(A_{(E)}\big)/J\big(A_{(K)}\big)_{(E)}$. Ainsi $J\big(A_{(E)}\big) = J\big(A_{(K)}\big)_{(E)}$ et l'algèbre $A_{(E)}/J\big(A_{(E)}\big)$ est isomorphe au produit $\prod_{i\in I}\mathbf{Mat}_{n_i}(E)$. D'après (i), cela signifie que E décompose A. (ii) est prouvée.

Compte-tenu des théorèmes de structure des algèbres semi-simples de dimension finie et de la proposition 3.2.2.1, l'assertion (iii) découle de (i).

Soit Ω une clôture algébrique de k. Choisissons une base $(a_s)_{s\in S}$ du k-espace vectoriel sous-jacent à A. Le (iii), combiné au (i), donne un isomorphisme de Ω-algèbres $A_{(\Omega)}/J\big(A_{(\Omega)}\big) \cong \prod_{i\in I}\mathbf{Mat}_{n_i}(\Omega)$. Par ailleurs, on peut trouver une base $(f_t)_{t\in T}$ du Ω-espace vectoriel sous-jacent à $A_{(\Omega)}$, avec T partitionné en $T' \sqcup T''$, de sorte que les f_t appartiennent au radical $J\big(A_{(\Omega)}\big)$ si $t \in T'$, et les images dans le quotient $A_{(\Omega)}/J\big(A_{(\Omega)}\big)$ des f_t restants soient envoyés sur les matrices élémentaires par notre isomorphisme. La base $(a_s)_{s\in S}$ peut être vue comme une base du Ω-espace vectoriel $A_{(\Omega)}$. On peut donc parler de la matrice de changement de base de $(a_s)_{s\in S}$ à $(f_t)_{t\in T}$. Le sous-corps de Ω engendré par les coefficients de cette matrice est une extension finie K de k. La famille $(f_t)_{t\in T}$ peut alors être vue comme une base de l'algèbre $A_{(K)}$, et la table de multiplication dans cette base est la même dans $A_{(K)}$ que dans $A_{(\Omega)}$. En particulier, le sous-K-espace vectoriel N engendré par les $(f_t)_{t\in T'}$ est alors un idéal nilpotent de $A_{(K)}$, et les éléments restants $(f_t)_{t\in T''}$, qui fournissent une base du quotient $A_{(K)}/N$, donnent un isomorphisme $A_{(K)}/N \cong \prod_{i\in I}\mathbf{Mat}_{n_i}(K)$. Alors N est inclus dans le radical de Jacobson $J\big(A_{(K)}\big)$ et le radical de Jacobson de $A_{(K)}/N$ est réduit à $\{0\}$. L'exercice (7) du paragraphe 2.2.1 conduit alors à $J\big(A_{(K)}\big) = N$, et l'assertion (i) nous permet de conclure que K décompose A. Cela prouve (iv). □

Exercices.

(1) Soient A une k-algèbre de dimension finie, K une extension de k, N un $A_{(K)}$-module simple. Montrer qu'il existe un A-module simple M tel que N soit isomorphe à un facteur de composition du $A_{(K)}$-module $M_{(K)}$. (Indication : N est isomorphe à un facteur de composition du $A_{(K)}$-module à gauche régulier. Par ailleurs, le foncteur d'extension des scalaires $?_{(K)}$ envoie une série de composition du A-module à gauche régulier sur une filtration du $A_{(K)}$-module à gauche régulier. Utiliser alors le théorème de raffinement de Schreier 1.2.4.4 ou le théorème de Jordan-Hölder 1.2.4.5.)

(2) Soient A une k-algèbre, M et N deux A-modules de dimension finie sur k, et K une extension de k. Montrer que M et N ont un facteur de composition commun si et seulement si les $A_{(K)}$-modules $M_{(K)}$ et $N_{(K)}$ ont un facteur de composition commun. (Indication : il suffit de traiter le cas où M et N sont simples et non-isomorphes. L'image B de A dans $\mathrm{End}_k(M \oplus N)$ est alors une algèbre semi-simple de dimension finie, et on peut trouver un idempotent central $\varepsilon \in B$ agissant par l'identité sur M et par zéro sur N. Soit $a \in A$ relevant ε. Alors $1 \otimes a \in A_{(K)}$ agit par l'identité sur $M_{(K)}$ et par zéro sur $N_{(K)}$. Il est alors impossible que $M_{(K)}$ et $N_{(K)}$ aient un facteur de composition commun.)

(3) Soient A et B deux k-algèbres de dimension finie, avec A décomposée. Montrer que $J(A \otimes_k B) = J(A) \otimes_k B + A \otimes_k J(B)$ et que les $A \otimes_k B$-modules simples sont les $M \otimes_k N$, où M est un A-module simple et N est un B-module simple. (Indication : utiliser l'exemple 3.1.2.1 (7) pour démontrer que $A/J(A) \otimes_k B/J(B)$ est semi-simple. Puis utiliser l'exercice (7) du paragraphe 2.2.1 pour prouver que l'inclusion évidente $J(A \otimes_k B) \supseteq J(A) \otimes_k B + A \otimes_k J(B)$ est une égalité. La simplicité des $A \otimes_k B$-modules $M \otimes_k N$ de l'énoncé est conséquence de la proposition 1.4.5.1 (iii). Pour conclure, utiliser un argument de comptage.)

3.2.7 Caractères linéaires d'une algèbre, caractère central d'une représentation

Soit k un corps et A une k-algèbre. Un caractère linéaire de A est un homomorphisme d'algèbres $h : A \to k$. Autrement dit, c'est une représentation matricielle de degré 1. On peut identifier cette représentation à son caractère (il n'y a pas grande différence entre une matrice 1×1 et sa trace...), ce qui justifie l'emploi du même mot qu'au paragraphe 3.2.5.

Un A-module M est dit avoir un caractère central si le centre de A agit de façon scalaire : on demande l'existence d'un caractère linéaire $h : Z(A) \to k$ tel que chaque élément $a \in Z(A)$ agisse comme $h(a)\,\mathrm{id}_M$. On vérifie immédiatement que si M admet h comme caractère central, tout A-module isomorphe à M admet aussi h pour caractère central.

3.2.7.1 Proposition. *Tout A-module absolument simple de dimension finie sur k possède un caractère central.*

Preuve. Soit $\pi : A \to \mathrm{End}_k(M)$ l'homomorphisme d'algèbres définissant la structure de A-module sur M. Alors π induit par restriction un homomorphisme d'algèbres de $Z(A)$ dans $\mathrm{End}_A(M)$. La conclusion provient alors du théorème 3.2.6.1 (iv). □

3.2.7.2 Corollaire. *Soit A une k-algèbre commutative. Tout A-module absolument simple de dimension finie sur k est de dimension 1 sur k.*

Preuve. Soit M un A-module absolument simple de dimension finie. D'après la proposition précédente, M admet un caractère central $h : Z(A) \to k$. Puisque k est commutative, $Z(A) = A$. L'action de chaque $a \in A$ est donc donnée par un opérateur scalaire, ce qui implique que tout sous-espace vectoriel de M est un sous-A-module. Comme M est supposé simple, cela force M à être de dimension 1 sur k. □

On notera que quand k est algébriquement clos, on peut supprimer le mot « absolument » dans l'énoncé de cette proposition et de son corollaire (théorème 3.2.6.1 (iii)).

Supposons k algébriquement clos. Étant donnée une k-algèbre commutative A, nous notons $A^\wedge$ l'ensemble des caractères linéaire de A. Ainsi $A^\wedge$ est l'ensemble des classes d'isomorphisme de A-modules simples de dimension finie sur k. Le groupe de Grothendieck $K_0(\text{A-mod}_{\text{df}})$ de la catégorie des A-modules de dimension finie sur K (voir le paragraphe 1.2.5) est alors un $\mathbf{Z}$-module libre de base $A^\wedge$.

Toujours avec k algébriquement clos, prenons une k-algèbre A, et supposons avoir explicité une sous-algèbre commutative B de A. Chaque A-module M de dimension finie sur k peut alors être vu comme un B-module, de sorte que l'on dispose du symbole $[M] \in K_0(B\text{-mod}_{\text{df}})$. Quand B est assez grosse dans A, M est entièrement déterminé par ce symbole. C'est par exemple le cas quand A est l'algèbre enveloppante d'une algèbre de Lie semi-simple $\mathfrak{g}$ et B est l'algèbre enveloppante d'une sous-algèbre de Cartan $\mathfrak{h}$ de $\mathfrak{g}$.

Exercices.

(1) Soient k un corps, A une k-algèbre. Montrer que les caractères linéaires de A sont des éléments linéairement indépendants de l'espace dual A^*. (Indication : procédant par l'absurde, on considère une relation de dépendance linéaire non-triviale de longueur minimale entre les caractères linéaires de A, disons $a_1h_1 + \cdots + a_nh_n = 0$. Alors tous les a_i sont non-nuls et $n \geq 2$. Trouvant $y \in A$ tel que $h_1(y) \neq h_2(y)$, on peut alors fabriquer une relation de dépendance linéaire plus courte en soustrayant l'une de l'autre les deux relations suivantes

$$h_1(y)(a_1h_1(x) + \cdots + a_nh_n(x)) = 0 \quad \text{et} \quad a_1h_1(yx) + \cdots + a_nh_n(yx) = 0.)$$

(2) Soient k un corps et A une k-algèbre de dimension finie. On note Z le centre de A et J le radical de Jacobson de A.

(i) Montrer que le radical de Jacobson de Z est $Z \cap J$ et que $Z/(Z \cap J)$ est un produit de corps. (Indication : utiliser le théorème 2.2.2.3 (i).)

On note $(B_i)_{i\in I}$ la famille des blocs de A (paragraphe 2.4). Pour chaque $i \in I$, soit ε_i l'idempotent primitif central du bloc B_i. Enfin, on suppose que k est algébriquement clos.

(ii) Montrer que pour chaque $i \in I$, il existe un unique caractère linéaire $h_i : Z \to k$ tel que $h_i(\varepsilon_i) = \delta_{ij}$. Montrer qu'on obtient ainsi tous les caractères linéaires de l'algèbre Z. (Indication : soit $\overline{Z}$ le quotient $Z/(Z\cap J)$. La structure de $\overline{Z}$ obtenue à la question précédente permet une description complète des caractères linéaires de $\overline{Z}$. En outre, chaque caractère linéaire de l'algèbre Z s'annule sur le radical de Jacobson $Z\cap J$, de sorte qu'on peut identifier l'ensemble des caractères linéaires de Z avec l'ensemble des caractères linéaires de $\overline{Z}$. Enfin, la proposition 2.3.2.1 montre que les $(\varepsilon_i)_{i\in I}$ sont les éléments qu'on obtient en relevant à Z les idempotents primitifs de $\overline{Z}$.)

(iii) En déduire que deux A-modules simples appartiennent au même bloc si et seulement s'ils ont même caractère central.

(3) Soit k un corps algébriquement clos et soit A une k-algèbre commutative de type fini (autrement dit, A est un quotient d'une algèbre de polynômes en un nombre fini

d'indéterminées). Montrer que tout A-module simple M est de dimension 1 sur k. (Note : on ne suppose pas que le module M est de dimension finie sur k. Indication : utiliser le Nullstellensatz.)

3.3 Algèbres séparables

3.3.1 Complète réductibilité et changement de base

Algèbre séparable : une algèbre A de dimension finie est dite séparable sur k si pour toute extension K de k, la K-algèbre $A_{(K)}$ est semi-simple.

Exemple. Une algèbre de matrice $\mathbf{Mat}_n(k)$ est séparable sur k. Plus généralement, une algèbre A semi-simple et décomposée sur k est séparable sur k.

3.3.1.1 Proposition. *Soit E une extension finie du corps k. Alors E est séparable sur k en tant qu'algèbre si et seulement si l'extension E/k est séparable au sens de la théorie des corps.*

Preuve. Supposons que E/k soit séparable au sens de la théorie des corps. D'après le théorème de l'élément primitif, on peut écrire $E \cong k[X]/(P)$, où P est un polynôme sans racine multiple. Pour chaque extension K de k, on peut décomposer $P = Q_1 \cdots Q_r$ en produit de facteurs irréductibles dans $K[X]$, et les Q_i sont deux à deux non-associés. Par le théorème des restes chinois,

$$E_{(K)} \cong K[X]/(P) \cong K[X]/(Q_1) \times \cdots \times K[X]/(Q_r)$$

est un produit de corps, donc est semi-simple. L'algèbre E est donc bien séparable sur k.

Supposons au contraire que E/k ne soit pas séparable au sens de la théorie des corps. Il existe alors un élément $x \in E$ qui est racine multiple de μ, son polynôme minimal sur k. Écrivons la décomposition en facteurs irréductibles dans $E[X]$: $\mu = u \prod_{i\in I} \nu_i^{n_i}$, avec $u \in E^*$ et les ν_i polynômes unitaires irréductibles dans $E[X]$ et deux à deux distincts. Alors un des n_i est supérieur ou égal à 2. En utilisant le théorème des restes chinois, on obtient un isomorphisme

$$\big(k(x)\big)_{(E)} = E \otimes_k k(x) \cong E[X]/(\mu) \cong \prod_{i\in I} E[X]/\big(\nu_i^{n_i}\big).$$

Pour le i tel que $n_i \geq 2$, l'image de ν_i dans $E[X]/\big(\nu_i^{n_i}\big)$ est non-nulle et nilpotente. Cela montre que $\big(k(x)\big)_{(E)}$ possède un élément nilpotent. L'algèbre $E_{(E)}$ possède donc un élément nilpotent ; comme elle est commutative, son radical de Jacobson ne peut pas être nul. Ainsi l'algèbre E n'est pas séparable sur k. □

On dit qu'une k-algèbre A est simple centrale si elle est simple et si son centre est la droite $k1$. (L'étude des algèbres simples centrales conduit à la définition du groupe de Brauer de k, dont les propriétés dépendent de l'arithmétique du corps k.) Le lemme ci-dessous a pour conséquence qu'une k-algèbre simple centrale est séparable.

3.3.1.2 Lemme. *Soient A et B deux algèbres de dimension finie sur un corps k. On suppose que la k-algèbre A est simple centrale.*

(i) Un élément x de $A \otimes_k B$ qui vérifie $(a \otimes 1)x = x(a \otimes 1)$ pour tout $a \in A$ est de la forme $1 \otimes b$, avec $b \in B$.

(ii) L'application $I \mapsto A \otimes_k I$ est une bijection de l'ensemble des idéaux bilatères de B sur l'ensemble des idéaux bilatères de $A \otimes_k B$.

(iii) $J(A \otimes_k B) = J(A) \otimes_k B$.

Preuve. Choisissons une base $(e_i)_{i \in I}$ du k-espace vectoriel sous-jacent à B. Soit x un élément de $A \otimes_k B$ vérifiant $(a \otimes 1)x = x(a \otimes 1)$ pour tout $a \in A$. Il existe une unique famille $(x_i) \in A^I$ telle que $x = \sum_{i \in I} x_i \otimes e_i$. Pour chaque $a \in A$, l'égalité

$$0 = (a \otimes 1)x - x(a \otimes 1) = \sum_{i \in I} (ax_i - x_i a) \otimes e_i$$

entraîne $ax_i - x_i a$. Ainsi chaque x_i est de la forme $\lambda_i 1$, avec $\lambda_i \in k$, et donc $x = 1 \otimes \left(\sum_{i \in I} \lambda_i e_i \right)$. Cela montre (i).

À présent, nous regardons $A \otimes_k B$ comme un A-A-bimodule pour la multiplication à gauche et à droite de A sur le premier facteur du produit tensoriel. Comme A est une algèbre simple, le A-A-bimodule régulier est simple. La décomposition $A \otimes_k B = \bigoplus_{i \in I} A \otimes e_i$ en somme directe de bimodules isomorphes à ce bimodule régulier montre que $A \otimes_k B$ est un bimodule complètement réductible. Qui plus est, pour chaque homomorphisme $f : A \to A \otimes_k B$ de bimodules, l'élément $f(1)$ vérifie les hypothèses de (i), donc s'écrit $1 \otimes b$. On en déduit que chaque sous-bimodule simple de $A \otimes_k B$ est de la forme $A \otimes b$ pour un élément $b \in B$, puis que chaque sous-bimodule de $A \otimes_k B$ est de la forme $A \otimes I$ pour un sous-espace vectoriel I de B. L'assertion (ii) découle facilement de cela.

En particulier, le radical de Jacobson $J(A \otimes_k B)$ est de la forme $A \otimes_k I$, où I est un idéal bilatère de B. Comme $J(A \otimes_k B)$ est nilpotent, I est nilpotent, donc $I \subseteq J(B)$. Dans l'autre sens, $A \otimes_k J(B)$ est nilpotent, parce que $J(B)$ l'est, et donc $A \otimes_k J(B) \subseteq J(A \otimes_k B)$. Tout cela prouve (iii). □

3.3.1.3 Théorème. *Soit A une algèbre de dimension finie sur un corps k. Les neuf propriétés suivantes sont équivalentes.*

(i) L'algèbre A est séparable sur k.

(ii) Pour toute extension finie K de k, l'algèbre $A_{(K)}$ est semi-simple.

(iii) Il existe une extension algébriquement close Ω de k telle que $A_{(\Omega)}$ est semi-simple.

(iv) Le centre de A est une algèbre séparable sur k.

(v) Pour toute k-algèbre semi-simple B, l'algèbre $A \otimes_k B$ est semi-simple.

(vi) Pour toute k-algèbre B de dimension finie, $J(A \otimes_k B) = A \otimes_k J(B)$.

(vii) L'algèbre $A \otimes_k A^{\mathrm{op}}$ est semi-simple.

(viii) Le A-A-bimodule régulier ${}_A A_A$ est projectif.

(ix) Il existe un élément $\sum_{i\in I} a_i \otimes b_i \in A \otimes_k A$ *tel que* $\sum_{i\in I} a_i b_i = 1$ *et que pour tout* $c \in A$, *on ait*

$$\sum_{i\in I} ca_i \otimes b_i = \sum_{i\in I} a_i \otimes b_i c \quad \textit{dans } A \otimes_k A.$$

Preuve. Preuve de (iii) ⇒ (i).
Supposons (iii). Pour chaque extension K de k, il existe une extension L de k contenant à la fois K et Ω. (On peut construire un tel L en quotientant l'algèbre $K \otimes_k \Omega$ par un idéal maximal.) Comme $A_{(\Omega)}$ est semi-simple et scindée, c'est un produit d'algèbres de matrices à coefficients dans Ω, donc l'algèbre $\big(A_{(\Omega)}\big)_{(L)} = A_{(L)}$ est un produit d'algèbres de matrices à coefficients dans L, donc $A_{(L)}$ est semi-simple. Il s'ensuit que $\{0\}$ est le seul idéal nilpotent de $A_{(L)}$. Comme $J\big(A_{(K)}\big)_{(L)}$ est un idéal nilpotent de $A_{(L)}$, nous avons $J\big(A_{(K)}\big) = \{0\}$. Ainsi $A_{(K)}$ est semi-simple, et cela est vrai pour chaque extension K de k. Ainsi (i) est vraie.

Preuve de (i) ⇔ (iv).
Pour étudier la séparabilité sur k de A ou de son centre, nous pouvons procéder composante simple par composante simple. Sans nuire à la généralité, nous pouvons donc supposer que A est une k-algèbre simple. Son centre Z est alors une extension de k d'après l'exercice (1) du paragraphe 2.1.1.1 et A est une Z-algèbre simple centrale. Soit K une extension de k. Le lemme 3.3.1.2 montre que le radical de Jacobson de

$$A_{(K)} = K \otimes_k A \cong K \otimes_k Z \otimes_Z A \cong Z_{(K)} \otimes_Z A$$

est $J\big(Z_{(K)}\big) \otimes_Z A$. Ainsi $J\big(A_{(K)}\big)$ est réduit à $\{0\}$ si et seulement $J\big(Z_{(K)}\big)$ l'est. Les algèbres $A_{(K)}$ et $Z_{(K)}$ sont donc simultanément semi-simples ou non-semi-simples. Faisant varier K, nous obtenons l'équivalence (i) ⇔ (iv).

Preuve de (ii) ⇒ (v).
Soit B une k-algèbre semi-simple. Procédant composante simple par composante simple, nous pouvons supposer que B est une k-algèbre simple. Appelons Z son centre ; c'est une extension finie de k et B est une Z-algèbre simple centrale. Le lemme 3.3.1.2 montre que le radical de Jacobson de

$$A \otimes_k B \cong A \otimes_k Z \otimes_Z B = A_{(Z)} \otimes_Z B$$

est $J\big(A_{(Z)}\big) \otimes_Z B$. Sous l'hypothèse (ii), ce radical de Jacobson est réduit à $\{0\}$ et donc l'algèbre $A \otimes_k B$ est semi-simple.

Preuve de (v) ⇒ (vi).
Supposons (v). Soit B une k-algèbre de dimension finie. L'idéal $J(B)$ est nilpotent ; l'idéal bilatère $A \otimes_k J(B)$ de $A \otimes_k B$ est ainsi nilpotent, donc inclus dans $J(A \otimes_k B)$. Par ailleurs, l'algèbre $B/J(B)$ est semi-simple, donc l'algèbre quotient $A\otimes_k B/A\otimes_k J(B) \cong A\otimes_k \big(B/J(B)\big)$ est semi-simple. Son radical est donc réduit à $\{0\}$. L'exercice (7) du paragraphe 2.2.1 nous dit alors que $J(A \otimes_k B) = A \otimes_k J(B)$, ce qui est la conclusion désirée.

Preuve de (vii) ⇒ (viii).
Cette implication découle du fait que sur une algèbre semi-simple, tout suite exacte courte de modules est scindée, donc tout module est projectif.

Preuve de (viii) ⇒ (ix).
Regardons la structure de A-bimodule régulier sur A comme une structure de $A \otimes_k A^{\mathrm{op}}$-module à gauche. L'assertion (viii) signifie alors que ce module est projectif. L'application

$g : x \otimes y \mapsto xy$ de $A \otimes_k A^{\mathrm{op}}$ dans A étant un épimorphisme de $A \otimes_k A^{\mathrm{op}}$-module à gauche, il existe un homomorphisme $k : A \to A \otimes_k A^{\mathrm{op}}$ tel que $g \circ k = \mathrm{id}_A$. Écrivons $k(1)$ sous la forme $k(1) = \sum_{i\in I} a_i \otimes b_i$. Alors $\sum_{i\in I} a_i b_i = g(k(1)) = 1$, et pour chaque $c \in A$, l'égalité $(c \otimes 1)k(1) = k((c \otimes 1) \cdot 1) = k(c) = k((1 \otimes c) \cdot 1) = (1 \otimes c)k(1)$ fournit la relation

$$\sum_{i\in I} ca_i \otimes b_i = \sum_{i\in I} a_i \otimes b_i c \quad \text{dans } A \otimes_k A.$$

Preuve de (ix) ⇒ (i).
Nous montrons d'abord que si (ix) est vraie, alors A est semi-simple. Supposons (ix). Soit M un A-module et N un sous-module de M. Nous munissons $\mathrm{Hom}_k(M, N)$ de sa structure de A-A-bimodule : pour $f \in \mathrm{Hom}_k(M, N)$ et $(a, b) \in A^2$, l'application k-linéaire $afb : M \to N$ est $m \mapsto af(bm)$. Soit $\sum_{i\in I} a_i \otimes b_i$ l'élément dont (ix) affirme l'existence, soit L un sous-espace vectoriel de M supplémentaire de N, et soit $f \in \mathrm{Hom}_k(M, N)$ la projection de M sur N parallèlement à L. Alors $g = \sum_{i\in I} a_i f b_i$ appartient à $\mathrm{Hom}_A(M, N) \subseteq \mathrm{Hom}_k(M, N)$ et la restriction de g à N est l'identité de N. De là vient alors facilement que le A-module $\ker g$ est un supplémentaire de N dans M. Ainsi un sous-module d'un A-module admet toujours un supplémentaire ; en d'autres termes, tout A-module est complètement réductible. Cela signifie que A est semi-simple. Cet argument peut être repris pour chaque extension K de k : si A vérifie (ix), alors $A_{(K)}$ vérifie également (ix), donc $A_{(K)}$ est semi-simple. Nous avons prouvé l'implication (ix) ⇒ (i).

Les implications (i) ⇒ (ii), (i) ⇒ (iii), (vi) ⇒ (v) et (v) ⇒ (vii) découlent directement des définitions. □

3.3.1.4 Proposition. *Soit A une k-algèbre de dimension finie. On suppose que $A/J(A)$ est séparable sur k. Alors :*

(i) Pour toute k-algèbre B de dimension finie, $J(A \otimes_k B) = J(A) \otimes_k B + A \otimes_k J(B)$. En particulier, pour tout A-module complètement réductible M et tout B-module complètement réductible N, le $A \otimes_k B$-module $M \otimes_k N$ est complètement réductible.

(ii) Pour toute extension K de k, $J\big(A_{(K)}\big) = J(A)_{(K)}$. En particulier, pour tout A-module complètement réductible M, le $A_{(K)}$-module $M_{(K)}$ est complètement réductible.

Preuve. Soient A et B deux k-algèbres de dimension finie. L'idéal $J(A) \otimes_k B + A \otimes_k J(B)$ de $A \otimes_k B$ est nilpotent, donc est inclus dans le radical de Jacobson $J(A \otimes_k B)$. D'après l'exercice (7) du paragraphe 2.2.1, $J(A \otimes_k B)/\big(J(A) \otimes_k B + A \otimes_k J(B)\big)$ est le radical de Jacobson du quotient

$$(A \otimes_k B)/\big(J(A) \otimes_k B + A \otimes_k J(B)\big) \cong \big(A/J(A)\big) \otimes_k \big(B/J(B)\big).$$

Supposons que $A/J(A)$ soit séparable. D'après le théorème 3.3.1.3 (v), le membre de droite ci-dessus est semi-simple. On en déduit que $J(A \otimes_k B)/\big(J(A) \otimes_k B + A \otimes_k J(B)\big)$.

Maintenant, si M est un A-module complétement réductible et N est un B-module complètement réductible, alors $\mathrm{ann}\, M \supseteq J(A)$ et $\mathrm{ann}\, N \supseteq J(B)$, donc l'annulateur du $A \otimes_k B$-module $M \otimes_k N$ contient $J(A \otimes_k B)$. Cela entraîne que $M \otimes_k N$ est un $A \otimes_k B$-module complètement réductible. L'assertion (i) est entièrement prouvée.

La preuve de l'assertion (ii) suit les mêmes lignes que celle de l'assertion (i). Les détails sont laissés au lecteur, qui pourra d'ailleurs remarquer que quand K est une extension finie de k, (ii) est un cas particulier de (i). □

Exercices.

(1) Soit A une k-algèbre de dimension finie, et soit $\mathrm{tr}_{A/k} : A \to k$ l'application qui à $a \in A$ associe la trace de la multiplication à gauche par a dans A (autrement dit, $\mathrm{tr}_{A/k}$ est le caractère de la représentation régulière de A). Vérifier que la forme bilinéaire $T : (a, b) \mapsto \mathrm{tr}_{A/k}(ab)$ sur A est symétrique. Montrer que si T est non-dégénérée, alors A est une k-algèbre séparable. (Indication : si $a \in J(A)$, alors a est nilpotent, et il s'ensuit que $\mathrm{tr}_{A/k}(a) = 0$. En déduire que si $a \in J(A)$, alors $T(a, b) = 0$ pour chaque $b \in A$. Ainsi $J(A) = \{0\}$ dès que T est non-dégénérée. Le même raisonnement prouve la semi-simplicité de $A_{(K)}$ pour chaque extension K de k.)

(2) (Opérateur de Reynolds) Soit A une algèbre de dimension finie séparable sur k, et soit $\sum_{i\in I} a_i \otimes b_i$ un élément de $A \otimes_k A$ dont le théorème 3.3.1.3 (ix) assure l'existence. À un A-A-bimodule M, on associe son centre $Z^0(A, M) = \{m \in M \mid am = ma\}$. Montrer que l'application $\natural : m \mapsto m^\natural = \sum_{i\in I} a_i m b_i$ est une projection k-linéaire de M sur son centre. Vérifier que pour tout élément a du centre $Z(A)$ de A et tout $m \in M$, on a $(am)^\natural = am^\natural = m^\natural a = (ma)^\natural$. Vérifier enfin que chaque homomorphisme de A-A-bimodules $f : M \to N$ donne lieu à un diagramme commutatif

$$\begin{array}{ccc} M & \xrightarrow{\quad f \quad} & N \\ \downarrow{\scriptstyle \natural} & & \downarrow{\scriptstyle \natural} \\ Z^0(A, M) & \xrightarrow[f]{} & Z^0(A, N). \end{array}$$

(3) (Relations d'orthogonalité des caractères) Soit A une algèbre de dimension finie séparable sur k, et soit $\sum_{i\in I} a_i \otimes b_i$ un élément de $A \otimes_k A$ dont le théorème 3.3.1.3 (ix) assure l'existence. Soient M et N deux A-modules de dimension finie sur k. Montrer que

$$\dim_k \mathrm{Hom}_A(M, N) = \sum_{i\in I} \chi_N(a_i)\chi_M(b_i).$$

(Indication : on munit $\mathrm{Hom}_k(M, N)$ de la structure de A-A-bimodule donnée par $afb = (m \mapsto af(bm))$, pour $f \in \mathrm{Hom}_k(M, N)$, $(a, b) \in A^2$ et $m \in M$. L'application linéaire $\natural : f \mapsto \sum_{i\in I} a_i f b_i$ de $\mathrm{Hom}_k(M, N)$ dans lui-même est un projecteur sur le sous-espace vectoriel $\mathrm{Hom}_A(M, N)$. La dimension de ce dernier est donc égale à la trace de $\natural$.)

3.3.2 Cohomologie de Hochschild

Ce bref paragraphe n'a d'autre but que de préparer le terrrain pour la preuve du théorème principal de Wedderburn, qui sera donnée au paragraphe suivant. Hormis la dernière proposition, il n'est en rien spécifique des algèbres séparables. On se fixe un corps k et une k-algèbre A pour tout ce paragraphe.

Soit A une k-algèbre et M un A-A-bimodule. Pour un entier $n \geq 1$, on note $C^n(A, M)$ le k-espace vectoriel des applications multilinéaires de A^n dans M. Un élément de $C^n(A, M)$ peut aussi être vu comme une application k-linéaire de la puissance tensorielle n-ième $A^{\otimes n}$ dans M, où la puissance tensorielle $A^{\otimes n}$ est le produit $A \otimes_k \cdots \otimes_k A$ de n facteurs. Pour $n = 0$, on pose $C^0(A, M) = \mathrm{Hom}_k(k, M) \cong M$. Les éléments de $C^n(A, M)$ sont appelés n-cochaînes de Hochschild.

À $f \in C^n(A, M)$, on associe $df \in C^{n+1}(A, M)$ de la façon suivante :

$$\begin{aligned} df(a_1, \ldots, a_{n+1}) = a_1 f(a_2, \ldots, a_{n+1}) & \\ + \sum_{i=1}^{n} (-1)^i f(a_1, \ldots, a_{i-1}, a_i a_{i+1}, a_{i+2}, \ldots, a_{n+1}) & \\ + (-1)^{n+1} f(a_1, \ldots, a_n) a_{n+1}. & \end{aligned}$$

On définit ainsi une application k-linéaire $d : C^n(A, M) \to C^{n+1}(A, M)$, appelée différentielle de Hochschild. Un calcul rapide montre que la composée $d \circ d$ de $C^{n-1}(A, M)$ dans $C^{n+1}(A, M)$ est nulle. La suite

$$0 \to C^0(A, M) \to \cdots \to C^n(A, M) \xrightarrow{d} C^{n+1}(A, M) \to \cdots$$

s'appelle le complexe de Hochschild.

On note $Z^n(A, M)$ le noyau de $d : C^n(A, M) \to C^{n+1}(A, M)$; les éléments de $Z^n(A, M)$ sont appelés les n-cocycles de Hochschild. On note $B^n(A, M)$ l'image de $d : C^{n-1}(A, M) \to C^n(A, M)$; les éléments de $B^n(A, M)$ sont appelés les n-cobords de Hochschild. L'égalité $d \circ d = 0$ entraîne l'inclusion $B^n(A, M) \subseteq Z^n(A, M)$. On peut donc poser $HH^n(A, M) = Z^n(A, M)/B^n(A, M)$, qu'on appelle n-ième groupe de cohomologie de Hochschild de A à coefficients dans M. Ces groupes mesurent le défaut d'exactitude du complexe de Hochschild.

Regardons à présent quelques exemples.

Cas $n = 0$. Un élément de $C^0(A, M)$ est une application k-linéaire de k dans M, autrement dit un élément $m \in M$. Sa différentielle est l'application $a \mapsto am - ma$. Ainsi $Z^0(A, M) = \{m \in M \mid \forall a \in A,\ am = ma\}$ est ce qu'on appelle le centre du A-A-bimodule M. On convient de poser $B^0(A, M) = 0$, de sorte que $HH^0(A, M) = Z^0(A, M)$.

Cas $n = 1$. Un élément de $Z^1(A, M)$ est appelé dérivation de A à valeurs dans M. C'est une application k-linéaire $f : A \to M$ vérifiant $f(ab) = af(b) + f(a)b$ pour tout $(a, b) \in A^2$. Un élément de $B^1(A, M)$ est appelé dérivation intérieure : c'est une dérivation f pour laquelle existe un élément $m \in M$ tel que $f(a) = ma - am$ pour tout $a \in A$. Le quotient $HH^1(A, M)$ est parfois appelé groupe des dérivations extérieures de A à valeurs dans M.

Cas $n = 2$. Un élément de $Z^2(A, M)$ est appelé ensemble de facteurs (faute d'une meilleure traduction de l'anglais *factor set*). C'est une application bilinéaire $f : A \times A \to M$ vérifiant $af(b, c) - f(ab, c) + f(a, bc) - f(a, b)c = 0$ pour tout $(a, b, c) \in A^3$. Un élément de $B^2(A, M)$ est appelé ensemble scindé de facteurs (*split factor set* en anglais) : c'est un ensemble de facteurs tel qu'il existe une application k-linéaire $F : A \to M$ telle que $f(a, b) = aF(b) - F(ab) + F(a)b$ pour tout $(a, b) \in A^2$.

Remarque. Ces définitions peuvent en fait s'inscrire dans un cadre plus général. Notons $A^e = A \otimes_k A^{\mathrm{op}}$ l'algèbre enveloppante de A ; elle est définie de sorte que les A^e-modules soient exactement les A-A-bimodules. Ainsi A et M sont des A^e-modules.

Posons $C_n^{\mathrm{bar}}(A) = A^{\otimes n+2}$. Les éléments de $C_n^{\mathrm{bar}}(A)$ sont combinaisons linéaires d'éléments de la forme $a_0 \otimes a_1 \otimes \cdots \otimes a_n \otimes a_{n+1}$; on convient de simplifier la notation en écrivant plutôt $a_0 [\, a_1 \mid \cdots \mid a_n \,] a_{n+1}$ pour ce dernier. On munit $C_n^{\mathrm{bar}}(A)$ d'une structure de A-A-bimodule en faisant agir A par multiplication à gauche sur le premier facteur et par multiplication à droite sur le dernier facteur. La suite

$$\cdots \to C_{n+1}^{\mathrm{bar}}(A) \xrightarrow{\delta} C_n^{\mathrm{bar}}(A) \to \cdots \to C_0^{\mathrm{bar}}(A) \xrightarrow{m} A \to 0,$$

où m est induite par la multiplication dans A (c'est-à-dire $m(a \otimes b) = ab$) et où

$$\begin{aligned}\delta\big(a_0 [\, a_1 \mid \cdots \mid a_{n+1} \,] a_{n+2}\big) = {} & (a_0 a_1) [\, a_2 \mid \cdots \mid a_{n+1} \,] a_{n+2} \\ & + \sum_{i=1}^{n} (-1)^i a_0 [\, a_1 \mid \cdots \mid a_{i-1} \mid a_i a_{i+1} \mid a_{i+2} \mid \cdots \mid a_{n+1} \,] a_{n+2} \\ & + (-1)^{n+1} a_0 [\, a_1 \mid \cdots \mid a_n \,] (a_{n+1} a_{n+2}),\end{aligned}$$

est alors une suite exacte de A-A-bimodules. De plus, chaque $C_n^{\mathrm{bar}}(A)$ est un A^e-module libre. On dit que $C_\bullet^{\mathrm{bar}}(A)$ est la résolution bar de A.

Le complexe de Hochschild s'obtient alors en prenant l'image par le foncteur $\mathrm{Hom}_{A^e}(?, M)$ de cette résolution bar. Les méthodes de l'algèbre homologique nous assurent alors de l'existence d'un isomorphisme canonique $HH^n(A, M) \cong \mathrm{Ext}^n_{A^e}(A, M)$.

3.3.2.1 Lemme. *Soit $0 \to L \xrightarrow{u} M \xrightarrow{v} N \to 0$ une suite exacte courte de A-modules. On munit $T = \mathrm{Hom}_k(N, L)$ de sa structure de A-A-bimodule naturelle : pour $g \in T$ et $(a, b) \in A^2$, l'application linéaire $agb : N \to L$ est $n \mapsto ag(bn)$. Soit $s : N \to M$ une application k-linéaire telle que $v \circ s = \mathrm{id}_N$. Pour $a \in A$, l'homomorphisme de k-modules $n \mapsto as(n) - s(an)$ de N dans M est à valeurs dans $\mathrm{im}\, u$, donc s'écrit $u \circ (f(a))$, avec $f(a) \in \mathrm{Hom}_k(N, L)$ uniquement déterminé. Nous définissons ainsi une application $f : A \to T$.*

(i) L'application f est une dérivation de A à valeurs dans T, autrement dit un 1-cocyle de Hochschild appartenant à $Z^1(A, T)$.

(ii) La classe de cohomologie $[f] \in HH^1(A, T)$ ne dépend que de la suite exacte, et pas du choix de s.

(iii) La suite exacte est scindée si et seulement si f est une dérivation intérieure, autrement dit si et seulement si $[f] = 0$ dans $HH^1(A, T)$.

Preuve. Soit $(a, b) \in A^2$. Alors $u \circ (f(ab))$ est l'application $n \mapsto abs(n) - s(abn)$ de N dans M, $u \circ (f(a)b)$ est l'application $n \mapsto as(bn) - s(abn)$, et la A-linéarité de u montre que $u \circ (af(b))$ est l'application $n \mapsto a(u \circ f(b))(n) = a(bs(n) - s(bn))$. Cela prouve (i).

Soit $t \in \mathrm{Hom}_k(N, L)$. Les définitions montrent que quand on remplace s par $s + u \circ t$, la dérivation f est changée en $f + dt$. La classe de cohomologie $[f] \in HH^1(A, T)$ ne change donc pas dans cette transformation. L'assertion (ii) découle ainsi du fait que toute section k-linéaire de v s'écrit sous cette forme $s + u \circ t$.

Si la suite exacte courte est scindée, alors on peut choisir une section A-linéaire s, et la dérivation associée est $f = 0$. Dans l'autre sens, supposons que $[f] = 0$. Alors f s'écrit dt pour un élément $t \in T$. Le remplacement de s par $s - u \circ t$ fait que f est changée en $f - dt = 0$. Cela signifie que $s - u \circ t$ est A-linéaire. Ainsi $s - u \circ t : N \to M$ est un homomorphisme de A-modules tel que $v \circ (s - u \circ t) = v \circ s = \mathrm{id}_N$, ce qui montre que la suite exacte courte est scindée. Nous avons montré (iii). □

3.3.2.2 Lemme. *Soit E une k-algèbre et $v : E \to A$ un homomorphisme surjectif de k-algèbres. Le noyau N de v est un idéal de E. On suppose que le produit de deux éléments quelconques de N est nul. Soit u l'injection de N dans E, de façon à avoir une suite exacte courte de k-espaces vectoriels $0 \to N \xrightarrow{u} E \xrightarrow{v} A \to 0$. On munit N d'une structure de A-A-bimodule en décrétant que pour chaque $(a, n) \in A \times N$, l'action à gauche (respectivement, à droite) de a sur n soit le produit $\tilde{a}n$ (respectivement, $n\tilde{a}$), pour tout $\tilde{a} \in v^{-1}(a)$. (L'hypothèse $N^2 = 0$ fait que le résultat ne dépend pas du choix de $\tilde{a}$.) Soit $s : A \to E$ une application k-linéaire telle que $v \circ s = \mathrm{id}_A$. Pour $(a, b) \in A^2$, l'élément $s(ab) - s(a)s(b)$ de E appartient à $\ker v = \mathrm{im}\, u$, donc s'écrit $u(f(a, b))$. On définit ainsi une application $f : A \times A \to N$.*

(i) L'application f est un ensemble de facteurs, autrement dit un 2-cocyle de Hochschild appartenant à $Z^2(A, N)$.

(ii) La classe de cohomologie $[f] \in HH^2(A, N)$ ne dépend que de v, et pas du choix de s.

(iii) La classe de cohomologie $[f]$ est nulle si et seulement s'il est possible de trouver s qui soit un homomorphisme d'algèbres.

Preuve. La preuve, semblable en tout point à celle du lemme précédent, est laissée au lecteur. La seule petite difficulté supplémentaire est dans la preuve de (iii) : il faut montrer que si $f = 0$, alors s est un homomorphisme d'algèbres. Il est manifeste qu'alors s préserve le produit, mais il faut aussi montrer que s préserve l'élément neutre.

Pour chaque $a \in A$, l'égalité $f(1, a) = 0$ signifie que $s(1)s(a) = s(a)$. De plus, $s(1) - 1$ appartient au noyau de v (car v est un homomorphisme d'algèbres), donc appartient à N. Il s'ensuit que pour chaque $n \in N$, on a $(s(1) - 1)n = 0$. L'ensemble des éléments $x \in E$ tels que $s(1)x = x$ contient donc $s(A)$ et N ; c'est donc E tout entier, et en substituant $x = 1$, nous obtenons $s(1) = 1$. □

3.3.2.3 Théorème. *Soit A une algèbre de dimension finie séparable sur k. Alors pour tout A-bimodule M, on a $HH^n(A,M)=0$ en tout degré $n>0$.*

Preuve. Prenons A, M, n comme dans l'énoncé. Soit $\sum_{i\in I} a_i\otimes b_i$ un élément de $A\otimes_k A^{\mathrm{op}}$ vérifiant les propriétés énoncées dans le théorème 3.3.1.3 (ix). Soit $f:A^n\to M$ un n-cocycle de Hochschild. Définissons une $n-1$-cochaîne de Hochschild $g:A^{n-1}\to M$ par

$$g(c_1,\dots,c_{n-1})=\sum_{i\in I} a_i f(b_i,c_1,\dots,c_{n-1}).$$

Prenons $(c_1,\dots,c_n)\in A^n$. Un calcul direct et facile basé sur les définitions et utilisant les égalités $df(b_i,c_1,\dots,c_n)=0$, $\sum_{i\in I} c_1a_i\otimes b_i=\sum_{i\in I} a_i\otimes b_ic_1$ et $\sum_{i\in I} a_ib_i=1$ donne $f=dg$. Le cocycle f est donc un cobord. □

Exercice. Soit A une k-algèbre de dimension finie. Montrer que si $HH^1(A,M)=0$ pour tout A-A-bimodule M, alors A est séparable sur k.

3.3.3 Théorème de Wedderburn-Malcev

3.3.3.1 Théorème (Wedderburn, Malcev). *Soit B une algèbre de dimension finie sur un corps k. On note N le radical de Jacobson de B et on suppose que $A=B/N$ est séparable sur k.*

(i) Il existe une sous-algèbre semi-simple S de B telle que $B=S\oplus N$.

(ii) Si S et S' sont deux sous-algèbres de B telles que $B=S\oplus N=S'\oplus N$, alors il existe $n\in N$ tel que $S'=(1-n)S(1-n)^{-1}$.

Preuve. (i) L'assertion est vraie quand la dimension de B est 1, puisqu'alors $B=k$ et $N=\{0\}$. Nous pouvons donc procéder par récurrence sur la dimension de B et supposer que (i) vaut pour toutes les algèbres de dimension plus petite que celle de B. Le lemme 3.3.2.2 et le théorème 3.3.2.3 montrent que l'assertion (i) est vraie quand $N^2=\{0\}$. Nous nous plaçons donc dans le cas restant $N^2\neq\{0\}$. D'après l'exercice (7) du paragraphe 2.2.1, le radical de $\overline{B}=B/N^2$ est $\overline{N}=N/N^2$. Le quotient $\overline{B}/\overline{N}$ est séparable, donc par hypothèse de récurrence, on peut trouver une sous-algèbre semi-simple $\overline{S}$ dans $\overline{B}$ telle que $\overline{B}=\overline{S}\oplus\overline{N}$. L'image réciproque de $\overline{S}$ dans B est une sous-algèbre S_1 telle que $B=S_1+N$ et $S_1\cap N=N^2$. L'idéal N^2 étant nilpotent, il est inclus dans le radical de Jacobson de S_1. De plus, $S_1/N^2\cong A$ est semi-simple, et l'exercice (7) du paragraphe 2.2.1 à nouveau nous dit que N^2 est le radical de Jacobson de S_1. Nous pouvons alors appliquer notre hypothèse de récurrence à S_1, en notant que $B\neq S_1$ puisque $N\neq N^2$. On peut donc trouver une sous-algèbre S de S_1 telle que $S_1=S\oplus N^2$. On a alors $B=S\oplus N$, ce qui termine la preuve de (i).

(ii) Soit $\varphi:B\to A$ l'application de passage au quotient. La donnée des sous-algèbres S et S' équivaut à celle d'homomorphismes d'algèbres ψ de ψ' de A dans B telles que $\varphi\circ\psi=\varphi\circ\psi'=\mathrm{id}_A$. Munissons N d'une structure de A-A-bimodule en posant $an=\psi'(a)n$ et $na=n\psi(a)$ pour $(a,n)\in A\times N$. La fonction $f:a\mapsto\psi(a)-\psi'(a)$ est alors une dérivation de A à valeurs dans N. Le théorème 3.3.2.3 dit que cette dérivation est intérieure : il existe $n\in N$ tel que $f(a)=n\psi(a)-\psi'(a)n$ pour chaque $a\in A$. Ainsi $\psi'(a)=(1-n)\psi(a)(1-n)^{-1}$, d'où $S'=(1-n)S(1-n)^{-1}$. □

Exemple. Soient V un k-espace vectoriel de dimension finie, u un endomorphisme de V, et μ le polynôme minimal de u. La sous-algèbre B de $\mathrm{End}_k(V)$ engendrée par u est isomorphe à $k[X]/(\mu)$. On suppose que chaque diviseur irréductible unitaire de μ est séparable sur k (c'est-à-dire, à racines simples). Notant ν le produit des diviseurs irréductibles distincts de μ, nous savons que le radical de Jacobson de $k[X]/(\mu)$ est $(\nu)/(\mu)$ (exercice (7) du paragraphe 2.2.2). Notons N le radical de Jacobson de B ; d'après l'exercice (6) du paragraphe 2.2.2, N est l'ensemble des éléments nilpotents de B. L'algèbre $A = B/N$ est isomorphe à $k[X]/(\nu)$, donc est un produit d'extensions séparables de k, donc est une k-algèbre séparable. Nous pouvons donc appliquer le théorème de Wedderburn-Malcev : il existe une unique sous-algèbre S de B telle que $B = S \oplus N$. Manifestement $S \cong k[X]/(\nu)$; chaque élément de S est ainsi annulé par le polynôme ν, donc est semi-simple (exercice (3) du paragraphe 1.3.1).

Décomposons $u \in B$ selon la somme directe $S \oplus N$ en $u = s+n$. Alors s et n sont des polynômes en u, donc commutent. De plus, n est nilpotent car $n \in N$, et s est semi-simple car $s \in S$. Nous montrons ainsi l'existence d'une décomposition de Jordan-Dunford de u. Examinons à présent l'unicité. On part d'une décomposition $u = s + n$, avec s semi-simple, n nilpotent, et s et n des polynômes en u (cette hypothèse affaiblit notre résultat d'unicité en comparaison de l'énoncé habituel du théorème de Jordan-Dunford). Alors $n \in N$ et $B = k[s] + N$, car pour tout polynôme $P \in k[X]$, on a $P(u) \equiv P(s) \bmod (n)$. Par ailleurs, $k[s]$ est une algèbre semi-simple et commutative ; elle n'a donc pas d'élément nilpotent, d'où $k[s] \cap N = \{0\}$. Ainsi $B = k[s] \oplus N$ est la décomposition de Wedderburn-Malcev de B. Cela montre que $S = k[s]$, et par suite notre écriture $u = s + n$ était celle qu'on obtenait en décomposant u selon la somme directe $B = S \oplus N$.

Remarque. L'existence de la décomposition de Jordan-Dunford est généralement prouvée par des méthodes de décomposition spectrale. Néanmoins, il existe également une démonstration basée sur un principe itératif semblable à la preuve du lemme de Hensel (autrement dit, à la méthode de Newton de résolution des équations, mais dans un cadre ultramétrique). Cette démonstration est en fait celle donnée ci-dessus, à cette différence non-négligeable près qu'on fait abstraction de tout le matériel nécessaire au cadre non-commutatif. Du reste, en y regardant de plus près, on constate que la preuve du théorème principal de Wedderburn que nous avons présentée procède elle aussi par approximations successives : le cas général $N^k = \{0\}$ où $k > 2$ est ramené au cas $N^2 = \{0\}$. Les moyens sophistiqués développés aux paragraphes 3.3.1 et 3.3.2 sont destinés à traiter ce dernier cas.

3.3.4 Le théorème de réciprocité de Brauer

3.3.4.1 Théorème. *Soient A et B deux algèbres de dimension finie sur un corps k, et soit M un A-B-bimodule de dimension finie sur k. On suppose que les images de A et B dans $\mathrm{End}_k(M)$ sont les commutants l'une de l'autre. On suppose l'existence d'une sous-algèbre A' de A telle que $A = A' \oplus J(A)$.*

(i) Pour chaque A-module simple S, le B-module $T = \mathrm{Hom}_{A'}(S, M)$ est soit nul, soit indécomposable.

(ii) L'application $S \mapsto T$ est une bijection entre l'ensemble des classes d'isomorphismes de A-modules simples apparaissant comme sous-quotients de M et l'ensemble des classes d'isomorphisme de B-modules indécomposables apparaissant comme facteurs directs de M.

(iii) Soient S un A-module simple, $\Delta = \mathrm{End}_A(S)^{\mathrm{op}}$, $T = \mathrm{Hom}_{A'}(S, M)$. La multiplicité de Jordan-Hölder du A-module S dans M est égale à $\dim_\Delta T = \dim_k T / \dim_k \Delta$. La multiplicité (de Krull-Schmidt) avec laquelle T apparaît dans les décompositions de M en somme directe de B-modules indécomposables est égale à $\dim_\Delta S = \dim_k S / \dim_k \Delta$.

Preuve. Le A'-module M est complètement réductible, car $A' \cong A/J(A)$ est semi-simple. Posons $B' = \mathrm{End}_{A'}(M)^{\mathrm{op}}$; alors $B' \supseteq \mathrm{End}_A(M) = B$. Nous pouvons écrire M comme somme de ses composantes A'-isotypiques. D'après le paragraphe 1.4.5, cela donne l'isomorphisme de A'-B'-bimodules $M \cong \bigoplus_{(S)\in\mathscr{S}} \big(S \otimes_\Delta T\big)$. Cette somme porte sur l'ensemble des classes d'isomorphisme de A'-modules simples S apparaissant comme sous-quotients de M ; $\Delta = \mathrm{End}_{A'}(S)$ est un anneau à division ; $T = \mathrm{Hom}_{A'}(S, M)$ est un B'-module simple ; enfin les B'-modules T correspondant à deux A'-modules S non-isomorphes sont non-isomorphes. En choisissant une base du Δ-module S, lequel est nécessairement libre (Proposition 1.3.1.3), on met en évidence que T est un facteur direct du B'-module M, de multiplicité $\dim_\Delta S$. De même, on voit que la multiplicité de S dans le A'-module M est égale à $\dim_\Delta T$.

Soit $0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_{\ell-1} \subseteq M_\ell = M$ une série de composition du A-module M. Les sous-quotients sont des A-modules simples. Étant annulés par $J(A)$, ces sous-quotients sont aussi simples sur l'anneau A'. Ainsi notre série de composition est également une série de composition de A'-modules. Cela entraîne que la multiplicité de Jordan-Hölder d'un module simple S dans M ne varie pas, qu'on regarde S et M comme des modules sur A ou sur A'.

À ce stade, il nous reste à montrer que les B'-modules simples T sont indécomposables et deux-à-deux non-isomorphes quand on les regarde comme des B-modules. Reprenons notre série de composition. Pour chaque $n \in \{1, \ldots, \ell\}$, nous pouvons trouver un sous-A'-module N_n supplémentaire de M_{n-1} dans M_n. Alors $M = N_1 \oplus \cdots \oplus N_\ell$ en tant que A'-module.

Fixons-nous un A-module simple S apparaissant dans M. Posons $\Delta = \mathrm{End}_A(S)^{\mathrm{op}}$ et $T = \mathrm{End}_{A'}(S, M)$. Soit $\varphi \in \mathrm{End}_B(T)$. Prenons une base $(e_1, \ldots, e_m)$ du Δ-module à droite S et écrivons la composante S-isotypique du A'-module M sous la forme $S \otimes_\Delta T = \bigoplus_{i=1}^m e_i \otimes T$. Définissons $\tilde{\varphi} \in \mathrm{End}_B(M)$ en demandant que $\tilde{\varphi}(e_i \otimes t) = e_i \otimes \varphi(t)$ pour chaque $t \in T$ et que $\tilde{\varphi}$ soit nulle sur les autres composantes isotypiques de ${}_{A'}M$. Par hypothèse, $\tilde{\varphi}$ est l'image dans $\mathrm{End}_k(M)$ d'un élément de A, élément que nous écrivons $a' + u$, avec $a' \in A'$ et $u \in J(A)$.

Supposons qu'il existe $i \in \{1, \ldots, m\}$ tel que $a'e_i = 0$. Pour chaque $t \in T$, on a alors

$$e_i \otimes \varphi(t) = \tilde{\varphi}(e_i \otimes t) = (a' + u)(e_i \otimes t) = u(e_i \otimes t).$$

On en déduit que $e_i \otimes \varphi^k(t) = u^k(e_i \otimes t)$. Comme u est nilpotent, il existe un k, qui ne dépend pas de t, tel que e_i appartienne au noyau de $\varphi^k(t)$. Comme S est un A'-module simple, cela signifie que $\varphi^k(t) = 0$. Ceci étant vrai pour chaque $t \in T$, φ est nilpotent.

Supposons au contraire que $a'e_i$ n'est nul pour aucun indice i. Définissons alors une matrice $(\alpha_{ij})_{1\le i,j\le m}$ d'éléments de Δ de sorte que $a'e_i = \sum_{j=1}^m e_j\alpha_{ji}$ pour chaque i. Appelons N_{p_1}, ..., N_{p_r} ceux des sous-modules N_n qui sont isomorphes à S et choisissons des isomorphismes

de A'-module $f_1 : S \to N_{p_1}$, ..., $f_r : S \to N_{p_r}$. Alors $(f_1, \ldots, f_r)$ est une base du Δ-module T. Définissons alors une matrice $(\phi_{kl})_{1\leq k,l\leq r}$ d'éléments de Δ par $\varphi(f_k) = \sum_{l=1}^{r} \phi_{kl} f_l$. Pour chaque $i \in \{1, \ldots, m\}$ et chaque $k \in \{1, \ldots, r\}$, l'élément

$$\sum_{l=1}^{r} e_i \otimes \phi_{kl} f_l - \sum_{j=1}^{m} e_j \alpha_{ji} \otimes f_k = \tilde{\varphi}(e_i \otimes f_k) - a'(e_i \otimes f_k) = u(e_i \otimes f_k)$$

appartient à

$$\big(S \otimes_\Delta T\big) \cap u\big(M_{p_k}\big) = \big(S \otimes_\Delta T\big) \cap M_{p_k - 1} = \bigoplus_{l<k} S \otimes f_l.$$

On en déduit que $e_i \phi_{kl} = 0$ si $l > k$, et que $e_i \phi_{kk} = \sum_{j=1}^{m} e_j \alpha_{ji}$. Ceci devant être valable pour chaque i et chaque k, nous en déduisons que $\phi_{kl} = 0$ si $l > k$, que $\alpha_{ji} = 0$ si $i \neq j$, et que les α_{ii} et les ϕ_{kk} sont tous égaux. Nous voyons ainsi qu'il existe $\alpha \in \Delta^\times$ tel que $\varphi(f_k) - \alpha f_k \in \sum_{l<k} \Delta f_l$ pour chaque $k \in \{1, \ldots, r\}$. Cette conclusion n'est en rien liée au choix de $(f_1, \ldots, f_r)$ auquel nous avons procédé ; on peut y remplacer f_k par $\lambda_k f_k$ chaque fois que c'est utile, pour n'importe quel $\lambda_k \in \Delta^\times$, sans que la valeur de α soit altérée. Il est alors aisé de voir que φ est bijective. (La dernière observation est nécessaire pour s'accomoder de ce que φ n'est pas Δ-linéaire.)

Les deux étapes précédentes montrent qu'un élément φ de $\mathrm{End}_B(M)$ est toujours nilpotent ou inversible, d'où l'indécomposabilité du B-module M.

Supposons enfin qu'on puisse trouver deux A-modules simples S et S' non-isomorphes pour lesquels existe un isomorphisme de B-modules φ entre $T = \mathrm{Hom}_{A'}(S, M)$ et $T' = \mathrm{Hom}_{A'}(S', M)$. Parmi les modules N_n de notre suite de composition, énumérons (dans l'ordre croissant des indices) les modules N_{p_1}, ..., N_{p_r} isomorphes à S et les modules N_{q_1}, ..., N_{q_s} isomorphes à S'. Quitte à échanger les rôles de S et S', nous pouvons supposer que $p_1 < q_1$. Posons $\Delta = \mathrm{End}_A(S)^{\mathrm{op}}$, $T = \mathrm{Hom}_{A'}(S, M)$, $\Delta' = \mathrm{End}_A(S')^{\mathrm{op}}$ et $T' = \mathrm{Hom}_{A'}(S', M)$. Choisissons une base $(e_1, \ldots, e_m)$ du Δ-module à droite S et un élément non-nul $e' \in S'$. La composante S-isotypique du A'-module M s'écrit sous la forme $S \otimes_\Delta T = \bigoplus_{i=1}^{m} e_i \otimes T$; la composante S'-isotypique de M est $S' \otimes_{\Delta'} T'$. Définissons $\tilde{\varphi} \in \mathrm{End}_B(M)$ en demandant que $\tilde{\varphi}(e_1 \otimes t) = e' \otimes \varphi(t)$ pour chaque $t \in T$, que $\varphi(e_i \otimes t) = 0$ si $i > 1$, et que φ soit nulle sur les composantes isotypiques de ${}_{A'}M$ autres que $S \otimes_\Delta T$. Par hypothèse, φ est donnée par l'action sur M d'un élément a de A. Soit $f : S \to N_{p_1}$ un isomorphisme de A'-modules. Alors

$$e' \otimes \varphi(f) = \tilde{\varphi}(e_1 \otimes f) = a(e_1 \otimes f) \in M_{p_1}.$$

Cependant le membre de gauche appartient à la composante S'-isotypique du A'-module M, laquelle est $N_{q_1} \oplus \cdots \oplus N_{q_s}$. De l'inégalité $p_1 < q_1$ vient alors que $e' \otimes \varphi(f) = 0$. Ainsi e' appartient au noyau de $\varphi(f) \in T'$. Ce noyau est ainsi un sous-A'-module non-nul de S', donc est S' tout entier, d'où $\varphi(f) = 0$, ce qui contredit l'injectivité de φ. Bref notre hypothèse de départ était absurde : deux B-modules indécomposables T et T' correspondant à deux A-modules simples S et S' non isomorphes ne peuvent être isomorphes. □

Remarque. L'hypothèse du théorème sur l'existence d'une décomposition $A = A' \oplus J(A)$ est satisfaite dès que $A/J(A)$ est une algèbre séparable, d'après le théorème de Wedderburn-Malcev. Dans ce cas, on a en plus unicité de A' à conjugaison près : pour toute autre décomposition $A = A'' \oplus J(A)$, il existe $n \in J(A)$ tel que $A'' = (1-n)A'(1-n)^{-1}$. Alors pour chaque

A-module S, les B-modules indécomposables $\mathrm{Hom}_{A'}(S, M)$ et $\mathrm{Hom}_{A''}(S, M)$ sont isomorphes ; en utilisant que $J(A)$ annule S, on vérifie en effet sans peine qu'une application $f : S \to M$ est A'-linéaire si et seulement si l'application $g : S \to M$ définie par $g(s) = (1 - n)f(s)$ est A''-linéaire. Ainsi la correspondance bijective mise en place dans l'assertion (ii) du théorème 3.3.4.1 est indépendante du choix de A'.

Cette hypothèse que $A/J(A)$ est séparable est automatiquement satisfaite quand k est un corps algébriquement clos. C'est dans ce cas particulier que se place en fait Brauer ; sa preuve (paragraphe II de [4]) ne fait même pas appel au théorème de Wedderburn-Malcev.

4 Représentations des groupes

Introduction

Le père fondateur de la théorie des représentations est Ferdinand Georg Frobenius (1849–1917). Le problème qui a initié ses recherches était le calcul du *Gruppendeterminant*. Partant d'un groupe fini G, on introduit une famille d'indéterminées $(X_g)_{g\in G}$. On regarde la matrice $(X_{gh})_{(g,h)\in G^2}$, dont les coefficients sont des indéterminées, et on cherche à calculer son déterminant, qui est un polynôme homogène de degré égal à l'ordre de G. Le cas où G est un groupe abélien avait été traité par Dedekind pour des travaux sur les bases normales des extensions galoisiennes : sur $\mathbf{C}$, le polynôme se factorise en produit de facteurs de degré 1. Dedekind avait signalé à Frobenius que le cas général était une question ouverte. Frobenius a prouvé que le *Gruppendeterminant* avait s facteurs irréductibles distincts, où s est le nombre de classes de conjugaison de G, que chaque facteur irréductible apparaissait avec une multiplicité égale à son degré, et que les degrés des facteurs irréductibles divisaient l'ordre de G.

Une représentation linéaire d'un groupe G est un homomorphisme de G dans un groupe de matrices $\mathbf{GL}_n(k)$. Le but est d'utiliser les outils du calcul matriciel pour pouvoir ensuite dire des choses sur G. Une autre façon de dire cela est d'avoir la prétention de penser connaître suffisamment bien le groupe concret $\mathbf{GL}_n(k)$ pour en tirer des informations sur tous les autres groupes. On peut justifier cette approche à travers deux résultats dûs à Schur, et dont on pourra trouver une preuve dans le chapitre 36 de [6] :

— Soit G un sous-groupe de $\mathbf{GL}_n(\mathbf{C})$. On suppose que G est engendré par un nombre fini d'éléments et que tout élement de G est d'ordre fini. Alors G est fini.
— Soit G un sous-groupe de $\mathbf{GL}_n(\mathbf{C})$. On suppose que tout élement de G est d'ordre fini. Alors G possède un sous-groupe abélien distingué d'indice au plus

$$(\sqrt{8n}+1)^{2n^2} - (\sqrt{8n}-1)^{2n^2}.$$

Un autre point de vue est le suivant. Un groupe n'existe qu'à travers ses actions. Vu que l'algèbre linéaire est un pilier de notre culture mathématique, il est naturel d'étudier les actions d'un groupe sur un espace vectoriel. Des applications apparaissent alors, tant en géométrie élémentaire (l'existence de l'icosaèdre reflète l'existence d'une représentation réelle de dimension 3 du groupe alterné $\mathfrak{A}_5$) qu'en analyse (la théorie des séries de Fourier permet d'écrire une fonction sur $\mathbf{U}(1)$ comme combinaison linéaire de caractères du groupe $\mathbf{U}(1)$).

Enfin, la théorie a aussi des applications dans le grand monde, puisque ce dernier est écrit en caractères mathématiques. Par exemple, le formalisme de la mécanique quantique est basé sur les espaces de Hilbert. Toute symétrie d'un système physique provient donc d'une action d'un groupe sur un espace de Hilbert. Ainsi le spin des particules élémentaires, si important pour la résonance magnétique nucléaire par exemple, provient d'une représentation de $\mathbf{SU}(2)$ sur l'espace des états internes de la particule.

4.1 Définition, premiers exemples et constructions

Bien qu'il soit parfois utile d'examiner des représentations de groupes sur des anneaux commutatifs quelconques, **nous conviendrons dans tout ce chapitre que k est un corps.**

4.1.1 k-algèbre d'un groupe

Représentation matricielle d'un groupe : soient G un groupe et k un corps. Une représentation matricielle de G sur k est un homomorphisme de groupes de G dans un groupe linéaire $\mathbf{GL}_n(k)$. Ici n est un entier strictement positif, appelé degré de la représentation.

Une variante sans coordonnée de cette définition est la suivante. Une représentation k-linéaire d'un groupe G est une action de G sur un k-espace vectoriel (souvent de dimension finie), chaque élément de G agissant par un automorphisme de V. Autrement dit, une représentation k-linéaire de G est la donnée d'un k-espace vectoriel V et d'un homomorphisme de groupes de G dans $\mathbf{GL}(V)$.

Expliquons tout de suite comment cette notion se rapporte aux chapitres précédents du cours. Donnons-nous G et k comme ci-dessus. On peut alors définir une k-algèbre, notée kG (ou $k[G]$), et appelée la k-algèbre du groupe G, de la façon suivante. Comme k-espace vectoriel, kG est l'ensemble des combinaisons k-linéaires formelles $\sum_{g\in G} a_g g$, où $(a_g)_{g\in G}$ est une famille d'éléments de k presque tous nuls. Autrement dit, kG est le k-espace vectoriel de base G, ce qui permet d'identifier G à un sous-ensemble de kG.

Le produit sur kG est défini par bilinéarité à partir du produit de G :

$$\left(\sum_{g\in G} a_g g\right)\left(\sum_{h\in G} b_h h\right) = \sum_{(g,h)\in G^2} a_g b_h\ (gh) = \sum_{g\in G}\left(\sum_{h\in G} a_{gh^{-1}} b_h\right) g.$$

Si e désigne l'élement neutre du groupe G, alors le neutre multiplicatif de l'anneau kG est $1e$, qu'on note plus simplement 1 ou e.

4.1.1.1 Proposition. *Soit G un groupe, k un corps, et A une k-algèbre. Tout homomorphisme de groupes de G dans $A^\times$ se prolonge en un unique homomorphisme de k-algèbres de kG dans A. Réciproquement, la restriction à G d'un homomorphisme d'algèbres de kG dans A est un homomorphisme de groupes de G dans $A^\times$.*

Preuve. Soit π un homomorphisme de groupes de G dans $A^\times$. La seule application k-linéaire de kG dans A qui prolonge π est donnée par

$$\sum_{g\in G} a_g g \mapsto \sum_{g\in G} a_g \pi(g).$$

On vérifie alors sans peine que cette application est un homomorphisme d'algèbres, c'est-à-dire qu'elle préserve le produit et le neutre multiplicatif. Les détails et la preuve de la réciproque sont laissés en exercice au lecteur. □

Appliquée à la k-algèbre $A = \mathbf{Mat}_n(k)$, cette proposition montre que la donnée d'une représentation matricielle de G sur k est équivalente à la donnée d'une représentation matricielle de kG de même degré. Appliqué à la k-algèbre $A = \mathrm{End}_k(V)$, où V est un k-espace vectoriel, cette proposition montre que la donnée d'une représentation linéaire de G sur V est équivalente à la donnée d'une structure de kG-module sur V.

Dans la suite, nous utiliserons ainsi librement le langage établi au chapitre 3. Seule variation : si M et N sont deux représentations de G sur k, on note souvent $\mathrm{Hom}_G(M,N)$ au lieu de $\mathrm{Hom}_{kG}(M,N)$.

EXERCICE. Soit k un anneau commutatif, soient G et H deux groupes. Construire un isomorphisme naturel de k-algèbres $k(G\times H)\cong kG\otimes_k kH$.

4.1.2 Exemples

4.1.2.1 Représentations de permutation. Soit G un groupe agissant sur un ensemble fini Ω. Soit k un corps. Construisons le k-espace vectoriel $V=k^{(\Omega)}$ de base $(e_\omega)_{\omega\in\Omega}$. À $g\in G$, on associe l'automorphisme $e_\omega\mapsto e_{g\omega}$ de V ; dans la base $(e_\omega)_{\omega\in\Omega}$, la matrice de cet automorphisme est une matrice de permutation. On obtient ainsi un homomorphisme de groupes de G dans $\mathbf{GL}(V)$, ce qui munit V d'une structure de kG-module. On dit que V est la représentation de permutation associée au G-ensemble Ω.

4.1.2.2 Caractères linéaires. Une représentation de degré 1 d'un groupe G s'appelle un caractère linéaire de G. C'est donc un homomorphisme de G dans le groupe abélien $\mathbf{GL}_1(k)\cong k^*$. Une telle représentation est évidemment irréductible.

Si λ et μ sont deux caractères linéaires, alors leur produit $g\mapsto\lambda(g)\mu(g)$ est encore un caractère linéaire. L'ensemble des caractères linéaires de G est ainsi un groupe abélien : l'élement neutre est le caractère unité $g\mapsto 1$, et l'inverse d'un caractère linéaire λ est $g\mapsto\lambda(g)^{-1}$.

4.1.2.3 Groupe cyclique C_n. Ici nous prenons $k=\mathbf{C}$. Soit g un générateur de C_n. Pour chaque racine n-ième ζ de l'unité dans $\mathbf{C}$, il existe un caractère linéaire de G qui envoie g sur ζ. On obtient ainsi n caractères linéaires, qui sont autant de représentations irréductibles deux à deux non-équivalentes.

4.1.2.4 Groupe diédral D_n. Ici nous prenons $k=\mathbf{R}$ ou $\mathbf{C}$. Le groupe diédral D_n possède $2n$ éléments ; il est engendré par deux éléments r et s, qui vérifient $r^n=s^2=(rs)^2=1$. On voit facilement que chaque élément de D_n s'écrit r^k ou r^ks, avec $k\in\{0,\dots,n-1\}$ unique. L'élement r engendre un sous-groupe cyclique d'ordre n et d'indice 2 (donc distingué). Posons $\theta=2\pi/n$.

L'application constante égale à 1 et l'application appelée « signature »

$$\varepsilon : r^k\mapsto 1,\quad r^ks\mapsto -1,$$

toutes deux de G dans k^*, sont des caractères linéaires de D_n. Nous avons donc déjà trouvé deux représentations irréductibles de D_n.

Pour n impair, D_n possède $2+(n-1)/2$ classes de conjugaison : $\{1\}$, $\{r^k s \mid 0 \leq k < n\}$, et les paires $\{r^j, r^{-j}\}$ pour j entier entre 1 et $(n-1)/2$. Pour chaque tel j, posons

$$R_j = \begin{pmatrix} \cos j\theta & -\sin j\theta \\ \sin j\theta & \cos j\theta \end{pmatrix} \quad \text{et} \quad S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Ces matrices appartiennent à $\mathbf{GL}_2(k)$ et vérifient les relations $(R_j)^n = S^2 = (R_j S)^2 = I$. Il existe donc un homomorphisme de groupes de D_n dans $\mathbf{GL}_2(k)$ qui envoie r sur R_j et s sur S ; dans cet homomorphisme,

$$r^k \mapsto \begin{pmatrix} \cos jk\theta & -\sin jk\theta \\ \sin jk\theta & \cos jk\theta \end{pmatrix} \quad \text{et} \quad r^k s \mapsto \begin{pmatrix} \cos jk\theta & \sin jk\theta \\ \sin jk\theta & -\cos jk\theta \end{pmatrix}.$$

Cette représentation est irréductible, car R_j et S n'ont pas de vecteur propre commun (ni sur $\mathbf{R}$, ni sur $\mathbf{C}$). Nous obtenons ainsi $(n-1)/2$ représentations irréductibles de degré 2 de D_n. Elles sont par ailleurs deux à deux non-équivalentes : les matrices R_j ont des traces différentes, donc appartiennent à des classes de conjugaison différentes dans $\mathbf{GL}_2(k)$. Au total, nous avons donc construit $2+(n-1)/2$ représentations irréductibles de D_n.

Pour n pair, D_n possède $3+n/2$ classes de conjugaison : $\{1\}$, $\{r^{n/2}\}$, $\{r^{2k}s \mid 0 \leq k < n/2\}$, $\{r^{2k+1}s \mid 0 \leq k < n/2\}$, et les paires $\{r^j, r^{-j}\}$ pour j entier entre 1 et $n/2-1$. Pour chaque tel j, nous pouvons à nouveau poser

$$R_j = \begin{pmatrix} \cos j\theta & -\sin j\theta \\ \sin j\theta & \cos j\theta \end{pmatrix} \quad \text{et} \quad S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

constater que ces matrices appartiennent à $\mathbf{GL}_2(k)$ et vérifier les relations $(R_j)^n = S^2 = (R_j S)^2 = I$. Il existe donc une représentation de degré 2 de D_n qui envoie r sur R_j et s sur S. Nous obtenons ainsi $n/2-1$ représentations irréductibles distinctes de degré 2 de D_n. Par ailleurs, le groupe D_n possède deux autres caractères linéaires, donnés par

$$r^k \mapsto (-1)^k,\ r^k s \mapsto (-1)^k \quad \text{et} \quad r^k \mapsto (-1)^k,\ r^k s \mapsto (-1)^{k+1}.$$

Au total, nous avons construit $3+n/2$ représentations irréductibles deux à deux non-équivalentes de D_n.

4.1.2.5 Groupe quaternionique Q d'ordre 8. Ici nous prenons $k = \mathbf{C}$. Le groupe Q est le sous-groupe du groupe des quaternions inversibles formé par les 8 éléments ± 1, $\pm i$, $\pm j$, $\pm k$. On a les relations $i^2 = j^2 = k^2 = ijk = -1$ et $(-1)^2 = 1$. Le centre de Q est le sous-groupe $\{\pm 1\}$ à deux éléments. Il y a cinq classes de conjugaison : $\{1\}$, $\{-1\}$, $\{\pm i\}$, $\{\pm j\}$ et $\{\pm k\}$. Les quatre homomorphismes suivants de Q dans $\mathbf{C}^*$

$\pm 1 \mapsto 1$,	$\pm i \mapsto 1$,	$\pm j \mapsto 1$,	$\pm k \mapsto 1$
$\pm 1 \mapsto 1$,	$\pm i \mapsto 1$,	$\pm j \mapsto -1$,	$\pm k \mapsto -1$
$\pm 1 \mapsto 1$,	$\pm i \mapsto -1$,	$\pm j \mapsto 1$,	$\pm k \mapsto -1$
$\pm 1 \mapsto 1$,	$\pm i \mapsto -1$,	$\pm j \mapsto -1$,	$\pm k \mapsto 1$

fournissent quatre représentations de degré 1 de Q. Par ailleurs, les trois matrices (de Pauli)

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \text{et} \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

vérifient $(-i\sigma_x)^2 = (-i\sigma_y)^2 = (-i\sigma_z)^2 = (-i\sigma_x)(-i\sigma_y)(-i\sigma_z) = -I$. Il existe donc une représentation matricielle de Q de degré 2 qui envoie -1, i, j et k sur $-I$, $-i\sigma_x$, $-i\sigma_y$ et $-i\sigma_z$, respectivement. Cette représentation de Q est irréductible, car $-i\sigma_x$, $-i\sigma_y$ et $-i\sigma_z$ n'ont pas de vecteur propre commun.

Une remarque pour conclure : adoptons les notations usuelles pour l'algèbre $\mathbf{H}$ des quaternions. En particulier, $\mathbf{H}$ est un $\mathbf{R}$-espace vectoriel de dimension 4, de base $(1, i, j, k)$. L'ensemble $\mathbf{Sp}(1) = \{q \in \mathbf{H} \mid q\bar{q} = 1\}$ des quaternions de norme 1 est un groupe, homéomorphe à la sphère de dimension 3. Le plongement de $\mathbf{R}$-algèbres

$$a + bi + cj + dk \mapsto \begin{pmatrix} a - id & -c - bi \\ c - bi & a + id \end{pmatrix}$$

de $\mathbf{H}$ dans $\mathbf{Mat}_2(\mathbf{C})$ induit par restriction un isomorphisme de groupes de $\mathbf{Sp}(1)$ sur $\mathbf{SU}(2)$. La représentation de Q de degré 2 que nous venons de définir est la composée

$$Q \hookrightarrow \mathbf{Sp}(1) \cong \mathbf{SU}(2) \hookrightarrow \mathbf{GL}_2(\mathbf{C}).$$

4.1.3 Opérations sur les représentations

On se fixe un groupe G et un corps k.

Représentation unité (ou triviale) : c'est l'homomorphisme constant $g \mapsto (1)$ de G dans $\mathbf{GL}_1(k)$. On la note 1, ou k quand on veut indiquer le corps de base.

Somme directe : soient deux représentations linéaires de G, sur des k-espaces vectoriels V et W. On définit une représentation linéaire de G sur $V \oplus W$ en faisant agir G diagonalement, c'est-à-dire simultanément sur les deux termes de la somme : l'action de $g \in G$ sur un élément $v \oplus w$ est donnée par $g(v \oplus w) = gv \oplus gw$. On peut dire cela d'une autre manière : étant donnés deux représentations matricielles $X : G \to \mathbf{GL}_m(k)$ et $Y : G \to \mathbf{GL}_n(k)$, on définit $X \oplus Y : G \to \mathbf{GL}_{m+n}(k)$ comme la composée de l'homomorphisme de groupes $g \mapsto (X(g), Y(g))$ avec le plongement $\mathbf{GL}_m(k) \times \mathbf{GL}_n(k) \hookrightarrow \mathbf{GL}_{m+n}(k)$ obtenu en bâtissant une matrice carrée de taille $(m + n) \times (m + n)$ à partir de deux blocs diagonaux de taille $m \times m$ et $n \times n$.

Produit tensoriel : soient deux représentations linéaires de G, sur des k-espaces vectoriels V et W. On définit une représentation linéaire de G sur $V \otimes_k W$ en faisant agir G simultanément sur les deux facteurs du produit : l'action de $g \in G$ sur un tenseur $\sum_{i \in I} v_i \otimes w_i$ est donnée par $g\Big(\sum_{i \in I} v_i \otimes w_i\Big) = \sum_{i \in I} gv_i \otimes gw_i$. On peut dire cela d'une autre manière : étant donnés deux homomorphismes de groupes $X : G \to \mathbf{GL}_m(k)$ et $Y : G \to \mathbf{GL}_n(k)$, on définit $X \otimes Y : G \to \mathbf{GL}_{mn}(k)$ comme la composée de l'homomorphisme $g \mapsto (X(g), Y(g))$ avec le plongement

$\mathbf{GL}_m(k) \times \mathbf{GL}_n(k) \hookrightarrow \mathbf{GL}_{mn}(k)$ provenant de l'isomorphisme de k-algèbres $\mathbf{Mat}_m(k) \otimes_k \mathbf{Mat}_n(k) \cong \mathbf{Mat}_{mn}(k)$ de l'exemple 3.1.2.1 (7) [15].

Le produit tensoriel de deux représentations est une opération commutative quand on ne regarde les représentations qu'à équivalence près. De fait, étant données deux représentations linéaires de G sur des espaces vectoriels V et W, le *flip* $\sum_{i\in I} v_i \otimes w_i \mapsto \sum_{i\in I} w_i \otimes v_i$ de $V \otimes_k W$ sur $W \otimes_k V$ est un isomorphisme de kG-modules. De la même manière, la somme directe de deux représentations est une opération commutative quand on ne regarde les représentations qu'à équivalence près.

Contragrédiente : soit V un kG-module à gauche. Alors le k-espace vectoriel $V^* = \mathrm{Hom}_k(V, k)$ est muni d'une structure de kG-module à droite, ainsi que nous l'avons observé dans la remarque 3.2.1.1. On peut transformer cette action à droite de G sur V^* en une action à gauche en utilisant l'involution $g \mapsto g^{-1}$ de G. Concrètement, l'action de g sur une forme linéaire $f \in V^*$ est donnée par $gf = \big(m \mapsto f(g^{-1}m)\big)$. On peut dire cela d'une autre manière : étant donné un homomorphisme de groupes $X : G \to \mathbf{GL}_n(k)$, on définit $X^* : G \to \mathbf{GL}_n(k)$ en disant que $X^*(g)$ est la transposée de $X(g^{-1})$.

$\mathrm{Hom}_k(?, ?)$: soient deux représentations linéaires de G, sur des k-espaces vectoriels V et W. On définit une représentation de G sur l'espace $\mathrm{Hom}_k(M, N)$ en décrétant que l'action de $g \in G$ sur une application k-linéaire f est donnée par $gf = \big(m \mapsto gf(g^{-1}m)\big)$. On peut définir cette action d'une autre manière, en transportant à $\mathrm{Hom}_k(M, N)$ la structure de kG module par l'isomorphisme naturel de k-modules $M^* \otimes_k N \cong \mathrm{Hom}_k(M, N)$ (voir l'exercice du paragraphe 3.1.1). Vice-versa, la représentation contragrédiente M^* s'identifie à la représentation $\mathrm{Hom}_k(M, k)$, le deuxième kG-module k étant ici la représentation unité.

Puissances tensorielles, symétriques et extérieures : si on se donne une représentation linéaire de G sur un espace vectoriel V, alors chaque $\mathsf{T}^n V$ est muni d'une action linéaire de G (par itération de la construction ci-dessus du produit tensoriel de deux représentations). Ainsi G agit par automorphismes sur l'algèbre $\mathsf{T}\, V$. Les noyaux des applications canoniques de $\mathsf{T}\, V$ sur $\mathsf{S}\, V$ et $\bigwedge V$ sont des idéaux et des sous-kG-modules de $\mathsf{T}\, V$: cela permet de définir une action de G sur les quotients $\mathsf{S}\, V$ et $\bigwedge V$. Alors chaque pièce graduée $\mathsf{S}^n V$ et $\bigwedge^n V$ est l'espace d'une représentation linéaire de G. Enfin les complexes de Koszul (théorème 3.1.4.6) sont des suites exactes de kG-modules.

Invariants : soit $\pi : G \to \mathbf{GL}(V)$ une représentation d'un groupe G sur un k-espace vectoriel V. L'espace des invariants est le sous-espace vectoriel $\mathrm{inv}_G V = \bigcap_{g\in G} \ker(\pi(g) - \mathrm{id}_V)$; c'est le plus grand sous-espace sur lequel l'action de G est triviale. (On note souvent V^G au lieu de $\mathrm{inv}_G V$, mais cette notation prête confusion avec celle employée pour indiquer la puissance d'un ensemble ou l'induite d'une représentation.)

Coinvariants : soit $\pi : G \to \mathbf{GL}(V)$ une représentation d'un groupe G sur un k-espace vectoriel V. Posons $J = \sum_{g\in G} \mathrm{im}(\pi(g) - \mathrm{id}_V)$. L'espace des coinvariants est l'espace vectoriel quotient $\mathrm{coinv}_G V = V/J$; c'est le plus grand quotient de V sur lequel l'action de G est triviale.

15. L'isomorphisme $\mathbf{Mat}_m(k) \otimes_k \mathbf{Mat}_n(k) \cong \mathbf{Mat}_{mn}(k)$ n'est pas canonique, mais déterminé seulement à composition par un automorphisme de $\mathbf{Mat}_{mn}(k)$ près. Cependant, l'exercice (2) du paragraphe 2.1.1 montre que les automorphismes de la k-algèbre $\mathbf{Mat}_{mn}(k)$ sont de la forme $A \mapsto SAS^{-1}$, où $S \in \mathbf{GL}_{mn}(k)$. Le plongement $\mathbf{GL}_m(k) \times \mathbf{GL}_n(k) \hookrightarrow \mathbf{GL}_{mn}(k)$ est donc déterminé à conjugaison près, et la représentation matricielle $X \otimes Y$ est déterminée à équivalence près.

Exercices.

(1) Soient V et W deux k-représentations de G. Montrer que $\mathrm{Hom}_G(V,W)$ est l'espace des G-invariants de la représentation $\mathrm{Hom}_k(V,W)$.

(2) Soient G un groupe et V une représentation de G sur un corps k. Construire des isomorphismes canoniques de k-espaces vectoriels $\mathrm{Hom}_G(k,V) = \mathrm{inv}_G V$, $\mathrm{coinv}_G V = k \otimes_{kG} V$ et $\mathrm{Hom}_G(V,k) = \big(\mathrm{coinv}_G V\big)^*$, où k est la représentation unité de G.

(3) Soit V une k-représentation de G. Montrer que $\mathrm{inv}_G V$ et J sont des sous-kG-modules de V. Montrer que si le kG-module V est complètement réductible, alors $V = \mathrm{inv}_G V \oplus J$ et la composée $\mathrm{inv}_G V \hookrightarrow V \twoheadrightarrow \mathrm{coinv}_G V$ est un isomorphisme d'espaces vectoriels. (Indication : pour montrer que $V = \mathrm{inv}_G V \oplus J$, on commencera par traiter le cas où π est irréductible en distinguant selon que π est la représentation triviale ou non.)

4.1.4 Fonctions centrales et caractères

4.1.4.1 Rappels sur la trace d'une application linéaire. Soit k un corps. Dans ces rappels, tous les espaces vectoriels seront des k-espaces vectoriels de dimension finie.

(1) La trace d'une matrice carrée A est la somme $\mathrm{tr}\, A$ des éléments diagonaux de A. Si m et n sont deux entiers strictement positifs, si $A \in \mathbf{Mat}_{m,n}(k)$ et $B \in \mathbf{Mat}_{n,m}(k)$, alors $\mathrm{tr}(AB) = \mathrm{tr}(BA)$. Deux matrices A et B carrées de même taille et semblables ont même trace. Une matrice a même trace que sa transposée.

(2) Soit f un endomorphisme d'un espace vectoriel V. La trace de la matrice représentant f ne dépend pas du choix de la base utilisée ; on la note $\mathrm{tr}\, f$.

(3) Si V et W sont deux espaces vectoriels, si $f : V \to W$ et $g : W \to V$ sont deux applications linéaires, alors $\mathrm{tr}(f \circ g) = \mathrm{tr}(g \circ f)$. La forme bilinéaire $(f,g) \mapsto \mathrm{tr}(f \circ g)$ de $\mathrm{Hom}_k(V,W) \times \mathrm{Hom}_k(W,V)$ dans k est non-dégénérée et permet d'identifier chacun des espaces $\mathrm{Hom}_k(V,W)$ et $\mathrm{Hom}_k(W,V)$ au dual de l'autre.

(4) Soit V un espace vectoriel de dimension finie et V^* le dual de V. L'application $\sum_{i\in I} v_i^* \otimes v_i \mapsto \Big(w \mapsto \sum_{i\in I} v_i^*(w) v_i\Big)$ de $V^* \otimes V$ dans $\mathrm{End}_k(V)$ est un isomorphisme d'espaces vectoriels ; notons le Φ. Alors $\mathrm{tr} \circ \Phi : V^* \otimes V \to k$ est la forme linéaire $\sum_{i\in I} v_i^* \otimes v_i \mapsto \sum_{i\in I} \langle v_i^*, v_i \rangle$.

(5) Soient V et W deux espaces vectoriels et soient $f \in \mathrm{End}_k(V)$ et $g \in \mathrm{End}_k(W)$. Notons $f \oplus g$ l'endomorphisme de $V \oplus W$ défini comme $v \oplus w \mapsto f(v) \oplus g(w)$. De même, soit $f \otimes g$ l'endomorphisme de $V \otimes_k W$ défini comme $\sum_{i\in I} v_i \otimes w_i \mapsto \sum_{i\in I} f(v_i) \otimes g(w_i)$. Alors $\mathrm{tr}(f \oplus g) = (\mathrm{tr}\, f) + (\mathrm{tr}\, g)$ et $\mathrm{tr}(f \otimes g) = (\mathrm{tr}\, f)(\mathrm{tr}\, g)$.

(6) Soit V un espace vectoriel et $f \in \mathrm{End}_k(V)$. Par définition, la transposée de f est l'endomorphisme $\mathrm{Hom}_k(f,k) : v^* \mapsto v^* \circ f$ de V^*. Si B est une base de V et B^* est la base duale de V^*, alors la matrice de la transposée de f dans B^* est la transposée de la matrice de f dans B. On en déduit que f et sa transposée ont même trace.

Donnons-nous un groupe G et un corps k.

Fonction centrale (ou fonction de classe) : une fonction $\varphi : G \to k$ est dite centrale si elle est constante sur chaque classe de conjugaison. En formules, cela signifie que $\varphi(ghg^{-1}) = \varphi(h)$

pour tout couple $(g,h) \in G^2$. On note $\mathrm{cf}_k(G)$ le k-espace vectoriel des fonctions centrales sur G à valeurs dans k.

Caractère d'une représentation : soit $\pi : G \to \mathbf{GL}(V)$ une représentation linéaire d'un groupe G sur un k-espace vectoriel V de dimension finie. Le caractère de π est la fonction $\chi_\pi : g \mapsto \operatorname{tr}\pi(g)$ de G à valeurs dans k. Le caractère χ_π appartient à $\mathrm{cf}_k(G)$, car

$$\chi_\pi(ghg^{-1}) = \operatorname{tr}\pi(ghg^{-1}) = \operatorname{tr}(\pi(g)\pi(h)\pi(g)^{-1}) = \operatorname{tr}(\pi(h)\pi(g)^{-1}\pi(g)) = \operatorname{tr}\pi(h) = \chi_\pi(h).$$

Si on choisit une base de V et qu'on appelle X la représentation matricielle définie par π dans cette base, on a $\chi_\pi(g) = \operatorname{tr} X(g)$ pour tout $g \in G$. On notera éventuellement χ_X au lieu de χ_π. De même, si on sous-entend que V est un kG-module et non un simple espace vectoriel, on pourra noter χ_V au lieu de χ_π.

4.1.4.2 Remarque. Dans le paragraphe 3.2.5, nous avons défini le caractère d'une représentation d'une algèbre A comme une forme linéaire sur A. Le lien avec la notion de caractère définie ci-dessus est le suivant. L'algèbre A utilisée est évidemment l'algèbre kG du groupe, de façon à pouvoir identifier représentations de G et représentations de A. Une forme linéaire sur A est déterminée dès qu'on se donne ses valeurs sur une base de A. Comme G est une base de A, cela signifie qu'on peut identifier l'espace des formes linéaires sur A avec l'espace des fonctions sur G.

Opérateurs d'Adams : soit $m \in \mathbf{Z}$ un entier. Pour chaque fonction centrale φ, on note $\psi_m(\varphi)$ la fonction $g \mapsto \varphi(g^m)$. Manifestement $\psi_m(\varphi)$ est une fonction centrale et l'application $\psi_m : \mathrm{cf}_k(G) \to \mathrm{cf}_k(G)$ est un endomorphisme de la k-algèbre $\mathrm{cf}_k(G)$. Quand $m \geq 1$, ψ_m est appelé opérateur d'Adams. L'opérateur ψ_{-1} est une involution, et est habituellement noté avec une étoile : $\psi_{-1}(\varphi) = \varphi^*$.

4.1.4.3 Théorème. *Soient k un corps et G un groupe.*

(i) Deux représentations équivalentes de G ont même caractère.

(ii) Soit $0 \to L \to M \to N \to 0$ une suite exacte de représentations de G sur k. Alors $\chi_M = \chi_L + \chi_N$.

(iii) Soit $\pi : G \to \mathbf{GL}(M)$ une représentation k-linéaire de G sur un espace vectoriel M. Soit $\{S_1, \ldots, S_r\}$ un ensemble de représentations irréductibles de G, deux à deux inéquivalentes, telles que tout sous-quotient irréductible de M soit isomorphe à une de ces représentations. Enfin, soit $(M : S_i)$ la multiplicité de Jordan-Hölder de S_i dans M, pour chaque $i \in \{1, \ldots, r\}$. Alors $\chi_M = \sum_{i=1}^r (M : S_i)\chi_{S_i}$.

(iv) Soient deux représentations k-linéaires de G, sur des espaces vectoriels V et W. Alors $\chi_{V\oplus W} = \chi_V + \chi_W$, $\chi_{V\otimes_k W} = \chi_V\chi_W$, $\chi_{V^*} = \big(\chi_V\big)^*$, et $\chi_{\mathrm{Hom}_k(V,W)} = (\chi_V)^*\chi_W$. Par ailleurs, le caractère de la représentation triviale est la fonction constante égale à 1.

(v) Supposons que k soit de caractéristique 0. Soit V une représentation de G sur k. Alors on a des égalités entre séries formelles à coefficients dans $\mathrm{cf}_k(G)$

$$\sum_{n\geq 0} t^n \chi_{\mathsf{S}^n V} = \exp\left(\sum_{m\geq 1} \frac{t^m}{m}\psi_m(\chi_V)\right) \quad \textit{et} \quad \sum_{n\geq 0}(-t)^n \chi_{\bigwedge^n V} = \exp\left(-\sum_{m\geq 1} \frac{t^m}{m}\psi_m(\chi_V)\right).$$

Preuve. L'assertion (i) est presque évidente (et a été considérée comme telle dans le paragraphe 3.2.5). On peut par exemple dire que si X et $Y : G \to \mathbf{GL}_n(k)$ sont deux représentations matricielles équivalentes, alors il existe $P \in \mathbf{GL}_n(k)$ telle que $Y(g) = PX(g)P^{-1}$ pour chaque $g \in G$, d'où $\operatorname{tr} X(g) = \operatorname{tr} Y(g)$.

L'assertion (ii) a été prouvée dans un contexte plus général à la proposition 3.2.5.1. L'assertion (iv) résulte des définitions et des rappels 4.1.4.1 (5) et (6).

L'assertion (iii) résulte de la proposition 3.2.5.3. La preuve qui en a été alors donnée peut être réécrite sans faire appel à la notion de groupe de Grothendieck. On raisonne par récurrence sur le degré de la représentation (c'est-à-dire sur la dimension du k-espace vectoriel M). Si M est une représentation irréductible, alors $r = 1$, $S_1 = M$, et il n'y a rien à démontrer. Sinon, M contient un sous-espace vectoriel non-banal L stable par l'action de tous les éléments du groupe. On obtient alors une suite exacte courte $0 \to L \to M \to N \to 0$ de représentations de G, avec $N = M/L$. Puisque les dimensions de L et M sont strictement inférieures à la dimension de M, l'hypothèse de récurrence nous permet d'écrire $\chi_L = \sum_{i=1}^{r}(L : S_i)\chi_{S_i}$ et $\chi_N = \sum_{i=1}^{r}(N : S_i)\chi_{S_i}$. Les égalités $(M : S_i) = (L : S_i) + (N : S_i)$ et $\chi_M = \chi_L + \chi_N$, prouvées respectivement dans la proposition 1.2.5.1 et dans l'assertion (ii), entraînent alors la formule souhaitée pour χ_M. Ceci achève la preuve de (iii).

Il reste à prouver l'assertion (v). Quitte à passer à une extension du corps de base, on peut supposer que k est algébriquement clos. Soit $\pi : G \to \mathbf{GL}(V)$ l'homomorphisme de groupes définissant la structure de kG-module de V. Soit $g \in G$. Il existe une base $(e_1, \dots, e_p)$ de V dans laquelle la matrice de $\pi(g)$ est triangulaire supérieure, avec les valeurs $(\xi_1, \dots, \xi_p)$ sur la diagonale. Alors pour chaque entier $m \geq 1$,

$$\psi_m(\chi_V)(g) = \chi_V(g^m) = \operatorname{tr} \pi(g)^m = \xi_1^m + \cdots + \xi_p^m.$$

Appelons $C_n(p)$ l'ensemble des suites croissantes de n éléments $i_1 \leq \cdots \leq i_n$ d'éléments de $\{1, \dots, p\}$ et munissons $\mathsf{S}^n V$ de la base $\{e_{i_1} \cdots e_{i_n} \mid (i_1, \dots, i_n) \in C_n(p)\}$, conformément au théorème 3.1.4.2. Si nous ordonnons $C_n(p)$ lexicographiquement, alors la matrice par laquelle g agit sur $\mathsf{S}^n V$ est triangulaire supérieure, avec

$$\{\xi_{i_1} \cdots \xi_{i_n} \mid (i_1, \dots, i_n) \in C_n(p)\}$$

pour valeurs diagonales. La trace de cette matrice est donc

$$\chi_{\mathsf{S}^n V}(g) = \sum_{1 \leq i_1 \leq \cdots \leq i_n \leq p} \xi_{i_1} \cdots \xi_{i_n}.$$

Nous pouvons maintenant calculer

$$\begin{aligned}
\sum_{n \geq 0} t^n \chi_{\mathsf{S}^n V}(g) &= \sum_{\substack{n \geq 0 \\ 1 \leq i_1 \leq \cdots \leq i_n \leq p}} (t\xi_{i_1}) \cdots (t\xi_{i_n}) \\
&= \prod_{i=1}^{p} (1 + t\xi_i + (t\xi_i)^2 + \cdots) \\
&= \prod_{i=1}^{p} \frac{1}{1 - t\xi_i}
\end{aligned}$$

$$= \exp\left(-\sum_{i=1}^{p} \log(1-t\xi_i)\right)$$
$$= \exp\left(\sum_{i=1}^{p}\sum_{m\geq 1} \frac{t^m}{m}\xi_i^m\right)$$
$$= \exp\left(\sum_{m\geq 1} \frac{t^m}{m}\psi_m(\chi_V)(g)\right).$$

Ceci fournit la première égalité voulue. La seconde résulte d'un calcul analogue, qui débute par

$$\sum_{n\geq 0} t^n \chi_{\bigwedge^n V}(g) = \sum_{\substack{n\geq 0 \\ 1\leq i_1<\cdots<i_n\leq p}} (t\xi_{i_1})\cdots(t\xi_{i_n}) = \prod_{i=1}^{p}(1+t\xi_i).$$

Les détails de ce second calcul sont laissés au lecteur. □

On note $\operatorname{ch} kG$ le sous-groupe additif de $\operatorname{cf}_k(G)$ engendré par les caractères des représentations de G sur k. Ainsi chaque élément de $\operatorname{ch} kG$ s'écrit comme une somme finie $\sum_{i\in I} n_i \operatorname{ch}_{V_i}$, avec $n_i \in \mathbf{Z}$. Le théorème 4.1.4.3 (iv) montre alors que $\operatorname{ch} kG$ est en fait un sous-anneau de $\operatorname{cf}_k(G)$ stable par l'involution *. Cet anneau $\operatorname{ch} kG$ a été introduit par Brauer. Ses éléments sont appelés caractères virtuels de G (sur k).

4.1.4.4 Théorème. *Soit G un groupe et k un corps. Supposons que l'une des trois hypothèses suivantes soit satisfaite :*

(a) k est algébriquement clos.

(b) k est de caractéristique 0.

(c) G est fini.

Si M_1, ..., M_r sont des kG-modules simples de dimension finie sur k et deux à deux non-isomorphes, alors les caractères χ_{M_1}, ..., χ_{M_r} sont linéairement indépendants dans $\operatorname{cf}_k(G)$.

Preuve. Le résultat a déjà été prouvé sous l'hypothèse (a) (c'était notre proposition 3.2.5.2) et sous l'hypothèse (b) (voir l'exercice du paragraphe 3.2.5). La preuve sous l'hypothèse (c) nécessite un peu de théorie de Galois ; je renvoie au paragraphe (17.3) de [7]. □

Ce théorème montre en particulier que sous n'importe laquelle des hypothèses (a), (b) ou (c), une représentation irréductible de G est déterminée à équivalence près par son caractère. Plutôt que de parler de classe d'équivalence de représentation irréductible, nous parlerons donc de caractère irréductible. Nous notons $\operatorname{Irr}(G)$ l'ensemble des caractères irréductibles de G sur k.

4.1.4.5 Théorème. *Soit G un groupe et k un corps de caractéristique 0. Alors $\operatorname{ch} kG$ est un $\mathbf{Z}$-module libre de base $\operatorname{Irr}_k(G)$.*

Preuve. D'après le théorème 4.1.4.4, $\mathrm{Irr}_k(G)$ est une partie linéairement indépendante du k-espace vectoriel $\mathrm{cf}_k(G)$. D'après le théorème 4.1.4.3 (iii), c'en est aussi une partie génératrice. □

On peut résumer les théorèmes de ce paragraphe en disant que si k est de caractéristique 0, alors le caractère d'une représentation de G sur k détermine les multiplicités de Jordan-Hölder de cette représentation. Il détermine donc la classe d'isomorphisme de cette représentation si celle-ci est complètement réductible. Nous verrons dans le prochain paragraphe que c'est toujours le cas si G est fini (théorème de Maschke 4.2.1.4). On peut alors utiliser concurremment les mots « caractères » et « classes d'isomorphisme de représentations ».

Exercices.

(1) (i) Soit G un groupe fini agissant sur un ensemble fini Ω et soit k un corps de caractéristique 0. Soit χ le caractère de la représentation de permutation de G sur $k^{(\Omega)}$ (paragraphe 4.1.2.1). Montrer que pour chaque $g \in G$, $\chi(g)$ est le nombre de points fixes de g dans Ω. Montrer que la dimension de l'espace des G-invariants dans $k^{(\Omega)}$, le nombre d'orbites de G dans Ω, et $\frac{1}{|G|}\sum_{g\in G}\chi(g)$ sont trois quantités égales.

(ii) Soit $\mathbf{F}$ un corps fini et soit $G = \mathbf{GL}_3(\mathbf{F})$. On fait agir G à gauche sur l'ensemble $\Omega = \mathbf{F}_c^3$ des vecteurs colonnes de la façon habituelle. On munit l'ensemble $\Omega' = \mathbf{F}_l^3$ des vecteurs lignes d'une action de G en posant $g \cdot v = vg^{-1}$, le membre de droite étant le produit matriciel ordinaire d'un vecteur ligne par une matrice. Enfin, soit k un corps de caractéristique 0. Montrer que les représentations de permutation de G sur $k^{(\Omega)}$ et $k^{(\Omega')}$ ont même caractère. (Note : ces deux représentations de permutation sont donc isomorphes. On montre cependant sans grande difficulté qu'il n'existe pas de bijection G-équivariante entre les ensembles Ω et Ω'.)

(2) Soit k un corps de caractéristique 0, soit G un groupe, soit $\pi : G \to \mathbf{GL}(V)$ une représentation de G sur un k-espace vectoriel V. Calculer $\chi_{\mathsf{S}^2\pi}$ et $\chi_{\bigwedge^2\pi}$ en fonction de χ_π et de $\psi_2(\chi_\pi)$.

(3) Soit k un corps de caractéristique 0, soit G un groupe, soit $\pi : G \to \mathbf{GL}(V)$ une représentation de G sur un k-espace vectoriel V. Montrer que pour tout entier $n \geq 1$,

$$\sum_{p=0}^{n}(-1)^p\chi_{\mathsf{S}^{n-p}V}\chi_{\bigwedge^p V} = 0.$$

(Indication : on peut utiliser soit le théorème 3.1.4.6, soit le théorème 4.1.4.3 (v).)

(4) Soient k un corps de caractéristique 0 et G un groupe. On note $A = \mathrm{cf}_k(G)[[t]]$ l'anneau des séries formelles en t à coefficients dans $\mathrm{cf}_k(G)$. Construire deux homomorphismes de groupes abéliens H_t et E_t de $\mathrm{cf}_k(G)$ dans $A^\times$ tels que pour chaque k-représentation V de G, on ait

$$H_t(\chi_V) = \sum_{n\geq 0} t^n\chi_{\mathsf{S}^n V} \quad \text{et} \quad E_t(\chi_V) = \sum_{n\geq 0} t^n\chi_{\bigwedge^n V}.$$

4.1.5 Anneau de Grothendieck

Le théorème 4.1.4.5 met le doigt sur un petit inconvénient des caractères : la théorie ne marche bien que sur un corps de caractéristique 0. Pour pallier cette limitation, on utilise le groupe de Grothendieck $G_0(kG)$ [16], qu'on munit d'une structure d'anneau. Rappelons brièvement la construction.

Soit $\mathscr{I}$ l'ensemble des classes d'équivalence de représentations de G sur k. Le groupe abélien libre $\mathbf{Z}^{(\mathscr{I})}$ possède une base naturelle, en bijection avec $\mathscr{I}$: à la classe d'équivalence d'une représentation X correspond un élément (X) de la base de $\mathbf{Z}^{(\mathscr{I})}$. Les éléments de $\mathbf{Z}^{(\mathscr{I})}$ sont les combinaisons $\mathbf{Z}$-linéaires des symboles (X), où il y a un symbole par classe d'équivalence de k-représentation de G. On munit $\mathbf{Z}^{(\mathscr{I})}$ d'une structure d'anneau en définissant le produit des vecteurs de base par la formule $(X)(Y) = (X \otimes Y)$; l'unité multiplicative est alors le symbole (k) correspondant à la représentation triviale de G. On munit $\mathbf{Z}^{(\mathscr{I})}$ d'une involution $*$ en posant $(X)^* = (X^*)$.

4.1.5.1 Proposition. *Soit J le sous-groupe de $\mathbf{Z}^{(\mathscr{I})}$ engendré par les éléments de la forme $(Y) - (X) - (Z)$, chaque fois qu'il existe une suite exacte courte $0 \to X \to Y \to Z \to 0$ de k-représentations (vues comme des kG-modules à gauche). Alors J est un idéal stable par l'involution $*$.*

Preuve. Soit T une k-représentation de G, et montrons que J est stable par multiplication à gauche par (T). Considérons un générateur de J, disons $(Y) - (X) - (Z)$, où $0 \to X \to Y \to Z \to 0$ est une suite exacte de k-représentations de G. Regardons cette suite comme une suite exacte de kG-modules à gauche et appliquons le foncteur $T \otimes_k ?$. Puisque le k-module T est libre, donc plat, nous obtenons une suite exacte de k-modules

$$0 \to T \otimes_k X \to T \otimes_k Y \to T \otimes_k Z \to 0.$$

Munissant chacun des k-espaces vectoriels de sa structure de représentation de G, nous obtenons une suite exacte de k-représentations de G. Le produit $(T)\big((Y) - (X) - (Z)\big)$ dans l'anneau $\mathbf{Z}^{(\mathscr{I})}$ est égal à $(T \otimes_k Y) - (T \otimes_k X) - (T \otimes_k Z)$; la suite exacte ci-dessus montre que cet élément appartient à J. Ainsi J est bel et bien stable par multiplication à gauche par (T). L'anneau $\mathbf{Z}^{(\mathscr{I})}$ étant commutatif, nous en déduisons que J est un idéal.

Montrons que J est stable sous l'involution $*$. Considérons un générateur de J, disons $(Y) - (X) - (Z)$, où $0 \to X \to Y \to Z \to 0$ est une suite exacte de k-représentations de G. En appliquant le foncteur $D = \mathrm{Hom}_k(?, k)$, nous obtenons une suite exacte $0 \to\!\!\to D(Z) \to D(Y) \to D(X) \to 0$ de kG-modules à droite. C'est une suite exacte $0 \to Z^* \to Y^* \to X^* \to 0$ reliant les représentations contragrédientes. L'image par $*$ de notre générateur $(Y)-(X)-(Z)$, égale à $(Y^*) - (Z^*) - (X^*)$, appartient donc à J. Ainsi J est stable par $*$. □

On définit l'anneau de Grothendieck $G_0(kG)$ comme étant le quotient $\mathbf{Z}^{(\mathscr{I})}/J$, où J est l'idéal construit dans l'énoncé de la proposition 4.1.5.1. On note $[X]$ l'image de (X) dans $G_0(kG)$;

16. *Stricto sensu,* le groupe $G_0(kG)$ introduit ci-dessous ne coïncide avec celui du paragraphe 1.2.5 que quand kG est de dimension finie, c'est-à-dire quand G est fini.

d'après la proposition 1.2.5.2, sa donnée est équivalente à celle des multiplicités de Jordan-Hölder des représentations irréductibles dans X.

Tout élément de $G_0(kG)$ est égal à une différence $[X] - [Y]$, où X et Y sont deux k-représentations de G ; pour le voir, il suffit d'écrire que dans $G_0(kG)$,

$$\sum_{X \in \mathscr{I}} n_X [X] = \left[\bigoplus_{n_X > 0} X^{\oplus n_X} \right] - \left[\bigoplus_{n_X < 0} X^{\oplus (-n_X)} \right].$$

Le théorème 4.1.4.3 (ii) et (iv) implique l'existence d'un homomorphisme d'anneaux

$$\mathrm{ch} : G_0(kG) \to \mathrm{cf}_k(G)$$

tel que $\mathrm{ch}[M] = \chi_M$ pour chaque représentation M de G sur k ; son image est $\mathrm{ch}\, kG$. La proposition 1.2.5.2 et les théorèmes 4.1.4.3 (iii) et 4.1.4.4 montrent que ch est injectif dès que le corps k est de caractéristique 0.

Exercices.

(1) Soient k un corps, G un groupe, M une représentation k-linéaire de G, et n un entier strictement positif. Montrer que dans $G_0(kG)$, $\sum_{k=0}^{n} (-1)^k [\mathsf{S}^k M][\bigwedge^{n-k} M] = 0$. (Indication : utiliser le théorème 3.1.4.6.)

(2) Soient k un corps, G un groupe, et n un entier strictement positif. Montrer que pour toute suite exacte courte $0 \to L \to M \to N \to 0$ de k-représentations de G, l'égalité $[\mathsf{S}^n M] = \sum_{i=0}^{n} [\mathsf{S}^{n-i} L][\mathsf{S}^i N]$ a lieu dans l'anneau $G_0(kG)$. En déduire que si M est une k-représentation de G, alors $[\mathsf{S}^n M]$ ne dépend que de $[M]$ et pas de M. (Indication : pour la première question, construire explicitement une filtration $0 = P_0 \subset P_1 \subset \cdots \subset P_{n+1} = S^n M$ telle que $P_{i+1}/P_i \cong \mathsf{S}^{n-i} L \otimes \mathsf{S}^i N$. Pour la seconde, raisonner par récurrence sur la longueur de M.)

(3) Soient k un corps, G un groupe, et n un entier strictement positif. Montrer que pour toute suite exacte courte $0 \to L \to M \to N \to 0$ de k-représentations de G, l'égalité $[\bigwedge^n M] = \sum_{i=0}^{n} [\bigwedge^{n-i} L][\bigwedge^i N]$ a lieu dans l'anneau $G_0(kG)$. En déduire que si M est une k-représentation de G, alors $[\bigwedge^n M]$ ne dépend que de $[M]$ et pas de M.

(4) Soient k un corps, G un groupe, et n un entier strictement positif. Soit $\xi \in G_0(kG)$. Il existe alors des k-représentations M et N de G telles que $\xi = [M] - [N]$. On pose

$$\mathsf{S}^n \xi = \sum_{i=0}^{n} (-1)^i [\mathsf{S}^{n-i} M][\textstyle\bigwedge^i N] \quad \text{et} \quad \textstyle\bigwedge^n \xi = \sum_{i=0}^{n} (-1)^i [\bigwedge^{n-i} M][\mathsf{S}^i N].$$

Montrer que $\mathsf{S}^n \xi$ et $\bigwedge^n \xi$ ne dépendent que de ξ et pas du choix de M et N. Comparer $\mathsf{S}^n(-\xi)$ et $(-1)^n \bigwedge^n \xi$. (Indication : soit $\xi = [M'] - [N']$ une autre écriture de ξ. Alors $[M \oplus N'] = [M' \oplus N]$ dans $G_0(kG)$. Pour chaque $(j,k) \in \mathbf{N}^2$ tel que $j + k \leq n$, on a alors $[\mathsf{S}^{n-j-k}(M \oplus N')] = [\mathsf{S}^{n-j-k}(M' \oplus N)]$, ce qui donne

$$\sum_{i=0}^{n-j-k} [\mathsf{S}^{n-i-j-k} M][\mathsf{S}^i N'] = \sum_{i=0}^{n-j-k} [\mathsf{S}^{n-i-j-k} M'][\mathsf{S}^i N].$$

En multipliant cette formule par $(-1)^{j+k}[\bigwedge^j N][\bigwedge^k N']$, en sommant sur j et k et en utilisant la relation provenant du complexe de Koszul, on trouve

$$\sum_{j=0}^{n}(-1)^j[\mathsf{S}^{n-j}\,M][\bigwedge^j N] = \sum_{k=0}^{n}(-1)^k[\mathsf{S}^{n-k}\,M'][\bigwedge^k N'].$$

Ainsi $\mathsf{S}^n\,\xi$ est bien défini. Le cas de $\bigwedge^n \xi$ se traite de manière analogue ou bien en utilisant la formule $\mathsf{S}^n(-\xi) = (-1)^n \bigwedge^n \xi$.)

4.2 Représentations ordinaires des groupes finis

Dans toute cette section, G sera un groupe fini et k sera un corps dont la caractéristique ne divise pas l'ordre de G.

4.2.1 Séparabilité

4.2.1.1 Théorème. *L'algèbre kG est séparable sur k. Plus précisément, l'élément*

$$\frac{1}{|G|}\sum_{g\in G} g\otimes g^{-1}$$

de $kG\otimes_k kG$ vérifie la condition (ix) du théorème 3.3.1.3.

Preuve. Une réindexation de la somme montre que pour chaque $h\in G$, l'égalité

$$\frac{1}{|G|}\sum_{g\in G} hg\otimes g^{-1} = \frac{1}{|G|}\sum_{g\in G} g\otimes g^{-1}h$$

a lieu dans $kg\otimes_k kG$. Par linéarité, on en déduit l'égalité

$$\frac{1}{|G|}\sum_{g\in G} cg\otimes g^{-1} = \frac{1}{|G|}\sum_{g\in G} g\otimes g^{-1}c$$

pour chaque $c\in kG$. □

Remarque. Ce théorème entraîne que $J(kG)=\{0\}$, et donc que $kG/J(kG)$ est séparable. On peut en fait montrer (voir [7], paragraphe (7.10)) que $kG/J(kG)$ est séparable pour tout groupe fini G, quelle que soit la caractéristique de k.

Le théorème 3.3.1.3, et plus particulièrement l'implication (ix) ⇒ (i), montre que tout kG-module est complètement réductible. Par commodité pour le lecteur, nous allons redonner cette preuve ici en faisant appel à l'opérateur de Reynolds. (Le lien avec l'exercice (2) du paragraphe 3.3.1 est le suivant : une représentation de G sur un espace vectoriel V peut être vu comme un kG-kG-bimodule en faisant agir G à droite sur V de façon triviale ; de cette

façon, l'espace des invariants $\mathrm{inv}_G V$ est vu comme le centre $Z^0(kG, V)$ du bimodule ainsi obtenu.)

Opérateur de Reynolds : soit $\pi : G \to \mathbf{GL}(V)$ une représentation k-linéaire de G. L'opérateur de Reynolds est l'application linéaire $\natural = \frac{1}{|G|} \sum_{g \in G} \pi(g)$ de V dans lui-même.

Rappelons-nous de la définition de l'espace des invariants et de l'espace des coinvariants de la représentation π (paragraphe 4.1.3) : on pose $\mathrm{inv}_G V = \bigcap_{g \in G} \ker(\pi(g) - \mathrm{id}_V)$, $J = \sum_{g \in G} \mathrm{im}(\pi(g) - \mathrm{id}_V)$ et $\mathrm{coinv}_G V = V/J$. L'espace des invariants est le plus grand sous-espace de V lequel l'action de G est triviale ; l'espace des coinvariants est le plus grand quotient de V sur lequel l'action de G est triviale.

4.2.1.2 Proposition.

(i) Soit $\pi : G \to \mathbf{GL}(V)$ une représentation linéaire de G. Posons $J = \sum_{g \in G} \mathrm{im}(\pi(g) - \mathrm{id}_V)$. Alors $V = \mathrm{inv}_G V \oplus J$, et l'opérateur de Reynolds $\natural$ est le projecteur d'image $\mathrm{inv}_G V$ et de noyau J.

(ii) L'opérateur de Reynolds commute à l'action de G sur V ; autrement dit, c'est un endomorphisme de π.

(iii) L'opérateur de Reynolds est naturel : chaque homomorphisme de représentations $f : V \to W$ donne lieu à un diagramme commutatif

$$\begin{array}{ccc} V & \xrightarrow{f} & W \\ \downarrow{\scriptstyle \natural} & & \downarrow{\scriptstyle \natural} \\ \mathrm{inv}_G V & \xrightarrow[f]{} & \mathrm{inv}_G W. \end{array}$$

Preuve. Pour chaque $g \in G$, on a $\pi(g) \circ \natural = \natural \circ \pi(g) = \natural$. Cela montre que l'image de $\natural$ est incluse dans $\mathrm{inv}_G V$ et que le noyau de $\natural$ contient J. Par ailleurs, $\mathrm{id}_V - \natural = \frac{1}{|G|} \sum_{g \in G} (\mathrm{id}_V - \pi(g))$; ainsi inv_G est inclus dans le noyau de $\mathrm{id}_V - \natural$ et J contient l'image de $\mathrm{id}_V - \natural$. Nous en déduisons que $\mathrm{inv}_G V \cap J \subseteq \ker(\mathrm{id}_V - \natural) \cap \ker \natural = 0$, que $\mathrm{inv}_G V + J \supseteq \mathrm{im}\, \natural + \mathrm{im}(\mathrm{id}_V - \natural) = V$, donc que $V = \mathrm{inv}_G V \oplus J$. De plus, $\natural$ s'annule sur J et $\mathrm{id}_V - \natural$ s'annule sur $\mathrm{inv}_G V$. Tout cela montre l'assertion (i). Chemin faisant, nous avons aussi montré l'assertion (ii).

Soit $\hat{\pi} : kG \to \mathrm{End}_k(V)$ l'homomorphisme d'algèbres de kG dans $\mathrm{End}_k(V)$ qui définit la structure de représentation linéaire de G sur V ; autrement dit, $\hat{\pi}$ est le prolongement k-linéaire de π. Soit e l'élement $\left(\sum_{g \in G} g\right)/|G|$ de kG. L'opérateur de Reynolds sur V est $\natural = \hat{\pi}(e)$. Par définition, un homomorphisme de représentations est un homomorphisme de kG-modules, c'est-à-dire une application linéaire qui commute à l'action de kG. Cela donne l'assertion (iii). □

4.2.1.3 Corollaire.

Soit $\pi : G \to \mathbf{GL}(V)$ une représentation linéaire de dimension finie de G. Alors

$$\dim(\mathrm{inv}_G V) = \frac{1}{|G|} \sum_{g \in G} \chi_\pi(g).$$

Preuve. L'opérateur de Reynolds est un projecteur sur $\mathrm{inv}_G V$. La dimension de cet espace est donc égale à

$$\mathrm{tr}\,\natural = \mathrm{tr}\left(\frac{1}{|G|}\sum_{g\in G}\pi(g)\right) = \frac{1}{|G|}\sum_{g\in G}\mathrm{tr}\,\pi(g) = \frac{1}{|G|}\sum_{g\in G}\chi_\pi(g).$$

□

4.2.1.4 Théorème de Maschke. *Soient G un groupe fini, k un corps de caractéristique première à l'ordre de G, et V un k-espace vectoriel muni d'une action linéaire de G. Alors tout sous-espace vectoriel G-stable de V possède un supplémentaire G-stable.*

Preuve. Soit W un sous-espace vectoriel G-stable de V. On considère la représentation $E = \mathrm{Hom}_k(V,V)$ de G et on choisit un projecteur $p : V \to V$ d'image W. On regarde à présent l'action sur E de l'opérateur de Reynolds. L'application linéaire $p^\natural$ est définie par l'égalité

$$p^\natural(v) = \frac{1}{|G|}\sum_{g\in G} gp(g^{-1}v),$$

pour tout $v \in V$. Cette formule montre que $p^\natural$ prend ses valeurs dans W et que $p^\natural(w) = w$ pour chaque $w \in W$. Ainsi p est un projecteur sur W, de sorte que son noyau est un supplémentaire de W. Par ailleurs, $p^\natural$ est un élément G-invariant de E, donc appartient à $\mathrm{Hom}_G(V,V)$ (voir éventuellement l'exercice (1) du paragraphe 4.1.3). Son noyau est donc un sous-espace G-stable. C'est le supplémentaire G-stable de W cherché. □

Le théorème de Maschke affirme que tout kG-module est complètement réductible, autrement dit que l'algèbre kG est semi-simple [17].

Le théorème de Maschke a la conséquence très importante suivante, déjà signalée à la fin du paragraphe 4.1.4, et que nous ne répéterons jamais assez : quand k est de caractéristique 0, le caractère d'une représentation de dimension finie de G détermine cette représentation à isomorphisme près.

À présent, démontrons la première relation d'orthogonalité entre les caractères, selon les lignes de l'exercice (3) du paragraphe 3.3.1.

4.2.1.5 Proposition. *Soient G un groupe fini, k un corps de caractéristique première à $|G|$, et V et W deux k-espaces vectoriels munis d'une action linéaire de G. Alors*

$$\dim \mathrm{Hom}_G(V,W) = \frac{1}{|G|}\sum_{g\in G}\chi_V\big(g^{-1}\big)\chi_W\big(g\big).$$

Preuve. Le caractère de la représentation de G sur l'espace $\mathrm{Hom}_k(V,W)$ est la fonction centrale $(\chi_V)^*\chi_W$. Il suffit alors d'appliquer le corollaire 4.2.1.3 pour déterminer la dimension de l'espace $\mathrm{Hom}_G(V,W) = \mathrm{inv}_G \mathrm{Hom}_k(V,W)$. □

17. Pour une algèbre A de dimension finie sur un corps k, il y a équivalence entre les assertions : (i) toute représentation de dimension finie sur k est complètement réductible ; (ii) A est un anneau semi-simple ; (iii) tout A-module est complètement réductible. En fait, (i) entraîne que le A-module régulier à gauche est complètement réductible, d'où (ii) ; (ii) entraîne (iii) en vertu du théorème 2.1.2.1 ; et l'implication (iii) ⇒ (i) est banale.

Exercice. Soit k un corps algébriquement clos de caractéristique 0. Soit G un groupe et soit $\pi : G \to \mathbf{GL}(V)$ une représentation linéaire de G sur un k-espace vectoriel V. On regarde l'action par automorphismes de G sur l'algèbre $\mathsf{S}\, V^*$ des fonctions polynomiales sur V. Notons $I = \mathrm{inv}_G\big(\mathsf{S}\, V^*\big)$ le sous-espace des invariants de G dans $\mathsf{S}\, V^*$; ainsi $I \cap \mathsf{S}^n\, V^* = \mathrm{inv}_G\big(\mathsf{S}^n\, V^*\big)$.

(i) Vérifier que I est une sous-algèbre de $\mathsf{S}\, V^*$ et que $I = \bigoplus_{n\in\mathbf{N}}\big(I \cap \mathsf{S}^n\, V^*\big)$.

(ii) Soit $f \in \mathrm{End}_k(V)$, et soit $\{\xi_1, \ldots, \xi_p\}$ l'ensemble des valeurs propres de f, répétées selon leurs multiplicités. Introduisons une indéterminée t et étendons les scalaires de k à $k(t)$; ainsi $\mathrm{id} - tf$ est un endomorphisme du $k(t)$-espace vectoriel $k(t) \otimes_k V$. Vérifier que $\det(\mathrm{id} - tf) = \prod_{i=1}^{p}(1 - t\xi_i)$.

(iii) (Théorème de Molien) Montrer que dans l'anneau $k[[t]]$ des séries formelles en t,

$$\sum_{n\geq 0} t^n \dim_k\big(I \cap \mathsf{S}^n\, V^*\big) = \frac{1}{|G|}\sum_{g\in G}\frac{1}{\det(\mathrm{id} - t\pi(g))}.$$

4.2.2 Caractères irréductibles

Commençons avec un groupe fini G. Énumérons les classes de conjugaison de G : $\mathfrak{C}_1$, ..., $\mathfrak{C}_s$. Pour chaque $i \in \{1, \ldots, s\}$, posons $C_i = \sum_{g\in\mathfrak{C}_i} g$. Ainsi C_i est un élément de l'algèbre du groupe kG, appelé somme de la classe $\mathfrak{C}_i$.

4.2.2.1 Proposition. *Le centre $Z(kG)$ de l'algèbre du groupe de G est de dimension s sur k ; la famille $(C_i)_{1\leq i\leq s}$ en forme une base. L'espace vectoriel $\mathrm{cf}_k(G)$ est de dimension s.*

Preuve. Un élément $x = \sum_{g\in G} a_g g$ de kG appartient au centre de kG si et seulement si $yx = xy$ pour chaque $y \in kG$. Par linéarité, il suffit d'exiger que $hx = xh$ pour chaque $h \in G$. Multipliant à gauche par h^{-1}, cette condition se réécrit $\sum_{g\in G} a_g g = \sum_{g\in G} a_g h^{-1}gh$. Un changement de variable montre que le membre de droite est égal à $\sum_{g\in G} a_{hgh^{-1}} g$. Ainsi $x \in Z(kG)$ si et seulement si $a_g = a_{hgh^{-1}}$ pour chaque $(g, h) \in G^2$, autrement dit si et seulement si a_g ne dépend que de la classe de conjugaison à laquelle g appartient, et pas de g lui-même.

Ceci montre que chaque C_i appartient à $Z(kG)$, et que la famille $(C_i)_{1\leq i\leq s}$ engendre $Z(kG)$ en tant que k-espace vectoriel. Enfin, on voit que les C_i sont k-linéairement indépendants en observant qu'ils font intervenir des paquets disjoints de vecteurs de la base naturelle de kG.

De la même manière, on observe que les fonctions indicatrices des $\mathfrak{C}_i$ forment une base de $\mathrm{cf}_k(G)$; cet espace vectoriel est donc de dimension s. □

À présent, et jusqu'à la fin du paragraphe, nous supposons que le corps k est tel que l'algèbre kG est décomposée (voir le paragraphe 3.2.6). D'après la proposition 3.2.6.2, il suffit pour cela que k soit algébriquement clos ; en outre, on peut trouver un tel k qui est une extension finie de $\mathbf{Q}$ ou de $\mathbf{F}_p$. Afin de disposer des résultats du paragraphe 4.2.1, nous demandons que la caractéristique de k ne divise pas l'ordre de G.

D'après le théorème de Maschke, kG est une algèbre semi-simple. Le théorème 2.1.2.1 dit alors que kG s'écrit comme le produit de ses composantes simples. Il y en a autant que de

classes d'isomorphisme de kG-modules simples. Prenons un représentant de chacune des classes d'isomorphisme de kG-modules simples : S_1, ..., S_t. Pour chaque $m \in \{1, \ldots, t\}$, l'anneau des endomorphismes de S_m est $\mathrm{End}_G(S_m) = k$ id, d'après la proposition 3.2.6.1. Appelons z_m la dimension sur k de S_m. D'après le théorème de Wedderburn-Artin 2.1.1.1, la composante simple B_m de kG correspondant à S_m est isomorphe à $\mathbf{Mat}_{z_m}(k)$; en tant que B_m-module régulier à gauche, B_m est complètement réductible, somme directe de z_m sous-modules simples isomorphes à S_m. La remarque 2.1.2.4 dit enfin que l'annulateur dans kG du module S_m est $\bigoplus_{n \neq m} B_n$.

Ainsi $kG \cong \prod_{m=1}^{t} \mathbf{Mat}_{z_m}(k)$ en tant qu'anneau, et $kG \cong \bigoplus_{m=1}^{t} (S_m)^{\oplus z_m}$ en tant que kG-module à gauche (le membre de gauche est ici le kG-module à gauche régulier). Nous en déduisons l'égalité

$$|G| = \dim_k kG = \sum_{m=1}^{t} \dim_k \mathbf{Mat}_{z_m}(k) = \sum_{m=1}^{t} z_m^2.$$

Par ailleurs, le centre de kG est le produit des centres de chacune des algèbres $\mathbf{Mat}_{z_m}(k)$, d'où $Z(kG) \cong k^t$. Le nombre de classes d'isomorphismes de kG-modules simples (c'est-à-dire de représentations irréductibles de G sur k) est égal à la dimension sur k de $Z(kG)$.

4.2.2.2 Théorème. *Le groupe G possède autant de caractères irréductibles sur k que de classes de conjugaison. L'ensemble* $\mathrm{Irr}_k(G)$ *est une base de* $\mathrm{cf}_k(G)$.

Preuve. Le nombre t de classes d'équivalence de représentations irréductibles de G sur k est égal à la dimension du centre de kG. D'après la proposition 4.2.2.1, cette dimension est égale au nombre s de classes de conjugaison dans G.

Ceci établi, la proposition 4.2.2.1 affirme que la dimension de $\mathrm{cf}_k(G)$ est égale au nombre de caractères irréductibles de G sur k. Par ailleurs, ces caractères irréductibles forment une famille linéairement indépendante dans $\mathrm{cf}_k(G)$, d'après le théorème 4.1.4.4. □

Donnons-nous deux représentations k-linéaires irréductibles de G sur des espaces V et W. Si V et W ne sont pas isomorphes, alors $\mathrm{Hom}_G(V, W) = 0$, d'après le lemme de Schur. Si V et W sont isomorphes, alors $\mathrm{Hom}_G(V, W) \cong \mathrm{End}_G(V)$ est de dimension 1, d'après la proposition 3.2.6.1. La relation d'orthogonalité 4.2.1.5 s'écrit alors

$$\frac{1}{|G|} \sum_{g \in G} \chi_V\big(g^{-1}\big) \chi_W\big(g\big) = \begin{cases} 1 & \text{si } V \cong W, \\ 0 & \text{sinon.} \end{cases}$$

L'indépendance linéaire dans $\mathrm{cf}_k(G)$ des caractères des représentations irréductibles, proclamée dans le théorème 4.1.4.4, se déduit facilement de cette relation d'orthogonalité.

On note $\zeta^{(m)}$ le caractère de la représentation S_m. Ainsi, on a une énumération des caractères irréductibles de G sur k : $\mathrm{Irr}_k(G) = \big\{\zeta^{(1)}, \ldots, \zeta^{(s)}\big\}$. En général, on numérote de sorte que $\zeta^{(1)}$ soit le caractère de la représentation triviale : $\zeta^{(1)}(g) = 1$ pour tout $g \in G$. De la même façon, on arrange la numérotation des classes de conjugaison de sorte que $\mathfrak{C}_1 = \{1\}$.

On note h_i le nombre d'éléments dans la classe de conjugaison $\mathfrak{C}_i$; ainsi h_i est l'indice dans G du centralisateur de chaque élément dans $\mathfrak{C}_i$.

Pour chaque $i \in \{1, \ldots, s\}$, l'ensemble $\{g^{-1} \mid g \in \mathfrak{C}_i\}$ est une classe de conjugaison de G ; disons que c'est $\mathfrak{C}_{i^*}$. On définit ainsi une involution $i \mapsto i^*$ sur l'ensemble $\{1, \ldots, s\}$.

La fonction $\zeta^{(m)}$ prend une valeur constante sur $\mathfrak{C}_i$; on note $\zeta_i^{(m)}$ cette valeur.

4.2.2.3 Relations d'orthogonalité.

Avec les notations ci-dessus,

$$\sum_{i=1}^{s} h_i \zeta_i^{(m)} \zeta_{i^*}^{(n)} = \delta_{mn}|G| \quad et \quad \sum_{m=1}^{s} \zeta_i^{(m)} \zeta_{j^*}^{(m)} = \delta_{ij} \frac{|G|}{h_i}.$$

Preuve. La première relation a été vue au début de ce paragraphe, comme conséquence de la proposition 4.2.1.5. Introduisons la matrice $Z = (\zeta_i^{(m)})$, de taille $s \times s$. Ici m est l'indice de ligne et i est l'indice de colonne. Soit D la matrice diagonale, avec h_1, ..., h_s comme coefficients diagonaux. La relation d'orthogonalité que nous venons d'obtenir est $ZD\,{}^tZ = |G|I$. On en déduit que Z est inversible, d'inverse $\frac{1}{|G|} D\,{}^tZ$, d'où ${}^tZZ = |G|D^{-1}$. C'est notre seconde relation d'orthogonalité. □

4.2.2.4 Table des caractères. On prend k de caractéristique 0. La table des caractères de G est le tableau à s lignes et s colonnes formé des valeurs des $\zeta_j^{(i)}$.

(1) Les degrés des caractères irréductibles sont dans la table de caractères : $z_m = \zeta_1^{(m)}$. (Noter ici que l'entier z_m est entièrement déterminé par son image dans k, vu que k est de caractéristique 0.)

(2) En faisant $i = j = 1$ dans la seconde relation d'orthogonalité, on trouve $\sum_{m=1}^{s} z_m^2 = |G|$. Cette information nous était aussi livrée par nos considérations au début de ce paragraphe.

(3) La remarque précédente montre que la table des caractères contient assez d'information pour qu'on puisse déterminer l'ordre de G. En utilisant la seconde relation d'orthogonalité, on voit que les h_i sont eux aussi déterminés par la table des caractères.

4.2.2.5 (In)dépendance par rapport au choix du corps k. La théorie des caractères est essentiellement indépendante du choix de k, pourvu que celui-ci soit de caractéristique 0 et que l'algèbre kG soit décomposée. Expliquons brièvement pourquoi.

Prenons d'abord un corps k de caractéristique 0 et tel que l'algèbre kG soit décomposée. Soit K une extension de k. Alors l'algèbre KG est décomposée (proposition 3.2.6.2 (ii)). Chaque représentation irréductible $X : G \to \mathbf{GL}_n(k)$ de G sur k fournit alors par extension des scalaires une représentation de G sur K, et cette dernière est irréductible, par définition du fait que kG est décomposée. On obtient ainsi une bijection entre classes d'isomorphisme de représentations de G sur k et classes d'isomorphisme de représentation de G sur K. Plus précisément, appelant ι le plongement de k dans K, l'application $\chi \mapsto \iota \circ \chi$ est une bijection de $\mathrm{Irr}_k(G)$ sur $\mathrm{Irr}_K(G)$.

Maintenant, soient k et k' sont deux corps de caractéristique 0 tels que les algèbres kG et $k'G$ soient décomposées. On peut alors trouver une extension commune K de k et k' : il suffit de prendre un quotient de $k \otimes_{\mathbf{Z}} k'$ par un idéal maximal. Les plongements $k \hookrightarrow K$ et $k' \hookrightarrow K$ induisent des bijections $\mathrm{Irr}_k(G) \cong \mathrm{Irr}_K(G) \cong \mathrm{Irr}_{k'}(G)$, dans lesquelles les tables des caractères de G sur k, K et k' se trouvent identifiées.

Des considérations analogues valent quand k et k' sont de caratéristique différentes. Soit en effet p un nombre premier qui ne divise pas l'ordre de G. Soit K une extension finie du corps $\mathbf{Q}_p$ des nombres p-adiques telle que l'algèbre KG soit décomposée (l'existence de K est assurée par la proposition 3.2.6.2 (iv)). Soit $\mathscr{O}$ l'anneau des entiers de K, soit k le corps résiduel de $\mathscr{O}$. Alors k est de caractéristique p. Quitte à grossir K, on peut supposer que l'algèbre kG est décomposée. On peut alors mettre en place une correspondance bijective entre caractères de KG et caractères de kG. Cela se fait en passant par les $\mathscr{O}G$-modules projectifs, voir par exemple [6], §82. Dans notre contexte $p \nmid |G|$, la matrice de décomposition est nécessairement une matrice de permutation (on le montre en utilisant que le nombre de caractères irréductibles et la somme des degrés des caractères irréductibles est le même sur k et sur K).

Exercices.

(1) Déterminer les degrés des caractères irréductibles du groupe alterné $\mathfrak{A}_5$.

(2) Comparer les tables des caractères du groupe diédral D_4 et du groupe quaternionique Q, tous deux d'ordre 8.

(3) Dresser la table des caractères du groupe alterné $\mathfrak{A}_4$ et construire les représentations correspondantes.

(4) Soient k un corps algébriquement clos de caractéristique zéro, G un groupe fini et H un sous-groupe distingué de G. Considérant l'action de G sur G/H par translations à gauche, on construit une représentation de permutation V de G sur k. Déterminer les multiplicités des représentations simples dans V. (Indication : considérer V comme une représentation de G/H plutôt que comme une représentation de G.)

(5) (Calcul du *Gruppendeterminant*) Soit G un groupe fini. On conserve les notations introduites plus haut : s est le nombre de classes de conjugaison, les z_m sont les dimensions des kG-modules simples. On introduit une famille d'indéterminées $(x_g)_{g\in G}$. On regarde la matrice $(x_{gh^{-1}})_{(g,h)\in G^2}$, dont les lignes et les colonnes sont indexées par G. Son déterminant Δ est un polynôme à coefficients entiers, homogène de degré $|G|$. Montrer que la factorisation de Δ sur $\mathbf{C}$ en produit de facteurs irréductibles s'écrit $\delta_1^{z_1} \cdots \delta_s^{z_s}$, où chaque δ_m est homogène de degré z_m en les indéterminées x_g. (Indication : on considère l'élément $X = \sum_{g\in G} x_g g$, qui vit dans l'algèbre du groupe de G à coefficients dans l'anneau des polynômes en les x_g. La matrice de l'énoncé donne l'action de X dans la représentation régulière. L'isomorphisme $\mathbf{C}G \cong \prod_{m=1}^{s} \mathbf{Mat}_{z_m}(\mathbf{C})$ conduit à réécrire X comme une famille (Y_m) de matrices : les coefficients $y_{m,i,j}$ de Y_m sont des polynômes homogènes de degré 1 en les x_g, algébriquement indépendants. Soit δ_m le déterminant de la matrice Y_m. Le résultat annoncé traduit le fait que chaque représentation simple de G intervient dans la représentation régulière avec une multiplicité égale à son degré.)

4.2.3 Un peu d'analyse hilbertienne

Dans ce paragraphe, nous prenons $k = \mathbf{C}$. Soit G un groupe fini. Une représentation complexe de G est une représentation $\mathbf{C}$-linéaire de G. Un caractère complexe de G est le caractère d'une représentation $\mathbf{C}$-linéaire de G ; c'est une fonction de G dans $\mathbf{C}$.

4.2.3.1 Proposition. *Soit G un groupe fini et ζ un caractère complexe de G de degré $n = \zeta(1)$.*

(i) Chaque valeur $\zeta(g)$ est une somme de n racines $|G|$-ièmes de l'unité. On a $\zeta^* = \overline{\zeta}$, où le membre de droite est le conjugué complexe de ζ.

(ii) Soit $X : G \to \mathbf{GL}_n(\mathbf{C})$ une représentation matricielle de G dont ζ est le caractère. Pour chaque $g \in G$, $|\zeta(g)| \leq \zeta(1)$, avec égalité si et seulement si $X(g)$ est une matrice scalaire.

Preuve. Adoptons les notations de l'énoncé. Posons $N = |G|$. Soit $g \in G$. Alors $g^N = 1$, donc $X(g)^N = I$, ce qui montre que $X(g)$ annule le polynôme $T^n - 1$. Ce polynôme étant séparable sur k (sans racine multiple), $X(g)$ est diagonalisable, et ses valeurs propres ξ_1, ..., ξ_n (répétées selon leurs multiplicités) sont des racines de $T^N - 1$ dans k.

On a alors $\zeta(g) = \xi_1 + \cdots + \xi_n$. Puisque les valeurs propres de $X\big(g^{-1}\big)$ sont ξ_1^{-1}, ..., ξ_n^{-1}, avec multiplicité, on a aussi

$$\zeta^*\big(g\big) = \zeta\big(g^{-1}\big) = \xi_1^{-1} + \cdots + \xi_n^{-1} = \overline{\xi_1} + \cdots + \overline{\xi_n} = \overline{\zeta(g)}.$$

Enfin pour que $|\zeta(g)| = n$, il faut et il suffit que les ξ_i soient tous égaux. Alors $X(g)$ est semblable, donc égale, à une matrice scalaire. □

L'assertion (i) de la proposition 4.2.3.1 explique comment se lit l'involution $i \mapsto i^*$ sur la table des caractères complexes de G : on a $\zeta_{i^*}^{(m)} = \overline{\zeta_i^{(m)}}$ pour chaque $m\{1, \ldots, s\}$.

On définit un produit scalaire hermitien sur l'espace $\mathbf{C}^G$ des fonctions sur G à valeurs complexes en posant

$$(\varphi, \psi)_G = \frac{1}{|G|} \sum_{g \in G} \overline{\varphi(g)} \psi(g)$$

pour $\varphi, \psi \in \mathbf{C}^G$. Par restriction, le sous-espace $\mathrm{cf}_{\mathbf{C}}(G)$ des fonctions de classe est alors muni lui aussi d'un produit scalaire hermitien.

4.2.3.2 Proposition.

(i) La famille $\mathrm{Irr}_k(G)$ est une base orthonormée de $\mathrm{cf}_{\mathbf{C}}(G)$.

(ii) Soient deux représentations linéaires V et W de G sur $\mathbf{C}$. Alors $\dim \mathrm{Hom}_G(V, W) = (\chi_V, \chi_W)_G$.

(iii) Décomposons une représentation linéaire de G sur un $\mathbf{C}$-espace vectoriel V en somme directe de sous-représentations simples. Alors la multiplicité avec laquelle la représentation simple de caractère $\zeta^{(m)}$ apparaît dans V est égale à $(\zeta^{(m)}, \chi_V)_G$.

(iv) *Une fonction* $\varphi \in \mathrm{cf}_{\mathbf{C}}(G)$ *appartient à l'anneau des caractères virtuels* $\mathrm{ch}\,\mathbf{C}G$ *si et seulement si* $(\zeta^{(m)}, \varphi)_G \in \mathbf{Z}$ *pour chaque* $m \in \{1, \ldots, s\}$.

(v) *Une fonction centrale* $\varphi : G \to \mathbf{C}$ *est un caractère irréductible si et seulement si*
(a) $\varphi \in \mathrm{ch}\,\mathbf{C}G$; *(b)* $(\varphi, \varphi)_G = 1$; *(c)* $\varphi(1) \geq 0$.

Preuve. Le théorème 4.2.2.2 dit que $\mathrm{Irr}_{\mathbf{C}}(G)$ est une base de $\mathrm{cf}_{\mathbf{C}}(G)$. Compte-tenu de la proposition 4.2.3.1, l'assertion (i) découle directement de la première relation d'orthogonalité 4.2.2.3.

L'assertion (ii) est la relation d'orthogonalité 4.2.1.5.

Considérons une représentation de G sur un espace vectoriel V. Décomposons cette représentation en somme directe de sous-représentations simples et appelons a_m la multiplicité avec laquelle la représentation simple de caractère $\zeta^{(m)}$ intervient. Alors $\chi_V = \sum_{m=1}^{s} a_m \zeta^{(m)}$. D'après (i), on a donc $a_m = (\zeta^{(m)}, \chi_V)$.

Pour chaque fonction de classe φ, nous pouvons écrire, compte-tenu de (i),

$$\varphi = \sum_{m=1}^{s} (\zeta^{(m)}, \varphi)_G \ \zeta^{(m)}.$$

L'assertion (iv) est ainsi une réécriture du théorème 4.1.4.5.

Enfin, soit φ une fonction centrale vérifiant les conditions (a), (b) et (c) de l'énoncé (v). Écrivons $\varphi = \sum_{m=1}^{s} a_m \zeta^{(m)}$. La condition (a) signifie que chaque a_m appartient à $\mathbf{Z}$. La condition (b) s'écrit $\sum_{m=1}^{s} |a_m|^2 = 1$; compte tenu de (a), tous les a_m sont nuls sauf un, qui vaut ± 1. La condition (c) impose alors que le a_m non-nul est $+1$. Alors $\varphi = \zeta^{(m)}$ est bien un caractère irréductible. □

Exemple et application.

(1) Le caractère ρ de la représentation régulière de G est donné par

$$\rho(g) = \begin{cases} |G| & \text{si } g = 1, \\ 0 & \text{si } g \neq 1. \end{cases}$$

D'après la proposition 4.2.3.2 (iii), la multiplicité avec laquelle la représentation linéaire de caractère $\zeta^{(m)}$ apparaît dans $\mathbf{C}G$ est égale au produit scalaire $(\zeta^{(m)}, \rho)_G = \zeta^{(m)}(1) = z_m$. On retrouve par cette voie l'isomorphisme $\mathbf{C}G \cong \bigoplus_{m=1}^{s} (S_m)^{\oplus z_m}$ du début du paragraphe 4.2.2.

(2) Les caractères irréductibles de G forment une base de l'algèbre $\mathrm{cf}_{\mathbf{C}}G$ des fonctions de classe. Les constantes de structure (c'est-à-dire la table de multiplication) de cette algèbre dans cette base décrivent la façon dont le produit tensoriel de deux représentations simples se décompose en somme directe de représentations simples. Utilisant la proposition 4.2.3.2 (iii), nous obtenons le résultat suivant : étant données trois représentations irréductibles de G sur des espaces vectoriels complexes L, M et N, la multiplicité avec laquelle L apparaît dans le produit tensoriel $M \otimes_{\mathbf{C}} N$ est égale au produit scalaire $(\chi_L, \chi_M \chi_N)_G$.

D'autres propriétés des représentations de groupes s'inscrivent agréablement dans le cadre de l'analyse hilbertienne. Le lecteur est ici invité à consulter le paragraphe 4.4.6 ; il y trouvera notamment une autre voie d'accès au théorème de Maschke 4.2.1.4 et à une partie de la proposition 4.2.3.1.

EXERCICE. Soient G et H deux groupes finis. À $(\varphi, \psi) \in \mathrm{cf}_{\mathbf{C}}(G) \times \mathrm{cf}_{\mathbf{C}}(H)$, on associe la fonction $\varphi \times \psi : (g, h) \mapsto \varphi(g)\psi(h)$ sur $G \times H$. Montrer que l'application $(\varphi, \psi) \mapsto \varphi \times \psi$ induit une bijection de $\mathrm{Irr}_{\mathbf{C}}(G) \times \mathrm{Irr}_{\mathbf{C}}(H)$ sur $\mathrm{Irr}_{\mathbf{C}}(G \times H)$.

4.2.4 Cas particulier des groupes abéliens

En appliquant le corollaire 3.2.7.2 à l'algèbre d'un groupe, on obtient le résultat suivant.

4.2.4.1 Proposition. *Soient G un groupe abélien et k un corps algébriquement clos. Alors toute représentation irréductible de G est de degré* 1.

Le cas des groupes abéliens est ainsi relativement simple. On cherche donc à y ramener le cas d'un groupe G quelconque. Cela peut être fait de deux manières : en regardant des quotients commutatifs de G ou en regardant les sous-groupes commutatifs de G. Regardons à ce propos les quotients commutatifs de G.

Sous-groupe dérivé : soit G un groupe. Le sous-groupe dérivé de G est le sous-groupe de G engendré par les commutateurs $(g, h) = ghg^{-1}h^{-1}$, avec $(g, h) \in G^2$. C'est un sous-groupe distingué, noté G' ou $D(G)$.

Le sous-groupe dérivé G' est contenu dans le noyau de tout homomorphisme de G dans un groupe abélien. Le groupe quotient G/G' est le plus grand quotient abélien de G, au sens où un sous-groupe distingué H de G contient G' si et seulement si G/H est abélien.

Un caractère linéaire d'un groupe G, c'est-à-dire un homomorphisme de G dans k^* (voir le paragraphe 4.1.2.2), se factorise ainsi à travers l'abélianisé G/G'. Il y a donc une bijection canonique entre l'ensemble des caractères linéaires de G et l'ensemble des caractères linéaires de G/G'. En outre si k est algébriquement clos, ce dernier est l'ensemble des caractères irréductibles de G/G', d'après la proposition 4.2.4.1.

Revenons au cas particulier d'un groupe abélien fini G. Pour fixer les choses, nous prenons $k = \mathbf{C}$. Pour G, les notions de (classes d'équivalence de) représentation irréductible, de caractère irréductible, et de caractère linéaire sont identiques. Plutôt que $\mathrm{Irr}_{\mathbf{C}}(G)$, nous noterons dans ce paragraphe $G^\wedge$ l'ensemble des caractères irréductibles de G. D'après le théorème 4.2.2.2, c'est un ensemble qui possède autant d'éléments que G, puisque les classes de conjugaison de G sont réduites à un élément.

Nous savons que l'ensemble des caractères linéaires de G est un groupe (paragraphe 4.1.2.2) [18]. On peut en fait voir $G^\wedge$ comme un ensemble de fonctions jamais nulles de G à valeurs com-

18. En utilisant le théorème 4.1.4.3 (iv), on voit que le produit sur $G^\wedge$ n'est autre que le produit tensoriel des représentations.

plexes, c'est-à-dire comme un sous-groupe du groupe des éléments inversibles de l'algèbre $\mathbf{C}^G$. Le théorème 4.2.2.2 dit que $G^\wedge$ est une base de $\mathbf{C}^G$. Nous pouvons donc identifier l'algèbre du groupe $\mathbf{C}G^\wedge$ à l'algèbre $\mathbf{C}^G$.

Enfin comme $G^\wedge$ est un groupe abélien fini, on peut itérer la construction et considérer $(G^\wedge)^\wedge$. Chaque élément $g \in G$ fournit alors un caractère linéaire de $G^\wedge$, à savoir l'évaluation $\mathrm{ev}_g : \lambda \mapsto \lambda(g)$. On obtient ainsi un homomorphisme ev de G dans $(G^\wedge)^\wedge$.

4.2.4.2 Théorème. *Soient G et H deux groupes abéliens finis. Conservons les notations ci-dessus.*

(i) L'application $\mathrm{ev} : G \to (G^\wedge)^\wedge$ *est un isomorphisme de groupes.*

(ii) À deux caractères linéaires $\lambda \in G^\wedge$ et $\mu \in H^\wedge$, associons le caractère linéaire $\lambda \times \mu : (g,h) \mapsto \lambda(g)\mu(h)$ de $G \times H$. Alors l'application $(\lambda, \mu) \mapsto \lambda \times \mu$ est un isomorphisme de groupes de $G^\wedge \times H^\wedge$ sur $(G \times H)^\wedge$.

(iii) Les groupes G et $G^\wedge$ sont isomorphes.

Preuve. Soient g et h deux éléments distincts de G. L'espace des fonctions $\zeta : G \to \mathbf{C}$ qui prennent la même valeur en g et en h est un hyperplan de $\mathbf{C}^G$. En tant que base de $\mathbf{C}^G$, $G^\wedge$ ne peut pas être inclus dans cet hyperplan. Il existe donc $\lambda \in G^\wedge$ tel que $\lambda(g) \neq \lambda(h)$. Cela signifie que $\mathrm{ev}_g \neq \mathrm{ev}_h$. Ainsi ev est un homomorphisme injectif de groupes. Pour des raisons de cardinalité, c'est un isomorphisme. Nous avons montré (i).

L'assertion (ii) est de démonstration immédiate : avec les notations de l'énoncé, on vérifie que $\lambda \times \mu$ est bien un caractère linéaire de $G \times H$ et que l'application $(\lambda, \mu) \mapsto \lambda \times \mu$ est un homomorphisme injectif de groupes. On conclut en remarquant que $G^\wedge \times H^\wedge$ et $(G \times H)^\wedge$ ont même ordre.

L'exemple 4.1.2.3 montre que si G est un groupe cyclique d'ordre n, alors $G^\wedge$ est isomorphe au groupe des racines n-ièmes de l'unité dans $\mathbf{C}$, lequel est aussi cyclique. L'assertion (iii) vaut donc quand G est cyclique. Grâce à (iii) et au théorème de structure des groupes abéliens finis (exemple 1.2.3.7), elle vaut aussi dans le cas général. □

On peut pousser plus loin le développemement de cette théorie. D'une part, on peut mettre en place une correspondance entre sous-groupes de G et quotients de $G^\wedge$ (et vice-versa). Ensuite, on peut identifier $\mathbf{C}^G$ au dual de $\mathbf{C}G$ et $\mathbf{C}^{G^\wedge}$ au dual de $\mathbf{C}G^\wedge$ (voir la remarque 4.1.4.2) ; ceci fait, la transposée de l'isomorphisme $\mathbf{C}G^\wedge \cong \mathbf{C}^G$ du (ii) de la proposition ci-dessus s'identifie à l'isomorphisme $\mathbf{C}G \cong \mathbf{C}^{G^\wedge}$. Enfin, cette théorie n'est autre que la transformation de Fourier discrète. Elle rejoint la théorie des séries de Fourier et de la transformation de Fourier dans le cadre plus vaste de la dualité de Pontrjagin entre groupes localement compacts abéliens ; pour plus de détails, je renvoie à Walter Rudin, *Fourier analysis on groups,* Pure and Applied Mathematics, Vol. XII, Interscience Publishers (John Wiley & Sons), 1962.

Exercice. Soit G un groupe fini. Montrer que le nombre de caractères linéaires de G est égal à l'indice dans G du sous-groupe dérivé G'.

4.2.5 Centre de l'algèbre du groupe

Nous reprenons notre groupe fini G et un corps k algébriquement clos de caractéristique première à $|G|$.

D'après la proposition 3.2.7.1, chaque représentation linéaire irréductible $\pi : G \to \mathbf{GL}(V)$ de G sur un k-espace vectoriel de dimension finie possède un caractère central : il existe un homomorphisme de k-algèbres $\omega : Z(kG) \to k$ tel que pour chaque $x \in Z(kG)$, $\pi(x) = \omega(x)\,\mathrm{id}_V$. De plus, deux représentations irréductibles équivalentes ont même caractère central.

Nous nous étions donné une énumération $\zeta^{(1)}$, ..., $\zeta^{(s)}$ des caractères irréductibles de G. Elle correspond à une énumération S_1, ..., S_s des représentations irréductibles de G. Nous noterons $\omega^{(1)}$, ..., $\omega^{(s)}$ les caractères centraux de ces représentations.

Concomitamment, nous avons une énumération B_1, ..., B_s des composantes simples de l'algèbre kG. Appelons ε_m le neutre multiplicatif de l'algèbre B_m : dans l'isomorphisme $B_m \cong \mathbf{Mat}_{z_m}(k)$, ε_m correspond à la matrice identité. Le centre de B_m est donc la droite $k\varepsilon_m$, ce qui montre que la famille $(\varepsilon_1, \ldots, \varepsilon_s)$ est une base de $Z(kG)$. La base duale de cette famille n'est autre que $\big(\omega^{(1)}, \ldots, \omega^{(s)}\big)$, car l'élément ε_m agit par l'identité sur S_m et par zéro sur les S_n pour $n \neq m$.

Notons enfin que les ε_m sont des idempotents ; en fait, ce sont les idempotents primitifs de $Z(kG)$ (voir le paragraphe 2.4.1 pour plus de détails).

Nous disposons donc de deux bases de $Z(kG)$: la base $(C_1, \ldots, C_s)$ formée des sommes de classe, et la base $(\varepsilon_1, \ldots, \varepsilon_s)$ des idempotents primitifs de $Z(kG)$. Nous voulons déterminer la matrice de passage entre ces deux bases. Pour cela, nous nous plaçons dans le cas où k est de caractéristique 0 et nous posons $\omega_i^{(m)} = \omega^{(m)}(C_i)$. Appelant $X^{(m)}$ une représentation matricielle de caractère $\zeta^{(m)}$ et prenant la trace de l'équation $X^{(m)}(C_i) = \omega_i^{(m)} I$, nous obtenons

$$z_m \omega_i^{(m)} = h_i \zeta_i^{(m)}.$$

4.2.5.1 Proposition. *Les idempotents primitifs centraux sont reliés aux sommes de classe par les formules*

$$C_i = h_i \sum_{m=1}^{s} \frac{\zeta_i^{(m)}}{z_m} \varepsilon_m \quad \textit{et} \quad \varepsilon_m = \frac{z_m}{|G|} \sum_{i=1}^{s} \zeta_{i^*}^{(m)} C_i.$$

Preuve. Comme $(\omega^{(1)}, \ldots, \omega^{(s)})$ est la base duale de la base $(\varepsilon_1, \ldots, \varepsilon_s)$, on a

$$C_i = \sum_{i=1}^{s} \omega^{(m)}(C_i)\varepsilon_m = \sum_{i=1}^{s} \omega_i^{(m)} \varepsilon_m.$$

La matrice de passage de la base (ε_m) à la base C_i est donc $(h_i \zeta_i^{(m)}/z_m)$. Les relations d'orthogonalité 4.2.2.3 montrent que l'inverse de cette matrice est $(z_m \zeta_{i^*}^{(m)}/|G|)$. Cela donne la seconde égalité. □

Dans la base des sommes de classe, l'élément neutre pour la multiplication est C_1. La multiplication s'écrit avec des formules $C_iC_j = \sum_{k=1}^{s} c_{ijk}C_k$, où pour chaque $z \in \mathfrak{C}_k$, c_{ijk} est le nombre de couples $(x, y) \in \mathfrak{C}_i \times \mathfrak{C}_j$ tels que $xy = z$. Les c_{ijk} sont des entiers naturels.

En revanche, dans la base des idempotents primitifs, la multiplication de $Z(kG)$ est donnée par une règle très simple : $\varepsilon_m\varepsilon_n = \delta_{mn}\varepsilon_m$, l'élement neutre étant $1 = \varepsilon_1 + \cdots + \varepsilon_s$.

Le passage de la base « naturelle » de $Z(kG)$ donnée par les sommes de classe à la base des idempotents primitifs fournie par la théorie des représentations permet de passer d'une table de multiplication compliquée à une table de multiplication très simple. Le coût de cette opération est la connaissance de la table des caractères de G. Il n'y a donc rien de surprenant à ce que la connaissance de la table des caractères de G entraîne celle des constantes c_{ijk}. Une formule fermée existe :

$$c_{ijk} = \frac{h_ih_j}{|G|} \sum_{m=1}^{s} \frac{\zeta_i^{(m)}\zeta_j^{(m)}\zeta_{k^*}^{(m)}}{z_m}.$$

Réciproquement, la connaissance des c_{ijk} permet de calculer la table des caractères de G. La proposition suivante explique comment déterminer les $\omega_i^{(m)}$ en fonction des c_{ijk}.

4.2.5.2 Proposition. *Fixons $i \in \{1, \ldots, s\}$. Alors $\left(\omega_i^{(1)}, \ldots, \omega_i^{(s)}\right)$ sont les valeurs propres de la matrice $(c_{ijk})_{1\leq j,k\leq s}$, avec multiplicité.*

Preuve. Appliquant le caractère central $\omega^{(m)}$ à la relation $C_iC_j = \sum_{k=1}^{s} c_{ijk}C_k$, nous obtenons $\omega_i^{(m)}\omega_j^{(m)} \sum_{k=1}^{s} c_{ijk}\omega_k^{(m)}$. Cette relation dit que le vecteur $\left(\omega_1^{(m)}, \ldots, \omega_s^{(m)}\right)$ est un vecteur propre de la matrice $(c_{ijk})_{1\leq j,k\leq s}$ pour la valeur propre $\omega_i^{(m)}$.

Par ailleurs, les relations d'orthogonalité s'écrivent ici

$$\sum_{j=1}^{s} \frac{1}{h_j}\omega_j^{(m)}\omega_{j^*}^{(n)} = \frac{|G|}{z_mz_n}\delta_{mn}$$

pour $1 \leq m, n \leq s$. Étant orthogonaux, les vecteurs $\left(\omega_1^{(m)}, \ldots, \omega_s^{(m)}\right)$ sont linéairement indépendants, pour $1 \leq m \leq s$. Nous avons ainsi décrit une base de diagonalisation pour la matrice $(c_{ijk})_{1\leq j,k\leq s}$. □

Ainsi la connaissance des constantes de structures c_{ijk} permet en théorie de déterminer les $\omega_i^{(m)}$. Elle donne également les $h_i = c_{ii^*1}$. On trouve alors les degrés z_m par la relation

$$\sum_{i=1}^{s} \frac{1}{h_i}\omega_i^{(m)}\omega_{i^*}^{(m)} = \frac{|G|}{z_m^2},$$

puis enfin les $\zeta_i^{(m)} = z_m\omega_i^{(m)}/h_i$.

À présent, et jusqu'à la fin de ce paragraphe, nous prenons pour k un sous-corps algébriquement clos de $\mathbf{C}$. La proposition précédente a alors un corollaire remarquable.

4.2.5.3 Corollaire. *Les $\omega_i^{(m)}$ sont des entiers algébriques.*

Preuve. Fixons $i \in \{1, \ldots, s\}$. La proposition 4.2.5.2 affirme que $\omega_i^{(m)}$ est une valeur propre de la matrice à coefficients entiers $(c_{ijk})_{1 \leq j,k \leq s}$. Le polynôme caractéristique de cette matrice, qui est unitaire et à coefficients entiers, annule donc $\omega_i^{(m)}$. Ceci montre que ce nombre est un entier algébrique. □

4.2.5.4 Théorème. *Le degré de chaque caractère irréductible de G divise $|G|$.*

Preuve. Insérant $z_m \omega_i^{(m)} = h_i \zeta_i(m)$ dans la première relation d'orthogonalité 4.2.2.3, nous obtenons

$$\sum_{i=1}^{s} \omega_i^{(m)} \zeta_{i^*}^{(m)} = \frac{|G|}{z_m}.$$

Maintenant, chaque $\omega_i^{(m)}$ est un entier algébrique d'après le corollaire 4.2.5.3 et chaque $\zeta_{i^*}^{(m)}$ est un entier algébrique d'après la proposition 4.2.3.1. Ainsi $|G|/z_m$ est un entier algébrique. Comme c'est un rationnel, c'est un entier. □

Exercice. Soit G un groupe fini et $g \in G$. Montrer que le nombre de couples $(x, y) \in G^2$ tels que $g = xyx^{-1}y^{-1}$ est égal à

$$|G| \sum_{\zeta \in \mathrm{Irr}_{\mathbf{C}}(G)} \frac{\zeta(g)}{\zeta(1)}.$$

(Indication : soit $\mathfrak{C}_1$, ..., $\mathfrak{C}_s$ une énumération des classes de conjugaison dans G. Prenons une représentation irréductible complexe de G, de caractère ζ et de caractère central ω. Pour chaque $i \in \{1, \ldots, s\}$, notons ζ_i la valeur de ζ en un point de $\mathfrak{C}_i$ et ω_i la valeur de ω sur la somme de classe $C_i = \sum_{g \in \mathfrak{C}_i} g$. Montrer qu'alors

$$\frac{1}{|G|} \sum_{(x,y) \in G^2} \zeta\big(xyx^{-1}y^{-1}\big) = \sum_{i=1}^{s} \zeta_i \omega_{i^*} = \frac{|G|}{\zeta(1)}.$$

Conclure en observant que la quantité $\varphi(g)$ cherchée définit une fonction de classe $\varphi \in \mathrm{cf}_{\mathbf{C}} G$.)

4.2.6 Théorème $p^a q^b$ de Burnside

Nous en arrivons à un très beau résultat, prouvé par Burnside en 1911. La théorie des caractères fournit une preuve particulièrement courte et élégante. Rappelons qu'un groupe est dit simple s'il ne possède pas de sous-groupe distingué non-banal.

4.2.6.1 Proposition. *Soient q un nombre premier et d un entier strictement positif. Un groupe G ayant une classe de conjugaison de cardinal q^d ne peut pas être simple.*

Preuve. Soit k une extension finie de $\mathbf{Q}$ telle que l'algèbre de groupe kQ soit décomposée (l'existence de k est assurée par la proposition 3.2.6.2). Nous pouvons plonger k dans $\mathbf{C}$. Nous utilisons nos notations habituelles $\mathfrak{C}_i$, $\zeta_i^{(m)}$, etc. Appelant $\mathscr{O}$ l'anneau des éléments de k entiers sur $\mathbf{Z}$, la proposition 4.2.3.1 montre que chaque $\zeta_i^{(m)}$ appartient à $\mathscr{O}$.

Supposons que G soit un groupe ayant une classe de conjugaison, disons $\mathfrak{C}_j$, de cardinal $h_j = q^d$. De la seconde relation d'orthogonalité

$$0 = \sum_{m=1}^{s} \zeta_1^{(m)} \zeta_j^{(m)} = 1 + \sum_{m=2}^{s} z_m \zeta_j^{(m)},$$

on tire l'existence d'un $m > 1$ tel que $z_m \zeta_j^{(m)} \notin q\mathscr{O}$, et donc tel que $q \nmid z_m$ et $\zeta_j^{(m)} \neq 0$.

Le corollaire 4.2.5.3 dit que $\omega_j^{(m)} = h_j \zeta_j^{(m)} / z_m$ est un entier algébrique. Comme h_j et z_m sont premiers entre eux, $\upsilon = \zeta_j^{(m)} / z_m$ est aussi un entier algébrique. (Pour le voir, on multiplie υ par une relation de Bézout $1 = ah_j + bz_m$; chaque terme de la somme donnant υ appartient alors à $\mathscr{O}$, d'où $\upsilon \in \mathscr{O}$.)

La proposition 4.2.3.1 dit que $\zeta_j^{(m)}$ est somme de z_m racines complexes de l'unité. Il en est de même des conjugués algébriques de ce nombre. Cela entraîne que les conjugués algébriques de $\zeta_j^{(m)}$ sont tous de module au plus z_m. Les conjugués algébriques de υ sont donc tous de module au plus 1. Le produit Υ de tous les conjugués de υ est donc de module au plus 1, avec égalité si et seulement si $|\upsilon| = 1$.

Un peu de théorie de Galois à présent : Υ est un nombre rationnel. C'est aussi un entier algébrique. C'est donc un entier rationnel. Comme $\zeta_j^{(m)} \neq 0$, on a $\upsilon \neq 0$, et donc $\Upsilon \neq 0$. L'inégalité $|\Upsilon| \leq 1$ de l'alinéa précédent est donc une égalité, ce qui force $|\upsilon| = 1$, c'est-à-dire $\left|\zeta_j^{(m)}\right| = z_m$.

D'après la proposition 4.2.3.1, cela signifie que dans la représentation matricielle X dont $\zeta^{(m)}$ est le caractère, chaque élément de $\mathfrak{C}_j$ est envoyé sur une matrice scalaire. L'image réciproque par X de l'ensemble des matrices scalaires est alors un sous-groupe distingué de G qui contient $\mathfrak{C}_j$.

À présent, raisonnons par l'absurde. Supposons que G soit simple. Alors ce sous-groupe est G tout entier. Autrement dit, chaque élément de G est représenté par une matrice scalaire. Comme X est une représentation irréductible, elle est de degré 1. Comme $m > 1$, cela entraîne que G possède au moins deux caractères linéaires. Or tout caractère linéaire se factorise à travers l'abélianisé G/G' de G (paragraphe 4.2.4). L'existence de deux caractères distincts se factorisant à travers G/G' interdit à G/G' d'être réduit à un seul élément. Ainsi G' est un sous-groupe distingué de G différent de G. Mais G est supposé simple. Finalement, G' est réduit à l'élément neutre, donc G est abélien. Nous obtenons alors une contradiction avec l'hypothèse que G possède une classe de conjugaison de cardinal $q^d > 1$. Cette contradiction montre que G est simple. □

4.2.6.2 Théorème. *Un groupe fini dont l'ordre est de la forme $p^a q^b$, avec p et q deux nombres premiers, ne peut être simple que s'il est cyclique d'ordre premier.*

Preuve. Supposons qu'il existe un groupe simple non-abélien d'ordre $p^a q^b$. Alors le centre de G est réduit à l'élément neutre (c'est un sous-groupe distingué de G, différent de G tout entier puisque G n'est pas abélien).

Soit P un p-Sylow de G. Soit h un élément du centre de P autre que l'élément neutre. Le centralisateur $C_G(h)$ de h dans G est un sous-groupe de G qui contient P. L'indice dans G de $C_G(h)$ divise l'indice de P, donc est de la forme q^d. Certainement $d > 0$, car h n'appartient pas au centre de G. Le cardinal de la classe de conjugaison de h est alors égal à q^d, et nous nous trouvons donc en situation d'appliquer la proposition 4.2.6.1. La contradiction que nous obtenons montre l'absurdité de notre hypothèse de départ. □

Ainsi l'ordre d'un groupe simple non-abélien fait intervenir au moins trois nombres premiers ; on vérifie ce phénomène sur l'exemple du groupe alterné $\mathfrak{A}_5$, d'ordre $60 = 2^2 \cdot 3 \cdot 5$. Un résultat dû à Feit et Thomson, de démonstration beaucoup plus longue que le théorème 4.2.6.2, dit qu'un groupe simple non-abélien est d'ordre pair.

Un groupe G est dit résoluble s'il existe une suite de sous-groupes $\{e\} = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_n = G$ tels que chaque H_m est distingué dans H_{m+1} et H_{m+1}/H_m est abélien. Le théorème 4.2.6.2 entraîne alors par une récurrence immédiate le résultat suivant.

4.2.6.3 Théorème (Burnside). *Un groupe fini dont l'ordre est de la forme $p^a q^b$, avec p et q deux nombres premiers, est résoluble.*

4.3 Représentations et caractères induits

Dans toute cette section, k est un corps quelconque (voire un anneau commutatif quelconque).

4.3.1 Restriction, induction, coinduction

4.3.1.1 Restriction. Soient G un groupe et H un sous-groupe de G. Chaque représentation $\pi : G \to \mathbf{GL}(V)$ de G sur un espace vectoriel V donne lieu à une représentation de H sur V, obtenue en restreignant le domaine de π à H. On note $\mathrm{res}^G_H V$ le résultat de cette opération.

4.3.1.2 Induction. Une des technique les plus efficaces pour construire des représentations de G est la méthode des représentations induites. Cette notion généralise les représentations de permutation vues au paragraphe 4.1.2.1. Là, nous partions d'un ensemble Ω muni d'une action de G, considérions le k-espace vectoriel $k^{(\Omega)}$ de base $(e_\omega)_{\omega\in\Omega}$, et définissions un homomorphisme de groupes de G dans $\mathbf{GL}\big(k^{(\Omega)}\big)$. Cette représentation de G se décompose en somme directe d'une façon dictée par la partition en G-orbites de Ω. Pour qui ne s'intéresse qu'aux représentations indécomposables, il est suffisant de se limiter aux ensembles Ω sur lesquels G agit transitivement. Plaçons-nous dans ce cas.

Pour $\omega \in \Omega$, le vecteur e_ω est fixé par le stabilisateur $\mathrm{Stab}_G(\omega)$ de ω dans G. Une idée qui vient à l'esprit est de remplacer la droite ke_ω de $k^{(\Omega)}$ par une représentation W_ω de $\mathrm{Stab}_G(\omega)$.

Pour que la somme directe $V = \bigoplus_{\omega\in\Omega} W_\omega$ soit une représentation de G, il faut disposer, pour chaque $g \in G$, d'un isomorphisme d'espace vectoriel entre W_ω et $W_{g\omega}$ qui échange l'action de $\mathrm{Stab}_G(\omega)$ sur W_ω avec l'action de $g\,\mathrm{Stab}_G(\omega)g^{-1} = \mathrm{Stab}_G(g\omega)$ sur $W_{g\omega}$. On voit ainsi que si l'on se donne un seul W_ω, les autres sont dictés par la condition d'avoir une représentation de G sur V tout entier.

Fixons donc un point $\omega \in \Omega$ et appelons H son stabilisateur. L'application $g \mapsto g\omega$ induit donc une bijection G-équivariante de G/H sur Ω. Donnons-nous une représentation W de H et fabriquons l'espace

$$V = k^{(G/H)} \otimes_k W = \bigoplus_{gH\in G/H} ke_{gH} \otimes_k W.$$

Supposant Ω fini, H est d'indice fini dans G et la somme directe est finie. Prenons une famille $(g_i)_{i\in I}$ de représentants dans G des classes à gauche modulo H. Ainsi $G/H = \{g_iH \mid i \in I\}$. On note $g_i \otimes W$ au lieu de $ke_{g_iH} \otimes_k W$. On peut alors définir une action de G sur V de la façon suivante : pour $g \in G$ et $i \in I$, il existe $j \in I$ et $h \in H$ tel que $gg_i = g_jh$, et pour $w \in W$, on pose $g(g_i \otimes w) = g_j \otimes (hw)$.

Reformulons cette construction en termes d'algèbres de groupe. On constate que kG est un kH-module à droite libre de base $(g_i)_{i\in I}$. Voyant W comme un kH-module à gauche, on peut former le produit tensoriel $kG \otimes_{kH} W$. Par distributivité du produit tensoriel sur la somme directe, on a

$$kG \otimes_{kH} W = \left(\bigoplus_{i\in I} g_ikH\right) \otimes_{kH} W = \bigoplus_{i\in I}\Big(g_ikH \otimes_{kH} W\Big),$$

où chaque terme $g_ikH \otimes_{kH} W$ est un espace vectoriel isomorphe à W, vu que g_ikH est un kH-module à droite libre de rang 1. Identifiant $g_i \otimes W$ à $g_ikH \otimes_{kH} W$ par l'application évidente ($g_i \otimes w$ est envoyé sur lui-même), on obtient un isomorphisme d'espaces vectoriels $V \cong kG \otimes_{kH} W$. On vérifie alors que l'action de kG sur V correspond à l'action de kG sur $kG \otimes_{kH} W$ par multiplication à gauche sur le premier facteur.

Conclusion : soient G un groupe, H un sous-groupe d'indice fini de G, et W une représentation de H sur un espace vectoriel W. L'induite à G de la représentation W de H est le kG-module $kG \otimes_{kH} W$, où l'action de kG est la multiplication à gauche sur le premier facteur. On note $\mathrm{ind}_H^G W$ cette représentation de G. Son degré est $(G : H)$ fois le degré de W. On notera qu'on a une application injective $\iota_W : w \mapsto 1 \otimes w$ de W dans $\mathrm{ind}_H^G W$. On vérifie facilement que ι_W est un homomorphisme de kH-modules de W dans $\mathrm{res}_H^G \mathrm{ind}_H^G W$.

Exemples.

(1) Soit Ω un ensemble fini muni d'une action transitive d'un groupe G. Soit H le stabilisateur d'un point de Ω. Alors la représentation de permutation de G sur $k^{(\Omega)}$ est isomorphe à l'induite à G de la représentation triviale de H.

(2) Soit G un groupe fini. La représentation régulière de G, c'est-à-dire le kG-module régulier à gauche, est isomorphe à l'induite à G de la représentation triviale du sous-groupe trivial $\{1\}$.

4.3.1.3 Coinduction. La coinduction est une technique duale de la technique d'induction. Repartons d'un ensemble Ω sur lequel G agit. Une forme linéaire sur $k^{(\Omega)}$ est spécifiée par les valeurs qu'elle donne des vecteurs de base e_ω. On a ainsi une bijection entre l'espace $\big(k^{(\Omega)}\big)^*$ des formes linéaires sur $k^{(\Omega)}$ et l'espace k^Ω des fonctions sur Ω. L'espace $k^{(\Omega)}$ étant une représentation de G, son dual $\big(k^{(\Omega)}\big)^*$ peut être vu comme l'espace sous-jacent à la représentation contragrédiente. Ainsi k^Ω est l'espace d'une représentation de G, l'action d'un $g \in G$ sur une fonction $f : \Omega \to k$ étant donnée par $gf = \big(\omega \mapsto f(g^{-1}\omega)\big)$.

À nouveau, nous allons généraliser cette construction. Nous supposons que l'action de G sur Ω est transitive, nous choisissons $\omega \in \Omega$ et appelons H son stabilisateur dans G. Toute fonction de $\Omega \cong G/H$ dans k s'identifie alors à une fonction sur G constante sur chaque classe à gauche gH. Considérant une représentation linéaire de H sur un espace vectoriel W, nous pouvons considérer une variante de cette construction en regardant

$$V = \big\{ f : G \to W \;\big|\; \forall (g,h) \in G \times H,\ f(gh^{-1}) = hf(g) \big\}\ ^{19}.$$

On définit une action linéaire de G sur cet espace V en posant $gf = f\big(g^{-1}?\big)$, pour $g \in G$ et $f \in V$.

Cette construction se traduit aisément en termes d'algèbres de groupes. De fait, kG est un kH-module grâce à la multiplication à gauche ; ce module est libre, n'importe quel système de représentants des classes à droite en formant une base. À une fonction $f : G \to W$, on associe l'application linéaire $\hat{f} : \sum_{g\in G} a_g g \mapsto \sum_{g\in G} a_g f(g^{-1})$ de kG dans W. Cette correspondance $f \mapsto \hat{f}$ est un isomorphisme d'espaces vectoriels $V \cong \mathrm{Hom}_{kH}(kG, W)$. L'action à droite de kG sur lui-même définit une structure de kG-module à gauche sur $\mathrm{Hom}_{kH}(kG, W)$, qui coïncide avec la représentation de G sur V.

Conclusion : soient G un groupe, H un sous-groupe d'indice fini de G, et W une représentation de H sur un espace vectoriel W. La coinduite à G de la représentation W de H est le kG-module $\mathrm{Hom}_{kH}(kG, W)$, où l'action de kG est induite par la multiplication à droite sur le domaine. On note $\mathrm{coind}_H^G W$ cette représentation de G ; son degré est $(G : H)$ fois le degré de W. On note qu'on a une application $\kappa_W : f \mapsto f(1)$ de $\mathrm{coind}_H^G W$ dans W. On vérifie que κ_W est un homomorphisme de kH-modules de $\mathrm{res}_H^G \mathrm{coind}_H^G W$ dans W.

Notre résultat de changement de base (paragraphe 1.4.4) donne alors immédiatement :

4.3.1.4 Théorème (réciprocité de Frobenius). *Soient G un groupe, H un sous-groupe d'indice fini de G, V une représentation linéaire de G, W une représentation linéaire de H. Alors les applications*

$$f \mapsto f \circ \iota_W \quad \textit{et} \quad f \mapsto \kappa_W \circ f$$

définissent des isomorphismes

$$\mathrm{Hom}_G(\mathrm{ind}_H^G W, V) \cong \mathrm{Hom}_H(W, \mathrm{res}_H^G V) \quad \textit{et} \quad \mathrm{Hom}_G(V, \mathrm{coind}_H^G W) \cong \mathrm{Hom}_H(\mathrm{res}_H^G V, W).$$

19. Faisons agir H sur $G \times W$ par la règle $h \cdot (g,w) = (gh^{-1}, hw)$. L'ensemble des orbites $(G \times W)/H$ est noté $G \times_H W$; on note traditionnellement $[g,w]$ l'image dans $G \times_H W$ d'un élément (g,w) de $G \times W$. L'ensemble $G \times_H W$ est un fibré au dessus de G/H et l'espace V s'identifie à l'ensemble des sections de ce fibré : à $f \in V$ correspond la section $gH \mapsto [g, f(g)]$.

Afin de pouvoir rester en dimension finie, nous avons limité notre définition des représentations induites et coinduites au cas des sous-groupes d'indice fini. Cette restriction peut être levée, le prix à payer étant évidemment d'accepter les contraintes de l'étude des représentations de dimension infinie. Toutefois, le cas des sous-groupes d'indice fini présente une autre particularité : il n'y a pas de différence fondamentale entre représentation induite et représentation coinduite (voir l'exercice ci-dessous). Autrement dit, on peut oublier la coinduction et penser à l'induction comme l'adjoint à gauche et à droite du foncteur de restriction.

EXERCICE. Soient H un sous-groupe d'indice fini d'un groupe G et W une représentation de H. Soit $(g_i)_{i\in I}$ un système de représentants des classes à gauche de G selon H ; ainsi $G/H = \{g_iH \mid i \in I\}$. Montrer qu'on définit un isomorphisme de kG-modules de $\operatorname{ind}_H^G W$ sur $\operatorname{coind}_H^G W$ en envoyant $g_i \otimes w$ sur la fonction

$$g \mapsto \begin{cases} (g^{-1}g_i)w & \text{si } g^{-1}g_i \in H, \\ 0 & \text{si } g^{-1}g_i \notin H, \end{cases}$$

pour chaque $i \in I$ et $w \in W$.

4.3.2 Propriétés de l'induction

4.3.2.1 Proposition. *Soit k un corps.*

(i) Soit G un groupe, H un sous-groupe de G. L'induction $\operatorname{ind}_H^G?$ est un foncteur additif de la catégorie des kH-modules dans la catégorie des kG-modules.

(ii) Soient $K \subseteq H \subseteq G$ des inclusions de groupes. Il existe un isomorphisme canonique de foncteurs $\operatorname{ind}_H^G(\operatorname{ind}_K^H?) \cong \operatorname{ind}_K^G?$ de la catégorie des kK-modules dans la catégorie des kG-modules.

Preuve. L'assertion (i) provient directement de la définition $\operatorname{ind}_H^G? = kG \otimes_{kH} ?$. Soit W un kK-module. Alors

$$\operatorname{ind}_H^G(\operatorname{ind}_K^H W) = kG \otimes_{kH} \big(kH \otimes_{kK} W\big) = \big(kG \otimes_{kH} kH\big) \otimes_{kK} W = kG \otimes_{kK} W = \operatorname{ind}_K^G W.$$

Cela montre (ii). □

Soient k un corps et H un sous-groupe d'indice fini d'un groupe G. On choisit une famille $(g_i)_{i\in I}$ de représentants des classes à gauche de G modulo H. À une fonction de classe $\lambda \in \operatorname{cf}_k(H)$ sur H, on associe la fonction $\lambda^G : G \to k$ définie par

$$g \mapsto \sum_{i\in I} \dot{\lambda}\big(g_i^{-1} g g_i\big),$$

où $\dot{\lambda} : G \to k$ est la fonction qui coïncide avec λ sur H et qui vaut 0 hors de H. À une fonction de classe $\mu \in \operatorname{cf}_k(G)$ sur G, on associe sa restriction μ_H, qui est une fonction sur H à valeurs dans k.

4.3.2.2 Proposition. *Partant des objets ci-dessus, nous avons les propriétés suivantes.*

(i) Si $\lambda \in \mathrm{cf}_k(H)$, alors $\lambda^G \in \mathrm{cf}_k(G)$. Si λ est le caractère d'une représentation de H sur un espace vectoriel W, alors λ^G est le caractère de l'induite $\mathrm{ind}_H^G W$. Si $\lambda \in \mathrm{ch}\, kH$, alors $\lambda^G \in \mathrm{ch}\, kG$.

(ii) Si $\mu \in \mathrm{cf}_k(G)$, alors $\mu_H \in \mathrm{cf}_k(H)$. Si μ est le caractère d'une représentation de G sur un espace vectoriel V, alors μ_H est le caractère de la restriction $\mathrm{res}_H^G V$. Si $\mu \in \mathrm{ch}\, kG$, alors $\mu_H \in \mathrm{ch}\, kH$.

(iii) Supposons que k soit de caractéristique 0. Pour chaque $\lambda \in \mathrm{cf}_k(H)$, on a $\lambda^G(g) = \Big(\sum_{x\in G} \dot\lambda\big(x^{-1}gx\big)\Big)/|H|$.

(iv) Prenons $k = \mathbf{C}$ et supposons que G soit un groupe fini. Munissons $\mathrm{cf}_{\mathbf{C}}(H)$ et $\mathrm{cf}_{\mathbf{C}}(G)$ des produits scalaires hermitiens du paragraphe 4.2.3. Soient $\lambda \in \mathrm{cf}_{\mathbf{C}}(H)$ et $\mu \in \mathrm{cf}_{\mathbf{C}}(G)$. Alors $(\lambda^G, \mu)_G = (\lambda, \mu_H)_H$.

Preuve. Plaçons-nous dans le cadre de l'assertion (i). Chaque $x \in G$ induit par multiplication à gauche une permutation de l'ensemble G/H. Il existe donc une permutation σ de I et des éléments h_i de H tels que $xg_i = g_{\sigma(i)}h_i$ pour chaque $i \in I$. Pour chaque $g \in G$, on a alors

$$\lambda^G(x^{-1}gx) = \sum_{i\in I} \dot\lambda\big(g_i^{-1}x^{-1}gxg_i\big) = \sum_{i\in I} \dot\lambda\big(h_i^{-1}g_{\sigma(i)}^{-1}gg_{\sigma(i)}h_i\big) = \sum_{i\in I} \dot\lambda\big(g_{\sigma(i)}^{-1}gg_{\sigma(i)}\big) = \lambda^G(g).$$

Ainsi $\lambda^G \in \mathrm{cf}_k(G)$.

Supposons que λ soit le caractère d'une représentation de H sur un espace vectoriel W. Prenant une base $(w_1, \dots, w_m)$ de W, nous obtenons une représentation matricielle $X : H \to \mathbf{GL}_m(k)$. Prolongeons X en une application $\dot X : G \to \mathbf{Mat}_m(k)$ en décrétant que $\dot X(g) = 0$ si $g \notin H$. À réindexation près, nous pouvons supposer que $I = \{1, \dots, n\}$. Munissant $\mathrm{ind}_H^G W$ de la base $(g_1 \otimes w_1, \dots, g_1 \otimes w_m, g_2 \otimes w_1, \dots, g_2 \otimes w_m, \dots, g_n \otimes w_1, \dots, g_n \otimes w_m)$, on vérifie que l'induite à G de notre représentation de H est fournie par la représentation matricielle

$$g \mapsto \begin{pmatrix} \dot X(g_1^{-1}gg_1) & \dots & \dot X(g_1^{-1}gg_n) \\ \vdots & & \vdots \\ \dot X(g_n^{-1}gg_1) & \dots & \dot X(g_n^{-1}gg_n) \end{pmatrix}.$$

Le caractère de cette représentation est λ^G.

Ce qui précède montre que λ^G est un caractère de G dès que λ est un caractère de H. Par $\mathbf{Z}$-linéarité, on en déduit que λ^G est un caractère virtuel de G dès que λ est un caractère virtuel de H. Cela achève la preuve de l'assertion (i).

La preuve de l'assertion (ii) est du même genre (en plus simple). L'assertion (iii) se montre en sommant par paquets, obtenus en partitionnant G selon ses classes à gauche modulo H.

Enfin, l'assertion (iv) provient du calcul suivant :

$$\begin{aligned}(\lambda^G,\mu)_G &= \frac{1}{|G|}\sum_{g\in G}\left(\frac{1}{|H|}\sum_{x\in G}\overline{\dot\lambda(x^{-1}gx)}\right)\mu(g)\\ &= \frac{1}{|G|}\sum_{x\in G}\left(\frac{1}{|H|}\sum_{g\in G}\overline{\dot\lambda(x^{-1}gx)}\mu(x^{-1}gx)\right)\\ &= \frac{1}{|H|}\sum_{z\in G}\overline{\dot\lambda(z)}\mu(z)\\ &= \frac{1}{|H|}\sum_{h\in H}\overline{\lambda(h)}\mu(h)\\ &= (\lambda,\mu_H)_H.\end{aligned}$$

Dans le cas où λ est le caractère d'une représentation de H et μ est le caractère d'une représentation de G, l'assertion (iv) traduit la réciprocité de Frobenius (théorème 4.3.1.4), compte tenu de l'interprétation du produit scalaire comme dimension d'un espace d'homomorphismes (proposition 4.2.3.2 (ii)). □

Exemple. Prenons $k = \mathbf{C}$ et $G = D_n$ le groupe diédral à $2n$ éléments, engendré par r et s comme au paragraphe 4.1.2.4. Soit H le sous-groupe cyclique d'ordre n engendré par r et soit $\theta = 2\pi/n$. Pour $0 \leq j < n$ entier, soit λ_j le caractère linéaire de H qui envoie r sur $e^{ij\theta}$. Des calculs montrent alors que :

(1) $\mathrm{ind}_H^G \lambda_0$ est la somme de deux caractères linéaires, à savoir le caractère trivial 1 et la signature ε.

(2) Pour j entier entre 1 et $n-1$, $\mathrm{ind}_H^G \lambda_j = \mathrm{ind}_H^G \lambda_{n-j}$.

(3) Si n est impair (respectivement, pair), alors pour chaque j entier entre 1 et $(n-1)/2$ (respectivement, $n/2-1$), la fonction $\mathrm{ind}_H^G \lambda_j$ est le caractère de la représentation $r \mapsto R_j$, $s \mapsto S$ de D_n construite dans le paragraphe 4.1.2.4.

(4) Si n est pair, alors $\mathrm{ind}_H^G \lambda_{n/2}$ est la somme des deux caractères linéaires de D_n définis à la fin du paragraphe 4.1.2.4.

On trouvera dans les livres bon nombre d'autres résultats basiques concernant les représentations et les caractères induits. Citons ici pour mémoire les résultats classiques de Mackey (voir par exemple [7], §10B) :

(1) Quand H et K sont deux sous-groupes d'un groupe G, avec H d'indice fini, on peut décrire explicitement la restriction de l'induction $\mathrm{res}_K^G(\mathrm{ind}_H^G W)$ d'une représentation W de H en termes d'induites $\mathrm{ind}_L^K(\mathrm{res}^H_{g^{-1}Lg}(W))$, où chaque L est un sous-groupe de la forme $gHg^{-1} \cap K$.

(2) Quand H et K sont deux sous-groupes d'indice fini de G et W et X sont des représentations de H et K respectivement, on peut décrire explicitement le produit tensoriel $(\mathrm{ind}_H^G W) \otimes_k (\mathrm{ind}_K^G X)$ des représentations induites en termes d'induites $\mathrm{ind}_L^G Y$, où chaque L est un sous-groupe de la forme $gHg^{-1} \cap K$.

EXERCICE. Soit H un sous-groupe d'un groupe fini G. Soient $\lambda \in \mathrm{cf}_k(H)$ et $\mu \in \mathrm{cf}_k(G)$. Montrer que $\lambda^G \, \mu = \big(\lambda \, \mu_H\big)^G$.

4.3.3 Trois théorèmes de Brauer

Dans tout ce paragraphe, G est un groupe fini.

Un sous-groupe de G est dit p-élémentaire, pour un nombre premier p, s'il est le produit direct d'un p-groupe et d'un groupe cyclique. Un sous-groupe de G est dit élémentaire s'il est p-élémentaire pour un certain nombre premier p.

Nous admettrons le résultat suivant. Pour une preuve, le lecteur est invité à consulter [6], §40, ou [7], §15B.

4.3.3.1 Théorème d'induction de Brauer. *Chaque caractère complexe de G est une combinaison $\mathbf{Z}$-linéaire de caractères induits à partir de caractères linéaires de sous-groupes élémentaires de G.*

Tout sous-groupe cyclique de G étant élémentaire, chaque élément de G appartient à un sous-groupe élémentaire de G. Un caractère de G est donc entièrement déterminé par la donnée de ses restrictions aux sous-groupes élémentaires de G. Plus étonnant est le résultat suivant.

4.3.3.2 Critère pour les caractères virtuels. *Une fonction de classe $\varphi \in \mathrm{cf}_{\mathbf{C}}(G)$ appartient à $\mathrm{ch}\,\mathbf{C}G$ si et seulement si φ_H appartient à $\mathrm{ch}\,\mathbf{C}H$ pour chaque sous-groupe élémentaire H de G.*

Preuve. Le sens direct est conséquence immédiate de la proposition 4.3.2.2 (ii). Réciproquement, soit $\varphi \in \mathrm{cf}_{\mathbf{C}}(G)$ tel que $\varphi_H \in \mathrm{ch}\,\mathbf{C}H$ pour chaque sous-groupe élémentaire H. Le théorème d'induction de Brauer dit qu'on peut écrire le caractère trivial de G comme une combinaison $\mathbf{Z}$-linéaire $1 = \sum_{i\in I} a_i \lambda_i^G$ d'induits de caractères linéaires λ_i de sous-groupes élémentaires H_i de G. Chaque restriction φ_{H_i} étant un caractère virtuel de H_i, l'induite $(\varphi_{H_i}\ \lambda_i)^G$ est un caractère virtuel de G. Utilisant l'exercice du paragraphe 4.3.2, nous pouvons donc exprimer

$$\varphi = \varphi\ 1 = \sum_{i\in I} a_i\ \varphi\ \lambda_i^G = \sum_{i\in I} a_i (\varphi_{H_i}\ \lambda_i)^G$$

comme combinaison $\mathbf{Z}$-linéaire de caractères virtuels de G. Ainsi $\varphi \in \mathrm{ch}\,\mathbf{C}G$, comme désiré. □

Soit k un corps de caractéristique 0. On dit que k est un corps de décomposition pour G si l'algèbre kG est décomposée. Cela est équivalent à dire que chaque représentation irréductible de G sur k est absolument irréductible (paragraphe 3.2.6), ou encore que l'algèbre des endomorphismes d'un kG-module simple M est égale à $k\,\mathrm{id}_M$. Une condition suffisante est que k soit algébriquement clos.

Le paragraphe 4.2.2.5 prouve qu'un sous-corps k de $\mathbf{C}$ est un corps de décomposition pour G si et seulement si chaque représentation matricielle irréductible de G sur $\mathbf{C}$ est réalisable

sur k, c'est-à-dire équivalente sur $\mathbf{C}$ à une représentation matricielle de G sur k. La proposition 3.2.6.2 (iv) affirme l'existence d'une extension finie de $\mathbf{Q}$ qui décompose G. Le résultat suivant est plus précis.

4.3.3.3 Théorème du corps de décomposition. *Soit n l'exposant de G, c'est-à-dire le* PPCM *des ordres des éléments de G. Soit ω une racine primitive n-ième de l'unité dans $\mathbf{C}$. Alors l'extension cyclotomique $\mathbf{Q}(\omega)$ est un corps de décomposition de G.*

Preuve. Soit H un sous-groupe élémentaire de G. Toute représentation de degré 1 de H est un caractère linéaire du groupe abélien H/H', donc est réalisable sur $\mathbf{Q}(\omega)$ (si besoin est, réexaminer la preuve du théorème 4.2.4.2 et l'exemple 4.1.2.3). L'induite à G d'une telle représentation est donc réalisable sur $\mathbf{Q}(\omega)$.

Maintenant soit T une représentation de G sur $\mathbf{C}$ et soit ζ le caractère de T. Le théorème d'induction de Brauer permet d'écrire

$$\zeta = \sum_{i \in I} a_i \lambda_i^G,$$

avec $a_i \in \mathbf{Z}$ et λ_i un caractère linéaire d'un sous-groupe élémentaire de G. Réarrangeant les termes, nous écrivvons

$$\zeta = \left(\sum_{a_i > 0} a_i \lambda_i^G \right) - \left(\sum_{a_i < 0} (-a_i) \lambda_i^G \right) = \mu - \nu.$$

Le premier alinéa montre que chaque λ_i^G est le caractère d'une représentation de G réalisable sur $\mathbf{Q}(\omega)$. Il existe donc des représentations matricielles X et Y de G sur $\mathbf{Q}(\omega)$ dont μ et ν sont les caractères, respectivement. L'égalité $\zeta + \nu = \mu$ se traduit alors par un isomorphisme $T \oplus Y_{(\mathbf{C})} \cong X_{(\mathbf{C})}$, où $X_{(\mathbf{C})}$ et $Y_{(\mathbf{C})}$ sont les représentations X et Y, vues comme représentations sur $\mathbf{C}$.

En décomposant X et Y en somme directe de représentations simples sur $\mathbf{Q}(\omega)$, on parvient à une décomposition $X \cong X' \oplus Z$ et $Y \cong Y' \oplus Z$ telle que X' et Y' n'aient aucune composante irréductible en commun, ce qui se traduit par $\mathrm{Hom}_G(X', Y') = 0$. La proposition 3.1.3.2 (ou l'argument dans la preuve du théorème de Noether-Deuring 3.2.3.1) dit qu'alors $\mathrm{Hom}_G\big(X'_{(\mathbf{C})}, Y'_{(\mathbf{C})}\big) = 0$, c'est-à-dire que $X'_{(\mathbf{C})}$ et $Y'_{(\mathbf{C})}$ n'ont aucune composante irréductible en commun (voir aussi l'exercice (2) du paragraphe 3.2.6). L'isomorphisme $T \oplus Y'_{(\mathbf{C})} \cong X'_{(\mathbf{C})}$ amène alors $Y'_{(\mathbf{C})} = 0$, et ainsi T est réalisée sur $\mathbf{Q}(\omega)$ par X'.

Nous avons donc montré que chaque représentation T de G sur $\mathbf{C}$ est réalisable sur $\mathbf{Q}(\omega)$. Le théorème est prouvé. □

4.4 Représentations continues des groupes compacts

4.4.1 Groupes topologiques

Groupe topologique : une topologie sur un groupe G est dite compatible avec la structure de groupe si le produit $(g, h) \mapsto gh$ et l'inversion $g \mapsto g^{-1}$ sont des applications continues de

$G \times G$ ou G dans G. Un groupe muni d'une topologie compatible est dit groupe topologique. Tout groupe fini, muni de la topologie discrète, est un groupe topologique.

Espaces vectoriels topologiques : ici k est un corps valué complet non discret, par exemple $\mathbf{R}$, $\mathbf{C}$ ou $\mathbf{Q}_p$. Sur un k-espace vectoriel V de dimension finie existe une topologie canonique obtenue en transportant la topologie produit sur $k^{\dim V}$ à V grâce au choix d'une base de V (le résultat ne dépend pas du choix de la base). Le groupe $\mathbf{GL}(V)$, en tant qu'ouvert de l'espace vectoriel de dimension finie $\mathrm{End}_k(V)$, est lui aussi muni d'une topologie canonique ; c'est en fait un groupe topologique.

Représentation continue : soit G un groupe topologique et k un corps valué complet non discret. Soit $\pi : G \to \mathbf{GL}(V)$ une représentation linéaire de G sur un k-espace vectoriel V de dimension finie. Alors les trois conditions suivantes sont équivalentes :

(1) $\pi : G \to \mathbf{GL}(V)$ est une application continue ;

(2) l'action $(G \times V \to V, (g, v) \mapsto \pi(g)(v))$ est une application continue ;

(3) pour chaque vecteur $v \in V$ et chaque forme linéaire $v^* \in V^*$, la fonction (appelée « coefficient matriciel ») $g \mapsto \langle v^*, \pi(g)(v)\rangle$ sur G à valeurs dans k est continue.

Si ces conditions sont vérifiées, on dit que π est continue. Nous n'étudierons pas le cas des représentations de dimension infinie, pour lequel plusieurs définitions différentes sont utilisées de manière concurrente.

4.4.2 Coefficients d'une représentation

Dans ce paragraphe, G est un groupe et k est un corps, sans hypothèse supplémentaire.

La k-algèbre kG du groupe G est un k-espace vectoriel. Son dual s'identifie à l'espace k^G des fonctions de G dans k (voir la remarque 4.1.4.2).

Nous munissons kG de sa structure de kG-bimodule régulier. L'espace k^G des fonctions sur G à valeurs dans k peut être identifié au dual de kG (voir la remarque 4.1.4.2) ; il se trouve ainsi muni d'une structure de kG-bimodule. Concrètement, les actions à gauche et à droite d'un élément $g \in G \subseteq kG$ sur une fonction $\varphi \in k^G$ sont données par

$$g \cdot \varphi = (h \mapsto \varphi(hg)) \quad \text{et} \quad \varphi \cdot g = (h \mapsto \varphi(gh)).$$

Enfin si $\varphi \in k^G$ est une fonction sur G, on note φ^* la fonction $g \mapsto \varphi(g^{-1})$, prolongeant ainsi la notation du paragraphe 4.1.4 pour les fonctions de classe.

Soit π une représentation de G dans un k-espace vectoriel V. On munit V^* de la structure de kG-module à droite induite par la structure de kG-module à gauche sur V. L'espace $V \otimes_k V^*$ se trouve ainsi muni d'une structure de kG-bimodule : les actions à gauche et à droite d'un élément $g \in G \subseteq kG$ sur un tenseur $t = \sum v_i \otimes f_i$ sont données par

$$g \cdot t = \sum_i \pi(g)(v_i) \otimes f_i \quad \text{et} \quad t \cdot g = \sum_i v_i \otimes ({}^t\pi(g))(f_i).$$

Pour $v \in V$ et $v^* \in V^*$, on note $\theta^\pi(v, v^*)$ la fonction $g \mapsto \langle v^*, \pi(g)(v)\rangle$ sur G. Les $\theta^\pi(v, v^*)$, pour $v \in V$ and $v^* \in V^*$, s'appellent les coefficients de π. L'application θ^π de $V \times V^*$ dans k^G

définit alors une application linéaire de $V \otimes_k V^*$ dans k^G, que nous noterons également θ^π. On note $\mathscr{M}_\pi = \theta^\pi(V \otimes_k V^*)$; c'est le sous-espace vectoriel de k^G engendré par les coefficients de π. Le caractère χ_π de π appartient à $\mathscr{M}_\pi$.

4.4.2.1 Proposition. *Soit $\pi : G \to \mathbf{GL}(V)$ une représentation de G. Alors l'application $\theta^\pi : V \otimes_k V^* \to k^G$ est un homomorphisme de kG-bimodules. Son image $\mathscr{M}_\pi$ est un sous-kG-bimodule de k^G.*

Preuve. Soient $g \in G$, $v \in V$ et $v^* \in V^*$. Alors

$$g \cdot \theta^\pi(v, v^*) = \big(h \mapsto \theta^\pi(v, v^*)(hg)\big) = \big(h \mapsto \langle v^*, \pi(h)\pi(g)v\rangle\big) = \theta^\pi(\pi(g)v, v^*)$$

et

$$\theta^\pi(v, v^*) \cdot g = \big(h \mapsto \theta^\pi(v, v^*)(gh)\big) = \big(h \mapsto \langle {}^t\pi(g)v^*, \pi(h))v\rangle\big) = \theta^\pi(v, {}^t\pi(g)v^*).$$

La première assertion de la proposition se déduit facilement de ces égalités par linéarité, et la seconde est conséquence de la première. □

4.4.2.2 Remarques.

(1) Soit $\pi : G \to \mathbf{GL}(V)$ une représentation de G. Alors l'orthogonal dans kG de $\mathscr{M}_\pi$, relativement à la dualité entre kG et k^G, est l'annulateur du kG-module V. Supposons que V soit de dimension finie sur k. Alors $\mathscr{M}_\pi$ est de dimension finie, et donc, par bidualité, $\mathscr{M}_\pi$ est l'orthogonal dans k^G de $\operatorname{ann} V$.

(2) Plaçons-nous dans les hypothèses de l'énoncé de la proposition 4.4.2.1. En confondant $V \otimes_k V^*$ avec l'espace vectoriel $\mathrm{Hom}_k(V, V)$, nous identifions θ^π à l'application qui envoie $u \in \mathrm{Hom}_k(V, V)$ sur la fonction $g \mapsto \mathrm{tr}(u \circ \pi(g))$. Considérons la représentation de G sur $\mathrm{Hom}_k(V, V)$ et munissons k^G d'une action à gauche de G en posant $g \cdot \varphi = \big(h \mapsto \varphi(g^{-1}hg)\big)$, pour $g \in G$ et $\varphi \in k^G$. Notre application $u \mapsto \mathrm{tr}(u \circ \pi(?))$ est alors un homomorphisme de représentations, qui envoie id_V sur le caractère χ_π.

La proposition suivante découle immédiatement des définitions du paragraphe 4.1.3.

4.4.2.3 Proposition.

(i) Soit $1 : G \to \mathbf{GL}_1(k)$ la représentation triviale. Alors $\mathscr{M}_1$ est l'ensemble des fonctions constantes sur G à valeurs dans k.

(ii) Soient $\pi : G \to \mathbf{GL}(V)$ et $\rho : G \to \mathbf{GL}(W)$ deux représentations de G, soient $v \in V$, $v^* \in V^*$, $w \in W$ et $w^* \in W^*$. On considère $v^* \oplus w^*$ comme un élément de $(V \oplus W)^*$ grâce à l'isomorphisme $V^* \oplus W^* \cong (V \oplus W)^*$. Alors $\theta^{\pi\oplus\rho}(v \oplus w, v^* \oplus w^*) = \theta^\pi(v, w^*) + \theta^\rho(w, w^*)$. On a $\mathscr{M}_{\pi\oplus\rho} = \mathscr{M}_\pi + \mathscr{M}_\rho$.

(iii) Soient $\pi : G \to \mathbf{GL}(V)$ et $\rho : G \to \mathbf{GL}(W)$ deux représentations de G, soient $v \in V$, $v^* \in V^*$, $w \in W$ et $w^* \in W^*$. On considère $v^* \otimes w^*$ comme un élément de $(V \otimes_k W)^*$ grâce au plongement $V^* \otimes W^* \subseteq (V \otimes_k W)^*$. Alors $\theta^{\pi\otimes\rho}(v \otimes w, v^* \otimes w^*) = \theta^\pi(v, v^*)\theta^\rho(w, w^*)$. On a $\mathscr{M}_{\pi\otimes\rho} = \mathscr{M}_\pi \mathscr{M}_\rho$.

(iv) Soit $\pi : G \to \mathbf{GL}(V)$ une représentation de G, soient $v \in V$ et $v^* \in V^*$. On note $\pi^* : G \to \mathbf{GL}(V^*)$ la représentation contragrédiente de π et on voit v comme une forme linéaire sur V^*. Alors $\theta^{\pi^*}(v^*, v) = (\theta^\pi(v, v^*))^*$. On a $\mathscr{M}_{\pi^*} = (\mathscr{M}_\pi)^*$.

On note $(kG)^\circ$ la somme dans k^G de tous les espaces $\mathscr{M}_\pi$, où π décrit l'ensemble des représentations de dimension finie de G. D'après les propositions 4.4.2.1 et 4.4.2.3, c'est un sous-kG-bimodule et une sous-algèbre de k^G stable par l'involution $*$.

4.4.2.4 Proposition. *L'espace $(kG)^\circ$ coïncide avec les trois ensembles suivants :*

- *L'ensemble des fonctions $\varphi : G \to k$ telles que le sous-espace vectoriel engendré par l'ensemble $\{g \cdot \varphi \mid g \in G\}$ des translatées à droite de φ est de dimension finie.*
- *L'ensemble des fonctions $\varphi : G \to k$ telles que le sous-espace vectoriel engendré par l'ensemble $\{\varphi \cdot g \mid g \in G\}$ des translatées à gauche de φ est de dimension finie.*
- *L'ensemble des fonctions $\varphi : G \to k$ telles que le sous-espace vectoriel engendré par l'ensemble $\{g \cdot \varphi \cdot h \mid (g,h) \in G^2\}$ de toutes les translatées de φ est de dimension finie.*

Preuve. Un sous-espace $\mathscr{M}_\pi$ est de dimension finie et stable par les translations à gauche et à droite. Il est donc inclus dans chacun des trois ensembles de l'énoncé.

À présent, soit $\varepsilon : k^G \to k$ l'évaluation d'une fonction en l'élément neutre de G et soit $\rho : G \to \mathbf{GL}(k^G)$ la représentation linéaire de G sur k^G donnée par la translation à droite. Alors chaque fonction $\varphi \in k^G$ est égale au coefficient matriciel $\theta^\rho(\varphi, \varepsilon)$.

Montrons l'inclusion du premier ensemble de l'énoncé dans $(kG)^\circ$. Soit $\varphi : G \to k$ une fonction et soit V le sous-espace vectoriel engendré par $\{g \cdot \varphi \mid g \in G\}$. Certainement V est un sous-kG-module à gauche de k^G ; ρ se restreint donc en une sous-représentation $\pi : G \to \mathbf{GL}(V)$. Alors $\varphi = \theta^\pi(\varphi, \varepsilon)$ appartient à $\mathscr{M}_\pi$. Donc $\varphi \in (kG)^\circ$ dès que V est de dimension finie.

L'inclusion du second ensemble de l'énoncé dans $(kG)^\circ$ se démontre de façon analogue (ou en utilisant l'involution $*$). Enfin, le troisième ensemble de l'énoncé est inclus dans le premier et le second. □

4.4.2.5 Remarque. Dans le cas où G est un groupe topologique et k est un corps valué complet non discret, l'espace $C(G,k)$ des fonctions continues de G dans k est un sous-kG-bimodule de k^G. Si π est une représentation continue, $\mathscr{M}_\pi$ est un sous-kG-bimodule de $C(G,k)$. On peut alors énoncer des résultats pour les représentations continues de dimension finie analogues aux propositions 4.4.2.1, 4.4.2.3 et 4.4.2.4 et aux remarques 4.4.2.2.

4.4.3 Mesure invariante

Soit G un groupe fini et k un corps dont la caractéristique ne divise pas l'ordre de G. On peut alors définir la moyenne d'une fonction $f : G \to k$ par la formule $\frac{1}{|G|} \sum_{g \in G} f(g)$.

Cette construction d'une moyenne s'étend aux groupes compacts à condition de prendre $\mathbf{R}$ ou $\mathbf{C}$ comme corps de base et de se restreindre aux fonctions continues. Pour une preuve du résultat suivant, voir par exemple John von Neumann, *Zum Haarschen Maß in topologischen Gruppen,* Compositio Math. **1** (1934), 106–114.

4.4.3.1 Théorème. *Soit G un groupe topologique compact et soit $C(G, \mathbf{R})$ l'espace des fonctions continues sur G à valeurs réelles. Alors il existe une unique forme $\mathbf{R}$-linéaire sur $C(G, \mathbf{R}) \to \mathbf{R}$, appelée moyenne, satisfaisant aux conditions (i) à (iii) ci-dessous. Elle satisfait en outre aux conditions (iv) et (v).*

(i) La moyenne d'une fonction à valeurs positives est positive.

(ii) La moyenne d'une fonction constante est égale à la valeur de cette fonction.

(iii) Pour toute fonction $f \in C(G, \mathbf{R})$ et tout $g \in G$, la fonction $h \mapsto f(g^{-1}h)$ a même moyenne que f.

(iv) Si une fonction continue positive est de moyenne nulle, alors elle est identiquement nulle.

(v) Pour toute fonction $f \in C(G, \mathbf{R})$ et tout $g \in G$, les fonctions $h \mapsto f(hg)$, $h \mapsto f(g^{-1}hg)$ et $h \mapsto f(h^{-1})$ ont même moyenne que f.

D'après le théorème de représentation de Riesz, la donnée d'une forme linéaire positive sur $C(G, \mathbf{R})$ est équivalente à la donnée d'une mesure de Radon positive sur G. La moyenne correspond ainsi à une mesure positive sur G, qu'on appelle mesure de Haar ou mesure invariante, et que nous noterons μ. On peut alors intégrer sur G toute fonction borélienne bornée à valeurs dans un $\mathbf{R}$-espace vectoriel de dimension finie. On peut aussi parler de fonctions mesurables et considérer les espaces $L^p(G, \mathbf{R})$ et l'espace de Hilbert complexe $L^2(G, \mathbf{C})$.

4.4.3.2 Exemples.

(1) Si $G = \mathbf{R}/2\pi\mathbf{Z}$, alors la moyenne d'une fonction continue $f : G \to \mathbf{R}$ est $\int_G f \, d\mu = \frac{1}{2\pi} \int_0^{2\pi} f(e^{it}) \, dt$.

(2) Si G_1, ..., G_n sont des groupes compacts et si μ_1, ..., μ_n sont leurs mesures de Haar, alors la moyenne d'une fonction $f : G \to \mathbf{R}$ sur le groupe produit $G = G_1 \times \cdots \times G_n$ est donnée par

$$\int_G f \, d\mu = \int_{G_1} \cdots \int_{G_n} f(g_1, \ldots, g_n) \, d\mu_1(g_1) \cdots d\mu_n(g_n).$$

4.4.4 Théorème de Maschke et relations d'orthogonalité

Dans ce paragraphe, G est un groupe compact et k est $\mathbf{R}$ ou $\mathbf{C}$. Toutes les représentations considérées sont continues et de dimension finie.

Grâce à la mesure invariante, on peut définir l'opérateur de Reynolds de la même façon qu'au paragraphe 4.2.1. De façon précise, si $\pi : G \to \mathbf{GL}(V)$ une représentation de G, l'opérateur de Reynolds est l'application linéaire $\natural = \int_G \pi(g) \, d\mu(g)$ de V dans lui-même. Ici, on intègre une fonction continue à valeurs dans un espace vectoriel de dimension finie, ce qui est licite.

La proposition 4.2.1.2 et le théorème de Maschke 4.2.1.4 restent valables sans changement. La formule du corollaire 4.2.1.3 devient

$$\dim(\mathrm{inv}_G V) = \int_G \chi_\pi \, d\mu.$$

Celle de la proposition 4.2.1.5 devient

$$\dim \mathrm{Hom}_G(V,W) = \int_G \chi_V\big(g^{-1}\big)\chi_W\big(g\big)\; d\mu(g).$$

De ces relations d'orthogonalité entre caractères, on déduit que les caractères des représentations de dimension finie irréductibles et continues sont linéairement indépendants. Joint au théorème de Maschke, ce fait implique que le caractère d'une représentation continue de dimension finie de G détermine cette représentation à isomorphisme près.

Sur $\mathbf{C}$, on a également une relation d'orthogonalité pour les coefficients d'une représentation. (Cette relation d'orthogonalité aurait pu être établie au paragraphe 4.2.1 pour un groupe fini G et un corps de base k algébriquement clos et de caractéristique ne divisant pas l'ordre de G ; nous n'en aurions cependant pas eu l'usage.) Reprenons le contexte du paragraphe 4.4.2, dans le cadre de la remarque 4.4.2.5.

4.4.4.1 Proposition. *Soient $\pi : G \to \mathbf{GL}(V)$ et $\rho : G \to \mathbf{GL}(W)$ deux représentations irréductibles de G. Soient $v \in V$, $v^* \in V^*$, $w \in W$, $w^* \in W^*$. Alors*

$$\int_G \theta^\pi(v,v^*)(g^{-1})\theta^\rho(w,w^*)(g)\; d\mu(g) = \begin{cases} 0 & \text{si } \pi \ncong \rho, \\ \dfrac{\langle w^*, f(v)\rangle\langle v^*, f^{-1}(w)\rangle}{\deg \pi} & \text{s'il existe un isomorphisme } f \in \mathrm{Hom}_G(\pi,\rho). \end{cases}$$

Preuve. On considère la représentation de G sur $\mathrm{Hom}_k(V,W)$, d'où un opérateur de Reynolds $\natural$ sur $\mathrm{Hom}_k(V,W)$. Soit $u \in \mathrm{Hom}_k(V,W)$ l'application linéaire $x \mapsto \langle v^*, x\rangle w$. Le membre de gauche dans la formule de la proposition est $\langle w^*, u^\natural(v)\rangle$.

Les invariants de $\mathrm{Hom}_k(V,W)$ sont les homomorphismes de représentations. Si π n'est pas isomorphe à ρ, alors $\mathrm{inv}_G\big(\mathrm{Hom}_k(V,W)\big) = \mathrm{Hom}_G(V,W) = 0$ d'après le lemme de Schur, et donc $u^\natural = 0$. Cela montre le résultat dans ce cas.

Si π est isomorphe à ρ, alors $\mathrm{Hom}_G(V,W)$ est une droite vectorielle complexe engendrée par chaque isomorphisme de kG-modules $f : V \to W$, toujours d'après le lemme de Schur. On peut alors écrire

$$u^\natural = \frac{\mathrm{tr}(f^{-1}\circ u^\natural)}{\mathrm{tr}(f^{-1}\circ f)} f = \frac{\mathrm{tr}(f^{-1}\circ u^\natural)}{\deg \pi} f.$$

Pour achever la démonstration, il nous reste à calculer la trace de $f^{-1}\circ u^\natural$. On observe que l'application $y \mapsto \mathrm{tr}(f^{-1}\circ y)$ est un homomorphisme de représentations de $\mathrm{Hom}_k(V,W)$ dans k, car pour $g \in G$ et $y \in \mathrm{Hom}_k(V,W)$,

$$\mathrm{tr}\big(f^{-1}\circ(g\cdot y)\big) = \mathrm{tr}\big(f^{-1}\circ\big(\rho(g)\circ y\circ\pi(g)^{-1}\big)\big) = \mathrm{tr}\big(\big(\pi(g)^{-1}\circ f^{-1}\circ\rho(g)\big)\circ y\big) = \mathrm{tr}\big(f^{-1}\circ y\big).$$

En utilisant la proposition 4.2.1.2 (iii), on calcule alors

$$\mathrm{tr}\big(f^{-1}\circ u^\natural\big) = \big(\mathrm{tr}(f^{-1}\circ u)\big)^\natural = \mathrm{tr}\big(f^{-1}\circ u\big) = \mathrm{tr}\big[x \mapsto \langle v^*, x\rangle f^{-1}(w)\big] = \langle v^*, f^{-1}(w)\rangle,$$

ce qui achève la démonstration. □

Remarque. Le caractère d'une représentation π est une combinaison linéaire de coefficients de π. Les relations d'orthogonalité entre les caractères peuvent ainsi être vues comme une conséquence directe de la proposition 4.4.4.1.

On note $\mathscr{M}$ la somme des sous-espaces $\mathscr{M}_\pi$ dans $C(G, \mathbf{C})$, quand π parcourt l'ensemble des représentations continues de dimension finie. C'est une sous-algèbre et un sous-kG-bimodule stable par l'involution $*$ de $C(G, \mathbf{C})$. Par ailleurs, notons $G^\wedge$ l'ensemble des classes d'isomorphisme de représentations linéaires irréductibles continues de dimension finie de G.

4.4.4.2 Proposition.

(i) Soit $\pi : G \to \mathbf{GL}(V)$ un élément de $G^\wedge$. Alors θ^π est un isomorphisme kG-bimodules de $V \otimes_k V^*$ sur $\mathscr{M}_\pi$.

(ii) Les sous-espaces $\mathscr{M}_\pi$ sont en somme directe dans k^G, pour π décrivant $G^\wedge$.

(iii) $\mathscr{M} = \bigoplus_{\pi \in G^\wedge} \mathscr{M}_\pi$.

Preuve. Munissons $C(G, \mathbf{C})$ d'une forme bilinéaire B en posant

$$B(\varphi, \psi) = \int_G \varphi\big(g^{-1}\big)\psi\big(g\big)\, d\mu(g).$$

Cette forme bilinéaire est symétrique, d'après le théorème 4.4.3.1 (v).

Soit $\pi : G \to \mathbf{GL}(V)$ un élément de $G^\wedge$. Prenons une base $(v_i)_{i\in I}$ de V, soit $(v_i^*)_{i\in I}$ la base duale de V^*. Appliquant $B(\theta^\pi(v_l, v_k^*), ?)$ à une relation de dépendance linéaire

$$\sum_{(i,j)\in I^2} \lambda_{ij}\, \theta^\pi(v_i, v_j^*) = 0,$$

on trouve que chaque $\lambda_{kl} = 0$ en utilisant les relations d'orthogonalité 4.4.4.1. Les coefficients $\theta^\pi(v_i, v_j^*)$ forment donc une famille libre dans $C(G, \mathbf{C})$. Cela montre l'injectivité de $\theta^\pi : V \otimes_k V^* \to C(G, \mathbf{C})$. Par définition, l'image de cette application est $\mathscr{M}_\pi$. Nous prouvons ainsi (i).

Les relations d'orthogonalité disent que les espaces $\mathscr{M}_\pi$ sont deux à deux orthogonaux pour la forme bilinéaire B. Comme la restriction de B à chaque $\mathscr{M}_\pi$ est non-dégénérée, cela entraîne que les $\mathscr{M}_\pi$ sont en somme directe, d'où (ii).

Enfin, l'assertion (iii) provient de (ii), de la proposition 4.4.2.3 (ii), et du théorème de Maschke. □

Remarques. Les assertions (i) et (ii) de la proposition ci-dessus peuvent être vues comme des cas particuliers du théorème de Frobenius-Schur 3.2.4.3. Notre preuve ici basée sur les relations d'orthogonalité présente l'avantage de ne pas faire appel au théorème de structure de Wedderburn-Artin, et l'inconvénient de nécessiter l'emploi de la mesure invariante.

Nous notons $\mathscr{C}$ le sous-espace vectoriel de $C(G, \mathbf{C})$ engendré par les caractères des représentations continues de dimension finie de G. C'est une sous-algèbre de $C(G, \mathbf{C})$ stable par l'involution $*$ et formée de fonctions de classe.

4.4.4.3 Proposition. *L'ensemble* $\{\chi_\pi \mid \pi \in G^\wedge\}$ *des caractères des représentations irréductibles continues est une base de* $\mathscr{C}$*. L'algèbre* $\mathscr{C}$ *est exactement l'ensemble des fonctions de classe appartenant à* $\mathscr{M}$*.*

Preuve. Chaque caractère χ_π appartient à l'espace $\mathscr{M}_\pi$. La proposition 4.4.4.2 (ii) montre que les χ_π sont linéairement indépendants. Le théorème de Maschke et le théorème 4.1.4.3 (iv) montrent que chaque caractère est combinaison $\mathbf{Z}$-linéaire de caractères irréductibles. On déduit de tout cela que $\{\chi_\pi \mid \pi \in G^\wedge\}$ est bien une base de $\mathscr{C}$.

Faisons agir G sur $C(G, \mathbf{C})$ par $g \cdot \varphi = \big(h \mapsto \varphi(g^{-1}hg)\big)$. Les invariants de cette action sont les fonctions de classe.

Soit $\pi : G \to \mathbf{GL}(V)$ une représentation continue de dimension finie. D'après la proposition 4.4.4.2 (i) et la remarque 4.4.2.2 (2), θ^π induit un isomorphisme de représentations de $\mathrm{Hom}_k(V, V)$ dans $C(G, \mathbf{C})$, d'image $\mathscr{M}_\pi$. D'après le lemme de Schur, les invariants sous l'action de G dans $\mathrm{Hom}_k(V, V)$ sont les éléments de la droite $\mathbf{C}\,\mathrm{id}_V$. Les invariants sous l'action de G dans $\mathscr{M}_\pi$ sont donc les éléments de la droite $\mathbf{C}\chi_\pi$.

Soit $\varphi \in \mathscr{M}$. La proposition 4.4.4.2 (iii) permet d'écrire $\varphi = \sum_{\pi \in G^\wedge} \varphi_\pi$, de façon unique, avec $\varphi_\pi \in \mathscr{M}_\pi$. Pour l'action par conjugaison définie plus haut, nous avons $g \cdot \varphi = \sum_{\pi \in G^\wedge} g \cdot \varphi_\pi$ pour chaque $g \in G$, avec $g \cdot \varphi_\pi \in \mathscr{M}_\pi$ car chaque $\mathscr{M}_\pi$ est une sous-représentation de $C(G, \mathbf{C})$. Pour que φ soit fixé par tous les $g \in G$, il est nécessaire et suffisant que chacun des φ_π soit fixé par g. En d'autres termes, pour que φ soit une fonction de classe, il faut et il suffit que chaque φ_π appartienne à la droite $\mathbf{C}\chi_\pi$. Cela prouve la seconde assertion de la proposition. □

Remarque. Dans le cas où G est fini, toutes les représentations sont continues, de sorte que l'espace $\mathscr{M}$ coïncide avec l'espace $(kG)^\circ$ du paragraphe 4.4.2, qui est lui-même égal à k^G tout entier d'après la proposition 4.4.2.4. De la proposition 4.4.4.2, on déduit que $|G| = \dim k^G = \sum_{\pi \in G^\wedge} (\deg \pi)^2$, un résultat que nous avions prouvé dans le paragraphe 4.2.2 en faisant appel au théorème de Wedderburn-Artin. La proposition 4.4.4.3 affirme pour sa part que le nombre de représentations irréductibles de G est égal à la dimension de $\mathscr{C}$, qui ici est l'algèbre $\mathrm{cf}_{\mathbf{C}}(G)$ toute entière puisque $\mathscr{M} = k^G$. Utilisant la proposition 4.2.2.1, on retrouve que G a autant de représentations irréductibles que de classes de conjugaison.

4.4.5 Le théorème de Peter-Weyl

4.4.5.1 Théorème (Peter, Weyl). *Soit* G *un groupe compact. Alors* $\mathscr{M}$ *est une sous-algèbre dense de* $C(G, \mathbf{C})$ *pour la norme de la convergence uniforme.*

Preuve. On définit le produit de convolution de deux fonctions continues φ et ψ sur G comme étant la fonction $\varphi * \psi : g \mapsto \int_G \varphi(gh^{-1})\psi(h)\, d\mu(h)$. Les propriétés du produit de convolution classique, étudiées dans tout bon cours d'analyse fonctionnelle, sont vraies dans ce cadre.

On se donne une fonction $\varphi \in C(G, \mathbf{C})$ et un réel $\varepsilon > 0$. Il existe un voisinage U de l'unité dans G tel que $|\varphi(gh) - \varphi(h)| \leq \varepsilon$ pour tous $g \in U$ et $h \in G$. Le lemme d'Urysohn montre l'existence d'une fonction ρ continue sur G à valeurs positives, nulle en dehors de $U \cap U^{-1}$, et

d'intégrale 1. Alors $\|\rho * \varphi - \varphi\| \leq \varepsilon$ pour la norme de la convergence uniforme dans $C(G, \mathbf{C})$. En outre, quitte à remplacer ρ par $(\rho + \rho^*)/2$, nous pouvons supposer que $\rho = \rho^*$.

L'opérateur $\rho*?$ sur $C(G, \mathbf{C})$ s'étend en un opérateur K sur l'espace de Hilbert $\mathscr{H} = L^2(G, \mathbf{C})$. Cet opérateur K est autoadjoint, puisque nous avons pris soin d'imposer $\rho = \rho^*$. Il est compact, car c'est un opérateur à noyau intégral. Enfin, son image est incluse dans $C(G, \mathbf{C})$, vu ici comme un sous-espace de $L^2(G, \mathbf{C})$.

D'après le théorème spectral pour les opérateurs autoadjoints compacts, K est diagonalisable en base hilbertienne. Plus précisément, soit $\sigma(K)$ l'ensemble des valeurs propres de K, et pour $\lambda \in \sigma(K)$, soit $\mathscr{H}_\lambda = \ker(K - \lambda \operatorname{id}_{\mathscr{H}})$ l'espace propre correspondant. On sait que $\mathscr{H}_\lambda$ est de dimension finie si $\lambda \neq 0$, que $\mathscr{H}$ est la somme directe hilbertienne des $\mathscr{H}_\lambda$, et que l'on peut ranger les éléments de $\sigma(K) \setminus \{0\}$ en une suite (éventuellement finie) $(\lambda_n)_{n \geq 0}$ tendant vers 0.

Si λ est une valeur propre non-nulle de K, alors $\mathscr{H}_\lambda$ est inclus dans $\operatorname{im} K$, donc dans $C(G, \mathbf{C})$. L'opérateur K agit sur une fonction ψ en faisant une moyenne, selon la mesure $\rho(h)\, d\mu(h)$, de translatées à gauche de ψ. Cette opération commute avec l'action de G par translations à droite. Cela entraîne que cette dernière laisse stables les espaces propres de K. Les $\mathscr{H}_\lambda$ sont donc des sous-espaces de dimension finie de $C(G, \mathbf{C})$, stables sous l'action de G par translations à droite. La proposition 4.4.2.4 dit alors que $\mathscr{H}_\lambda$ est inclus dans $\mathscr{M}$.

Développons φ sur la somme directe $\mathscr{H} = \bigoplus_{\lambda \in \sigma(K)} \mathscr{H}_\lambda$ en écrivant $\varphi = \sum_{\lambda \in \sigma(K)} \varphi_\lambda$. Cette série est convergente pour la norme de $\mathscr{H}$, autrement dit en moyenne quadratique. En utilisant l'inégalité de Cauchy-Schwarz, on montre alors que la série $K(\varphi) = \sum_{\lambda \in \sigma(K)} K(\varphi_\lambda)$ est convergente dans $C(G, \mathbf{C})$ pour la norme de la convergence uniforme. D'après l'alinéa précédent, chaque $K(\varphi_\lambda)$ appartient à $\mathscr{M}$. Ainsi $K(\varphi) = \rho * \varphi$ est limite dans $C(G, \mathbf{C})$ d'une suite d'éléments de $\mathscr{M}$.

Prenant alors $\varepsilon = 1/n$ et faisant tendre n vers l'infini, on en déduit que φ est limite dans $C(G, \mathbf{C})$ d'une suite d'éléménts de $\mathscr{M}$. □

L'ensemble des fonctions de classe continues est une sous-algèbre fermée de $C(G, \mathbf{C})$. On la munit de la norme de la convergence uniforme.

4.4.5.2 Corollaire. *Soit G un groupe compact. Alors $\mathscr{C}$ est une sous-algèbre dense de l'algèbre des fonctions de classe continues pour la norme de la convergence uniforme.*

Preuve. Soit φ une fonction de classe continue et soit $\varepsilon > 0$. Le théorème de Peter-Weyl garantit l'existence d'une fonction $\psi \in \mathscr{M}$ telle que $\|\varphi - \psi\| \leq \varepsilon$.

Nous munissons $C(G, \mathbf{C})$ de l'action de G par conjugaison, comme dans la preuve de la proposition 4.4.4.3. Chaque $\mathscr{M}_\pi$ en est une sous-représentation de dimension finie, ce qui permet d'introduire un opérateur de Reynolds $\natural : \mathscr{M}_\pi \to \operatorname{inv}_G \mathscr{M}_\pi$. On peut donc appliquer $\natural$ à ψ et obtenir un élément $\psi^\natural \in \mathscr{C}$.

Pour chaque $h \in H$, $\psi^\natural(h) = \int_G \psi(g^{-1}hg)\, d\mu(g)$, puis en utilisant que φ est centrale :

$$|\varphi(h) - \psi^\natural(h)| = \left| \int_G (\varphi - \psi)(g^{-1}hg)\, d\mu(g) \right| \leq \int_G \|\varphi - \psi\|\, d\mu(g) = \|\varphi - \psi\| \leq \varepsilon.$$

Ainsi $\|\varphi - \psi^\natural\| \leq \varepsilon$. Ceci achève la démonstration. □

4.4.6 Représentations unitaires

Considérons un groupe G, pas nécessairement compact. On dit qu'une représentation linéaire $\pi : G \to \mathbf{GL}(V)$ sur un $\mathbf{C}$-espace vectoriel complexe V est unitarisable s'il existe un produit scalaire hermitien $(?, ?)$ sur V qui fait de V un espace de Hilbert et qui est invariant sous G. Cette dernière condition signifie que pour tous $g \in G$ et $(v, w) \in V^2$, on a $(\pi(g)v, \pi(g)w) = (v, w)$; autrement dit, chaque opérateur $\pi(g)$ est unitaire.

4.4.6.1 Proposition. *Soit $\pi : G \to \mathbf{GL}(V)$ une représentation linéaire complexe unitarisable d'un groupe G. Fixons un produit scalaire hermitien $(?, ?)$ G-invariant sur V ; V devient ainsi un espace de Hilbert.*

(i) Si W est un sous-espace vectoriel fermé de V stable par l'action de chaque $\pi(g)$, alors le polaire (l'orthogonal) de W dans V pour le produit scalaire est un supplémentaire de W, stable par l'action de chaque $\pi(g)$.

(ii) Si V est de dimension finie, alors c'est une représentation complètement réductible de G (autrement dit, c'est un kG-module complètement réductible).

Preuve. Plaçons-nous dans les hypothèses de (i). Le fait que le polaire W° de W est un supplémentaire de W dans V est un résultat classique de théorie des espaces de Hilbert. Soit $g \in G$. Comme $\pi(g)$ est unitaire, son adjoint est son inverse $\pi\big(g^{-1}\big)$. Par hypothèse, cet adjoint laisse stable W. Un argument classique montre alors que $\pi(g)$ laisse stable le polaire W° de W, achevant la preuve de (i).

L'assertion (ii) est une conséquence immédiate de l'assertion (i). □

4.4.6.2 Proposition. *Soit $\pi : G \to \mathbf{GL}(V)$ une représentation linéaire complexe unitarisable de dimension finie d'un groupe G. Fixons un produit scalaire hermitien $(?, ?)$ G-invariant sur V. Pour $v \in V$, notons v^* la forme linéaire $(v, ?)$ sur V. Enfin, notons ζ le caractère de cette représentation.*

(i) Pour chaque $g \in G$ et $(v, w) \in V^2$, $\theta^\pi(v, w^*)\big(g^{-1}\big) = \overline{\theta^\pi(w, v^*)(g)}$.

(ii) Pour chaque $g \in G$, $\zeta\big(g^{-1}\big) = \overline{\zeta(g)}$.

(iii) Pour chaque $g \in G$, $|\zeta(g)| \leq \zeta(1)$, avec égalité si et seulement si $\pi(g)$ est un opérateur scalaire.

Preuve. Soient $g \in G$ et $(v, w) \in V^2$. Puisque $\pi(g)$ préserve le produit scalaire,

$$\theta^\pi(v, w^*)\big(g^{-1}\big) = (w, \pi(g)^{-1}v) = (\pi(g)w, v) = \overline{(v, \pi(g)w)} = \overline{\theta^\pi(w, v^*)(g)}.$$

Cela montre (i).

Prenons une base orthonormée de V et un élément $g \in G$. Dans cette base, la matrice U de $\pi(g)$ est unitaire : $U^{-1} = {}^t\overline{U}$. Ainsi

$$\zeta\big(g^{-1}\big) = \operatorname{tr} \pi(g)^{-1} = \operatorname{tr} U^{-1} = \overline{\operatorname{tr} U} = \overline{\operatorname{tr} \pi(g)} = \overline{\zeta(g)}.$$

Cela donne (ii).

Comme n'importe quelle matrice unitaire, U est diagonalisable et ses valeurs propres ξ_1, ..., ξ_n sont des nombres complexes de module 1. Ici, $n = \dim V = \zeta(1)$. Le module de $\zeta(g) = \xi_1 + \cdots + \xi_n$ est donc plus petit que n. Et pour que $|\zeta(g)| = n$, il faut et il suffit que les ξ_i soient tous égaux. Alors U est semblable, donc égale, à une matrice scalaire. Tout cela prouve (iii). □

4.4.6.3 Proposition. *Soit G un groupe compact et soit $\pi : G \to \mathbf{GL}(V)$ une représentation linéaire de G sur un espace vectoriel complexe V de dimension finie. Alors π est unitarisable.*

Preuve. Fixons un produit scalaire hermitien $(?,?)_0$ sur V. Pour $(v,w) \in V^2$, posons $(v,w) = \int_G (\pi(g)v, \pi(g)w)_0 \, d\mu(g)$. Alors $(?,?)$ est une forme sesquilinéaire hermitienne sur V. Elle est de plus définie positive, car si $v \neq 0$, l'intégrale $(v,v) = \int_G (\pi(g)v, \pi(g)v)_0 \, d\mu(g)$ est celle d'une fonction partout strictement positive. Enfin, on a fait tout ce qu'il fallait pour que $(?,?)$ soit invariante sous G. □

Cette proposition, jointe à la proposition 4.4.6.1 (ii), fournit une nouvelle démonstration du théorème de Maschke.

4.4.6.4 Théorème. *Soit G un groupe compact. Dans chaque représentation continue irréductible $\pi : G \to \mathbf{GL}(V)$, de dimension finie n_π, choisissons un produit scalaire hermitien G-invariant $(?,?)$ et une base orthonormée $(e_i)_{1 \leq i \leq n_\pi}$. On note c_{ij}^π le coefficient $g \mapsto (e_i, \pi(g)e_j)$ de la représentation π. Ainsi, le caractère de π est la fonction $\chi_\pi = \sum_{i=1}^{n_\pi} c_{ii}^\pi$.*

(i) Les éléments $\sqrt{n_\pi}\, c_{ij}^\pi$, pour $\pi \in G^\wedge$ et $1 \leq i,j \leq n_\pi$, forment une base hilbertienne de l'espace $L^2(G, \mathbf{C})$ des fonctions de carré sommable sur G.

(ii) Les caractères χ_π, pour $\pi \in G^\wedge$, forment une base hilbertienne de l'ensemble des fonctions de classe de carré sommable sur G.

Preuve. Les relations d'orthogonalité 4.4.4.1 et la proposition 4.4.6.2 (i) montrent que les éléments $\sqrt{n_\pi}\, c_{ij}^\pi$ forment une famille orthonormée dans $L^2(G, \mathbf{C})$. Le théorème de Peter-Weyl 4.4.5.1 dit que le sous-espace vectoriel que cette famille engendre est dense dans $C(G, \mathbf{C})$ pour la norme de la convergence uniforme, ce qui implique qu'il est dense dans $L^2(G, \mathbf{C})$ pour la norme de la convergence en moyenne quadratique. Ces deux faits donnent l'assertion (i). La preuve de l'assertion (ii) est analogue. □

Application. Soit $\mathbf{U}(1)$ le groupe compact des nombres complexes de module 1 ; ainsi $\theta \mapsto e^{i\theta}$ est un isomorphisme de $\mathbf{R}/2\pi\mathbf{Z}$ sur $\mathbf{U}(1)$. Les représentations irréductibles de $\mathbf{U}(1)$ sont de degré 1 d'après la proposition 4.2.4.1 ; ce sont les caractères linéaires $e_n : z \mapsto z^n$, vus comme fonctions de $\mathbf{U}(1)$ dans $\mathbf{C}^*$, pour $n \in \mathbf{Z}$. Le théorème 4.4.6.4 dit alors que la famille $(e_n)_{n \in \mathbf{Z}}$ est une base hilbertienne de l'espace $L^2(\mathbf{U}(1), \mathbf{C})$ des fonctions 2π-périodiques de carré sommable sur $\mathbf{R}$. On retrouve un fait bien connu de la théorie des séries de Fourier. Ainsi le théorème 4.4.6.4 généralise la théorie des séries de Fourier aux groupes compacts non-commutatifs.

Exercices.

(1) Soient G un groupe compact et $\pi : G \to \mathbf{GL}(V)$ une représentation de dimension finie. Soit $(?, ?)$ un produit scalaire hermitien invariant sous G. Montrer que l'opérateur de Reynolds $\natural$ est le projecteur orthogonal de V sur $\mathrm{inv}_G V$.

(2) Énoncer et prouver une généralisation aux groupes compacts de la proposition 4.2.3.2, pour les représentations linéaires continues.

5 Représentations du groupe symétrique et du groupe unitaire

5.1 L'anneau des fonctions symétriques

5.1.1 Partitions

Une partition est une suite décroissante $\lambda = (\lambda_1, \lambda_2, \ldots)$ d'entiers naturels nuls à partir d'un certain rang. On représente parfois une partition comme une suite finie, la convention étant que seuls des zéros ont été omis. Les λ_n sont appelées les parts de λ. On écrit parfois avec un exposant pour indiquer qu'une part est répétée un certain nombre de fois.

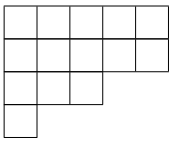
Exemple. $\lambda = (5, 5, 3, 1, 0, \ldots)$ est notée $\lambda = 5531$, voire $5^2 31$.

On note $\mathscr{P}$ l'ensemble des partitions.

Poids d'une partition : $|\lambda| = \lambda_1 + \lambda_2 + \cdots$. Si $|\lambda| = n$, on dit que λ est une partition de n et on écrit $\lambda \vdash n$.

Longueur d'une partition : $\ell(\lambda) = \mathrm{Card}\,\{n \geq 1 \mid \lambda_n > 0\}$.

Diagramme de Ferrers (ou de Young) de la partition λ : c'est un ensemble de $|\lambda|$ boîtes disposées de façon à décrire les parts de λ. Sur l'exemple de $\lambda = 5531$:



Partition conjuguée d'une partition λ : c'est la partition λ' dont les parts sont les $\lambda'_n = \mathrm{Card}\,\{i \geq 1 \mid \lambda_i \geq n\}$. Notamment $\lambda'_1 = \ell(\lambda)$. Pour $\lambda = 5531$, on trouve ainsi $\lambda' = 43322$. Le diagramme de Ferrers de λ' s'obtient en réfléchissant le diagramme de Ferrers de λ selon l'axe nord-ouest, sud-est. La conjugaison des partitions est une opération involutive : $\lambda'' = \lambda$.

Ordre de dominance : pour $\lambda, \mu \in \mathscr{P}$, on écrit $\lambda \geq \mu$ si

$$|\lambda| = |\mu| \quad \text{et} \quad \begin{cases} \lambda_1 \geq \mu_1, \\ \lambda_1 + \lambda_2 \geq \mu_1 + \mu_2, \\ \lambda_1 + \lambda_2 + \lambda_3 \geq \mu_1 + \mu_2 + \mu_3, \\ \cdots \end{cases}$$

On peut vérifier que $\lambda \geq \mu$ si et seulement si $\lambda' \leq \mu'$.

5.1.2 Sommes d'orbites

On se fixe un entier $n \geq 1$ (on fera $n \to \infty$ plus tard) et on se place dans l'anneau $\mathbf{Z}[x_1, \cdots, x_n]$ des polynômes en n variables à coefficients entiers. Étant donné un multi-exposant $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbf{N}^n$, on pose $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$.

Le groupe $\mathfrak{S}_n$ agit sur $\mathbf{Z}[x_1, \cdots, x_n]$ en permutant les indéterminées. Dans la partie 5.1, nous nous intéressons au sous-anneau $\Lambda_n = \mathbf{Z}[x_1, \cdots, x_n]^{\mathfrak{S}_n}$ des éléments invariants, appelés polynômes symétriques.

Le moyen le plus simple d'obtenir un polynôme symétrique est certainement de prendre un monôme x^α et de le symétriser. Le résultat ne dépend du multi-exposant α qu'à permutation près de ses termes α_1, ..., α_n, de sorte qu'on peut les supposer rangés dans l'ordre décroissant. Dit autrement, on part d'une partition λ de longueur $\ell(\lambda) \leq n$ on pose

$$m_\lambda = \text{somme de tous les monômes distincts de la forme } x_{\sigma(1)}^{\lambda_1} \cdots x_{\sigma(n)}^{\lambda_n},$$

où $\sigma \in \mathfrak{S}_n$. La somme comporte moins de $n!$ termes si λ présente des répétitions.

Le polynôme symétrique m_λ est appelé fonction monomiale.

Une autre façon de produire un polynôme symétrique est de faire le quotient de deux polynômes antisymétriques, et un moyen de produire un polynôme antisymétrique est d'antisymétriser un monôme. Posons ainsi

$$a_\alpha = \sum_{\sigma \in \mathfrak{S}_n} \operatorname{sgn}(\sigma) x_{\sigma(1)}^{\alpha_1} \cdots x_{\sigma(n)}^{\alpha_n} = \begin{vmatrix} x_1^{\alpha_1} & \dots & x_1^{\alpha_n} \\ \vdots & \ddots & \vdots \\ x_n^{\alpha_1} & \dots & x_n^{\alpha_n} \end{vmatrix}$$

pour chaque $\alpha \in \mathbf{N}^n$. Ce polynôme est nul si α a deux coordonnées égales, et il change de signe si l'on permute les coordonnées de α. Ainsi nous pouvons nous borner aux suites α strictement décroissantes ; elles s'écrivent sous la forme $\lambda + \delta$ où λ est une partition de longueur $\ell(\lambda) \leq n$ et $\delta = (n-1, n-2, \dots, 1, 0)$.

En effectuant une division euclidienne dans l'anneau $\mathbf{Z}[x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n][x_i]$, nous voyons qu'un polynôme antisymétrique en $x_1, \dots, x_n$ est divisible par chaque facteur $x_i - x_j$, donc est divisible par leur produit, le déterminant de Vandermonde

$$a_\delta = \prod_{1 \leq i < j \leq n} (x_i - x_j).$$

La multiplication par a_δ est donc une bijection de Λ_n sur l'ensemble des polynômes antisymétriques en x_1, ..., x_n.

Le quotient $s_\lambda = a_{\lambda+\delta}/a_\lambda$ est appelé fonction de Schur. Nous verrons plus loin (théorème de Littlewood 5.1.6.4) comment trouver une expression explicite de ces polynômes.

5.1.2.1 Proposition.

(i) $\{a_{\lambda+\delta} \mid \lambda \in \mathscr{P},\ \ell(\lambda) \leq n\}$ *est une base du sous-*$\mathbf{Z}$*-module de* $\mathbf{Z}[x_1, \cdots, x_n]$ *formé des polynômes antisymétriques.*

(ii) $\{m_\lambda \mid \lambda \in \mathscr{P},\ \ell(\lambda) \leq n\}$ *et* $\{s_\lambda \mid \lambda \in \mathscr{P},\ \ell(\lambda) \leq n\}$ *sont deux bases du* $\mathbf{Z}$*-module* Λ_n*.*

La preuve de cette proposition est laissée au lecteur.

5.1.3 Fonctions élémentaires

Pour $1 \leq k \leq n$, on définit la fonction symétrique élémentaire de degré k par

$$e_k = m_{(1^k)} = \sum_{1 \leq i_1 < \cdots < i_k \leq n} x_{i_1} \cdots x_{i_k}.$$

Pour $k \geq 1$, on définit la fonction symétrique complète de degré k par

$$h_k = \sum_{\lambda \vdash n} m_\lambda = \sum_{1 \leq i_1 \leq \cdots \leq i_k \leq n} x_{i_1} \cdots x_{i_k}.$$

Enfin, toujours pour $k \geq 1$, on définit la somme de puissances de degré k par

$$p_k = m_{(k)} = x_1^k + \cdots + x_n^k.$$

On pose $e_0 = h_0 = 1$ et $e_k = 0$ pour $k > n$. Les e_k, h_k, p_k sont des éléments de Λ_n.

On introduit les séries génératrices $E(t) = \sum_{k \geq 0} t^k e_k$, $H(t) = \sum_{k \geq 0} t^k h_k$.

Le théorème de Viète exprimant les coefficients d'un polynôme en fonction de ses racines conduit à l'identité

$$E(t) = \prod_{i=1}^{n} (1 + x_i t).$$

Par ailleurs,

$$H(t) = \sum_{\substack{k \geq 0 \\ 1 \leq i_1 \leq \cdots \leq i_k \leq n}} (x_{i_1} t) \cdots (x_{i_k} t) = \sum_{p_1, \ldots, p_n \geq 0} (x_1 t)^{p_1} \cdots (x_n t)^{p_n} = \prod_{i=1}^{n} \left(\sum_{p \geq 0} (x_i t)^p \right) = \prod_{i=1}^{n} \frac{1}{1 - x_i t}.$$

On en déduit l'égalité $H(t)E(-t) = 1$, puis les relations $\sum_{i=0}^{k} (-1)^i e_i h_{k-i} = 0$ pour tout $k \geq 1$.

Pour $\lambda \in \mathscr{P}$, on pose $e_\lambda = e_{\lambda_1} e_{\lambda_2} \cdots$ et $h_\lambda = h_{\lambda_1} h_{\lambda_2} \cdots$.

5.1.3.1 Théorème. *$\{e_{\lambda'} \mid \lambda \in \mathscr{P},\ \ell(\lambda) \leq n\}$ et $\{h_{\lambda'} \mid \lambda \in \mathscr{P},\ \ell(\lambda) \leq n\}$ sont deux bases du $\mathbf{Z}$-module Λ_n.*

Preuve. Pour λ et μ deux partitions de longueur au plus n, notons $C_{\lambda\mu}$ le coefficient du monôme x^μ dans le polynôme $e_{\lambda'}$. Un examen combinatoire simple [20] montre que $C_{\lambda\lambda} = 1$ et que $C_{\lambda\mu} \neq 0 \Rightarrow \mu \leq \lambda$. Ainsi $(C_{\lambda\mu})$ est une matrice unitriangulaire inférieure pour l'ordre de dominance sur $\{\lambda \in \mathscr{P} \mid \ell(\lambda) \leq n\}$; elle est donc inversible. Par ailleurs, la définition des fonctions symétriques monomiales et le fait que $e_{\lambda'}$ soit un polynôme symétrique entraînent

20. Les monômes dans $e_{\lambda'}$ correspondent à des remplissages des cases du diagramme de λ par des entiers entre 1 et n, de façon strictement croissante dans chaque colonne. À un tel remplissage correspond un monôme x^μ, où μ_i est le nombre de cases contenant i. Les entiers entre 1 et i ne peuvent apparaître que dans les i premières lignes du tableau, d'où $\mu_1 + \cdots + \mu_i \leq \lambda_1 + \cdots + \lambda_i$.

que $e_{\lambda'} = \sum_{\ell(\mu)\leq n} C_{\lambda\mu} m_\mu$. On passe ainsi des $\{m_\mu\}$ aux $\{e_{\lambda'}\}$ par une matrice inversible. La proposition 5.1.2.1 (ii) entraîne alors que $\{e_{\lambda'} \mid \ell(\lambda) \leq n\}$ est une base du $\mathbf{Z}$-module Λ_n.

Ainsi Λ_n est l'anneau des polynômes en e_1, ..., e_n à coefficients dans $\mathbf{Z}$. Il existe donc un homomorphisme d'anneaux $\omega_n : \Lambda_n \to \Lambda_n$ qui envoie e_k sur h_k pour chaque $1 \leq k \leq n$. À l'aide des relations $\sum_{i=0}^{k} (-1)^i e_i h_{k-i} = 0$, pour $1 \leq k \leq n$, on peut exprimer h_k comme un polynôme $P_k(e_1, \ldots, e_n)$ en les fonctions symétriques élémentaires. Ces relations faisant jouer des rôles symétriques aux variables $(e_k)_{1\leq k\leq n}$ et $(h_k)_{1\leq k\leq n}$, les mêmes manipulations conduisent à l'égalité $e_k = P_k(h_1, \ldots, h_n)$. Ainsi

$$\omega_n(h_k) = \omega_n(P_k(e_1, \ldots, e_n)) = P_k(\omega_n(e_1), \ldots, \omega_n(e_n)) = P_k(h_1, \ldots, h_n) = e_k.$$

Par conséquent, $(\omega_n)^2$ fixe les éléments e_k. Ceux-ci engendrant l'anneau Λ_n, cela montre que l'homomorphisme ω_n est involutif, donc en particulier est un isomorphisme. On en déduit que $\{h_{\lambda'} \mid \ell(\lambda) \leq n\}$ est également une base du $\mathbf{Z}$-module Λ_n. □

Le théorème 5.1.3.1 signifie que Λ_n est un anneau de polynômes en n indéterminées à coefficients dans $\mathbf{Z}$; comme base en tant que $\mathbf{Z}$-algèbre, on peut choisir la famille $(e_1, \ldots, e_n)$ ou la famille $(h_1, \ldots, h_n)$.

L'identité suivante permet de rattacher les sommes de puissances aux fonctions symétriques complètes et élémentaires.

$$H(t) = \prod_{i=1}^{n} \frac{1}{1 - x_i t} = \exp\left(- \sum_{i=1}^{n} \log(1 - x_i t) \right) = \exp\left(\sum_{i=1}^{n} \sum_{k\geq 1} \frac{(x_i t)^k}{k} \right) = \prod_{k\geq 1} \exp\left(\frac{p_k t^k}{k} \right)$$

Pour $\lambda \in \mathscr{P}$, on écrit $\lambda = \cdots 2^{m_2(\lambda)} 1^{m_1(\lambda)}$, où $m_i(\lambda) = \mathrm{Card}\,\{n \geq 1 \mid \lambda_n = i\}$. On pose $z_\lambda = \prod_{i\geq 1} \left(i^{m_i(\lambda)} m_i(\lambda)! \right)$ et $p_\lambda = \prod_{i\geq 1} p_i^{m_i(\lambda)}$.

5.1.3.2 Proposition. *Pour tout $k \geq 1$, on a*

$$h_k = \sum_{\lambda \vdash k} p_\lambda / z_\lambda \quad \textit{et} \quad e_k = \sum_{\lambda \vdash k} (-1)^{|\lambda| + \ell(\lambda)} p_\lambda / z_\lambda.$$

Preuve. La première égalité s'obtient en examinant le coefficient de t^k dans

$$\begin{aligned} H(t) &= \prod_{k\geq 1} \left(\sum_{m\geq 0} \frac{1}{m!} \left(\frac{p_k t^k}{k} \right)^m \right) \\ &= \sum_{m_1, m_2, \cdots \geq 0} \frac{1}{m_1!} \left(\frac{p_1 t^1}{1} \right)^{m_1} \frac{1}{m_2!} \left(\frac{p_2 t^2}{2} \right)^{m_2} \cdots \end{aligned}$$

La seconde s'obtient de façon similaire en partant de

$$E(t) = H(-t)^{-1} = \prod_{k\geq 1} \exp\left(- \frac{p_k (-t)^k}{k} \right).$$

□

Notons également l'identité

$$\sum_{k\geq 1} p_k t^k = t\frac{d}{dt}\left(\sum_{k\geq 1}\frac{p_k t^k}{k}\right) = t\frac{d}{dt}\log H(t) = \frac{tH'(t)}{H(t)} = \frac{tE'(-t)}{E(-t)}$$

qui conduit aux formules de Newton :

$$\sum_{i=1}^{k} p_i h_{k-i} = kh_k, \qquad \sum_{i=1}^{k}(-1)^{i+1} p_i e_{k-i} = ke_k.$$

5.1.3.3 Proposition. *$\{p_{\lambda'} \mid \ell(\lambda)\leq n\}$ est une base du $\mathbf{Q}$-espace vectoriel $\Lambda_n \otimes_{\mathbf{Z}} \mathbf{Q}$.*

Preuve. Nous venons de voir que les éléments e_1, ..., e_n sont des polynômes à coefficients rationnels en les variables p_1, ..., p_n. Par conséquent, tous les éléments de la famille $\{e_{\lambda'} \mid \lambda\in\ell(\lambda)\leq n\}$ appartiennent au sous-$\mathbf{Q}$-espace vectoriel de $\Lambda_n\otimes_{\mathbf{Z}}\mathbf{Q}$ engendré par la famille $\{p_{\lambda'} \mid \ell(\lambda)\leq n\}$. De plus, ces deux familles sont formées d'éléments homogènes et ont le même nombre fini d'éléments en chaque degré. Le fait que la première famille soit une base (théorème 5.1.3.1) entraîne alors que la seconde en est aussi une. □

5.1.4 Action par multiplication sur les fonctions de Schur

On convient que $s_\lambda = 0$ si $\ell(\lambda) > n$.

Notation : si λ est une partition et $k\geq 1$ est un entier, alors on désigne par $\lambda\otimes k$ (respectivement, $\lambda\otimes 1^k$) l'ensemble des partitions μ obtenues en ajoutant k cases au diagramme de λ, au plus une par colonne (respectivement, ligne).

5.1.4.1 Formules de Pieri. *Avec cette notation,*

$$s_\lambda h_k = \sum_{\mu\in\lambda\otimes k} s_\mu \qquad et \qquad s_\lambda e_k = \sum_{\mu\in\lambda\otimes 1^k} s_\mu.$$

Preuve. Pour $\alpha=(\alpha_1,\ldots,\alpha_n)\in\mathbf{N}^n$, posons $|\alpha| = \alpha_1+\cdots+\alpha_n$. Partons de

$$\begin{aligned} a_{\lambda+\delta}h_k &= \sum_{\sigma\in\mathfrak{S}_n}\operatorname{sgn}(\sigma)x_{\sigma(1)}^{\lambda_1+\delta_1}\cdots x_{\sigma(n)}^{\lambda_n+\delta_n}\left(\sum_{\substack{\alpha\in\mathbf{N}^n\\|\alpha|=k}} x_{\sigma(1)}^{\alpha_1}\cdots x_{\sigma(n)}^{\alpha_n}\right)\\ &= \sum_{\substack{\alpha\in\mathbf{N}^n\\|\alpha|=k}}\left(\sum_{\sigma\in\mathfrak{S}_n}\operatorname{sgn}(\sigma)x_{\sigma(1)}^{\lambda_1+\delta_1+\alpha_1}\cdots x_{\sigma(n)}^{\lambda_n+\delta_n+\alpha_n}\right)\\ &= \sum_{\substack{\alpha\in\mathbf{N}^n\\|\alpha|=k}} a_{\lambda+\delta+\alpha}. \end{aligned}$$

Ainsi

$$a_{\lambda+\delta}h_k = \sum_{\mu\in\lambda\otimes k} a_{\mu+\delta} + \sum_{\substack{|\alpha|=k\\ \lambda+\alpha\notin\lambda\otimes k}} a_{\lambda+\delta+\alpha}.$$

La condition $\lambda+\alpha\notin\lambda\otimes k$ signifie qu'il existe i tel que $\alpha_{i+1}>\lambda_i-\lambda_{i+1}$. Choisissant i le plus grand possible vérifiant cette inégalité et posant

$$\beta_j=\begin{cases}\alpha_{i+1}-(\lambda_i-\lambda_{i+1}+1) & \text{si } j=i,\\ \alpha_i+(\lambda_i-\lambda_{i+1}+1) & \text{si } j=i+1,\\ \alpha_j & \text{sinon,}\end{cases}$$

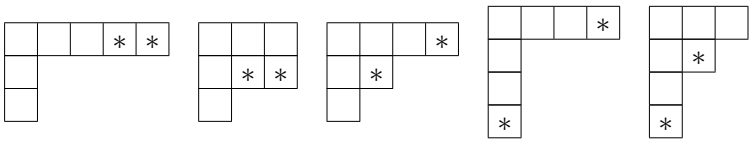
on définit une involution $\alpha\mapsto\beta$ de

$$\left\{\alpha\in\mathbf{N}^n \;\middle|\; |\alpha|=k,\ \lambda+\alpha\notin\lambda\otimes k\right\}$$

pour laquelle $a_{\lambda+\alpha+\delta}=-a_{\lambda+\beta+\delta}$. Les termes non nuls de la seconde somme s'annulent donc deux à deux, prouvant la première formule de Pieri.

La preuve de la seconde est similaire, en fait un peu plus simple. □

Exemple. $s_{311}h_2=s_{511}+s_{331}+s_{421}+s_{4111}+s_{3211}$; les cases rajoutées au diagramme de 311 sont indiquées par une étoile.



Les formules de Pieri entraînent immédiatement que $s_k=h_k$ et $s_{(1^k)}=e_k$. Plus généralement, elles permettent par itération de développer n'importe quel monôme en les fonctions symétriques complètes ou élémentaires sur la base des fonctions de Schur. Nous reverrons cela dans la section 5.1.6.

En sens inverse, on peut exprimer les fonctions de Schur comme des polynômes en les fonctions symétriques complètes ou élémentaires.

5.1.4.2 Formules de Jacobi-Trudi.

Soit λ une partition. Alors

$$s_\lambda=\det(h_{\lambda_i-i+j})_{1\le i,j\le n} \quad \textit{et} \quad s_{\lambda'}=\det(e_{\lambda_i-i+j})_{1\le i,j\le n}.$$

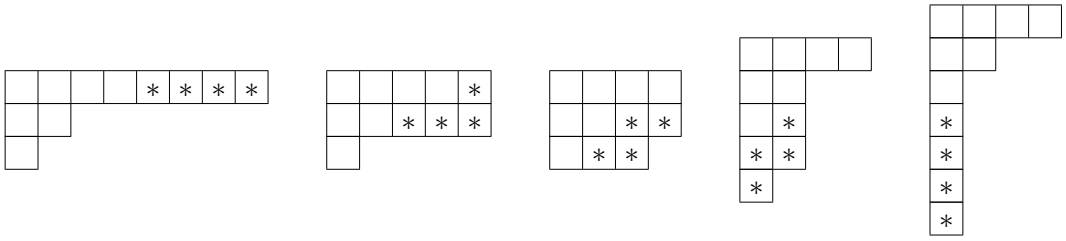
N'ayant pas besoin des formules de Jacobi-Trudi, nous ne les démontrons pas. Notons cependant que si $\ell(\lambda)>n$, alors le membre de gauche de la première formule est nul, donc le membre de droite l'est aussi ; cela donne une relation non triviale entre les fonctions symétriques complètes.

Maintenant, appelons bande un ensemble de cases contiguës, obtenu en parcourant un chemin formé de pas soit vers le haut, soit vers la droite. La hauteur $h(\theta)$ d'une bande θ est le nombre de lignes qu'elle occupe moins un.

5.1.4.3 Proposition. *$s_\lambda p_k = \sum_\theta (-1)^{h(\theta)} s_{\lambda+\theta}$, la somme portant sur les bandes θ à k cases telles que $\lambda+\theta$ soit une partition.*

Preuve. Soit ε_i le vecteur de base $(0,\dots,1,\dots,0)$ avec un 1 à la position i. Le même calcul que celui mené au début de la preuve des formules de Pieri donne $a_{\lambda+\delta}p_k = \sum_{i=1}^n a_{\lambda+k\varepsilon_i+\delta}$. Enroulons une bande θ autour du diagramme de λ en partant de la i-ème ligne et notons $\lambda+\theta$ la suite des longueurs des lignes du résultat de cette opération. Alors les suites $\lambda+\theta+\delta$ et $\lambda+k\varepsilon_i+\delta$ ne différent que par l'ordre de leurs termes. Si $\lambda+\theta$ est une partition, alors on passe de $\lambda+\theta+\delta$ à $\lambda+k\varepsilon_i+\delta$ en effectuant $h(\theta)$ inversions, d'où $a_{\lambda+k\varepsilon_i+\delta} = (-1)^{h(\theta)} a_{\lambda+\theta+\delta}$. Sinon, la suite $\lambda+k\varepsilon_i+\delta$ contient deux termes égaux et alors $a_{\lambda+k\varepsilon_i+\delta} = 0$. On obtient en fin de compte $a_{\lambda+\delta}p_k = \sum_\theta (-1)^{h(\theta)} a_{\lambda+\theta}$, et il n'y a plus qu'à diviser par a_δ. □

Exemple. $s_{421}p_4 = s_{821} - s_{551} - s_{443} + s_{42221} - s_{4211111}$, les différents termes correspondant aux bandes repérées ci-dessous par des $*$:



Un cas particulier amusant de la proposition 5.1.4.3 est que la somme de puissances p_k s'exprime comme une somme alternée de fonctions de Schur pour des partitions en forme d'équerres : $p_k = s_{(k)} - s_{(k-1,1)} + s_{(k-2,1^2)} - s_{(k-3,1^3)} + \cdots + (-1)^k s_{(1^k)}$.

5.1.5 L'anneau Λ

Pour $k > n$, on a $e_k = 0$ mais $h_k \neq 0$. Pour rendre la situation plus symétrique, on veut donner un sens à $n = \infty$.

L'évaluation $x_{n+1} \mapsto 0$ fournit un homomorphisme d'anneaux gradués $\mathbf{Z}[x_1,\cdots,x_{n+1}] \to \mathbf{Z}[x_1,\cdots,x_n]$, qui se restreint en un homomorphisme $\Lambda_{n+1} \to \Lambda_n$. Cet homomorphisme envoie les éléments h_k, e_k, p_k de Λ_{n+1} sur les éléments du même nom dans Λ_n, rendant la notation non ambiguë.

Nous avons convenu que $s_\lambda = 0$ dans Λ_n si $\ell(\lambda) > n$. De la même façon, nous convenons que $m_\lambda = 0$ dans dans Λ_n si $\ell(\lambda) > n$. Alors l'homomorphisme $\Lambda_{n+1} \to \Lambda_n$ envoie les fonctions monomiales m_λ de Λ_{n+1} sur les éléments du même nom dans Λ_n. Grâce aux formules de Pieri (théorème 5.1.4.1), on vérifie qu'il en est de même pour les fonctions de Schur.

L'anneau Λ_n est gradué par le degré total des polynômes :

$$\Lambda_n = \bigoplus_{k\in\mathbf{N}} \Lambda_n^k.$$

La proposition 5.1.2.1 (ii) affirme que $\{m_\lambda \mid \lambda \in \mathscr{P},\ |\lambda| = k,\ \ell(\lambda) \leq n\}$ est une base de Λ_n^k. Comme la longueur d'une partition est inférieure ou égale à son poids, on voit que la composante en degré k de notre homomorphisme $\Lambda_{n+1} \to \Lambda_n$ est bijective si $n \geq k$.

On peut donc noter Λ^k l'espace Λ_n^k pour n assez grand, car il devient alors essentiellement indépendant de n. Concrètement, on peut voir Λ comme l'ensemble de toutes les séries formelles en x_1, x_2, ... homogènes de degré k et symétriques. On pose ensuite

$$\Lambda = \bigoplus_{k \in \mathbf{N}} \Lambda^k.$$

Alors Λ hérite une structure d'anneau gradué. Pour chaque $n \geq 1$, 'évaluation $x_i \mapsto 0$ pour $i > n$ définit un homomorphisme surjectif d'anneaux de Λ sur Λ_n. Les fonctions symétriques h_k, e_k, p_k, m_λ, s_λ se remontent naturellement à Λ, et toutes les identités qu'elles satisfont dans Λ « descendent » ensuite dans les anneaux Λ_n. Utiliser Λ est ainsi une commodité qui ne présente aucun inconvénient.

5.1.5.1 Proposition.

(i) $\{m_\lambda \mid \lambda \in \mathscr{P}\}$, $\{h_\lambda \mid \lambda \in \mathscr{P}\}$, $\{e_\lambda \mid \lambda \in \mathscr{P}\}$ *et* $\{s_\lambda \mid \lambda \in \mathscr{P}\}$ *sont des bases du* $\mathbf{Z}$*-module* Λ. *En particulier,* Λ *est l'anneau des polynômes en* h_1, h_2, *... ; c'est aussi l'anneau des polynômes en* e_1, e_2, *...*

(ii) $\{p_\lambda \mid \lambda \in \mathscr{P}\}$ *est une base du* $\mathbf{Q}$*-espace vectoriel* $\Lambda \otimes_{\mathbf{Z}} \mathbf{Q}$.

L'anneau Λ est muni d'une involution ω qui échange h_k et e_k pour chaque $k \geq 1$. (Note : l'involution ω_n de l'anneau Λ_n utilisée dans la preuve du théorème 5.1.3.1 n'est pas induite par ω.) On vérifie sans difficulté (par exemple avec les formules de Newton) que $\omega(p_k) = (-1)^{k+1} p_k$. La symétrie présente dans les relations de Pieri ou les formules de Jacobi-Trudi entraîne que $\omega(s_\lambda) = s_{\lambda'}$ pour chaque $\lambda \in \mathscr{P}$.

À présent, nous cherchons à munir Λ d'un produit scalaire, pour lequel les composantes homogènes sont deux à deux orthogonales. Nous commençons par quelques formules, faisant intervenir deux jeux de variables $\{x_1, x_2, \ldots\}$ et $\{y_1, y_2, \ldots\}$.

5.1.5.2 Proposition.

$$\sum_{\lambda \in \mathscr{P}} h_\lambda(x) m_\lambda(y) = \prod_{i,j \geq 1} (1 - x_i y_j)^{-1}$$

$$\sum_{\lambda \in \mathscr{P}} \frac{p_\lambda(x) p_\lambda(y)}{z_\lambda} = \prod_{i,j \geq 1} (1 - x_i y_j)^{-1}$$

$$\sum_{\lambda \in \mathscr{P}} s_\lambda(x) s_\lambda(y) = \prod_{i,j \geq 1} (1 - x_i y_j)^{-1}$$

$$\sum_{\lambda \in \mathscr{P}} s_{\lambda'}(x) s_\lambda(y) = \prod_{i,j \geq 1} (1 + x_i y_j).$$

Preuve. La première formule est

$$\prod_{i,j\geq 1}(1-x_iy_j)^{-1}=\prod_{j\geq 1}H(y_j)=\prod_{j\geq 1}\left(\sum_{r\geq 0}h_r(x)y_j^r\right)=\sum_{\lambda\in\mathscr{P}}h_\lambda(x)m_\lambda(y).$$

La seconde formule résulte du calcul

$$\begin{aligned}\prod_{i,j\geq 1}(1-x_iy_j)^{-1}&=\exp\left(-\sum_{i,j\geq 1}\log(1-x_iy_j)\right)\\&=\exp\left(\sum_{k\geq 1}\sum_{i,j\geq 1}\frac{(x_iy_j)^k}{k}\right)\\&=\prod_{k\geq 1}\exp\frac{p_k(x)p_k(y)}{k}\\&=\sum_{m_1,m_2,\cdots\geq 0}\prod_{k\geq 1}\frac{1}{m_k!}\left(\frac{p_k(x)p_k(y)}{k}\right)^{m_k}\\&=\sum_{\lambda\in\mathscr{P}}\frac{1}{z_\lambda}\prod_{k\geq 1}\Big(p_k(x)p_k(y)\Big)^{m_k(\lambda)}\\&=\sum_{\lambda\in\mathscr{P}}\frac{p_\lambda(x)p_\lambda(y)}{z_\lambda}.\end{aligned}$$

Rappelons maintenant un calcul classique de déterminant connu sous le nom de déterminant de Cauchy (voir [17], p. 202, Lemma 7.6.A) :

$$\det\left(\frac{1}{1-x_iy_j}\right)_{1\leq i,j\leq n}=\frac{\prod_{1\leq i<j\leq n}(x_j-x_i)\ \prod_{1\leq i<j\leq n}(y_j-y_i)}{\prod_{1\leq i,j\leq n}(1-x_iy_j)}.$$

On prouve cette formule par des manipulations de lignes et de colonnes sur la matrice dont on veut calculer le déterminant. Écrivant

$$\frac{1}{1-x_iy_j}-\frac{1}{1-x_1y_j}=\frac{x_i-x_1}{1-x_1y_j}\cdot\frac{y_j}{1-x_iy_j},$$

et retranchant la première ligne des lignes suivantes, on voit que le déterminant cherché est

$$\frac{\prod_{i=2}^n(x_i-x_1)}{\prod_{j=1}^n(1-x_1y_j)}\begin{vmatrix}1&1&\dots&1\\ \frac{y_1}{1-x_2y_1}&\frac{y_2}{1-x_2y_2}&\cdots&\frac{y_n}{1-x_2y_n}\\ \vdots&\vdots&\ddots&\vdots\\ \frac{y_1}{1-x_ny_1}&\frac{y_2}{1-x_ny_2}&\cdots&\frac{y_n}{1-x_ny_n}\end{vmatrix}.$$

Soustrayant alors la première colonne des colonnes suivantes, et utilisant pour ce faire

$$\frac{y_j}{1-x_iy_j}-\frac{y_1}{1-x_iy_1}=\frac{y_j-y_1}{1-x_iy_1}\cdot\frac{1}{1-x_iy_j},$$

on obtient

$$\frac{\prod_{i=2}^n (x_i - x_1)}{\prod_{j=1}^n (1 - x_1 y_j)} \cdot \frac{\prod_{j=2}^n (y_j - y_1)}{\prod_{i=2}^n (1 - x_i y_1)} \begin{vmatrix} 1 & 0 & \dots & 0 \\ * & \frac{1}{1-x_2y_2} & \cdots & \frac{1}{1-x_2y_n} \\ \vdots & \vdots & \ddots & \vdots \\ * & \frac{1}{1-x_ny_2} & \cdots & \frac{1}{1-x_ny_n} \end{vmatrix}.$$

On conclut alors par récurrence sur n.

Soit $\delta = (n-1, n-2, \dots, 1, 0)$, comme dans le paragraphe 5.1.2. La formule du déterminant de Cauchy permet d'écrire l'égalité

$$\begin{aligned} a_\delta(x) a_\delta(y) \prod_{1 \le i,j \le n} (1 - x_i y_j)^{-1} &= \det\big((1 - x_i y_j)^{-1}\big)_{1 \le i,j \le n} \\ &= \begin{vmatrix} \vdots & & \vdots \\ \sum_{k \ge 0} x_i^k y_1^k & \dots & \sum_{k \ge 0} x_i^k y_n^k \\ \vdots & & \vdots \end{vmatrix} \\ &= \sum_{k_1, \dots, k_n \ge 0} y_1^{k_1} \cdots y_n^{k_n} \begin{vmatrix} x_1^{k_1} & \dots & x_1^{k_n} \\ \vdots & \ddots & \vdots \\ x_n^{k_1} & \dots & x_n^{k_n} \end{vmatrix} \\ &= \sum_{\substack{\lambda \in \mathscr{P} \\ \ell(\lambda) \le n}} a_{\lambda+\delta}(y) a_{\lambda+\delta}(x) \end{aligned}$$

dans $\mathbf{Z}[x_1, \dots, x_n, y_1, \dots, y_n]$. Le passage de la pénultième à la dernière ligne s'obtient en remarquant qu'il suffit de sommer sur les $(k_1, \dots, k_n)$ à coordonnées toutes distinctes, autrement dit $(k_1, \dots, k_n) = \sigma(\lambda + \delta)$, avec λ partition de longueur $\le n$ et $\sigma \in \mathfrak{S}_n$. Divisant par $a_\delta(x) a_\delta(y)$, on obtient la troisième formule, du moins pour n variables x et y, c'est-à-dire après substitution $x_k = y_k = 0$ pour $k > n$. On passe alors de Λ_n à Λ en comparant les coefficients des monômes présents dans chacun des membres de la formule.

Enfin, la quatrième formule s'obtient à partir de la troisième en appliquant l'involution ω sur les variables x :

$$\begin{aligned} \sum_{\lambda \in \mathscr{P}} s_{\lambda'}(x) s_\lambda(y) = \omega_x \left(\sum_{\lambda \in \mathscr{P}} s_\lambda(x) s_\lambda(y) \right) = \omega_x \left(\sum_{\lambda \in \mathscr{P}} h_\lambda(x) m_\lambda(y) \right) = \sum_{\lambda \in \mathscr{P}} e_\lambda(x) m_\lambda(y) \\ = \prod_{j \ge 1} \left(\sum_{r \ge 0} e_r(x) y_j^r \right) = \prod_{j \ge 1} E(y_j) = \prod_{i,j \ge 1} (1 + x_i y_j). \end{aligned}$$

□

On définit un produit scalaire $\langle ?, ? \rangle$ sur $\Lambda \otimes_{\mathbf{Z}} \mathbf{Q}$ en demandant que les fonctions de Schur forment une base orthonormée. L'involution ω de Λ permute les fonctions de Schur, donc préserve ce produit scalaire.

5.1.5.3 Proposition. *Pour $(\lambda, \mu) \in \mathscr{P}^2$, on a $\langle h_\lambda, m_\mu \rangle = \delta_{\lambda\mu}$ et $\langle p_\lambda, p_\mu \rangle = z_\lambda \delta_{\lambda\mu}$.*

Preuve. Nous allons montrer plus généralement que si $\{u_\lambda\}$, $\{v_\lambda\}$ sont deux familles de polynômes symétriques homogènes, avec u_λ et v_λ de degré $|\lambda|$, telles que

$$\sum_{\lambda \in \mathscr{P}} u_\lambda(x) v_\lambda(y) = \prod_{i,j \geq 1} (1 - x_i y_j)^{-1},$$

alors $\langle u_\lambda, v_\mu \rangle = \delta_{\lambda\mu}$.

Écrivons $u_\mu = \sum_{\lambda \in \mathscr{P}} B_{\lambda\mu} s_\lambda$ et $v_\mu = \sum_{\nu \in \mathscr{P}} C_{\mu\nu} s_\nu$. Alors

$$\sum_{\lambda \in \mathscr{P}} s_\lambda(x) s_\lambda(y) = \prod_{i,j \geq 1} (1 - x_i y_j)^{-1} = \sum_{\mu \in \mathscr{P}} u_\mu(x) v_\mu(y) = \sum_{\lambda,\mu,\nu \in \mathscr{P}} B_{\lambda\mu} C_{\mu\nu} s_\lambda(x) s_\nu(y),$$

d'où $\sum_{\mu \in \mathscr{P}} B_{\lambda\mu} C_{\mu\nu} = \delta_{\lambda\nu}$ puisque les éléments de $\{s_\lambda(x) s_\nu(y)\}$ forment une famille libre. Ainsi le produit de matrices BC est l'identité. Il en est donc de même du produit CB, d'où

$$\langle u_\mu, v_\rho \rangle = \sum_{\lambda,\nu \in \mathscr{P}} B_{\lambda\mu} C_{\rho\nu} \langle s_\lambda, s_\nu \rangle = \sum_{\lambda \in \mathscr{P}} C_{\rho\lambda} B_{\lambda\mu} = \delta_{\rho\nu}.$$

□

5.1.6 Tableaux

Soient $\lambda \in \mathscr{P}$ et $\mu = (\mu_1, \mu_2, \ldots)$ une suite d'entiers naturels presque tous nuls de somme $|\lambda|$.

On appelle tableau semi-standard de forme λ et de poids μ un remplissage du diagramme de λ par les éléments

$$\underbrace{1, \ldots, 1}_{\mu_1 \text{ fois}}, \ \underbrace{2, \ldots, 2}_{\mu_1 \text{ fois}}, \ \ldots$$

de façon croissante dans les lignes et strictement croissante dans les colonnes.

On appelle tableau multibande de forme λ et de poids μ un remplissage du diagramme de λ par les mêmes éléments, mais cette fois de façon croissante dans les lignes et dans les colonnes et de sorte que pour chaque i l'ensemble des cases contenant la valeur i forme une bande. La hauteur d'un tableau multibande est la somme des hauteurs des bandes qui le forment.

Exemple.

1	2	2	3	3	5
2	3	5	5		
4	4	6	6		
5	6				

et

1	3	3	3	4	4
2	5	5	6		
2	5	6	6		
2	5				

sont respectivement des tableaux semi-standard et multibande de forme $\lambda = 64^2 2$ et de poids $\mu = (1, 3, 3, 2, 4, 3)$ (les zéros traînant à la fin de μ ont été supprimés). Le tableau multibande est de hauteur 5.

On note $K_{\lambda,\mu}$ le nombre de tableaux semi-standards de forme λ et de poids μ. On se restreint souvent au cas où μ est une partition ; dans ce cas $K_{\lambda,\mu}$ s'appelle nombre de Kostka.

Enfin, soit λ une partition de poids n. On appelle tableau standard de forme λ un tableau semi-standard de poids $(1,\dots,1,0,\dots)$ (1 répété n fois). Ainsi, tous les chiffres entre 1 et n apparaissent exactement une fois dans les cases du diagramme de λ, de façon strictement croissante dans les lignes et dans les colonnes. Le nombre de tableaux standards de forme λ est le nombre de Kostka $K_{\lambda,(1^n)}$; il est strictement positif.

5.1.6.1 Proposition. *Soient λ et μ deux partitions. Si $K_{\lambda,\mu} \neq 0$, alors $\lambda \geq \mu$. De plus, $K_{\lambda,\lambda} = 1$.*

Preuve. Dans un tableau semi-standard, les entiers entre 1 et i ne peuvent apparaître que dans les i premières lignes. Par conséquent, s'il existe un tableau semi-standard de forme λ et de poids μ, alors nécessairement $\mu_1 + \cdots + \mu_i \leq \lambda_1 + \cdots + \lambda_i$ pour chaque i. □

5.1.6.2 Proposition. *Soit $\mu = (\mu_1, \mu_2, \dots)$ une suite d'entiers naturels presque tous nuls et soit $n = \mu_1 + \mu_2 + \cdots$. Alors dans l'anneau Λ*

$$h_{\mu_1} h_{\mu_2} \cdots = \sum_{\lambda \vdash n} K_{\lambda,\mu} s_\lambda \quad \textit{et} \quad p_{\mu_1} p_{\mu_2} \cdots = \sum_{\lambda \vdash n} \left(\sum_T (-1)^{h(T)} \right) s_\lambda,$$

la somme intérieure dans la deuxième formule portant sur l'ensemble des tableaux multibandes de forme λ et de poids μ et la notation $h(T)$ désignant la hauteur du tableau T.

Preuve. La preuve se fait par récurrence sur p, le plus grand des indices i tels que $\mu_i \neq 0$. Pour la première formule, l'hérédité se prouve à l'aide de la formule de Pieri 5.1.4.1 : un tableau semi-standard de poids μ s'obtient à partir d'un tableau de poids $(\mu_1, \mu_2, \dots, \mu_{p-1}, 0, 0, \dots)$ en ajoutant μ_p cases dans des colonnes différentes de façon à former encore une partition. Pour la seconde formule, on utilise la proposition 5.1.4.3. □

5.1.6.3 Corollaire. *Si λ et μ des partitions de même poids, alors $\langle h_\mu, s_\lambda \rangle = K_{\lambda,\mu}$.*

Preuve. Le corollaire découle de la proposition précédente et du fait que les fonctions de Schur forment une base orthonormée de Λ. □

Une conséquence de la proposition 5.1.6.2 est qu'à l'instar de h_μ, le nombre $K_{\lambda,\mu}$ ne dépend de μ qu'à permutation des μ_i près. Ce fait est exploité dans la preuve du théorème ci-dessous.

5.1.6.4 Théorème de Littlewood. *Dans l'anneau Λ_n,*

$$s_\lambda = \sum_\mu K_{\lambda,\mu}\, x^\mu, \qquad (*)$$

la somme portant sur tous les multi-exposants $\mu \in \mathbf{N}^n$ tels que $\mu_1 + \cdots + \mu_n = |\lambda|$.

Preuve. La remarque qui précède l'énoncé de ce théorème explique que le membre de droite de l'égalité $(*)$ est un polynôme symétrique. Il est donc égal à

$$\sum_{\mu\in\mathscr{P}} K_{\lambda,\mu} m_\mu.$$

En utilisant le corollaire 5.1.6.3 et le fait que $\{h_\mu\}$ et $\{m_\mu\}$ forment des bases duales pour $\langle ?, ?\rangle$, on est alors conduit à

$$\sum_{\mu\in\mathscr{P}} K_{\lambda,\mu} m_\mu = \sum_{\mu\in\mathscr{P}} \langle h_\mu, s_\lambda\rangle m_\mu = s_\lambda.$$

□

5.2 Représentations du groupe symétrique

5.2.1 Classes de conjugaison

À $\sigma \in \mathfrak{S}_n$, on associe la suite $\rho(\sigma)$ des longueurs des cycles de σ, classées par ordre décroissant ; c'est une partition de n. Cette application $\sigma \mapsto \rho(\sigma)$ induit une bijection entre l'ensemble des classes de conjugaison de $\mathfrak{S}_n$ et l'ensemble des partitions de poids n. Pour une partition λ de n, on note $C_\lambda \subset \mathfrak{S}_n$ la classe de conjugaison formée des permutations σ telles que $\rho(\sigma) = \lambda$.

Rappelons (voir la section 5.1.3) que pour chaque partition $\lambda = \cdots 2^{m_2} 1^{m_1}$, nous posons $z_\lambda = \prod_{i\geq 1}\Big(i^{m_i}\ m_i!\Big)$.

5.2.1.1 Proposition.

(i) Le centralisateur d'un élément $\sigma \in \mathfrak{S}_n$ est d'ordre $z_{\rho(\sigma)}$.

(ii) Pour toute partition λ de n, la classe de conjugaison C_λ contient $n!/z_\lambda$ éléments.

Preuve. Soit λ une partition de taille n et de longueur ℓ, et pour chaque $i \geq 1$, soit m_i le nombre de parts de λ égales à i. Tentons d'énumérer les éléments de C_λ.

Une permutation $\sigma \in C_\lambda$ est donnée par sa décomposition en cycles. On doit d'abord choisir les supports de ces cycles, disons ω_1, ..., ω_ℓ, qui doivent former une partition de $\{1, \ldots, n\}$, de sorte que chaque ω_j soit de cardinal λ_j. Le nombre de ℓ-uplets $(\omega_1, \ldots, \omega_\ell)$ satisfaisant à ces conditions est donné par le coefficient multinomial

$$\frac{n!}{\lambda_1!\ \lambda_2!\ \cdots}.$$

On doit ensuite choisir, dans chaque partie ω_j, l'ordre cyclique dans lequel σ permute les éléments de ω_j : cela nous donne $(\lambda_j - 1)!$ choix, pour chaque j. (En effet, le nombre de k-cycles dans $\mathfrak{S}_k$ est $(k-1)!$.)

À ce stade, nous avons obtenu toutes les permutations dans C_λ, mais nous les avons comptées plusieurs fois, car les cycles de la décomposition de σ ne sont pas numérotés. Il convient de

diviser le nombre obtenu par $m_i!$, pour chaque longueur i de cycle. Tout compte fait, le nombre d'éléments de C_λ est égal à

$$\frac{n!}{\lambda_1!\,\lambda_2!\,\cdots} \times (\lambda_1 - 1)! \times (\lambda_2 - 1)! \times \cdots \times \frac{1}{m_1!\,m_2!\,\cdots} = \frac{n!}{z_\lambda}.$$

Le raisonnement ci-dessus établit l'énoncé (ii). L'énoncé (i) s'en déduit par la formule des classes. Alternativement, on peut voir que le centralisateur dans $\mathfrak{S}_n$ d'une permutation $\sigma \in C_\lambda$ est isomorphe au groupe produit

$$\prod_{i \geq 1} \Big(\big(\mathbf{Z}/i\mathbf{Z}\big)^{m_i} \rtimes \mathfrak{S}_{m_i} \Big)$$

où la structure de produit semi-direct est donnée par l'action de $\mathfrak{S}_{m_i}$ sur $\big(\mathbf{Z}/i\mathbf{Z}\big)^{m_i}$ par permutation des facteurs. □

5.2.2 Sous-groupes de Young

Soit $\mu = (\mu_1, \mu_2, \ldots, \mu_p)$ une suite finie d'entiers strictement positifs de somme n. On dispose alors d'un homomorphisme injectif de groupes

$$\begin{pmatrix} \mathfrak{S}_\mu = \mathfrak{S}_{\mu_1} \times \cdots \times \mathfrak{S}_{\mu_p} \to \mathfrak{S}_n \\ (\sigma_1, \ldots, \sigma_p) \mapsto \sigma_1 \times \cdots \times \sigma_p \end{pmatrix},$$

où $\sigma_1 \times \cdots \times \sigma_p$ est la permutation obtenue en décomposant $\{1, \ldots, n\}$ en blocs $\{1, \ldots, \mu_1\} \sqcup \{\mu_1 + 1, \ldots, \mu_1 + \mu_2\} \sqcup \cdots$ et en faisant agir σ_1 sur le premier bloc, σ_2 sur le second, etc.

On identifie $\mathfrak{S}_\mu$ à son image, appelée sous-groupe de Young de $\mathfrak{S}_n$.

5.2.3 L'application caractéristique de Frobenius

Nous nous intéressons aux caractères complexes du groupe symétrique $\mathfrak{S}_n$, avec $n \geq 1$. Pour cela, introduisons l'espace $\mathscr{F}_n = \mathrm{cf}_{\mathbf{C}}(\mathfrak{S}_n)$ des fonctions de classes à valeurs complexes sur $\mathfrak{S}_n$. L'espace $\mathscr{F}^n$ est muni d'un produit scalaire hermitien $(?, ?)_{\mathfrak{S}_n}$. L'ensemble $\mathscr{R}^n = \mathrm{ch}\,\mathbf{C}\mathfrak{S}_n$ des caractères virtuels de $\mathfrak{S}_n$ est un sous-groupe de $\mathscr{F}^n$.

Nous avons vu dans la section 5.1.5 que l'espace des polynômes symétriques de degré n ne dépend pas du nombre d'indéterminées, pourvu que celui-ci soit au moins n. Notons-le Λ^n, et munissons $\Lambda^n \otimes_{\mathbf{Z}} \mathbf{C}$ du produit scalaire hermitien pour lequel les fonctions de Schur forment une base orthonormée.

L'application caractéristique de Frobenius $\mathrm{ch} : \mathscr{F}^n \to \Lambda^n \otimes_{\mathbf{Z}} \mathbf{C}$ est définie en posant

$$\mathrm{ch}(\varphi) = \frac{1}{n!} \sum_{\sigma \in \mathfrak{S}_n} \varphi(\sigma)\, p_{\rho(\sigma)}$$

pour chaque $\varphi \in \mathscr{F}^n$. Alternativement, on observe que l'espace vectoriel $\mathscr{F}^n$ admet pour base l'ensemble des fonctions indicatrices des classes de conjugaison dans $\mathfrak{S}_n$, et on demande que pour toute partition λ de n, l'application ch envoie la fonction indicatrice de la classe de conjugaison C_λ sur p_λ / z_λ (voir la proposition 5.2.1.1 (ii)).

5.2.3.1 Théorème. *L'application* ch *est un isomorphisme isométrique d'espaces vectoriels* $\mathscr{F}^n \xrightarrow{\sim} \Lambda^n \otimes_{\mathbf{Z}} \mathbf{C}$. *Elle se restreint en un isomorphisme de* $\mathbf{Z}$*-modules* $\mathscr{R} \xrightarrow{\sim} \Lambda^n$. *Les caractères irréductibles de* $\mathfrak{S}_n$ *sont les images inverses des fonctions de Schur de degré* n *par l'application* ch.

Preuve. Par construction, ch est linéaire. Son caractère isométrique résulte de la comparaison des propositions 5.1.5.3 et 5.2.1.1 : si λ et μ sont deux partitions de n, alors le produit scalaire dans $\mathscr{F}^n$ des fonctions indicatrices des classes de conjugaison C_λ et C_μ, à l'instar du produit scalaire $\langle p_\lambda/z_\lambda, p_\mu/z_\mu\rangle$ dans Λ, vaut $1/z_\lambda$ si $\lambda = \mu$ et zéro sinon.

Prenons à présent une suite finie $\mu = (\mu_1, \mu_2, \ldots, \mu_p)$ d'entiers strictement positifs de somme n, considérons la représentation de permutation définie par l'action de $\mathfrak{S}_n$ sur $\mathfrak{S}_n/\mathfrak{S}_\mu$ par translations à gauche (paragraphe 4.1.2.1), et notons η_μ le caractère de celle-ci. Alors la valeur de η_μ en une permutation $\sigma \in \mathfrak{S}_n$ est le nombre de points fixes de l'action de σ sur $\mathfrak{S}_n/\mathfrak{S}_\mu$ (exercice (1) de la section 4.1.4). Notant $\mathbf{1}_{\mathfrak{S}_\mu}$ la fonction indicatrice de $\mathfrak{S}_\mu$, nous avons donc

$$\eta_\mu(\sigma) = \frac{1}{|\mathfrak{S}_\mu|} \sum_{\tau \in \mathfrak{S}_n} \mathbf{1}_{\mathfrak{S}_\mu}(\tau^{-1}\sigma\tau)$$

vu que σ fixe la classe à gauche $\tau\mathfrak{S}_\mu$ si et seulement si $\tau^{-1}\sigma\tau \in \mathfrak{S}_\mu$.

Il vient ainsi

$$\begin{aligned}
\mathrm{ch}(\eta_\mu) &= \frac{1}{n!} \sum_{\sigma \in \mathfrak{S}_n} \eta_\mu(\sigma)\, p_{\rho(\sigma)} \\
&= \frac{1}{n!\,|\mathfrak{S}_\mu|} \sum_{\sigma,\tau \in \mathfrak{S}_n} \mathbf{1}_{\mathfrak{S}_\mu}(\tau^{-1}\sigma\tau)\, p_{\rho(\sigma)} \\
&= \frac{1}{n!\,|\mathfrak{S}_\mu|} \sum_{\sigma,\tau \in \mathfrak{S}_n} \mathbf{1}_{\mathfrak{S}_\mu}(\sigma)\, p_{\rho(\tau\sigma\tau^{-1})} \\
&= \frac{1}{|\mathfrak{S}_\mu|} \sum_{\sigma \in \mathfrak{S}_n} \mathbf{1}_{\mathfrak{S}_\mu}(\sigma)\, p_{\rho(\sigma)} \\
&= \frac{1}{|\mathfrak{S}_\mu|} \sum_{(\sigma_1,\ldots,\sigma_p) \in \mathfrak{S}_{\mu_1} \times \cdots \times \mathfrak{S}_{\mu_p}} p_{\rho(\sigma_1 \times \cdots \times \sigma_p)} \\
&= \prod_{i=1}^{p} \left(\frac{1}{\mu_i!} \sum_{\sigma \in \mathfrak{S}_{\mu_i}} p_{\rho(\sigma)} \right) \\
&= \prod_{i=1}^{p} \left(\sum_{\lambda \vdash \mu_i} p_\lambda/z_\lambda \right) \\
&= h_{\mu_1} h_{\mu_2} \cdots h_{\mu_p},
\end{aligned}$$

la dernière égalité provenant de la proposition 5.1.3.2.

Le groupe $\mathrm{ch}(\mathscr{R}^n)$ contient donc tous les polynômes symétriques de la forme $h_{\mu_1} h_{\mu_2} \cdots h_{\mu_p}$. En utilisant soit le théorème 5.1.3.1, soit la proposition 5.1.6.2 et l'inversibilité de la matrice

formée par les nombres de Kostka, on en déduit que $\mathrm{ch}(\mathscr{R}^n)$ contient Λ^n. Pour chaque partition λ de poids n, il existe donc $\chi^\lambda \in \mathscr{R}$ tel que $\mathrm{ch}\,\chi^\lambda = s_\lambda$. Alors $(\chi^\lambda, \chi^\lambda)_{\mathfrak{S}_n} = \langle s_\lambda, s_\lambda \rangle = 1$. En outre, l'égalité

$$s_\lambda = \mathrm{ch}(\chi^\lambda) = \frac{1}{n!} \sum_{\sigma \in \mathfrak{S}_n} \chi^\lambda(\sigma)\, p_{\rho(\sigma)}$$

conduit à $\chi^\lambda(1) = \langle p_{(1^n)}, s_\lambda \rangle = K_{\lambda,(1^n)}$ d'après la proposition 5.1.5.3 et le corollaire 5.1.6.3, et donc $\chi^\lambda(1)$ est positif. La proposition 4.2.3.2 (v) nous dit alors que χ^λ est un caractère irréductible de $\mathfrak{S}_n$.

Nous obtenons ainsi une famille (χ^λ) de caractères irréductibles de $\mathfrak{S}_n$ indexée par les partitions de poids n. Comme elle a autant de membres que $\mathfrak{S}_n$ a de classes de conjugaison, elle est la famille de tous les caractères irréductibles de $\mathfrak{S}_n$.

L'homomorphisme ch envoie donc les caractères irréductibles de $\mathfrak{S}_n$, qui forment une base du $\mathbf{Z}$-module $\mathscr{R}^n$, sur les fonctions de Schur, qui forment une base de la composante Λ^n de degré n. Par conséquent, $\mathrm{ch} : \mathscr{R}^n \to \Lambda^n$ est un isomorphisme de $\mathbf{Z}$-modules. □

5.2.3.2 Remarque. Le théorème 5.2.3.1 est parfois présenté plus abstraitement de la façon suivante. On traite tous les n en même temps en posant $\mathscr{F} = \bigoplus_{n \geq 0} \mathscr{F}^n$, où $\mathscr{F}^0 = \mathbf{C}1$. On munit $\mathscr{F}$ d'une structure d'algèbre graduée en décrétant que le produit de deux fonctions centrales $\varphi \in \mathscr{R}^m$ et $\psi \in \mathscr{R}^n$ est donné par l'induction

$$\varphi \cdot \psi = (\varphi \times \psi)^{\mathfrak{S}_{m+n}}$$

à $\mathfrak{S}_{m+n}$ de la fonction centrale $\varphi \times \psi : (\sigma, \tau) \mapsto \varphi(\sigma)\psi(\tau)$ sur $\mathfrak{S}_m \times \mathfrak{S}_n = \mathfrak{S}_{(m,n)}$; l'associativité se prouve en utilisant la transitivité de l'induction. Un calcul simple, semblable à la preuve de la proposition 4.3.2.2 (iv), prouve alors que l'application

$$\mathrm{ch} : \mathscr{F} \to \Lambda \otimes_{\mathbf{Z}} \mathbf{C}$$

définie en recollant par linéarité les applications $\mathscr{F}^n \xrightarrow{\simeq} \Lambda^n \otimes_{\mathbf{Z}} \mathbf{C}$ est un isomorphisme d'algèbres. Cet isomorphisme envoie le sous-anneau $\mathscr{R} = \bigoplus_{n \geq 0} \mathscr{R}^n$ de $\mathscr{F}$ sur Λ.

5.2.4 Caractères irréductibles

Adoptant les notations de la preuve du théorème 5.2.3.1, nous avons donc une indexation $(\chi^\lambda)_{\lambda \vdash n}$ des caractères irréductibles de $\mathfrak{S}_n$ par l'ensemble des partitions de poids n.

5.2.4.1 Premiers exemples.

(1) Le cas particulier $\mu = (n)$ du calcul effectué dans la démonstration du théorème 5.2.3.1 prouve que l'image par ch du caractère trivial de $\mathfrak{S}_n$ est $h_n = s_{(n)}$. Ainsi $\chi^{(n)}$ est le caractère trivial de $\mathfrak{S}_n$.

(2) Soit μ une partition de n. Chaque permutation appartenant à la classe de conjugaison C_μ se décompose en produit de $\ell(\mu)$ cycles à supports disjoints (y compris les cycles de longueur 1), donc a pour signature $(-1)^{n+\ell(\mu)}$. L'image par ch de la signature de $\mathfrak{S}_n$ est donc égale à

$$\sum_{\lambda\vdash n}(-1)^{|\lambda|+\ell(\lambda)}\, p_\lambda/z_\lambda = e_n = s_{(1^n)}$$

(voir la proposition 5.1.3.2). Ainsi $\chi^{(1^n)}$ est la signature de $\mathfrak{S}_n$.

Notons χ^λ_μ la valeur de χ^λ sur la classe C_μ.

5.2.4.2 Formule des caractères de Frobenius. *Pour chaque partition μ de n,*

$$p_\mu = \sum_{\lambda\vdash n} \chi^\lambda_\mu\, s_\lambda.$$

Preuve. La valeur d'une fonction centrale $\varphi \in \mathscr{F}^n$ sur la classe de conjugaison C_μ est égale à $\langle \mathrm{ch}\,\varphi, p_\mu\rangle$. En particulier, $\chi^\lambda_\mu = \langle s_\lambda, p_\mu\rangle$. Le résultat découle alors du fait que $\{s_\lambda \mid \lambda\vdash n\}$ est une base orthonormée de Λ^n. □

La table des caractères des groupes symétriques s'obtient donc comme une matrice de changement de base dans $\Lambda\otimes_{\mathbf{Z}}\mathbf{Q}$. Utilisant la proposition 5.1.2.1 (ii), on voit même que les nombres χ^λ_μ sont entiers.

5.2.4.3 Proposition.

(i) Pour chaque partition λ de n, le degré de χ^λ est égal au nombre $K_{\lambda,(1^n)}$ de tableaux standards de forme λ.

(ii) (Règle de Young.) Soit $\mu = (\mu_1, \mu_2, \ldots, \mu_p)$ une suite d'entiers strictement positifs, de somme n. Induisons à $\mathfrak{S}_n$ le caractère trivial $1_{\mathfrak{S}_\mu}$ du sous-groupe de Young $\mathfrak{S}_\mu$. Alors

$$\left(1_{\mathfrak{S}_\mu}\right)^{\mathfrak{S}_n} = \sum_{\lambda\vdash n} K_{\lambda,\mu}\,\chi^\lambda$$

où $K_{\lambda,\mu}$ est le nombre de Kostka.

(iii) (Règle de Murnaghan-Nakayama.) Soient λ et μ des partitions de n. Alors

$$\chi^\lambda_\mu = \sum_T (-1)^{h(T)},$$

la somme portant sur l'ensemble des tableaux multibandes de forme λ et de poids μ et la notation $h(T)$ désignant la hauteur du tableau T.

Preuve. L'énoncé (i) a été prouvé au cours de la démonstration du théorème 5.2.3.1. Les règles de Young et de Murnaghan-Nakayama s'obtiennent en appliquant ch^{-1} aux formules de la proposition 5.1.6.2. □

Exemple d'utilisation de la règle de Murnaghan-Nakayama. Prenons $n = 7$, $\lambda = 421$, $\mu = 331$. Il y a trois tableaux multibandes, à savoir

$$\begin{array}{|c|c|c|c|}\hline 1&1&1&3\\\hline 2&2\\\cline{1-2} 2\\\cline{1-1}\end{array}\quad,\quad \begin{array}{|c|c|c|c|}\hline 1&2&2&2\\\hline 1&3\\\cline{1-2} 1\\\cline{1-1}\end{array}\quad\text{et}\quad \begin{array}{|c|c|c|c|}\hline 1&2&2&3\\\hline 1&2\\\cline{1-2} 1\\\cline{1-1}\end{array}\quad,$$

de hauteurs 1, 2 et 3 respectivement, d'où $\chi^\lambda_\mu = -1$.

5.2.4.4 Autres exemples.

(1) Le groupe $\mathfrak{S}_n$ agit transitivement sur l'ensemble $\{1, \dots, n\}$, et le stabilisateur de l'élément 1 est le sous-groupe de Young $\mathfrak{S}_{(1,n-1)}$. La représentation standard de $\mathfrak{S}_n$ sur $\mathbf{C}^n$ étant la représentation de permutation associée à cette action, son caractère est simplement l'induite $(1_{\mathfrak{S}_{(1,n-1)}})^{\mathfrak{S}_n}$. D'après la règle de Young, ceci vaut $\chi^{(n)} + \chi^{(n-1,1)}$. Cette somme reflète la décomposition $\mathbf{C}^n = D \oplus H$ en somme directe de deux représentations irréductibles, où D est la droite engendrée par le vecteur $(1, 1, \dots, 1)$ et H est l'hyperplan $\{(z_1, \dots, z_n) \in \mathbf{C}^n \mid z_1 + \cdots + z_n = 0\}$.

(2) De même, pour $1 \leq k \leq n-1$, la représentation de $\mathfrak{S}_n$ sur $\bigwedge^k(\mathbf{C}^n)$ admet pour caractère le caractère induit $\left(\chi^{(1^k)} \times \chi^{(n-k)}\right)^{\mathfrak{S}_n}$. De la formule de Pieri

$$e_k h_{n-k} = s_{(n-k,1^k)} + s_{(n-k+1,1^{k-1})}$$

on déduit que $\chi^{(n-k,1^k)}$ est le caractère de la représentation de $\mathfrak{S}_n$ sur $\bigwedge^k H$.

(3) L'involution ω de l'anneau Λ introduite dans la section 5.1.5 vérifie $\omega(p_k) = (-1)^{k+1} p_k$. Il s'ensuit que $\omega(p_\mu) = (-1)^{n+\ell(\mu)} p_\mu$ pour toute partition μ de n. Par conséquent, si deux caractères virtuels $\varphi, \psi \in \mathscr{R}^n$ se déduisent l'un de l'autre par multiplication par la signature, alors leurs images $\mathrm{ch}(\varphi), \mathrm{ch}(\psi) \in \Lambda$ par l'application caractéristique se déduisent l'une de l'autre par l'involution ω. La formule $\omega(s_\lambda) = s_{\lambda'}$, où λ' est la partition conjuguée de λ, se traduit ainsi par l'égalité $\chi^{\lambda'} = \chi^\lambda \, \chi^{(1^n)}$ dans l'anneau $\mathrm{ch}\, \mathbf{C}\mathfrak{S}_n$.

5.2.4.5 Remarques.

(1) La somme des carrés des degrés des caractères irréductibles d'un groupe fini est égal à l'ordre du groupe. Ici, cela donne

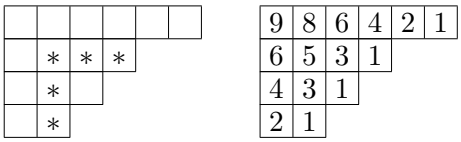
$$\sum_{\lambda \vdash n} \left(K_{\lambda,(1^n)}\right)^2 = n!.$$

On sait également prouver cette identité de façon combinatoire, en utilisant la bijection de Robinson-Schensted.

(2) Plutôt que de compter les tableaux standards, on peut déterminer le degré du caractère irréductible χ^λ par la formule de Frame-Robinson-Thrall :

$$K_{\lambda,(1^n)} = \frac{n!}{\prod_{x \in \lambda} h(x)},$$

où $h(x)$ est la longueur d'équerre de x : si x est la case (i,j), alors $h(x) = \lambda_i + \lambda'_j - i - j + 1$. Ainsi pour $x = (2,2)$ et $\lambda = 6432$, on a ainsi $h(x) = 5$, car il y a cinq $*$ dans le diagramme de gauche ci-dessous.



Les cases du tableau de droite ci-dessus sont remplies par les longueurs d'équerres. La formule de Frame-Robinson-Thrall donne ici

$$\deg \chi^\lambda = \frac{15!}{9 \times 8 \times 6 \times 4 \times 2 \times 6 \times 5 \times 3 \times 4 \times 3 \times 2} = 175175.$$

Malgré les apparences, il reste d'importants problèmes ouverts concernant les caractères du groupe symétrique. En voici deux :

(1) On ne connaît pas de règle combinatoire qui donne les multiplicités des représentations irréductibles dans les produits tensoriels, autrement dit, on ne sait pas évaluer $(\chi^\lambda, \chi^\mu \chi^\nu)_{\mathfrak{S}_n}$ pour λ, μ, ν partitions de poids n.

(2) On ne sait pas grand chose sur les représentations de $\mathfrak{S}_n$ en caractéristique finie. On ne connaît même pas leur degré !

5.2.5 Compléments

Nous avons déterminé ci-dessus les caractères irréductibles complexes du groupe symétrique $\mathfrak{S}_n$. Il est également possible de construire explicitement les représentations, appelées modules de Specht, de la façon suivante. Soit λ une partition de n. À un remplissage T du diagramme de λ par les entiers de 1 à n, chaque entier apparaissant une fois, on associe le polynôme $f_T \in \mathbf{Z}[x_1, \ldots, x_n]$ produit des $x_i - x_j$, pour tous les couples (i,j) tels que dans T, l'entier j est au dessus et dans la même colonne que l'entier i. Si par exemple $n = 7$ et $\lambda = 421$, alors au remplissage

$$T = \begin{array}{|c|c|c|c|}\hline 4 & 1 & 5 & 2 \\ \hline 7 & 3 \\ \cline{1-2} 6 \\ \cline{1-1} \end{array}$$

correspond le polynôme $f_T = (x_7 - x_4)(x_6 - x_7)(x_6 - x_4)(x_3 - x_1)$.

On appelle M_λ le sous-$\mathbf{Z}$-module de $\mathbf{Z}[x_1, \ldots, x_n]$ engendré par les polynômes f_T, pour tous les remplissages T du diagramme de λ. Manifestement, M_λ est stable sous l'action de $\mathfrak{S}_n$ sur $\mathbf{Z}[x_1, \ldots, x_n]$. On peut démontrer que les f_T pour T tableau standard forment une base du $\mathbf{Z}$-module M_λ, et que si k est un corps de caractéristique 0, alors la représentation de $\mathfrak{S}_n$ sur $M_\lambda \otimes_{\mathbf{Z}} k$ est absolument irréductible et de caractère χ^λ. En particulier, non seulement les caractères irréductibles complexes de $\mathfrak{S}_n$ sont à valeurs entières, mais les représentations correspondantes peuvent être réalisées sur $\mathbf{Z}$.

Une référence (assez condensée) pour la preuve de ces énoncés est l'exercice 15 de la section I.7 du livre de Macdonald [13].

D'autres approches permettent de présenter la théorie. L'une d'elles, due à Okounkov et Vershik, semble assez populaire ces dernières années. Donnons-nous $n \geq 1$ et plongeons $\mathfrak{S}_1 \subseteq \mathfrak{S}_2 \subseteq \cdots \subseteq \mathfrak{S}_n$. Ici pour $m < n$, une permutation $\sigma \in \mathfrak{S}_m$ est vue comme une permutation de $\{1, \ldots, n\}$ qui fixe les valeurs $m+1$, $m+2$, ... Nous obtenons alors des inclusions d'algèbres

$$\mathbf{C}\mathfrak{S}_1 \subseteq \mathbf{C}\mathfrak{S}_2 \subseteq \cdots \subseteq \mathbf{C}\mathfrak{S}_n.$$

Appelons $\mathscr{A}$ la sous-algèbre de $\mathbf{C}\mathfrak{S}_n$ engendrée par les centres $Z(\mathbf{C}\mathfrak{S}_1)$, $Z(\mathbf{C}\mathfrak{S}_2)$, ... $Z(\mathbf{C}\mathfrak{S}_n)$. $\mathscr{A}$ est une sous-algèbre commutative de $\mathbf{C}\mathfrak{S}_n$, car pour $i < j$, un élément de $Z(\mathbf{C}\mathfrak{S}_j)$ commute avec tout élément de $\mathbf{C}\mathfrak{S}_j$, donc en particulier avec tout élément de $\mathbf{C}\mathfrak{S}_i$.

On montre que $\mathscr{A}$ est une sous-algèbre commutative maximale de $\mathbf{C}\mathfrak{S}_n$. Il est alors intéressant de restreindre les $\mathbf{C}\mathfrak{S}_n$-modules à $\mathscr{A}$: comme $\mathscr{A}$ est commutative, ses représentations irréductibles sont de dimension 1. Il se trouve que la sous-algèbre A est assez grosse pour que la restriction à $\mathscr{A}$ d'un $\mathbf{C}\mathfrak{S}_n$-module détermine entièrement ce dernier, à isomorphisme près. Pour plus de détails, le lecteur est renvoyé au premier chapitre du livre [12].

5.3 Représentations du groupe unitaire

5.3.1 Rappels sur les groupes compacts et sur le groupe unitaire

Commençons par rappeler brièvement quelques faits concernant les groupes compacts et leurs représentations (voir le paragraphe 4.4 pour plus de détails).

Soit G un groupe compact. Nous nous intéressons exclusivement aux représentations complexes de dimension finie de G, c'est-à-dire aux homomorphismes de groupes $\pi : G \to \mathbf{GL}(V)$, où V est un $\mathbf{C}$-espace vectoriel de dimension finie. Alors V et $\mathbf{GL}(V)$ sont munis d'une topologie canonique, et on peut parler de représentation continue.

Un groupe compact possède une unique mesure μ de masse totale 1, invariante par translations à gauche et à droite, appelée mesure de Haar. On peut ainsi intégrer d'une façon canonique les fonctions continues sur G à valeurs dans un espace vectoriel réel ou complexe de dimension finie. L'intégrale $\int_G \varphi \, d\mu$ est l'analogue de la moyenne $\left(\sum_{g \in G} \varphi(g)\right)/|G|$ qui nous a servi à définir l'opérateur de Reynolds. De fait, on dispose encore d'un opérateur de Reynolds dans le cas des groupes compacts, qui peut être utilisé pour prouver le théorème de Maschke et la relation d'orthogonalité des caractères.

5.3.1.1 Exemple. Sur le groupe compact $G = (\mathbf{R}/2\pi\mathbf{Z})^n$, la mesure de Haar est donnée par

$$\int_G \varphi \, d\mu = \int_0^{2\pi} \cdots \int_0^{2\pi} \varphi(\theta_1, \ldots, \theta_n) \, \frac{d\theta_1}{2\pi} \cdots \frac{d\theta_n}{2\pi}.$$

L'espace des fonctions continues sur G à valeurs complexes est muni d'un produit scalaire

$$(\varphi, \psi)_G = \int_G \overline{\varphi(g)} \psi(g) \, d\mu(g).$$

Le sous-espace des fonctions de classe hérite de ce produit scalaire.

La théorie de Peter-Weyl (paragraphes 4.4.5 et 4.4.6) entraîne :

5.3.1.2 Fait. L'ensemble des caractères irréductibles (sous-entendu : continus) de G forme une famille orthonormée dans l'ensemble des fonctions de classe continue. Il n'existe pas de fonction de classe continue non-nulle qui soit orthogonale à tous les caractères irréductibles.

Voici maintenant quelques rappels concernant les groupes unitaires. On se donne un entier $n \geq 1$. Comme d'habitude, on note

$$\mathbf{U}(n) = \{U \in \mathbf{GL}_n(\mathbf{C}) \mid U^{-1} = {}^t\overline{U}\}$$

le groupe des matrices unitaires de taille n. Ainsi $\mathbf{U}(1)$ est le groupe des nombres complexes de module 1.

5.3.1.3 Faits.

(1) Les valeurs propres d'une matrice unitaire sont des nombres complexes de module 1.

(2) Une matrice unitaire et triangulaire est diagonale (le i-ième vecteur colonne C_i est de norme 1 ; la i-ième coordonnée de C_i est de module 1 ; les autres coordonnées de C_i sont donc nulles).

(3) Toute matrice $P \in \mathbf{GL}_n(\mathbf{C})$ s'écrit de façon unique $P = TU$, avec T triangulaire supérieure à valeurs réelles positives sur la diagonale et U unitaire (ce fait traduit le procédé de Gram-Schmidt).

(4) Pour toute matrice complexe M, il existe une matrice unitaire U telle que $U^{-1}MU$ est triangulaire supérieure (trianguler M et appliquer le point précédent à la matrice de passage).

(5) Toute matrice unitaire est diagonalisable avec une matrice de passage unitaire (combiner (2) et (4)).

(6) La transformée de Cayley

$$U \mapsto A = \frac{I-U}{I+U} \quad \text{et} \quad A \mapsto U = \frac{I-A}{I+A}$$

est une bijection bicontinue entre l'ensemble des matrices unitaires U n'ayant pas -1 comme valeur propre et l'ensemble des matrices antihermitiennes A n'ayant pas -1 comme valeur propre. Au prix de la restriction à des ouverts, on peut donc passer du groupe $\mathbf{U}(n)$ des matrices unitaires à l'espace vectoriel $\mathfrak{u}(n)$ des matrices antihermitiennes.

5.3.2 Restriction au tore

On se donne un groupe unitaire $G = \mathbf{U}(n)$, avec n fixé pour toute la suite. On note T l'ensemble des matrices diagonales de G. Les valeurs diagonales d'un élément de T étant des nombres complexes de module 1, on a $T \cong \mathbf{U}(1)^n$. Le sous-groupe T est appelé le tore maximal standard de G. C'est un groupe abélien compact connexe.

Une matrice $M \in \mathbf{GL}_n(\mathbf{C})$ est dite monomiale si chaque ligne et chaque colonne de M contient exactement une valeur non-nulle. On vérifie sans trop de peine que le normalisateur N de T

dans $\mathbf{U}(n)$ est l'ensemble des matrices monomiales unitaires. Comme T est abélien, l'action par conjugaison de N sur T se factorise à travers le quotient $W = N/T$. Concrètement, W est isomorphe au groupe symétrique $\mathfrak{S}_n$ et l'action d'une permutation $\sigma \in W$ sur une matrice diagonale $U \in T$ est de permuter les valeurs diagonales de U.

Pour voir cela, le plus simple est de plonger $\mathfrak{S}_n$ dans $\mathbf{GL}_n(\mathbf{C})$ par les matrices de permutations. On vérifie qu'alors $N = \mathfrak{S}_n T$ et $\mathfrak{S}_n \cap T = \{1\}$; on a ainsi une structure de produit semi-direct $N = \mathfrak{S}_n \ltimes T$. L'action d'une permutation $\sigma \in \mathfrak{S}_n$ sur T est donnée par la conjugaison $U \mapsto P_\sigma U P_\sigma^{-1}$ par la matrice de permutation correspondante : si $U = \mathrm{diag}(z_1, \ldots, z_n)$, alors $P_\sigma U P_\sigma^{-1} = \mathrm{diag}(z_{\sigma^{-1}(1)}, \ldots, z_{\sigma^{-1}(n)})$.

Notons $C(G, \mathbf{C})^G$ l'algèbre des fonctions de classe continues sur G à valeurs complexes ; notons $C(T, \mathbf{C})^W$ l'ensemble des fonctions continues sur T qui sont constantes sur les orbites de W (autrement dit : W agit sur T, donc sur l'espace $C(T, \mathbf{C})$ des fonctions continues sur T, et on prend les invariants pour cette action).

5.3.2.1 Théorème.

(i) Chaque classe de conjugaison de G rencontre T et l'intersection est une W-orbite.

(ii) L'opération de restriction à T d'une fonction sur G induit un isomorphisme d'algèbres de $C(G, \mathbf{C})^G$ sur $C(T, \mathbf{C})^W$.

Preuve. Le (i) traduit le fait que chaque matrice unitaire U est semblable à une matrice diagonale D avec une matrice de passage unitaire (fait 5.3.1.3 (5)), et que les coefficients de D sont déterminés à permutation près par U (ce sont les valeurs propres de U, avec multiplicité).

À ce stade, la seule chose non-banale à démontrer dans (ii) est la surjectivité de l'opération de restriction. Plus précisément, donnons-nous une fonction W-invariante $\psi : T \to \mathbf{C}$. Il est naturel de définir une fonction $\varphi \in C(G, \mathbf{C})^G$ en décrétant, pour chaque matrice $U \in G$, que $\varphi(U)$ est égal à la valeur de ψ sur l'intersection de T avec la classe de conjugaison de U. Certainement alors, ψ est la restriction de φ. La difficulté est de montrer que φ est continue.

Pour éviter de parler de topologie quotient, ce qui est toujours un peu délicat [21], nous considérons l'application

$$C : G \to \mathbf{C}^n, \quad U \mapsto (a_1, \ldots, a_n),$$

où les a_i sont les coefficients du polynôme caractéristique de U, à un signe près :

$$\det(TI - U) = T^n - a_1 T^{n-1} + a_2 T^{n-2} + \cdots + (-1)^n a_n.$$

À une matrice $\mathrm{diag}(z_1, \ldots, z_n) \in T$, l'application C associe le n-uplet $(\varepsilon_1, \ldots, \varepsilon_n)$, où ε_k est la valeur en $(z_1, \ldots, z_n)$ du polynôme symétrique élémentaire e_k de degré k.

Deux matrices de T ont même image par C si et seulement si elles ont le même polynôme caractéristique, autrement dit les mêmes valeurs propres avec les mêmes multiplicités, ce qui équivaut à dire qu'elles sont donc dans la même W-orbite. Ainsi les fibres de la restriction de C à T sont les W-orbites dans T. Notons K l'image de G par C ; c'est aussi l'image de T par C, et C induit une bijection $\tilde{C} : T/W \to K$.

21. Nous sommes ici dans le cas favorable où l'on fait le quotient par un groupe compact.

Choisissons une norme classique sur $\mathbf{C}^n$; elle nous donne une distance W-invariante sur $\mathbf{U}(1)^n \cong T$. On munit T/W de la distance induite : la distance entre deux W-orbites est le minimum de la distance entre deux points appartenant à l'une et l'autre orbite. Alors T/W est un espace topologique compact, car T est compact et la surjection canonique de T sur T/W est continue. Ainsi $\tilde{C} : T/W \to K$ est une bijection continue d'un espace compact vers un espace séparé, et est donc un homéomorphisme d'après le théorème de Poincaré.

Reprenons maintenant notre fonction $\psi \in C(T, \mathbf{C})^W$. Alors ψ se factorise à travers T/W, donnant une application $\tilde{\psi} : T/W \to \mathbf{C}$. En utilisant que la surjection canonique de T sur T/W est ouverte, on vérifie que $\tilde{\psi}$ est continue. On en déduit que la fonction φ est continue, car elle peut s'écrire $\varphi = \tilde{\psi} \circ \tilde{C}^{-1} \circ C$. □

La forme linéaire positive $\varphi \mapsto \int_G \varphi \, d\mu$ sur $C(G, \mathbf{C})^G$ peut donc être vue comme une forme linéaire positive sur $C(T, \mathbf{C})^W$. D'après le théorème de représentation de Riesz, elle est donnée par une mesure W-invariante sur T. Le résultat suivant explicite cette dernière. Il est dû à Weyl ([17], chapitre VII, §4) ; on pourra se référer au chapitre 18 de [5] pour une présentation plus moderne.

5.3.2.2 Formule d'intégration de Weyl.

Si $\varphi \in C(G, \mathbf{C})^G$, alors

$$\int_G \varphi \, d\mu = \frac{1}{n!} \int_0^{2\pi} \cdots \int_0^{2\pi} \varphi\Big(\mathrm{diag}\Big(e^{i\theta_1}, \ldots, e^{i\theta_n}\Big)\Big) \prod_{j<k} |e^{i\theta_j} - e^{i\theta_k}|^2 \, \frac{d\theta_1}{2\pi} \cdots \frac{d\theta_n}{2\pi}.$$

Preuve. L'application $(g, t) \mapsto gtg^{-1}$ de $G \times T$ dans G est surjective d'après le fait 5.3.1.3 (5). Elle se factorise en une application surjective $\Phi : (G/T) \times T \to G$.

Le groupe G est une variété différentielle réelle ; on note $\mathfrak{g}$ l'espace tangent à G en l'élément neutre e. Le tore T est une sous-variété différentielle de G ; l'espace tangent $\mathfrak{t}$ à T au point e est donc un sous-espace vectoriel de $\mathfrak{g}$. L'ensemble G/T a une structure de variété différentielle, et l'espace tangent à G/T au point eT (l'image de e dans G/T) peut être identifié à $\mathfrak{g}/\mathfrak{t}$.

Pour chaque $g \in G$, la différentielle en e du difféomorphisme $h \mapsto ghg^{-1}$ de G dans lui-même est notée $\mathrm{Ad}(g)$. L'application $\mathrm{Ad} : G \to \mathbf{GL}(\mathfrak{g})$ est appelée la représentation adjointe de G. Pour $t \in T$, l'endomorphisme $\mathrm{Ad}(t)$ laisse fixe chaque élément du sous-espace $\mathfrak{t}$ de $\mathfrak{g}$. Nous disposons ainsi d'une représentation quotient de T sur $\mathfrak{g}/\mathfrak{t}$, que nous noterons $t \mapsto (\mathrm{Ad}(t))_{\mathfrak{g}/\mathfrak{t}}$.

Concrètement pour $G = \mathbf{U}(n)$, $\mathfrak{g}$ est identifié à l'espace vectoriel $\mathfrak{u}(n)$ des matrices antihermitiennes de taille n, et $\mathrm{Ad}(g)$ est la conjugaison $X \mapsto gXg^{-1}$, pour $g \in \mathbf{U}(n)$ et $X \in \mathfrak{u}(n)$. On peut ici noter que la puissance extérieure maximale de la représentation adjointe est la représentation triviale de G, le déterminant fournissant un isomorphisme de représentations $\bigwedge^{\max} \mathfrak{g} \cong \mathbf{R}$. Par ailleurs, le sous-espace $\mathfrak{t}$ est l'ensemble des matrices diagonales de taille n à coefficients imaginaires purs.

Nous considérons maintenant la fonction $J : t \mapsto \det(\mathrm{Ad}(t^{-1}) - \mathrm{id})_{\mathfrak{g}/\mathfrak{t}}$ définie sur T et à valeurs réelles. Un calcul explicite montre que pour $G = \mathbf{U}(n)$,

$$J(\mathrm{diag}(z_1, \ldots, z_n)) = \prod_{j<k} |z_j - z_k|^2 \qquad (\dagger)$$

pour chaque $(z_1, \ldots, z_n) \in \mathbf{U}(1)^n$.

Soit ω une forme différentielle de degré maximal sur G. L'intégrale $\int_G \varphi\omega$ a alors un sens pour chaque fonction continue $\varphi : G \to \mathbf{C}$, et la forme linéaire $\varphi \mapsto \int_G \varphi\omega$ est une mesure sur G. En fait, la mesure de Haar sur G s'obtient de cette façon : il suffit de construire une forme différentielle ω invariante par les translations à gauche, ce qu'on fait en choisissant un élément non-nul $\omega_e \in \bigwedge^{\max} \mathfrak{g}^*$ et en le propageant à tout G via les translations à gauche.

De la même façon, on choisit des formes différentielles de degré maximal η sur T et λ sur G/T, invariantes par les translations à gauche par T et G, respectivement [22]. Ces formes différentielles η et λ fournissent des mesures sur T et G/T, la première étant la mesure de Haar de T. On normalise ω et η en imposant que

$$\int_G \omega = \int_T \eta = 1.$$

On peut identifier les droites vectorielles réelles $\bigwedge^{\max}(\mathfrak{g}/\mathfrak{t})^* \otimes \bigwedge^{\max} \mathfrak{t}^*$ et $\bigwedge^{\max} \mathfrak{g}^*$; on normalise λ de façon à avoir $\lambda_{eT} \otimes \eta_e \equiv \omega_e$ dans notre identification. Le théorème de Fubini entraîne alors

$$\int_{G/T} \lambda = 1.$$

Prenons $(g, t) \in G \times T$. La différentielle de la translation à gauche par g fournit un isomorphisme entre les espaces tangents à G/T aux points eT et gT ; cela permet de désigner l'espace tangent au point gT par la notation $g(\mathfrak{g}/\mathfrak{t})$. De même, l'espace tangent à T au point t est noté $t\,\mathfrak{t}$ et l'espace tangent à G au point gtg^{-1} est noté $(gtg^{-1})\mathfrak{g}$. Prenons donc $X \in \mathfrak{g}/\mathfrak{t}$ et $H \in \mathfrak{t}$. La différentielle de Φ au point (gT, t) est alors

$$(gX, tH) \mapsto (gtg^{-1})\big[\mathrm{Ad}(g)\big((\mathrm{Ad}(t^{-1}) - \mathrm{id})X + H\big)\big],$$

où $X \in \mathfrak{g}/\mathfrak{t}$ et $H \in \mathfrak{t}$. Le fait que X appartienne à $\mathfrak{g}/\mathfrak{t}$ et non à $\mathfrak{g}$ n'est pas ici un souci : comme l'endomorphisme $\mathrm{Ad}(t^{-1}) - \mathrm{id}$ de l'espace vectoriel $\mathfrak{g}$ est nul sur $\mathfrak{t}$, il se factorise à travers $\mathfrak{g}/\mathfrak{t}$, et donc $(\mathrm{Ad}(t^{-1}) - \mathrm{id})(X)$ est un élément bien défini de $\mathfrak{g}$, même si X n'est défini que modulo $\mathfrak{t}$. Maintenant, dans l'identification $\bigwedge^{\max}(\mathfrak{g}/\mathfrak{t}) \otimes \bigwedge^{\max} \mathfrak{t} \equiv \bigwedge^{\max} \mathfrak{g}$, la puissance extérieure maximale de l'application linéaire

$$(X, H) \mapsto \mathrm{Ad}(g)\big((\mathrm{Ad}(t^{-1}) - \mathrm{id})X + H\big)$$

de $(\mathfrak{g}/\mathfrak{t}) \oplus \mathfrak{t}$ dans $\mathfrak{g}$ est la multiplication par $J(t)$. Le formalisme de la géométrie différentielle nous conduit donc à la formule

$$\big(\Phi^*\omega\big)_{(gT,t)} = J(t)\ \lambda_{gT} \otimes \eta_t. \qquad (\ddagger)$$

Introduisons à présent l'ensemble G^{reg} des éléments réguliers de G, formé des matrices unitaires dont les valeurs propres sont deux-à-deux distinctes. C'est une partie ouverte de G, stable par

22. L'existence de λ n'est pas complètement évidente. On commence par observer que la puissance extérieure maximale de la représentation $t \mapsto (\mathrm{Ad}(t))_{\mathfrak{g}/\mathfrak{t}}$ de T sur $\mathfrak{g}/\mathfrak{t}$ est la représentation triviale de T. Ainsi un élément non-nul $\lambda_{eT} \in \bigwedge^{\max}(\mathfrak{g}/\mathfrak{t})^*$ est automatiquement invariant par le stabilisateur du point eT de G/T. On peut alors propager cet élément à tout G/T de façon G-invariante.

l'action par conjugaison de G sur lui-même. Posons $T^{\mathrm{reg}} = T \cap G^{\mathrm{reg}}$; ainsi $\Phi^{-1}(G^{\mathrm{reg}}) = (G/T) \times T^{\mathrm{reg}}$. La formule (†) montre que $J(t) \neq 0$ pour chaque $t \in T^{\mathrm{reg}}$. On déduit alors de (‡) que Φ est un difféomorphisme local au dessus de G^{reg}. De plus, un élément de G^{reg} possède exactement $|W| = n!$ antécédents par Φ [23].

Le complémentaire de G^{reg} est une sous-variété algébrique de G, donc il est de mesure nulle. De même, le complémentaire de T^{reg} est de mesure nulle dans T. On peut donc restreindre à G^{reg} ou à T^{reg} le domaine d'intégration d'une fonction continue sur G ou sur T sans changer la valeur de l'intégrale. Soit $\varphi \in C(G, \mathbf{C})^G$ une fonction de classe continue. Alors

$$\int_G \varphi \, d\mu = \int_{G^{\mathrm{reg}}} \varphi\omega = \frac{1}{|W|} \int_{(G/T)\times T^{\mathrm{reg}}} \Phi^*(\varphi\omega) = \frac{1}{|W|} \int_{(G/T)\times T^{\mathrm{reg}}} (\varphi \circ \Phi)\, \Phi^*\omega.$$

La fonction φ étant supposée centrale, on a

$$(\varphi \circ \Phi)(gT, t) = \varphi\big(gtg^{-1}\big) = \varphi(t)$$

pour chaque $(gT, t) \in (G/T) \times T^{\mathrm{reg}}$. Utilisant (‡) et le théorème de Fubini, nous concluons que

$$\int_G \varphi \, d\mu = \frac{1}{|W|} \left(\int_{G/T} \lambda \right) \left(\int_{T^{\mathrm{reg}}} \varphi J\eta \right) = \frac{1}{|W|} \int_T \varphi J\eta.$$

La forme différentielle η donnant la mesure de Haar sur T, l'exemple 5.3.1.1 et (†) donnent la formule de Weyl telle qu'écrite dans l'énoncé. □

5.3.3 Les caractères du tore

Le groupe T étant abélien, ses représentations irréductibles sont de degré 1, c'est-à-dire sont des caractères linéaires. Notons $X^*(T)$ l'ensemble des caractères linéaires continus de T.

5.3.3.1 Proposition. *À $(a_1, \ldots, a_n) \in \mathbf{Z}^n$, on associe un caractère linéaire φ de T par la formule*

$$\varphi(\mathrm{diag}(z_1, \ldots, z_n)) = z_1^{a_1} \cdots z_n^{a_n},$$

où $(z_1, \ldots, z_n) \in \mathbf{U}(1)^n$. L'application $(a_1, \ldots, a_n) \mapsto \varphi$ est une bijection $\mathbf{Z}^n \cong X^*(T)$.

Preuve. La proposition définit une application injective de $\mathbf{Z}^n$ dans $X^*(T)$. Il s'agit de voir qu'elle est surjective.

23. Dans la situation où l'on a un groupe G, un sous-groupe H de G et un ensemble X muni d'une action de H, on fait agir H sur $G \times X$ en posant $h \cdot (g, x) = (gh^{-1}, h \cdot x)$ pour $(h, g, x) \in H \times G \times X$, et on désigne par $G \times_H X$ l'ensemble quotient, c'est-à-dire l'ensemble des orbites. Revenant à notre cas $G = \mathbf{U}(n)$ et faisant agir N sur T par conjugaison, cette construction nous conduit à $G \times_N T$, qui est une variété différentielle. L'application $(g, t) \mapsto gtg^{-1}$ induit alors un homomorphisme de variétés $\widetilde{\Phi} : G \times_N T \to G$. Par restriction, ce dernier donne un difféomorphisme $G \times_N T^{\mathrm{reg}} \cong G^{\mathrm{reg}}$. Puisque T est un sous-groupe de N, il y a une application évidente de $G \times_T T = (G/T) \times T$ sur $G \times_N T$; le fait que T soit distingué dans N entraîne qu'elle est un revêtement galoisien de groupe $N/T = W$. Ainsi $\Phi : (G/T) \times T^{\mathrm{reg}} \to G^{\mathrm{reg}}$ est un revêtement galoisien de groupe W.

Une première possibilité consiste à écrire que si la construction proposée avait manqué un caractère φ de T, alors φ serait orthogonal à tous les caractères

$$\mathrm{diag}(z_1,\dots,z_n) \mapsto z_1^{a_1}\cdots z_n^{a_n},$$

ce qui impliquerait que tous les coefficients de Fourier de la fonction continue 2π-périodique en chaque variable $(\theta_1,\dots,\theta_n) \mapsto \varphi\big(\mathrm{diag}\big(e^{i\theta_1},\dots,e^{i\theta_n}\big)\big)$ soient nuls. Alors φ serait nulle d'après la formule de Plancherel, ce qui est impossible pour un caractère linéaire.

Une seconde possibilité consiste à traiter d'abord le cas $n = 1$ à l'aide du lemme 5.3.3.3 ci-dessous, puis à en déduire le cas n quelconque en adaptant la démarche de l'exercice du paragraphe 4.2.3. □

En utilisant le théorème de Maschke pour le groupe compact T, on en déduit :

5.3.3.2 Corollaire. *Soit $\pi : T \to \mathbf{GL}(V)$ une représentation continue de T dans un espace de dimension finie. Alors il existe un polynôme P à coefficients entiers positifs et un entier $m \in \mathbf{Z}$ tels que*

$$\chi_\pi(\mathrm{diag}(z_1,\dots,z_n)) = P(z_1,\dots,z_n)/(z_1\cdots z_n)^m$$

pour chaque $(z_1,\dots,z_n) \in \mathbf{U}(1)^n$.

5.3.3.3 Lemme. *Soit $f : \mathbf{R} \to \mathbf{C}^*$ un morphisme de groupes continu. Alors il existe $a \in \mathbf{C}$ tel que $f(t) = e^{at}$ pour chaque $t \in \mathbf{R}$.*

Preuve. Il existe $\varepsilon > 0$ tel que

$$t \in [-\varepsilon,\varepsilon] \Rightarrow \mathrm{Re} f(t) \geq 1/2.$$

On choisit ensuite une fonction ρ positive C^1 à support dans $[-\varepsilon,\varepsilon]$ d'intégrale 1. Le produit de convolution $\rho * f$ est alors une fonction C^1 et

$$(\rho * f)(t) = f(t)\left(\int_{\mathbf{R}} \rho(u) f(-u)\, du\right)$$

pour chaque $t \in \mathbf{R}$. La parenthèse à droite est non-nulle, car d'après les choix faits, sa partie réelle est $\geq 1/2$. On en déduit que f est nécessairement C^1. En dérivant en $h = 0$ la relation $f(t+h) = f(h)f(t)$, on obtient l'équation différentielle $f'(t) = f'(0)f(t)$, d'où $f(t) = e^{at}$ avec $a = f'(0)$. □

5.3.4 Les caractères irréductibles de $\mathbf{U}(n)$

À une suite finie décroissante $\mu = (\mu_1,\dots,\mu_n)$ d'entiers relatifs, on associe une fonction $\psi_\mu \in C(T,\mathbf{C})^W$ de la façon suivante : on choisit une partition λ de longueur au plus n et un entier $m \in \mathbf{Z}$ de sorte que

$$\mu = (\lambda_1 - m,\dots,\lambda_n - m)$$

et on définit

$$\psi_\mu : \mathrm{diag}(z_1, \ldots, z_n) \mapsto s_\lambda(z_1, \ldots, z_n)/(z_1 \cdots z_n)^m.$$

Dans la bijection du théorème 5.3.2.1 (ii), ces fonctions ψ_μ correspondent à des fonctions de classe continues $\varphi_\mu \in C(G, \mathbf{C})^G$. Autrement dit, pour chaque $U \in G$, on pose

$$\varphi_\mu(U) = s_\lambda(z_1, \ldots, z_n)/(z_1 \cdots z_n)^m$$

où z_1, ..., z_n sont les valeurs propres de U avec multiplicités. Le but de ce paragraphe est de montrer que les φ_μ sont les caractères des représentations irréductibles continues de G.

Afin de prouver ce résultat, énonçons deux propositions. La première est conséquence du théorème 5.3.2.1 et du corollaire 5.3.3.2.

5.3.4.1 Proposition. *Soit $\pi : G \to \mathbf{GL}(V)$ une représentation continue de dimension finie du groupe unitaire. Alors il existe un polynôme symétrique $P \in \mathbf{Z}[X_1, \ldots, X_n]^{\mathfrak{S}_n}$ à coefficients positifs et un entier $m \in \mathbf{Z}$ tels que la restriction à T du caractère de π soit donnée par*

$$\chi_\pi(\mathrm{diag}(z_1, \ldots, z_n)) = P(z_1, \ldots, z_n)/(z_1 \cdots z_n)^m,$$

pour tout $(z_1, \ldots, z_n) \in \mathbf{U}(1)^n$.

La seconde est un calcul d'intégrale.

5.3.4.2 Proposition. *Soient μ et ν deux suites décroissantes formées chacune de n entiers relatifs. Alors $(\varphi_\mu, \varphi_\nu)_G = \delta_{\mu\nu}$.*

Preuve. On utilise la formule d'intégration de Weyl pour se restreindre au tore T. On écrit $\varphi_\mu(z_1, \ldots, z_n) = s_\lambda(z_1, \ldots, z_n)/(z_1 \cdots z_n)^m$ et $\varphi_\nu(z_1, \ldots, z_n) = s_\tau(z_1, \ldots, z_n)/(z_1 \cdots z_n)^m$, avec un même m. Après substitution, les m disparaissent du calcul et on se retrouve à devoir calculer

$$\frac{1}{n!}\int_0^{2\pi} \cdots \int_0^{2\pi} \overline{s_\lambda(e^{i\theta_1}, \ldots, e^{i\theta_n})} s_\tau(e^{i\theta_1}, \ldots, e^{i\theta_n}) \left| \prod_{j<k} (e^{i\theta_j} - e^{i\theta_k}) \right|^2 \frac{d\theta_1}{2\pi} \cdots \frac{d\theta_n}{2\pi}.$$

Utilisant la définition $s_\lambda = a_{\lambda+\delta}/a_\delta$ des fonctions de Schur, les dénominateurs a_δ se simplifient avec le produit $\prod_{j<k}(e^{i\theta_j} - e^{i\theta_k})$. Il reste

$$\frac{1}{n!}\int_0^{2\pi} \cdots \int_0^{2\pi} \overline{a_{\lambda+\delta}(e^{i\theta_1}, \ldots, e^{i\theta_n})} a_{\tau+\delta}(e^{i\theta_1}, \ldots, e^{i\theta_n}) \frac{d\theta_1}{2\pi} \cdots \frac{d\theta_n}{2\pi}.$$

On développe ensuite les fonctions $a_{\lambda+\delta}$ et $a_{\tau+\delta}$ comme des sommes alternées sur le groupe symétrique, et on conclut par un calcul sans histoire. □

5.3.4.3 Théorème. *Les fonctions φ_μ sont les caractères des représentations irréductibles continues de G, où μ est une suite décroissante formée de n entiers relatifs.*

Preuve. Soit $\pi : G \to \mathbf{GL}(V)$ une représentation continue de dimension finie du groupe unitaire. Les propositions 5.3.4.1 et 5.1.2.1 (ii) nous disent qu'on peut écrire la restriction à T du caractère de π sous forme d'une combinaison $\mathbf{Z}$-linéaire des fonctions ψ_μ :

$$\chi_\pi \mid_T = \sum_\mu c_\mu \psi_\mu,$$

la somme portant sur des suites finies décroissantes formées de n entiers relatifs. Ainsi

$$\chi_\pi = \sum_\mu c_\mu \varphi_\mu.$$

Le fait 5.3.1.2 nous assure que $(\chi_\pi, \chi_\pi)_G = 1$. La proposition 5.3.4.2 donne alors $\sum_\mu |c_\mu|^2 = 1$, et donc tous les c_μ sont nuls, sauf un qui vaut ± 1. Ainsi $\chi_\pi = \pm\varphi_\mu$. Comme les restrictions à T de χ_π et de φ_μ sont toutes deux données par des polynômes à coefficients positifs, le signe est $+1$. Tout caractère irréductible de G est donc un φ_μ.

Si un φ_μ se trouvait oublié dans cette construction, c'est-à-dire n'était pas un caractère irréductible, alors ce serait une fonction de classe continue non-nulle orthogonale à tous les caractères irréductibles. Cela est impossible, toujours d'après le fait 5.3.1.2. □

Reprenons les notations du début du paragraphe 5.3.4. Le degré du caractère φ_μ est

$$\varphi_\mu(I) = s_\lambda(1, \ldots, 1).$$

D'après le théorème de Littlewood 5.1.6.4, il est égal au nombre de tableaux semi-standards de forme λ remplis par des entiers entre 1 et n. La proposition suivante fournit une formule explicite.

5.3.4.4 Formule des dimensions de Weyl. *Pour toute suite décroissante d'entiers relatifs $\mu = (\mu_1, \ldots, \mu_n)$, le degré de s_μ est égal à*

$$\prod_{1 \le i < j \le n} \frac{\mu_i - \mu_j + j - i}{j - i}.$$

Preuve. La suite μ étant donnée, on choisit une partition λ et un entier m comme au début du paragraphe 5.3.4. Alors, pour tout $t \in \mathbf{C}^*$ non racine de l'unité, le nombre $s_\lambda(t^0, t^1, \ldots, t^{n-1})$ s'exprime comme quotient de deux déterminants de Vandermonde. De fait, avec les notations du paragraphe 5.1.2, on a

$$s_\lambda(t^0, t^1, \ldots, t^{n-1}) = \frac{a_{\lambda+\delta}(t^0, t^1, \ldots, t^{n-1})}{a_\delta(t^0, t^1, \ldots, t^{n-1})} = \prod_{1 \le i < j \le n} \frac{t^{\lambda_j + (n-j)} - t^{\lambda_i - (n-i)}}{t^{n-j} - t^{n-i}}.$$

On obtient alors le degré de φ_μ en prenant la limite $t \to 1$:

$$s_\lambda(1, \ldots, 1) = \prod_{1 \le i < j \le n} \frac{\lambda_j + (n-j) - \lambda_i - (n-i)}{(n-j) - (n-i)}.$$

□

5.3.5 Exemples

Soit $\det : G \to \mathbf{C}^*$ le caractère linéaire donné par le déterminant. Restreint au tore, on a

$$\det(\mathrm{diag}(z_1, \ldots, z_n)) = z_1 \cdots z_n = e_n(z_1, \ldots, z_n) = s_{(1^n)}(z_1, \ldots, z_n).$$

Ainsi $\det = \varphi_{(1,\ldots,1)}$.

Soit $\pi : G \to \mathbf{GL}(\mathbf{C}^n)$ la représentation naturelle de G, donnée par l'inclusion $\mathbf{U}(n) \subseteq \mathbf{GL}_n(\mathbf{C})$. Alors $\chi_\pi(g) = \mathrm{tr}(g)$. En restriction au tore, cela donne

$$\chi_\pi(\mathrm{diag}(z_1, \ldots, z_n)) = z_1 + \cdots + z_n = s_{(1)}(z_1, \ldots, z_n).$$

Ici donc $\chi_\pi = \varphi_{(1,0,\ldots,0)}$.

On peut vérifier $\varphi_{(k,0,\ldots,0)}$ (respectivement, $\varphi_{(1,\ldots,1,0,\ldots,0)}$, avec k fois 1 et $n-k$ fois 0) est le caractère de la représentation de G sur la puissance symétrique (respectivement, extérieure) k-ième de cette représentation π. Il suffit en fait de le vérifier sur les restrictions au tore, ce qui est aisé en utilisant le théorème 3.1.4.2.

Signalons enfin que les tableaux semi-standards appartiennent à un ensemble d'outils très efficaces qui permettent par exemple de calculer combinatoirement les multiplicités des représentations irréductibles dans les produits tensoriels.

5.4 Application : symétrie des tenseurs

5.4.1 Tenseurs symétriques, tenseurs antisymétriques

Soit k un corps, V un espace vectoriel sur k, n un entier ≥ 1.

Le groupe $\mathfrak{S}_n$ agit sur $\mathsf{T}^n V$ par permutation des facteurs :

$$\sigma \cdot (v_1 \otimes \cdots \otimes v_n) = v_{\sigma^{-1}(1)} \otimes \cdots \otimes v_{\sigma^{-1}(n)}.$$

Un tenseur $t \in \mathsf{T}^n V$ est dit symétrique s'il est invariant par $\mathfrak{S}_n$. On note $\mathsf{TS}^n V$ l'ensemble des tenseurs symétriques de degré n sur V ; ainsi $\mathsf{TS}^n V = \mathrm{inv}_{\mathfrak{S}_n}\big(\mathsf{T}^n V\big)$. (Les objets $\mathsf{TS}^n V$ et $\mathsf{S}^n V$ sont très proches l'un de l'autre, mais ne sont pas vraiment égaux. Ainsi on notera que $\mathsf{TS}(V) = \bigoplus_{n\geq 0} \mathsf{TS}^n V$ n'est pas une sous-algèbre de $\mathsf{T}\,V$ (du moins pas pour le produit usuel), alors qu'au contraire, l'algèbre symétrique $\mathsf{S}(V)$ est un quotient de l'algèbre $\mathsf{T}\,V$.)

De même, on dira qu'un tenseur $t \in \mathsf{T}^n V$ est antisymétrique si $\sigma \cdot t = \mathrm{sgn}(\sigma)t$ pour chaque permutation $\sigma \in \mathfrak{S}_n$. On note $\mathsf{TA}^n V$ l'ensemble des tenseurs antisymétriques.

Exemple. Supposons que k soit de caractéristique $\neq 2$. Alors $\mathsf{T}^2 V = \mathsf{TS}^2 V \oplus \mathsf{TA}^2 V$. De fait, l'automorphisme de $\mathsf{T}^2 V$ par lequel agit la transposition de $\mathfrak{S}_2$ est une symétrie ; $\mathsf{TS}^2 V$ est l'espace propre pour la valeur $+1$ de cette symétrie, et $\mathsf{TA}^2 V$ en est l'espace propre pour la valeur -1. En termes terre-à-terre, tout tenseur d'ordre 2 peut être décomposé de façon unique en somme d'un tenseur symétrique et d'un tenseur antisymétrique.

5.4.1.1 Proposition. *Supposons que k soit de caractéristique 0. Alors les éléments de la forme $v^{\otimes n}$, pour $v \in V$, engendrent $\mathsf{TS}^n V$.*

Preuve. On dispose des identités de polarisation : pour chaque $(v_1, \dots, v_n) \in V^n$, on a

$$\sum_{\sigma \in \mathfrak{S}_n} v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(n)} = \frac{1}{2^n} \sum_{(\varepsilon_1, \dots, \varepsilon_n) \in \{-1,1\}^n} \varepsilon_1 \cdots \varepsilon_n (\varepsilon_1 v_1 + \cdots + \varepsilon_n v_n)^{\otimes n}.$$

Par ailleurs, l'opérateur de Reynolds

$$v_1 \otimes \cdots \otimes v_n \mapsto \frac{1}{n!} \sum_{\sigma \in \mathfrak{S}_n} v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(n)}$$

est un projecteur de $\mathsf{T}^n V$ sur $\mathsf{TS}^n V$. □

5.4.2 Dualité de Schur-Weyl

Soient V un espace vectoriel complexe de dimension finie n et $p \geq 1$ un entier. Moyennant le choix pour V d'un produit scalaire hermitien et d'une base orthonormale, on peut supposer que $V = \mathbf{C}^n$ est la représentation naturelle de $G = \mathbf{U}(n)$. Ainsi G agit aussi sur la puissance tensorielle $\mathsf{T}^p V$. Par ailleurs, le groupe $H = \mathfrak{S}_p$ agit sur $\mathsf{T}^p V$ par permutation des facteurs, comme expliqué dans le paragraphe précédent. Nous avons donc deux homomorphismes d'algèbres à valeurs dans $\mathrm{End}_{\mathbf{C}}(\mathsf{T}^p V)$, l'un de domaine $\mathbf{C}G$, l'autre de domaine $\mathbf{C}H$. Notons A et B les images de ces deux homomorphismes.

5.4.2.1 Proposition. *Les sous-algèbres A et B de $\mathrm{End}_{\mathbf{C}}(\mathsf{T}^p V)$ sont le commutant l'une de l'autre :*

$$A = \mathrm{End}_H(\mathsf{T}^p V) \quad \textit{et} \quad B = \mathrm{End}_G(\mathsf{T}^p V).$$

Preuve. On note $\overline{A}$ le sous-espace vectoriel de $\mathrm{End}_{\mathbf{C}}(\mathsf{T}^p V)$ engendré par les éléments de la forme $u^{\otimes p}$, pour $u \in \mathrm{End}_{\mathbf{C}}(V)$. Certainement $A \subseteq \overline{A}$. Si cette inclusion était stricte, A serait inclus dans une hypersurface de $\overline{A}$, dont on pourrait écrire une équation $\varphi = 0$. Alors $\{u \in \mathrm{End}_{\mathbf{C}}(V) \mid \varphi(u^{\otimes p}) = 0\}$ serait une hypersurface de degré p de $\mathrm{End}_{\mathbf{C}}(V)$, c'est-à-dire le lieu des zéros d'un polynôme de degré p, et cette hypersurface contiendrait $\mathbf{U}(n)$. Appliquant la transformation de Cayley (voir le paragraphe 5.3.1.3 (6)), nous obtiendrions une hypersurface de degré p de $\mathrm{End}_{\mathbf{C}}(V)$ qui contiendrait un ouvert non-vide de l'espace vectoriel des matrices antihermitiennes. Mais cela n'est pas possible, en vertu du résultat bien connu suivant : un polynôme $P \in \mathbf{C}[X_1, \dots, X_n]$ qui s'annule en tout point d'un ouvert non-vide de $\mathbf{R}^n$ est nul. (Il faut ici remarquer que l'espace des matrices antihermitiennes $\mathfrak{u}(n)$ est une forme réelle de $\mathrm{End}_{\mathbf{C}}(V)$, c'est-à-dire que $\mathrm{End}_{\mathbf{C}}(V) = \mathfrak{u}(n) \oplus i\mathfrak{u}(n)$.) Notre hypothèse $A \subsetneq \overline{A}$ est donc absurde. Ainsi $A = \overline{A}$.

Écrivons

$$\mathrm{End}_{\mathbf{C}}(\mathsf{T}^p V) \cong (\mathsf{T}^p V) \otimes_{\mathbf{C}} (\mathsf{T}^p V)^* \cong V^{\otimes p} \otimes_{\mathbf{C}} (V^*)^{\otimes p} \cong (V \otimes_{\mathbf{C}} V^*)^{\otimes p} = \mathsf{T}^p(\mathrm{End}_{\mathbf{C}}(V)).$$

Dans cet isomorphisme, $\mathrm{End}_H(\mathsf{T}^p V)$ correspond à $\mathsf{TS}^p(\mathrm{End}_{\mathbf{C}}(V))$. D'après la proposition 5.4.1.1, on a $\mathrm{End}_H(\mathsf{T}^p V) = \overline{A} = A$.

Par ailleurs, $\mathsf{T}^p V$ est un B-module complètement réductible d'après le théorème de Maschke, donc B est égal à son bicommutant d'après le théorème de densité de Jacobson-Chevalley. L'égalité $A = \mathrm{End}_H(\mathsf{T}^p V)$ signifie que A est le commutant de B dans $\mathrm{End}_{\mathbf{C}}(\mathsf{T}^p V)$. On en déduit que B est le commutant de A, c'est-à-dire que $B = \mathrm{End}_G(\mathsf{T}^p V)$. □

Appliquant la proposition 1.4.5.3, nous obtenons en fin de compte que $\mathsf{T}^p V$ se décompose en somme directe de ses composantes isotypiques

$$\mathsf{T}^p V = \bigoplus_{\lambda} (\mathsf{T}^p V)_\lambda,$$

chacune de ces composantes se décomposant sous forme du produit tensoriel d'un A-module simple par un B-module simple :

$$(\mathsf{T}^p V)_\lambda \cong V_\lambda \otimes_{\mathbf{C}} S_\lambda.$$

Ici S_λ est une représentation irréductible de $H = \mathfrak{S}_p$ et V_λ est une représentation irréductible de $G = \mathbf{U}(n)$.

Cette façon d'écrire rend compte de l'existence d'une bijection entre l'ensemble des classes d'isomorphismes de $\mathbf{C}G$-modules simples apparaissant dans $\mathsf{T}^p V$ et l'ensemble des classes d'isomorphismes de $\mathbf{C}H$-modules simples apparaissant dans $\mathsf{T}^p V$. Par un calcul de caractère, on peut s'assurer que cette bijection est celle qui nous a conduit à indexer les représentations de $\mathbf{U}(n)$ et de $\mathfrak{S}_p$ par un même ensemble, à savoir l'ensemble des partitions de poids p et de longueur $\leq n$.

En conclusion, on peut dire que $(\mathsf{T}^p V)_\lambda$ est l'ensemble des tenseurs d'ordre p qui présentent le type de symétrie dicté par le caractère irréductible χ^λ de $\mathfrak{S}_p$. Notamment $(\mathsf{T}^p V)_{(p)} = \mathsf{TS}^p V$ est l'espace des tenseurs symétriques et $(\mathsf{T}^p V)_{(1^p)} = \mathsf{TA}^p V$ est l'espace des tenseurs antisymétriques.

Références

[1] Frank W. Anderson, Kent R. Fuller, *Rings and categories of modules,* Graduate Texts in Mathematics, Vol. 13, Springer-Verlag, 1992.

[2] Maurice Auslander, Idun Reiten, Sverre O. Smalø, *Representation theory of Artin algebras,* Cambridge studies in advanced mathematics, Vol. 36, Cambridge, 1995.

[3] Nicolas Bourbaki, *Algèbre. Chapitre 8 : Modules et anneaux semi-simples,* Actualités scientifiques et industrielles, n° 1261, Hermann, 1958.

[4] Richard Brauer, *Über die Darstellung von Gruppen in Galoisschen Feldern,* Actualités scientifiques et industrielles, n° 195, Hermann, 1935.

[5] Daniel Bump, *Lie groups,* Graduate Texts in Mathematics, Vol. 225, Springer-Verlag, 2004.

[6] Charles W. Curtis, Irving Reiner, *Representation theory of finite groups and associative algebras,* Pure and Applied Mathematics, Vol. XI, Interscience Publishers (John Wiley & Sons), 1962.

[7] Charles W. Curtis, Irving Reiner, *Methods of representation theory, with applications to finite groups and orders,* Pure and Applied Mathematics, Wiley-Interscience, 1981 (Vol. I) et 1987 (Vol. II).

[8] Jacques Faraut, *Analyse sur les groupes de Lie,* Calvage et Mounet, 2006.

[9] William Fulton, *Young tableaux. With applications to representation theory and geometry,* London Mathematical Society Student Texts, Vol. 35, Cambridge University Press, 1997.

[10] Roger Godement, *Introduction à la théorie des groupes de Lie,* Springer-Verlag, 2004.

[11] Nathan Jacobson, *Basic algebra II,* W. H. Freeman and Company, 1989.

[12] Alexander Kleshchev, *Linear and projective representations of symmetric groups,* Cambridge Tracts in Mathematics, Vol. 163, Cambridge University Press, 2005.

[13] Ian G. Macdonald, *Symmetric functions and Hall polynomials. Second edition,* Oxford Mathematical Monographs, Oxford University Press, 1995.

[14] Rached Mneimné, Frédéric Testard, *Introduction à la théorie des groupes de Lie classiques,* Collection Méthodes, Hermann, 1986.

[15] Hirosi Nagao, Yukio Tsushima, *Representations of finite groups,* Academic Press, 1989.

[16] Jean-Pierre Serre, *Représentations linéaires des groupes finis,* Hermann, 1967.

[17] Hermann Weyl, *The Classical Groups. Their Invariants and Representations,* Princeton University Press, 1939.