Table des matières

Résumé

Notons $[G:H]$ l'indice d'un sous-groupe H d'un groupe fini G. Le théorème de Lagrange indique que $[G:H] \in \mathbb{N}^*$. En passant aux inclusions d'algèbres de groupes $kH \subset kG$, où k est un corps algébriquement clos tel que $car(k) = 0$ (typiquement, $k = \mathbb{C}$), on a $[G:H] = \frac{\dim(kG)}{\dim(kH)}$. Dans ce cours, on définit et on étudie l'indice $[A:B]$ d'une inclusion d'algèbres unifères associatives semi-simples de dimension finie $B \subset A$ sur k. Selon le théorème de Mashke, l'algèbre de groupe kG d'un groupe fini G est semi-simple donc cette nouvelle notion est une extension de la notion d'indice d'un sous-groupe. On verra, en particulier, que la valeur de $[A:B]$ n'est pas nécessairement un nombre entier. Ensuite, on étudie la tour d'algèbres construite à partir d'une inclusion $A \subset B$ donnée à l'aide de la construction fondamentale ainsi que les propriétés des traces de Markov et d'espérances conditionnelles associées.

1 Algèbres et modules : définitions et exemples de base. Lemme de Shur.

1.1 Algèbres, idéaux et morphismes.

Définitions 1.1. -

- Une **algèbre associative unifère** A sur k est un espace vectoriel muni d'une application bilinéaire dite multiplication associative $A \times A \to A : (a,b) \mapsto ab,\ \forall a,b \in A$ et d'unité 1_A.
- L'**algèbre opposée** A^{op} de A est le même espace vectoriel muni de la multiplication opposée $(a,b) \mapsto ba$.
- Une **sous-algèbre** $B \subset A$ est un sous-espace vectoriel stable pour la multiplication. B est **unifère** si $1_A \in B$.
- Le **centre** $Z(A)$ de A est l'ensemble de tous les $a \in A$ tels que $ab = ba,\ \forall b \in A$. Évidemment, $k1_A \subset Z(A)$. Si $Z(A) = k1_A$, on dit que A est un **facteur**.
- Un **idéal à gauche** (resp., **à droite**) $I \subset A$ est un sous-ensemble tel que $AI \subset I$ (resp., $IA \subset A$) . Un **idéal bilatère** de A est un idéal à gauche et à droite de A. Un **idéal propre** de A ne contient pas 1_A (le prouver).
- Une algèbre A est **commutative** (ou abélienne) si $Z(A) = A$.
- Une algèbre A est **simple** si elle n'a pas d'idéaux bilatères propres non nuls.
- On dit que $a \in A$ est **inversible** s'il existe un élément $a^{-1} \in A$ tel que $aa^{-1} = a^{-1}a = 1_A$. On note $A^\times$ l'ensemble de tous les éléments inversibles de A. Un idéal propre de A ne contient pas d'inversibles (le prouver). Si $A = A^\times \cup \{0\}$, on dit que A est une **algèbre à division**. Une telle algèbre ne contient pas de diviseurs de 0.

Exemples 1.1. (Algèbres)

a) $A = \mathrm{End}_k(V)$ - l'algèbre des endomorphismes d'un espace vectoriel V sur k, où la multiplication est la composition d'endomorphismes, $1_A = id_V$. Si V est de dimension finie n, alors $A = M_n(k)$ est un facteur (vérification directe) ; $A = \{a \oplus a \oplus \ldots \oplus a : a \in M_n(k)\}$ est un facteur.

b) $A = k[X]$ - l'algèbre commutative des polynômes en l'indéterminée X :
$$P_n(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0,$$
où $a_i \in k,\ \forall i \in \{1;2;\ldots;n\}$, et $n \in \mathbb{N}$, avec la multiplication usuelle et $1_A = 1(X) \equiv 1$.

c) kG - l'algèbre d'un groupe G est l'espace vectoriel des combinaisons linéaires formelles finies d'éléments de G muni de la multiplication suivante :
$$(\sum_{s\in G} a_s \cdot s)(\sum_{t\in G} b_t \cdot t) = \sum_{s\in G}\sum_{t\in G} a_s b_t \cdot st = \sum_{u\in G}(\sum_{s\in G} a_s b_{s^{-1}u}) \cdot u,$$
pour toutes suites $(a_s)_{s\in G}$ et $(b_t)_{t\in G}$ d'éléments de k. On a $1_A = e$, où e est l'élément neutre du groupe G. Évidemment, cette algèbre est associative car la multiplication dans G est associative ; elle est commutative ssi G est commutatif ; si G est un groupe fini, alors $\dim(kG) = |G|$.

d) $M_n(A)$, où A est une algèbre.

Exemples 1.2. (Sous-algèbres)

a) Le sous-espace vectoriel des matrices diagonales est une sous-algèbre de $M_n(k)$.

b) Le sous-espace vectoriel des matrices triangulaires est une sous-algèbre de $M_n(k)$.

c) Le sous-espace vectoriel des polynômes pairs (mais pas impairs !) en X est une sous-algèbre de $k[X]$.

d) kH est une sous-algèbre de kG, où H est un sous-groupe de G.

Exemples 1.3. (Idéaux)

a) Pour tout $a \in A$, $I_g := Aa$ (resp., $I_d := aA$) est un idéal à gauche (resp., à droite) ; si $a \in Z(A)$, $I := aA$ est bilatère ; $I = A$ ssi a est inversible.
b) L'ensemble des matrices lignes (resp., colonnes) forme un idéal à droite (resp., à gauche) de $M_n(k)$.
c) L'ensemble des polynômes qui s'annulent en $x_0 \in k$ forme un idéal bilatère de $k[X]$.

Remarque. Si A est simple, tout $a \in Z(A), a \neq 0$ est inversible donc $Z(A)$ est une algèbre à division car sinon, on peut fabriquer un idéal bilatère non trivial de A. On va montrer que si A est simple et $\dim(Z(A)) < \infty$, alors A est un facteur.

Proposition 1.1. Une algèbre à division D telle que $\dim(D) = m < \infty$ est isomorphe à k.

Preuve. Si $x \in D$, la famille $1_D, x, x^2, \ldots, x^m$ n'est pas libre donc il existe un polynôme normalisé $P \in k[X]$ de degré minimal tel que $P(x) = 0$. Comme D est une algèbre à division, le polynôme P est irréductible sur k. En effet, si $P = P_1P_2$ avec $\deg(P_1),\ \deg(P_2) < \deg(P)$, on a $P(x) = P_1(x)P_2(x) = 0$ avec $P_1(x) \neq 0,\ P_2(x) \neq 0$ par minimalité de $\deg(P)$: contradiction avec l'absence de diviseurs de 0 dans une algèbre à division. Mais comme k est algébriquement clos, pour tout polynôme irréductible, on a $P(X) = X - z$ pour un $z \in k$. Donc $x = z1_D$. ■

Définitions 1.2. -

– Un **morphisme** d'une algèbre A unifère dans une autre algèbre unifère B est un morphisme φ d'espaces vectoriels A et B tel que $\varphi(a{\cdot}b) = \varphi(a){\cdot}\varphi(b)$, pour tous $a \in A, b \in B$, et $\varphi(1_A) = 1_B$. On peut parler des morphismes injectifs (inclusions d'algèbres), surjectifs, isomorphismes, automorphismes. On dit qu'un **automorphisme** $\varphi : A \to A$ est **intérieur** s'il existe $b \in A^\times$ tel que $\varphi(a) = bab^{-1}$, pour tout $a \in A$.
– Une **représentation** d'une algèbre A sur un espace vectoriel V est un morphisme π de A dans $\mathrm{End}_k(V)$. π est dit **irréductible** si V n'a pas de sous-espaces non triviaux stables pour tous les endomorphismes de $\mathrm{Im}\,(\pi)$.
– Soit $(A_j)_{j\in J}$ une famille d'algèbres. La **somme directe** des algèbres A_j est par définition la somme directe $\oplus_{j\in J}A_j$ des espaces vectoriels A_j munie de la multiplication $(\oplus_{j\in J}a_j) \cdot (\oplus_{j\in J}b_j) := \oplus_{j\in J}(a_j \cdot b_j)$.

Exemples 1.4. -

a) Les morphismes de groupes engendrent les morphismes d'algèbres de groupes associés, les représentations (en particulier, irréductibles) d'un groupe G correspondent aux représentations (en particulier, irréductibles) de kG.
b) En particulier, les représentations **triviale** $\pi_{triv} : G \to k :\ \pi(g) \equiv 1_k$ et **régulière à droite** $\pi^d_{reg} : G \to \mathrm{End}_k(kG) : \pi^d_{reg}(g)h = hg,\ \forall g, h \in G$ d'un groupe G et de kG. De même pour la représentation **régulière à gauche** $\pi^g_{reg} : G \to \mathrm{End}_k(kG) : \pi^g_{reg}(g)h = g^{-1}h,\ \forall g, h \in G$.
c) L'inclusion $M_n(k) \subset M_{2n}(k) :\ a \mapsto a \oplus a$ n'est pas surjective.

Remarques. -

– On va voir dans le §2 la relation très étroite entre les notions de morphisme d'algèbres et d'idéal bilatère.
– L'algèbre de groupe kG n'est jamais simple (sauf si $G = \{e\}$). En effet, le noyau de la représentation triviale est un idéal bilatère non trivial.

1.2 Modules.

Définitions 1.3. -

– Soit A une algèbre unifère. Un A-**module** à gauche est un espace vectoriel M muni d'une application bilinéaire dite **action** de A sur M $\cdot : A \times M \to M$ telle que $(ab) \cdot m = a \cdot (b \cdot m),\ 1_A \cdot m = m,\ \forall a, b \in A,\ \forall m \in M$.
– On définit un A-module à droite de manière analogue. Toutes les définitions et tous les résultats ci-dessous, formulés pour les A-modules à gauche (resp., à droite), ont leurs analogues évidents pour les A-modules à droite (resp., à gauche).
– Un A-**bimodule** M est un A-module à gauche et à droite tel que $a \cdot (m \cdot b) = (a \cdot m) \cdot b,\ \forall a, b \in A,\ \forall m \in M$.
– Un **sous-module** d'un A-module M à gauche est un sous-espace vectoriel de M stable pour l'opération $\cdot$.
– On dit qu'un A-module non nul est **simple** s'il n'a aucun sous-module non-trivial.
– On dit qu'un sous-module de M est **minimal** s'il est simple en tant que A-module.
– Un **morphisme** de A-modules à gauche M et N est une application linéaire $\varphi : M \to N$ telle que $\varphi(a \cdot m) = a \cdot \varphi(m),\ \forall m \in M$. Parfois, on dit qu'une telle application est A-linéaire. On peut parler de morphismes injectifs, surjectifs et bijectifs (équivalence de modules).

- Une **somme directe** $M = \oplus_i M_i$ d'une famille de A-modules à gauche M_i est la somme directe des M_i en tant qu'espaces vectoriels (donc tout élément de M est une somme finie d'éléments de M_i) munie de l'opération $a\cdot(\oplus_i m_i) := \oplus_i(a\cdot m_i)$, $\forall a \in A, \forall m_i \in M_i$. De même, pour les A-modules à droite. On peut définir naturellement l'injection canonique $\nu_i : M_i \to M$ et la projection canonique $\pi_i : M \to M_i$ comme morphismes de A-modules.
- On dit qu'un sous-module N d'un A-module M est un **facteur direct** de M s'il existe un autre sous-module P de M tel que $M = N \oplus P$.
- On vérifie directement que, si $f_i : M_i \to N$ est un morphisme de A-modules pour tout i, alors il existe un morphisme $f : M = \oplus_i M_i \to N$ et un seul tel que $f \circ \nu_i = f_i$.
- On dit qu'un A-module à gauche M est **libre** s'il possède une **base** (finie ou infinie) $B = \{b_1, b_2, \ldots\}$, c-à-d :
  a) tout élément de M est une combinaison linéaire d'éléments de B à coefficients dans A ;
  b) B est libre : si $m_1b_1 + m_2b_2 + \ldots + m_nb_n = 0$ pour $m_1, \ldots, m_n \in M$, alors $m_1 = m_2 = \ldots = m_n = 0$.
- On dit qu'un A-module à gauche M est **de type fini** s'il existe un ensemble fini $B = \{b_1, b_2, \ldots, b_n\}$ (pas nécessairement libre) tel que tout élément de M est combinaison linéaire d'éléments de B à coefficients dans A. Un A-module à gauche est **cyclique** s'il est engendré par un seul élément.
- On dit qu'un A-module à gauche M est **projectif** s'il existe un autre A-module N tel que la somme directe $M \oplus N$ est un A-module libre.
- Soit $\pi : A \to \mathrm{End}_k(V)$ une représentation de A sur un espace vectoriel V. Dans ce cas, V est un A-module à gauche pour $a \cdot v := \pi(a)v$, $\forall a \in A$, $\forall v \in V$. Réciproquement, tout A-module V à gauche définit une représentation π de A sur V par la même formule. De plus, π est irréductible ssi le A-module V est simple.

Notations. -
- $\mathrm{Hom}^d_A(M, N)$ est l'ensemble de tous les morphismes de A-modules à droite M et N, c'est un A-module à gauche : $(a \cdot \varphi)(m) := a \cdot (\varphi(m)),\ \forall a \in A,\ \forall m \in M,\ \forall \varphi \in \mathrm{Hom}^d_A(M, N)$.
- $\mathrm{End}^d_A(M)$ est l'ensemble de tous les endomorphismes d'un A-module à droite M, c'est une algèbre (pour la composition des endomorphismes) et un A-module à gauche.

Exemples 1.5. (Modules)

a) Toute algèbre A définit un A-module à gauche ${}_gA$ (resp., à droite A_d) dit **régulier** - l'action de A est définie par la multiplication à gauche (resp., à droite). Ces modules sont cycliques car 1_A est vecteur cyclique.

b) De même, tout idéal à gauche de A est un A-module à gauche ; les sous-modules à gauche de ${}_gA$ sont exactement les idéaux à gauche de A.

c) Le sous-module M du module régulier à gauche ${}_gA$ sur l'algèbre $A := T_2^+(k) = \left\{\begin{pmatrix} a_{11} & a_{12} \\ 0 & a_{22}\end{pmatrix} : a_{ij} \in k\right\}$, défini par la condition $a_{22} = 0$ (A agit sur M par multiplication par a_{11}) n'a pas de complément direct qui soit un A-module. En effet, tout complément direct N du sous-espace vectoriel M dans l'espace vectoriel ${}_gA$ est de dimension 1 donc engendré par une matrice fixée avec $a_{22} \neq 0$. Mais on a toujours $\dim(A \cdot N) > 1$ donc N ne peut pas être un A-module.

Remarques. -
- Tout A-module simple à gauche M est nécessairement cyclique et tout vecteur non nul est cyclique car si $m \in M, m \neq 0$ n'est pas cyclique, le sous-module $A \cdot m$ de M est propre et non nul (il contient $m = 1_A \cdot m$).
- On a $\dim(M) \leqslant \dim(A)$, pour tout A-module simple à gauche M car $\dim(M) = \dim(A\cdot m) \leqslant \dim(A)$, $\forall m \in M$.

Lemme de Shur. -
Soient A une algèbre et $\varphi : M \to N$ un morphisme non nul de A-modules (à gauche ou à droite).
(i) Si M est simple, alors φ est injectif.
(ii) Si N est simple, alors φ est surjectif.

Preuve. Comme $\varphi \neq 0$, on a $\mathrm{Ker}\,\varphi \neq M$ et $\mathrm{Im}\,\varphi \neq 0$. Alors, si M est simple, on a $\mathrm{Ker}\,\varphi = 0$, et si N est simple, on a $\mathrm{Im}\,\varphi = N$. ■

Corollaire. **1.** Si M et N sont simples, alors ou bien ils sont équivalents, ou bien $\mathrm{Hom}_A(M, N) = 0$.
2. Soient N un idéal à droite minimal de A et $x \in A$. Alors ou bien $xN = 0$, ou bien xN est un idéal à droite minimal de A équivalent à N.

En effet, $n \mapsto xn$ est un morphisme surjectif de A-modules N et xN, et on applique le lemme de Shur.

2 Présentation d'une algèbre. Modules et algèbres semi-simples.

2.1 Définition d'une algèbre par présentation de générateurs et relations entre eux.

Définition 2.1. Soient A une algèbre et I un idéal bilatère de A. On définit la relation d'équivalence R suivante :

$$\forall (x,y) \in A^2, \quad xRy \Leftrightarrow (x-y) \in I.$$

Deux éléments de A sont ainsi en relation si leur différence appartient à I. L'espace vectoriel quotient A/I, muni de la multiplication induite par I : $(x+I)\times(y+I) = (x\cdot y)+I$, est une algèbre, nommée **algèbre quotient** de A par I. On a $1_{A/I} = 1_A + I$.

Évidemment, si $I = A$, alors A/A est l'algèbre triviale $\{0\}$, et si $I = \{0\}$, alors $A/\{0\}$ est isomorphe à A.

Propriétés. -

a) L'application $\pi : A \to A/I$ définie par $\pi(x) = x+I$ est un morphisme surjectif d'algèbres (appelée **projection canonique**) dont le noyau est I.

b) Si $f : A \to B$ est un homomorphisme d'algèbres, notons $I = \mathrm{Ker}\, f$ son noyau. C'est un idéal bilatère. Alors, f se factorise en un morphisme injectif $\bar{f} : A/I \to B$ défini par $\bar{f}(x+I) = f(x)$ (c'est le théorème fondamental des homomorphismes).

c) Soient A une algèbre commutative, I un idéal bilatère propre de A. Alors I est maximal ssi $A/I = k$.

Preuve. du c) : (i) Soit $A/I \neq k$ alors il existe $a \in A - I$, non inversible, car sinon A/I est une algèbre à division et donc $A/I = k$ par la proposition 1.1. Maintenant $I_1 := I + aA$ est un idéal bilatère propre de A, car I_1 ne contient pas 1_A, et $I \subset I_1$ donc I n'est pas maximal.
(ii) Si $A/I = k$, on a, par définition, $A = I + k1_A$ donc I est maximal propre. ■

Une algèbre peut se définir par sa **présentation** autrement dit la donnée d'un ensemble S de générateurs et de relations que ceux-ci doivent vérifier. Si les générateurs de S ne vérifient aucune relation, l'algèbre $AL(S)$ engendrée par S est dite **algèbre libre engendrée par** S. Elle est formée de toutes les combinaisons formelles sur k de monômes sur S, c'est-à-dire des mots formels $x_1x_2\ldots x_n$, où $x_i \in S$, $i \in \{1,2,\ldots,n\}$ et du mot vide $\mathbf{1}$. La multiplication associative dans cette algèbre est engendrée par la concaténation des mots.
En général, les générateurs de S vérifient certaines relations : il existe un certain ensemble P d'éléments de $AL(S)$ qui doivent être égaux à 0 dans notre algèbre. Plus formellement, on considère l'idéal bilatère minimal $I(P)$ de $AL(S)$ engendré par P, et on quotiente $AL(S)$ par cet idéal : $A(S,P) := AL(S)/I(P)$.
D'habitude, la présentation (S,P) d'une algèbre A se note en écrivant entre crochets une liste des générateurs de S et une liste des combinaisons formelles de mots en ces générateurs.

Exemples 2.1. -

a) $k[X,Y] = < X, Y \mid XY - YX >$.

b) $M_2(k) = < e_{ij} \mid e_{ij}e_{kl} - \delta_{j,k}e_{il} >$, où $i,j,k,l \in \{1,2\}$ et $\delta_{i,j}$ est le symbole de Kronecker.

2.2 Modules et algèbres semi-simples.

Définition 2.2. Soit A une algèbre. On dit qu'un A-module (à gauche ou à droite) est **semi-simple** s'il est égal à une somme directe de A-modules simples.

Par conséquent, une somme directe de A-modules semi-simples est un A-module semi-simple.

Proposition 2.1. -

(i) Dans $A = M_n(k)$, les ensembles N_i ($i \in \{1,2,\ldots,n\}$) de matrices lignes (resp., colonnes) forment des idéaux à droite (resp., à gauche) minimaux.

(ii) $A_d = \oplus_{i=1}^n N_i$ en tant que A-modules à droite.

(iii) Les A-modules à droite simples N_i et N_j sont isomorphes pour tous i et j.

(iv) $A = M_n(k)$ est simple (*i.e.* ne contient pas d'idéaux bilatères non triviaux).

Preuve.

(i) Soient e_{ij} **les unités matricielles** qui forment une base de A et $N_i = e_{ii}M_n(k)$ l'ensemble des matrices lignes pour $i \in \{1, \dots, n\}$ fixé. Alors N_i est un idéal à droite de A, et on va montrer que, pour toute matrice non nulle $\beta = \sum_{j=1}^n \beta_j e_{ij} \in N_i$, on a $\beta A = N_i$, ce qui prouvera que N_i est minimal. En effet, soit $\beta_{j0} \neq 0$, alors $\beta \sum_{l=1}^n \beta_{j0}^{-1} a_l e_{j_0 l} = \sum_{l=1}^n a_l e_{il}$ pour tout $a_l \in k$.

(ii) est évident.

(iii) On applique le corollaire 2 du lemme de Shur : si $N_i = e_{ii}A$ et $N_j = e_{jj}A$, alors l'égalité $N_j = e_{ji}e_{ij}A = e_{ji}N_i$ montre qu'ils sont équivalents.

(iv) Soit $I \subset M_n(k)$ un idéal bilatère non nul donc il contient une matrice β non nulle (disons, $\beta_{rs} \neq 0$). On va montrer que I contient alors n'importe quelle matrice $\alpha = (\alpha_{ij}) = \sum_{i,j=1}^n \alpha_{ij}e_{ij}$. On a :

$$(\alpha_{ij}) = \sum_{i,j=1}^{n} \alpha_{ij}e_{ij} = \sum_{i,j=1}^{n} \beta_{rs}^{-1}\alpha_{ij}(e_{ir}\beta e_{sj}) \in I$$

car I est un idéal bilatère de A.

■

Remarque. La proposition 2.1 montre que les modules réguliers à droite et à gauche sur $A = M_n(k)$ sont semi-simples.

Lemme 2.1. Soit $M = \oplus_{i\in I}N_i$ une somme directe de A-modules simples. Alors :

(i) Pour tout sous-module $P \in M$, il existe un sous-ensemble $J \subset I$ tel que $M = (\oplus_{i\in J}N_i) \oplus P$ donc P est un facteur direct de M.

(ii) Tout sous-module $Q \subset P$ est un facteur direct de P.

Preuve.

(i) Soit J le sous-ensemble maximal de I tel que $(\oplus_{i\in J}N_i) + P = (\oplus_{i\in J}N_i) \oplus P$. Il existe en vertu du

Lemme de Zorn. Tout ensemble partiellement ordonné dont toute partie totalement ordonnée admet un majorant, admet au moins un élément maximal.

J est non vide car $P \cap N_i = N_i$ ou 0 puisque les N_i sont simples. Par maximalité de J, l'intersection du module $M_J := (\oplus_{i\in J}N_i) \oplus P$ avec tout $N_i,\ (i \in I)$ est non vide donc M_J contient tout N_i donc $M_J = M$.

(ii) Par (i), il existe un sous-module $S \subset M$ tel que $M = Q \oplus S$ donc $P = P \cap (Q \oplus S) = (P \cap Q) \oplus (P \cap S) = Q \oplus (P \cap S)$.

■

Remarque. Le lemme 2.1 montre que pour qu'un A-module soit semi-simple, il faut et il suffit que tout sous-module soit facteur direct et que tout sous-module d'un A-module semi-simple est aussi semi-simple. En particulier, l'exemple 1.5 c) du §1 est un exemple de module qui n'est pas semi-simple.

Théorème de Mashke. Si G est un groupe fini, alors tout kG-module à gauche M est semi-simple.

Preuve. Soit N un sous-module minimal de M (son existence est évidente si $\dim(M) < \infty$; dans le cas général on peut utiliser le lemme de Zorn). On va montrer qu'il existe un autre sous-module N_1 de M tel que $M = N \oplus N_1$. A priori, il existe un **sous-espace vectoriel** N_0 de M tel que $M = N \oplus N_0$. Pour tout $x \in N_0$ et $g \in G$, on a : $g \cdot x = n + x'$, où $x' \in N_0,\ n \in N$. La dépendance x' de x est linéaire, elle définit un opérateur $T_g : N_0 \to N_0 : x \mapsto x'$, et on peut vérifier que $g \to T_g$ est une représentation de G sur N_0. En effet, $T_{g_1g_2}x = (g_1g_2) \cdot x - n'$ et $T_{g_1}(T_{g_2}x) = T_{g_1}(g_2 \cdot x - n_1) = g_1 \cdot (g_2 \cdot x - n_1) - n_1' = g_1 \cdot (g_2 \cdot x) - g_1 \cdot n_1 - n_1'$, où $n', n_1, g_1 \cdot n_1, n_1' \in N$. Donc, $T_{g_1g_2}x = T_{g_1}(T_{g_2}x)$ car la décomposition $(g_1g_2) \cdot x = g_1 \cdot (g_2 \cdot x) = x'' + n''$ avec $x'' \in N_0,\ n'' \in N$, est unique. Maintenant on pose :

$$y = \frac{1}{|G|}\sum_{g\in G} g^{-1} \cdot T_g x := Tx \quad \text{et} \quad N_1 := \{Tx \mid x \in N_0\}.$$

La dépendance y de x est linéaire donc N_1 est un sous-espace vectoriel de M. De plus, $y = x \mod N$ car

$$y - x = \frac{1}{|G|}\sum_{g\in G} g^{-1} \cdot (T_g x - g \cdot x) \in N,$$

donc $M = N \oplus N_1$. Finalement, pour tout $h \in G$,

$$hy = \frac{1}{|G|}\sum_{g\in G} hg^{-1}\cdot T_g x = \frac{1}{|G|}\sum_{g\in G}(gh^{-1})^{-1}\cdot T_g T_{h^{-1}} T_h x = T\cdot T_h x \in TN_0 = N_1.$$

Ainsi, N_1 est un sous-module de M. ■

Définition 2.3. On dit qu'une algèbre A est **semi-simple** à gauche (resp., à droite) si le A-module régulier à gauche (resp., à droite) est semi-simple.

Remarques. -
- Le théorème de Mashke dit que, si G est un groupe fini, alors l'algèbre kG est semi-simple à gauche. De manière analogue, on peut montrer qu'elle est aussi semi-simple à droite.
- La proposition 2.1 montre que l'algèbre $M_n(k)$ est semi-simple à gauche et à droite ; l'exemple 1.5 c) du module régulier à gauche sur $T_2^+(k)$ montre que cette algèbre n'est pas semi-simple.
- Tout A-module libre sur une algèbre A semi-simple est semi-simple.
- Dans le cours suivant, on va montrer que les notions d'algèbre semi-simple à gauche et à droite coïncident.

Lemme 2.2. Soit A une algèbre semi-simple. Alors, tout A-module à gauche M est semi-simple et projectif.

Preuve. Soit I une famille génératrice de M, et soit $A_I := \oplus_{i\in I}({}_gA)$ la somme directe de copies de ${}_gA$ qui est un A-module semi-simple et libre avec la base $e_i := \nu_i(1_A)$, où $\nu_i : {}_gA \to A_I$ est l'injection canonique, et on définit un morphisme surjectif de A-modules à gauche $\varphi : A_I \to M$ par $\varphi(a\cdot e_i) := a\cdot i$, $\forall i \in I$. Comme A_I est semi-simple, on a $A_I = \operatorname{Ker}\varphi \oplus P$, où P est un sous-module de A_I (il est semi-simple par la remarque précédente). Finalement, par construction, $\varphi|_P$ est un isomorphisme de A-modules P et M donc M est semi-simple et, par définition, projectif. ■

3 Structure d'une algèbre semi-simple de dimension finie.

Le but de ce cours est la preuve du théorème de Wedderburn qui dit que toute algèbre semi-simple de dimension finie est isomorphe à une somme directe d'algèbres de type $M_n(k)$.

3.1 Préparations.

Proposition 3.1. La représentation régulière à gauche λ d'une algèbre unifère A est un isomorphisme entre les algèbres A et $\mathrm{End}_A^d(A_d)$. La représentation régulière à droite ρ est un isomorphisme entre les algèbres A et $\mathrm{End}_A^g({}_gA)$.

Preuve. On vérifie directement que λ est un morphisme entre les algèbres A et $\mathrm{End}_A^d(A_d)$. $\mathrm{Ker}\,(\lambda) = \{a \in A : A\cdot a = 0\} = \{0\}$ car A est unifère. Si $\varphi \in \mathrm{End}_A^d(A_d)$, on a, pour tout $a \in A$: $\varphi(a) = \varphi(1_A\cdot a) = \varphi(1_A)\cdot a = \lambda_{\varphi(1_A)}(a)$ donc λ est un isomorphisme d'algèbres. De même pour ρ. ■

Si $\{M_1, \ldots, M_n\}$ est un ensemble fini de A-modules à droite, on note

$$[\mathrm{Hom}_A^d(M_j, M_i)] = \begin{pmatrix} \mathrm{Hom}_A^d(M_1, M_1) & \mathrm{Hom}_A^d(M_2, M_1) & \ldots & \mathrm{Hom}_A^d(M_n, M_1) \\ \mathrm{Hom}_A^d(M_1, M_2) & \mathrm{Hom}_A^d(M_2, M_2) & \ldots & \mathrm{Hom}_A^d(M_n, M_2) \\ \vdots & \vdots & \vdots & \vdots \\ \mathrm{Hom}_A^d(M_1, M_n) & \mathrm{Hom}_A^d(M_2, M_n) & \ldots & \mathrm{Hom}_A^d(M_n, M_n) \end{pmatrix}$$

l'ensemble de toutes matrices de la forme

$$\begin{pmatrix} \varphi_{11} & \varphi_{12} & \cdots & \varphi_{1n} \\ \varphi_{21} & \varphi_{22} & \cdots & \varphi_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ \varphi_{n1} & \varphi_{n2} & \cdots & \varphi_{nn} \end{pmatrix},$$

où $\varphi_{ij} \in \mathrm{Hom}_A^d(M_j, M_i)$. Cet ensemble est une algèbre unifère pour les opérations matricielles usuelles (en particulier, $[\varphi_{ij}][\psi_{jk}] = [\chi_{ik}]$, où $\chi_{ik} := \sum_j \varphi_{ij}\psi_{jk} \in \mathrm{Hom}_A^d(M_k, M_i)$).

Proposition 3.2. L'algèbre $[\mathrm{Hom}_A^d(M_j, M_i)]$ est isomorphe à $\mathrm{End}_A^d(M)$, où $M = M_1 \oplus M_2 \oplus \ldots \oplus M_n$.

Preuve. Soient $\pi_i : M \to M_i$ et $\nu_i : M_i \to M$ les morphismes canoniques de projection et d'inclusion. Alors $\sum_i(\nu_i \circ \pi_i) = id_M$ et $\pi_i \circ \nu_j = \delta_{i,j} id_{M_j}$. On définit maintenant deux applications : $\alpha : \mathrm{End}_A^d(M) \to [\mathrm{Hom}_A^d(M_j, M_i)]$ par $\alpha(\varphi) := [\pi_i \cdot \varphi \cdot \nu_j]$ et $\beta : [\mathrm{Hom}_A^d(M_j, M_i)] \to \mathrm{End}_A^d(M)$ par $\beta([\varphi_{ij}]) := \sum_{i,j=1}^n \nu_i \cdot \varphi_{ij}\pi_j$. Une vérification directe montre que α et β sont mutuellement inverses et que α est un morphisme d'algèbres. Par exemple,

$$\alpha(\varphi \cdot \psi) = \left[\pi_i \cdot \varphi \left(\sum_{j=1}^n \nu_j \cdot \pi_j\right) \psi \cdot \nu_j\right] = \left[\sum_{j=1}^n (\pi_i \cdot \varphi \cdot \nu_j) \cdot (\pi_j \cdot \psi \cdot \nu_j)\right] = \alpha(\varphi)\alpha(\psi)$$

Ainsi, α et β sont des isomorphismes d'algèbres. ■

Corollaire. -

1. Si M est un A-module à droite, alors les algèbres $\mathrm{End}_A^d(\oplus nM)$ et $M_n(\mathrm{End}_A^d(M))$ sont isomorphes.
2. Si M est un A-module à droite libre de rang n, alors les algèbres $\mathrm{End}_A^d(M)$ et $M_n(A)$ sont isomorphes.
3. Soient $M_1, M_2, \ldots, M_n$ des A-modules à droite tels que $\mathrm{Hom}_A^d(M_i, M_j) = 0$ si $i \neq j$, alors les algèbres $\mathrm{End}_A^d(M_1 \oplus M_2 \oplus \ldots \oplus M_n)$ et $\mathrm{End}_A^d(M_1) \oplus \mathrm{End}_A^d(M_2) \oplus \ldots \oplus \mathrm{End}_A^d(M_n)$ sont isomorphes.

Preuve.

2. Les A-modules à droite M et $\oplus nA_d$ étant isomorphes, le **1.** du corollaire dit que les algèbres $\mathrm{End}_A^d(M)$ et $M_n(\mathrm{End}_A^d(A_d))$ sont isomorphes. Mais la proposition 3.1 dit que les algèbres $\mathrm{End}_A^d(A_d)$ et A sont isomorphes.

3. Par la proposition 3.2, l'algèbre $\mathrm{End}_A^d(M_1 \oplus M_2 \oplus \ldots \oplus M_n)$ est isomorphe à $[\mathrm{Hom}_A^d(M_j, M_i)]$ donc à

$$\begin{pmatrix} \mathrm{End}_A^d(M_1) & 0 & \ldots & 0 \\ 0 & \mathrm{End}_A^d(M_2) & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & \mathrm{End}_A^d(M_n) \end{pmatrix},$$

donc à $\mathrm{End}_A^d(M_1) \oplus \mathrm{End}_A^d(M_2) \oplus \ldots \oplus \mathrm{End}_A^d(M_n)$.

■

Proposition 3.3. -
Soit $A = A_1 \oplus A_2$ une somme directe de sous-algèbres A_1 et A_2, et soit M un idéal à droite de A_1. Alors :

(i) M est un idéal à droite de A.

(ii) $\mathrm{End}_A^d(M) = \mathrm{End}_{A_1}^d(M)$.

(iii) $\mathrm{Hom}_A^d(M, A) = \mathrm{Hom}_A^d(M, A_1) = \mathrm{Hom}_{A_1}^d(M, A_1)$.

(iv) M est un idéal à droite minimal de A ssi il est un idéal à droite minimal de A_1.

(v) Tout idéal à droite minimal de A est ou bien un idéal à droite minimal de A_1, ou bien un idéal à droite minimal de A_2.

Preuve. Comme $M \cdot A_2 \subset A_1 \cdot A_2 = 0$, on vérifie (i) à (iv) directement.
(v) Soit M un idéal à droite minimal de A, alors on a, pour tout $i \in \{1, 2\}$: $M \cdot A_i \subset M \cap A_i \subset M$ donc ou bien $M = M \cap A_i \subset A_i$, ou bien $M \cdot A_i \subset M \cap A_i = 0$. Et le cas $M \cdot A_1 = M \cdot A_2 = 0$ est impossible parce qu'on aurait alors $M = M \cdot A_1 \oplus M \cdot A_2 = 0$. ■

Corollaire. Si les algèbres A_1 et A_2 sont semi-simples à droite, alors l'algèbre $A_1 \oplus A_2$ est aussi semi-simple à droite.

Proposition 3.4. -

(i) Soit $M = \oplus_{i \in I} N_i$ une somme directe de A-modules à droite simples, et soit $\varphi : N \to M$ un morphisme non nul d'un A-module à droite simple N vers M. Alors, il existe $j \in I$ tel que $M = \varphi(N) \oplus (\oplus_{i \neq j} N_i)$ et N est équivalent à N_j.

(ii) Soient N_i $(i \in I)$ des A-modules à droite simples tels que $\mathrm{Hom}_A^d(N_i, N_j) = 0$ si $i \neq j$, et soient $M = \oplus_{i \in I} M(i)$, $M' = \oplus_{i \in I} M'(i)$, où $M(i)$ (resp., $M'(i)$) est équivalent à une somme directe $\oplus \alpha_i N_i$ (resp., $\oplus \beta_i N_i$). Alors, les A-modules à droite M et M' sont équivalents ssi $\alpha_i = \beta_i$ pour tout i.

Preuve.

(i) Le lemme de Shur montre que $\varphi(N)$ est un sous-module simple non nul de M, et le lemme 2.1 (i) montre qu'il existe un sous-ensemble $J \subset I$ tel que $M = \varphi(N) \oplus (\oplus_{i \in J} N_i)$. Toute projection $\pi_i(\varphi(N))$ est soit 0, soit N_i (de nouveau en utilisant le lemme de Shur). Comme $\varphi(N)$ est non nul et simple, il existe exactement un seul $j \in I$ tel que N est équivalent à N_j et $M = \varphi(N) \oplus (\oplus_{i \neq j} N_i)$.

(ii) Si $\varphi : M \to M'$ est un isomorphisme, alors, pour toute copie de $N_i \subset M$, il existe, par (i), exactement une copie de N_i (nécessairement avec le même i car si $i \neq j$, N_i et N_j ne sont pas isomorphes !) tel que $M' = \varphi(N_i) \oplus \ldots$ et $\varphi(N_i)$ est équivalente à cette copie de N_i. En plus, pour deux copies différentes N_i' et N_i'' de $N_i \subset M$, on a $N_i' N_i'' = 0$ donc $\varphi(N_i')\varphi(N_i'') = 0$, alors les copies de N_i correspondantes sont différentes. Comme φ est un isomorphisme, on a $\alpha_i = \beta_i$. La réciproque est évidente.

■

3.2 Le théorème de Wedderburn.

Théorème de Wedderburn. Soit A une algèbre semi-simple (à gauche ou à droite) de dimension finie.

(i) Il existe $r, n_1, \ldots, n_r \in \mathbb{N}^*$ tels que A est isomorphe à $\oplus_{i=1}^r M_{n_i}(k)$.

(ii) Le vecteur $\overline{n} = (n_1, \ldots, n_r)$ est défini par A de manière unique à un isomorphisme près. On dit que ce vecteur est **le vecteur de dimension** de A et que A est de type $\overline{n} = (n_1, \ldots, n_r)$.

(iii) Réciproquement, pour tous $r, n_1, \ldots, n_r \in \mathbb{N}^*$, l'algèbre $A = \oplus_{i=1}^r M_{n_i}(k)$ est semi-simple (à gauche et à droite).

Preuve.

(i) Si A est semi-simple à droite, le A-module régulier à droite A_d se décompose en la somme directe d'idéaux à droite : $A_d = \oplus_i M_i$, où $M_i = n_i N_i$ est la somme directe de n_i copies d'un idéal minimal à droite avec $\mathrm{Hom}_A^d(N_i, N_j) = 0$ si $i \neq j$ d'après le corollaire 1 du lemme de Shur. On a $\mathrm{Hom}_A^d(M_i, M_j) = 0$ si $i \neq j$: en effet, si $\varphi : M_i \to M_j$ est un morphisme non nul, il existe une copie de N_i tel que $P_i := \varphi(N_i)$ est un sous-module simple de M_j isomorphe à N_i (lemme de Shur). La projection de P_i sur une des copies de N_j est un morphisme non nul de A-modules d'après la proposition 3.4 (i), et même un isomorphisme par le lemme de Shur : contradiction. Maintenant, la proposition 3.1 dit que les algèbres A et $\mathrm{End}_A^d(A_d)$ sont isomorphes, et le corollaire 3 de la proposition 3.2 dit, à son tour, que l'algèbre $\mathrm{End}_A^d(A_d)$ est isomorphe à $\mathrm{End}_A^d(M_1) \oplus \mathrm{End}_A^d(M_2) \oplus \ldots \oplus \mathrm{End}_A^d(M_n)$. Finalement, le corollaire 1 de la proposition 3.2 dit que l'algèbre $\mathrm{End}_A^d(M_i)$ est isomorphe à $M_{n_i}(\mathrm{End}_A(N_i))$, mais selon le lemme de Shur, $\mathrm{End}_A^d(N_i)$ est une k-algèbre à division de dimension finie et la proposition 1.1 implique qu'elle est isomorphe à k.

De manière analogue, on peut traiter le cas des algèbres semi-simples à gauche.

(ii) Si A est isomorphe a $\oplus_{i=1}^r A_i$, où l'algèbre A_i est isomorphe à $M_{n_i}(k)$, alors selon les propositions 2.1 (i) et 3.3, le A-module à droite A_i est isomorphe à la somme directe de n_i copies d'un idéal minimal à droite N_i de A tel que $N_i \subset A_i$. Comme $N_i N_j = \delta_{i,j} N_i$, les A-modules N_i et N_j ne sont pas isomorphes si $i \neq j$. En effet, s'il existe un isomorphisme $\varphi : N_i \to N_j$, on a : $0 = \varphi(N_i N_j) = \varphi(N_i) N_j = N_j^2 \neq 0$: contradiction. Maintenant, il ne reste qu'à appliquer la proposition 3.4.

(iii) La proposition 2.1 montre que toute algèbre $M_{n_i}(k)$ est semi-simple à gauche et à droite. Par suite, le corollaire de la proposition 3.3 montre que A l'est aussi.

∎

Corollaire. -

1. On a $A = \oplus_{i=1}^r p_i A$ (à un isomorphisme près), où $p_i \in Z(A)$ sont tels que $\sum_{i=1}^r p_i = 1_A$ et $p_i p_j = \delta_{i,j} p_i$, $\forall i, j \in \{1, \ldots, r\}$.

2. Une algèbre semi-simple est commutative ssi $n_i \equiv 1$.

3. $\dim(A) = \sum_i n_i^2$.

4. Soient G un groupe fini, kG son algèbre de groupe décomposée selon les théorèmes de Mashke et de Wedderburn. Alors G a exactement r représentations irréductibles de dimensions $n_1, \ldots, n_r$ respectivement. La décomposition de la représentation régulière à droite (ou à gauche) de G contient toute représentation irréductible avec multiplicité égale à sa dimension.

Exemple 3.1. Le groupe $G = S_3 = \{e = id, t_1 = (1,2), t_2 = (2,3), t_3 = (1,3), c = (1,2,3), c^2 = (1,3,2)\}$ a 3 représentations irréductibles : la représentation triviale, la signature et

$$\pi(e) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ \pi(c) = \begin{pmatrix} \cos\frac{2\pi}{3} & -\sin\frac{2\pi}{3} \\ \sin\frac{2\pi}{3} & \cos\frac{2\pi}{3} \end{pmatrix}, \ \pi(c^2) = \begin{pmatrix} \cos\frac{2\pi}{3} & \sin\frac{2\pi}{3} \\ -\sin\frac{2\pi}{3} & \cos\frac{2\pi}{3} \end{pmatrix},$$

$$\pi(t_1) = \begin{pmatrix} \cos\frac{2\pi}{3} & -\sin\frac{2\pi}{3} \\ -\sin\frac{2\pi}{3} & -\cos\frac{2\pi}{3} \end{pmatrix}, \ \pi(t_2) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \ \pi(t_3) = \begin{pmatrix} \cos\frac{2\pi}{3} & \sin\frac{2\pi}{3} \\ \sin\frac{2\pi}{3} & -\cos\frac{2\pi}{3} \end{pmatrix}.$$

Alors, on a $kS_3 = k \oplus k \oplus M_2(k)$.

4 Commutant et bicommutant.

Dans ce cours, nous préparons des outils pour l'étude des inclusions d'algèbres semi-simples.

4.1 Produit tensoriel de deux espaces vectoriels.

Soient V et W deux espaces vectoriels sur k. On considère l'espace vectoriel $Lin(V\times W)$ des combinaisons linéaires formelles sur k des éléments de $V\times W$ dont une base est formée des couples (v,w), $\forall v\in V$, $\forall w\in W$. Soit U le sous-espace de cet espace engendré par les éléments de la forme $(v_1+v_2,w)-(v_1,w)-(v_2,w)$, $(v,w_1+w_2)-(v,w_1)-(v,w_2)$ et $(\lambda v,w)-(v,\lambda w)$ pour tous $v,v_1,v_2\in V$, $w,w_1,w_2\in W$, et $\lambda\in k$.

Définition 4.1. On appelle **produit tensoriel** de V et W, et on note $V\otimes_k W$ (ou $V\otimes W$), l'espace vectoriel quotient $Lin(V\times W)/U$. Pour $v\in V, w\in W$, on note $v\otimes w$ l'image canonique de l'élément $(v,w)\in Lin(V\times W)$.

La propriété la plus importante du produit tensoriel est donnée par la

Proposition 4.1. -

(i) Soient V,W,X des espaces vectoriels, et soit $g:V\otimes W\to X$ une application linéaire. L'application $(v,w)\mapsto f(v,w):=g(v\otimes w)$ est une application bilinéaire de $V\times W$ dans X vérifiant la condition $f(\lambda v,w)=f(v,\lambda w)$, $\forall v\in V$, $\forall w\in W$, $\forall\lambda\in k$.

(ii) Réciproquement, soit f une application bilinéaire de $V\times W$ dans X vérifiant la dernière condition. Il existe alors une unique application linéaire $g:V\otimes W\to X$ telle que $f(v,w):=g(v\otimes w)$ pour tous $v\in V$, $w\in W$.

Preuve.

(i) Si $\varphi:V\times W\to V\otimes W$ est l'application canonique, on a $f=g\circ\varphi$.

(ii) On remarque que f se prolonge de manière unique en une application linéaire $\overline{f}:Lin(V\times W)\to X$ qui s'annule sur U. Donc, il existe une application linéaire $g:V\otimes W\to X$ telle que $\overline{f}=g\circ\pi$, où $\pi:Lin(V\times W)\to V\otimes W$ est l'application canonique. L'unicité de g est évidente car $V\otimes W$ est engendré, en tant qu'espace vectoriel, par les éléments de la forme $v\otimes w$, $\forall v\in V$, $\forall w\in W$.

■

Soient $\varphi:V\to V'$, $\psi:W\to W'$ deux applications linéaires d'espaces vectoriels. Comme l'application $(v,w)\mapsto\varphi(v)\otimes\psi(w)$ de $V\times W$ dans $V'\otimes W'$ vérifie les conditions de la proposition 4.1, il existe alors une unique application linéaire $\varphi\otimes\psi:V\otimes W\to V'\otimes W'$ telle que $(\varphi\otimes\psi)(v\otimes w)=\varphi(v)\otimes\psi(w)$ $\forall v\in V$, $\forall w\in W$: c'est par définition le **produit tensoriel** des applications linéaires φ et ψ.
Si $\dim(V)=n<\infty$, $\dim(W)=m<\infty$, et soit (a_i) (resp., (b_j)) une base de V (resp., W), il est alors possible d'identifier V (resp., W) à son espace dual. En effet, soit v (resp., w) un vecteur de V (resp., W) de coordonnées (α_i) (resp., (β_j)) dans la base précédente, alors a_i (resp., b_j) est identifié à la forme linéaire $<a_i,v>:=\alpha_i$ (resp., $<b_j,w>:=\beta_j$). Cette identification établit une application canonique $\otimes$ de $V\times W$ vers $V\otimes W$ définie par :

$$(a_i\otimes b_j)(v,w)=\alpha_i\beta_j.$$

La famille $(a_i\otimes b_j)$ est alors la base canonique de $V\otimes W$:

$$v\otimes w=\sum_{i,j}\alpha_i\beta_j(a_i\otimes b_j).$$

L'application précédente définit aussi une application de $\mathrm{End}_k(V)\times\mathrm{End}_k(W)$ dans $\mathrm{End}_k(V\otimes W)$.
Soit φ (resp., ψ) un endomorphisme de V (resp., W), alors, avec les notations précédentes, on obtient :

$$(\varphi\otimes\psi)(v\otimes w)=\varphi(v)\otimes\psi(w).$$

Si $A=(\alpha_{ik})$ (resp., $B=(\beta_{jl})$) désigne la matrice de φ (resp., ψ), alors la matrice $A\otimes B$ de $\varphi\otimes\psi$ dans la base $(a_i\otimes b_j)$ est :

$$(A\otimes B)_{ij,kl}=\alpha_{ik}\beta_{jl}.$$

Si on considère la base $(a_i\otimes b_j)$ dans l'ordre : $a_1\otimes b_1,a_2\otimes b_1,\dots,a_n\otimes b_1,\dots,a_1\otimes b_m,a_2\otimes b_m,\dots,a_n\otimes b_m$, on peut identifier la matrice $A\otimes B$ à la matrice de blocs $A\cdot B_{kl}$.

On note mV la somme directe de m copies de V, et on remarque que $\mathrm{End}_k(mV)$ est isomorphe **canoniquement** à $M_m(\mathrm{End}_k(V))$ et à $\mathrm{End}_k(V) \otimes M_m(k)$. En effet, soient $\pi_i : mV \to V$ la projection sur la i-ème composante et $\varepsilon_i : V \to mV$ l'injection telle que $\pi_i \circ \varepsilon_i = \delta_{ij}\mathrm{id}_V$, pour tout $i \in \{1, 2, \ldots, m\}$. Étant donné $x \in \mathrm{End}_k(mV)$, on définit une matrice $(x_{ij}) \in M_m(\mathrm{End}_k(V))$ par $x_{ij} := \pi_i \circ x \circ \varepsilon_j$. On peut vérifier que $x \mapsto (x_{ij})$ est un isomorphisme d'algèbres, et son inverse est $(x_{ij}) \mapsto \sum_{ij} \varepsilon_i \circ x_{ij}\pi_j \in \mathrm{End}_k(mV)$. Cela donne le premier isomorphisme.
Soit $\{e_{ij} : i, j \in \{1, \ldots, m\}\}$ le système standard des unités matricielles de $M_m(k)$. Alors, l'application $(x_{ij}) \mapsto \sum_{ij}(x_{ij} \otimes e_{ij})$ est un isomorphisme de $M_m(\mathrm{End}_k(V))$ sur $\mathrm{End}_k(V) \otimes M_m(k)$.
Nous allons identifier ces trois algèbres par ces isomorphismes. Donc, pour toute sous-algèbre A de $M_n(k)$, on peut identifier $A \otimes M_m(k)$ à l'algèbre $M_m(A)$ et $A \otimes I_m$ à $\mathrm{Diag}_m(A)$.

4.2 Commutant et bicommutant.

Définition 4.2. Soit F une k-algèbre. Le **commutant** $C_F(S)$ d'un sous-ensemble S de F est l'**algèbre** des éléments de F qui commutent à tous les éléments de S.

Évidemment, $S \subset C_F(C_F(S))$, d'où $C_F[C_F(C_F(S))] \subset C_F(S)$. Mais aussi $C_F(S) \subset C_F(C_F[C_F(S)]) = C_F[C_F(C_F(S))]$, d'où $C_F(C_F(C_F(S))) = C_F(S)$.

Lemme 4.1. Soient V un espace vectoriel et A une sous-algèbre unifère de $\mathrm{End}_k(V)$. On note $A' := C_{\mathrm{End}_k(V)}A$.

(i) Le commutant de $A \otimes I_m$ dans $\mathrm{End}_k(V) \otimes M_m(k)$ est $A' \otimes M_m(k)$.

(ii) Le commutant de $A \otimes M_m(k)$ dans $\mathrm{End}_k(V) \otimes M_m(k)$ est $A' \otimes I_m$.

Preuve.

(i) Comme $(a \otimes I_m)\sum_{ij}(x_{ij} \otimes e_{ij}) = \sum_{ij}(ax_{ij} \otimes e_{ij})$ et $\sum_{ij}(x_{ij} \otimes e_{ij})(a \otimes I_m) = \sum_{ij}(x_{ij}a \otimes e_{ij})$, pour tout coefficient matriciel x_{ij} de $\mathrm{End}_k(V)$ et toute unité matricielle e_{ij} de $M_m(k)$, on a que $\sum_{ij}(x_{ij} \otimes e_{ij})$ est dans le commutant de $A \otimes I_m$ ssi $x_{ij} \in A'$ pour tous i et j.

(ii) Si $x = \sum_{ij}(x_{ij} \otimes e_{ij})$ commute à $A \otimes M_m(k)$, il commute, en particulier, à $1_A \otimes e_{kl}$, pour tous k et l. On en déduit que $x_{lj} = 0$ si $l \neq j$ et $x_{ik} = 0$ si $i \neq k$, et que $x_{kk} = x_{ll}$. Donc, $x = \sum_i(y \otimes e_{ii}) = y \otimes I_m$, où $y \in \mathrm{End}_k(V)$. Comme x commute à $A \otimes I_m$, on a $x \in A'$. L'affirmation réciproque est évidente.

■

Lemme 4.2. Soient F un facteur isomorphe à $\mathrm{End}_k(V)$ et A un sous-facteur de F isomorphe à $\mathrm{End}_k(W)$ (ici V et W sont deux espaces vectoriels de dimension finie). Alors :

(i) $C_F(A)$ est un facteur.

(ii) $C_F(C_F(A)) = A$.

(iii) $A \otimes C_F(A)$ est isomorphe à F.

Preuve. On peut remplacer les isomorphismes ci-dessus par des égalités. L'inclusion $A = \mathrm{End}_k(W) \subset F = \mathrm{End}_k(V)$ est une représentation de A sur V. Mais comme A est **simple**, cette représentation est équivalente à la somme directe de, disons, $m \in \mathbb{N}$ copies de la représentation unique de A. Autrement dit, on peut identifier V à la somme directe de m copies de W, et l'image de A dans $F = \mathrm{End}_k(W) \otimes M_m(k)$ à $A \otimes I_m$. Le lemme 4.1 (i) dit que $C_F(A) = 1_A \otimes M_m(k)$ qui est un facteur. De plus, $C_F(C_F(A)) = \mathrm{End}_k(W) \otimes I_m = A$. Finalement, $A \otimes C_F(A)$ est isomorphe à $\mathrm{End}_k(W) \otimes M_m(k) = F$. ■

Lemme 4.3. Soit A une sous-algèbre semi-simple unifère d'un facteur F de dimension finie. Alors :

(i) $C_F(A)$ est semi-simple avec les mêmes idempotents minimaux centraux $p_1, \ldots, p_m$ que A.

(ii) $C_F(C_F(A)) = A$.

Preuve.

(i) $A = \oplus_i p_i A$, où chaque $p_i A$ est un facteur. Le centre $A \cap C_F(A)$ de A appartient au centre $C_F(A) \cap C_F(C_F(A))$ de $C_F(A)$, et comme $\sum_i p_i = 1$, on a $C_F(A) = \sum_i p_i C_F(A) p_i$. En utilisant le fait que $p_i \in A \cap C_F(A)$, on vérifie que $p_i C_F(A) p_i = C_{p_i F p_i}(p_i A)$. En effet, $C_{p_i F p_i}(p_i A) := \{p_i x p_i : x \in F, p_i x p_i a = p_i a p_i x p_i,\ \forall a \in A\} \subset p_i C_F(A) p_i$ et $p_i C_F(A) p_i := \{p_i x p_i : x \in F, xa = ax, \forall a \in A\} \subset C_{p_i F p_i}(p_i A)$. En plus, c'est un facteur selon le lemme 4.2 (i) car si F est isomorphe à $\mathrm{End}_k(V)$, alors $p_i F p_i$ est isomorphe à $\mathrm{End}_k(p_i V)$ et donc est un facteur. D'où (i).

(ii) De manière similaire, on a $p_iC_F(C_F(A))p_i = C_{p_iFp_i}(C_{p_iFp_i}(p_iA))$, et le lemme 4.2 (ii) implique :

$$C_F(C_F(A)) = \oplus_i p_iC_F(C_F(A))p_i = \oplus_i p_iA = A.$$

D'où (ii).

■

Lemme 4.4. Soit A un sous-facteur d'un facteur F de dimension finie et $q \in A \cup C_F(A)$ un idempotent non nul. Alors :

(i) qAq est un facteur.

(ii) $C_{qFq}(qAq) = qC_F(A)q$.

Preuve. Soit d'abord $q \in A$.

(i) Si on identifie A à $\mathrm{End}_k(V)$, alors qAq est isomorphe à $\mathrm{End}_k(qV)$.

(ii) D'une part, $qC_F(A)q \subset C_{qFq}(qAq)$, car pour $x \in qAq$ et $y \in qC_F(A)q$, on peut choisir $z \in C_F(A)$ tel que $y = qzq$, et calculer $xy = q(qxq)zq = qzqxq = yx$. D'autre part, si $s = qsq \in C_{qFq}(qC_F(A)q)$ et $t \in C_F(A)$ alors $tq = qt$, et on a : $st = sqqt = sqtq = qtqs = tqqs = ts$. Par suite, $C_{qFq}(qC_F(A)q) \subset qC_F(C_F(A))q = qAq$ en utilisant le lemme 4.2. On passe aux commutants et on applique le lemme 4.2 à qFq :

$$C_{qFq}(qAq) \subset C_{qFq}(C_{qFq}(qC_F(A)q)) = qC_F(A)q.$$

Soit maintenant $q \in C_F(A)$.

(i) L'application linéaire $\varphi : A \to qAq$ telle que $\varphi(x) = qxq$, pour tout $x \in A$, est un morphisme surjectif d'algèbres unitaires (car $q = q1_Aq$). Comme A est simple, c'est un isomorphisme.

(ii) Par la première partie de la preuve et en utilisant le fait que $C_F(C_F(A)) = A$, on a : $C_{qFq}(qC_F(A)q) = qC_F(C_F(A))q = qAq$. On passe aux commutants et on applique le lemme 4.2 à qFq pour conclure.

■

Lemme 4.5. Soient A une sous-algèbre semi-simple unifère d'un facteur F et $q \in A \cup C_F(A)$ un idempotent non nul. Alors :

(i) qAq est une algèbre semi-simple unifère.

(ii) $C_{qFq}(qAq) = qC_F(A)q$.

Preuve. Avec les notations du lemme 4.3, on pose $q_i = p_iq$, et on remarque que $q = \sum_i q_i$.

(i) On a $qAq = \sum_i q_iA_iq_i$, et chaque $q_iA_iq_i$ est un facteur par le lemme 4.4 (i).

(ii) On calcule

$$C_{qFq}(qAq) = \oplus_i q_iC_{qFq}(qAq)q_i = \oplus_i C_{q_iFq_i}(q_iAq_i),$$

et

$$qC_F(A)q = \oplus_i q_iC_F(A)q_i = \oplus_i q_iC_{p_iFp_i}(p_iAp_i)q_i.$$

Comme $C_{q_iFq_i}(q_iAq_i) = q_iC_{p_iFp_i}(p_iAp_i)q_i$ par le lemme 4.4 (ii), on a le résultat.

■

5 Inclusions d'algèbres semi-simples.

On considère une inclusion $A = \oplus_{j=1}^{r} q_j A \subset B \oplus_{i=1}^{l} p_i B$ d'algèbres semi-simples respectivement de type $\overline{n} = (n_1, \ldots, n_r)$ et $\overline{m} = (m_1, \ldots, m_l)$. Ici $p_i \in Z(B)$, $q_j \in Z(A)$ sont des idempotents minimaux. On dit que deux inclusions $A_1 \subset B_1$ et $A_2 \subset B_2$ de ce type sont **isomorphes** s'il existe un isomorphisme d'algèbres $\phi : B_1 \to B_2$ tel que $\phi(A_1) = A_2$.
Les vecteurs $\overline{n}$ et $\overline{m}$ ne donnent pas une description complète de l'inclusion $A \subset B$, il faut aussi rajouter **la matrice d'inclusion** de format $r \times l$: $\Lambda = \Lambda_A^B$. Pour définir cette matrice, on pose $B_{i,j} = p_i q_j B p_i q_j$, $A_{i,j} = p_i q_j A p_i q_j$ pour $i \in \{1, 2, \ldots, m\}$ et $j \in \{1, 2, \ldots, n\}$. Comme $p_i \in Z(B)$, le produit $p_i q_j$ est un idempotent dans $p_i B$. Le lemme 4.4 montre alors que $B_{i,j}$ est 0 si $p_i q_j = 0$ ou un facteur sinon. Dans le dernier cas, l'application $x \mapsto p_i x p_i$ de Aq_j dans $A_{i,j}$ est un morphisme d'algèbres dont l'image contient $p_i q_j$; comme $q_j A$ est simple, cette application est un isomorphisme. Maintenant, on définit les coefficients $\lambda_{i,j}$ de Λ_A^B : $\lambda_{i,j} = 0$ si $p_i q_j = 0$, et $\lambda_{i,j} = \frac{\dim(B_{i,j})}{\dim(A_{i,j})}$ sinon. Autrement dit, Λ_{ij} est la multiplicité de la j-ème représentation de A comme sous-représentation de la restriction sur A de la i-ème représentation de B. Pour l'inclusion composée $A \subset B \subset C$, on a évidemment $\Lambda_A^C = \Lambda_A^B \Lambda_B^C$.
Pour décrire quelques propriétés de cette matrice, on donne d'abord quelques

Définitions 5.1. -
- On dit qu'une matrice $X \in M_{m,n}(\mathbb{R})$ $m, n \geqslant 1$ est **irredondante** si elle n'a pas de lignes ou de colonnes nulles.
- Deux matrices $X_1, X_2 \in M_{m,n}(\mathbb{R})$ sont **pseudo-équivalentes** s'il existe des permutations $\alpha \in S_m$ de lignes et $\beta \in S_n$ de colonnes telles que $X_2 = \alpha X_1 \beta$. (on identifie ici une permutation α, à une matrice à coefficients 0 ou 1 de l'automorphisme de $\mathbb{R}^n$ qui envoie le vecteur e_i de la base canonique sur $e_{\alpha(i)}$ donc $\alpha^t = \alpha^{-1}$)
- Une matrice X irredondante est **décomposable** s'il existe des naturels non nuls m', m'', n', n'' tels que $m = m' + m'', n = n' + n''$ et deux matrices $X' \in M_{m',n'}(\mathbb{R}), X'' \in M_{m'',n''}(\mathbb{R})$ telles que X est pseudo-équivalente à $\begin{pmatrix} X' & 0 \\ 0 & X'' \end{pmatrix}$. Une matrice est **indécomposable** si elle est irredondante et non décomposable.
- Une matrice carrée $Z \in M_m(\mathbb{R})$ est **réductible** s'il existe deux naturels non nuls m', m'' tels que $m = m' + m''$ des matrices $Z' \in M_{m',m'}(\mathbb{R}), Z'' \in M_{m'',m''}(\mathbb{R}), Z''' \in M_{m',m''}(\mathbb{R})$ et une permutation $\gamma \in S_m$ telles que $\gamma Z \gamma^{-1}$ est de la forme à $\begin{pmatrix} Z' & Z''' \\ 0 & Z'' \end{pmatrix}$. Une matrice est **irréductible** si elle n'est pas réductible.
- Une matrice carrée $Z \in M_m(\mathbb{R})$ est **apériodique** s'il existe un naturel p tel que tous les coefficients de Z^p sont strictement positifs.

Par exemple, les matrices $\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$ et $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$ sont indécomposables, mais la matrice $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$ est décomposable et pseudo-équivalente à $\begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$. La matrice $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$ est irréductible.

Lemme 5.1. -

a) Pour $X \in M_{m,n}(\mathbb{R})$ les affirmations suivantes sont équivalentes :
   (i) X est irredondante ;
   (ii) $X^t X$ et $X X^t$ sont irredondantes.

b) Pour $X \in M_{m,n}(\mathbb{R}_+)$ les affirmations suivantes sont équivalentes :
   (i) X est indécomposable ;
   (ii) $X X^t$ est irréductible ;
   (iii) $X^t X$ est irréductible ;
   (iv) $X X^t$ est apériodique ;
   (v) $X^t X$ est apériodique.

Preuve. a) Si X a une ligne (resp., une colonne) nulle, alors XX^t a une ligne (resp., $X^t X$ a une colonne) nulle. Si, au contraire, toutes les lignes (resp., colonnes) de X son non nulles, alors tous les coefficients diagonaux de XX^t (resp., $X^t X$) sont non nuls donc cette matrice est irredondante.

b) On a $(XX^t)_{ik} = \sum_{j=1}^n X_{ij}X_{kj} > 0$ ssi il existe $j \in \{1, 2, \ldots, n\}$ tel que $X_{ij} > 0$ et $X_{kj} > 0$. Alors, XX^t est réductible ssi (après une permutation) $(XX^t)_{ik} = 0$ pour tous $i \in \{m'+1, m'+2, \ldots, m\}$ et $k \in \{1, 2, \ldots, m'\}$ donc ssi, pour tout $j \in \{1, 2, \ldots, n\}$, soit $X_{ij} = 0, \ \forall i \in \{m'+1, m'+2, \ldots, m\}$, soit $X_{kj} = 0, \ \forall k \in \{1, 2, \ldots, m'\}$. Donc, (i) et (ii) sont équivalents. De même pour (i) et (iii).
Pour l'équivalence de (i), (iv) et (v) voir [3], §XIII.5, Théorème 8. ■

Remarque. Concernant le lemme 5.1 a) : la matrice

$$X = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$$

est redondante ainsi que X^tX, mais XX^t n'est pas redondante.

Lemme 5.2. Soit $A = \oplus_{j=1}^r q_j A \subset B = \oplus_{i=1}^l p_i B$ une inclusion d'algèbres semi-simples respectivement de type $\overline{n} = (n_1, \ldots, n_r)$ et $\overline{m} = (m_1, \ldots, m_l)$ et soit Λ_A^B la matrice d'inclusion correspondante. Alors :

(i) $\Lambda_A^B \overline{n} = \overline{m}$.

(ii) Λ_A^B est irredondante.

(iii) Λ_A^B est indécomposable ssi $Z(A) \cap Z(B) = k1_B$.

Preuve.

(i) découle des définitions de $\overline{m}, \overline{n}$ et Λ_A^B.

(ii) Pour tout i fixé, il existe un j tel que $p_i q_j \neq 0$ puisque $\sum_{j=1}^r q_j = 1_A$ donc la i-ème ligne de Λ_A^B est non nulle. De même pour les colonnes de Λ_A^B car $\sum_{i=1}^l p_i = 1_B$.

(iii) Si $\dim(Z(A) \cap Z(B)) > 1$, il existe des idempotents non nuls s et $1-s$ dans $Z(A) \cap Z(B)$. Quitte à réordonner les p_i et les q_j, on a :

$$p_1, \ldots, p_{m'} \ , \ q_1, \ldots, q_{n'} \in sB \quad \text{ et } \quad p_{m'+1}, \ldots, p_l \ , \ q_{n'+1}, \ldots, q_r \in (1-s)B$$

pour certains $0 < m' < l, \ 0 < n' < r$ donc $A_{i,j} = 0$ et $\lambda_{i,j} = 0$, si $1 \leqslant i \leqslant m'$ et $n'+1 \leqslant j \leqslant r$, ou si $m'+1 \leqslant i \leqslant l$ et $1 \leqslant j \leqslant n'$ donc Λ_A^B est décomposable. Réciproquement, si Λ_A^B est décomposable, on peut vérifier que $Z(A) \cap Z(B)$ contient un idempotent non trivial qui est une somme de certains p_i ainsi qu'une somme de certains q_j.

■

Théorème de Skolem-Noether. Soient M un facteur, P et Q deux sous-facteurs de M, et $\varphi : P \to Q$ un isomorphisme. Alors, il existe un automorphisme intérieur θ de M tel que $\theta|_P = \varphi$.

Preuve. On considère M comme $\mathrm{End}_k(V)$, où V est un espace vectoriel sur k de dimension finie. Soit W un P-module simple, alors tout P-module X est équivalent à la somme directe de $d = \frac{\dim(X)}{\dim(W)}$ copies de W. En particulier, les deux structures de P-module sur V définies par les actions $(p, v) \mapsto p \cdot v$ et $(p, v) \mapsto \varphi(p) \cdot v$ sont équivalentes. Alors, il existe un inversible $u \in \mathrm{End}_k(V) = M$ tel que $u(p \cdot v) = \varphi(p) \cdot u(v), \ \forall p \in P, \ \forall v \in V$ donc $\varphi(p) = upu^{-1}$. ■

Proposition 5.1. Soient P et Q deux sous-algèbres semi-simples d'une algèbre semi-simple M, et $\varphi : P \to Q$ un isomorphisme. Si $\Lambda_P^M = \Lambda_Q^M$, il existe un automorphisme intérieur θ de M tel que $\theta|_P = \varphi$.

Preuve. Il suffit d'analyser le cas où $M = \mathrm{End}_k(V)$ et V est un espace vectoriel sur k de dimension finie. Dans ce cas,

$$\Lambda_P^M = \Lambda_Q^M = (\lambda_1, \ldots, \lambda_r) \in M_{r,1}(\mathbb{N}).$$

Soient

$$P = \oplus_{j=1}^r p_j P \quad \text{ et } \quad Q = \oplus_{j=1}^r q_j Q,$$

où $p_j P$ et $q_j Q$ sont des facteurs et p_j, q_j sont des idempotents minimaux centraux tels que $\varphi(p_j) = q_j$. Tout idempotent p_j est une somme de, disons, ν_j idempotents minimaux de $p_j P$ et donc de $\lambda_j \nu_j$ idempotents minimaux de $p_j M$ qui sont aussi minimaux dans M. De même pour q_j. Donc, il existe un automorphisme intérieur α de M tel que $\alpha(p_j) = q_j$. Alors, on peut supposer dès le début que $p_j = q_j, \ \forall j \in \{1, \ldots, r\}$.

Pour tout $j \in \{1, \ldots, r\}$, on pose $V_j = p_j V$. Le théorème de Skolem-Noether dit qu'il existe $u_j \in GL(V_j)$ tel que $\varphi(y) = u_j y u_j^{-1}$, $\forall y \in p_j P$. Comme $\sum_{j=1}^{r} p_j = 1$, on a $V = \oplus_{j=1}^{r} V_j$, et on peut définir $u = \oplus_{j=1}^{r} u_j \in GL(V)$ tel que la restriction de $\theta := Ad(u)$ sur P soit égal à φ. ■

PROPOSITION 5.2. Les inclusions $P \subset Q$ et $P^{op} \subset Q^{op}$ sont isomorphes.

Preuve. En effet, l'application $\alpha : Q \to Q^{op}$, définie comme la transposition sur tout bloc matriciel, est un isomorphisme d'algèbres qui envoie P sur P^{op}. ■

On peut également décrire l'inclusion $A \subset B$ par un **multigraphe bipartite pondéré** avec r sommets pairs et l sommets impairs munis de **poids** naturels n_j (resp., m_i), où le j-ème sommet pair est connecté au i-ème sommet impair par Λ_{ij} arêtes. On appelle ce multigraphe **le diagramme de Bratteli** $Br(A \subset B)$ de l'inclusion $A \subset B$. Alors, d'après la proposition 5.1, deux inclusions ayant le même diagramme de Bratteli sont isomorphes. De plus, un multigraphe bipartite pondéré dont les sommets sont munis de poids naturels n_j (resp., m_i), est le diagramme de Bratteli d'une inclusion ssi $\overline{m} = \Lambda \overline{n}$. En effet, $Br(A \subset B)$ vérifie évidemment cette équation. Réciproquement, si cette équation est vraie, on pose

$$A = \oplus_{j=1}^{r} M_{n_j}(k) \quad \text{et} \quad B = \oplus_{i=1}^{l} M_{m_i}(k),$$

et on définit l'inclusion $A \to B$ de la manière suivante : on associe à tout $(x_1, \ldots, x_r) \in A$ l'élément $(y_1, \ldots, y_l) \in B$, où tout y_i est une matrice diagonale par bloc de la forme $y_i = diag(x_1, \ldots, x_1; \ldots; x_r, \ldots, x_r)$, où on répète λ_{ij} fois chaque x_j.
On dit que $Br(A \subset B)$ est **non connexe** si on peut décomposer les ensembles de sommets pairs et impairs en deux groupes de telle manière que les sommets pairs du 1er (resp., 2-ème) groupe sont connectés uniquement aux sommets impairs du 1er (resp., 2-ème) groupe. Sinon on dit que $Br(A \subset B)$ est **connexe**. Cette définition et la construction du diagramme de Bratteli impliquent que $Br(A \subset B)$ est non connexe ssi la matrice Λ_A^B est décomposable. En particulier, le lemme 4.2 (iii) dit que $Br(A \subset B)$ est connexe ssi $Z(A) \cap Z(B) = k1_B$.

EXEMPLES 5.1. -

a) Soient $A = M_2(k) \oplus k \subset B = M_3(k) \oplus M_2(k) \oplus k$, où, pour tous $X \in M_2(k)$ et $x \in k$, les composantes de l'image sont : $X \oplus x$, $x \oplus x$, x. Dans ce cas, $\overline{n} = (2, 1)$, $\overline{m} = (3, 2, 1)$,

$$\Lambda_A^B = \begin{pmatrix} 1 & 1 \\ 0 & 2 \\ 0 & 1 \end{pmatrix}.$$

On peut dessiner le diagramme de Bratteli correspondant (il y a évidemment 2 sommets pairs et 3 impairs).

b) Soient G un groupe fini et H un sous-groupe de G. On considère l'inclusion $A = kH \subset B = kG$ d'algèbres de groupes. A et B sont semi-simples (théorème de Mashke) respectivement de type $\overline{n} = (n_1, \ldots, n_r)$ et $\overline{m} = (m_1, \ldots, n_l)$, où r et l sont respectivement le nombre de représentations irréductibles de H et de G. En particulier, soient $G = S_3 = \{e = id, t_1 = (1,2), t_2 = (2,3), t_3 = (1,3), c = (1,2,3), c^2 = (1,3,2)\}$ et $H = \mathbb{Z}_3 = \{e = id, c = (1,2,3), c^2 = (1,3,2)\}$, sous-groupe distingué de G d'indice 2. On a $r = l = 3$ car G a 3 représentations irréductibles (voir exemple 3.1) ainsi que $\mathbb{Z}_3$: triviale, $\rho_1(c) = \exp\left(\frac{2i\pi}{3}\right)$ et $\rho_2(c) = \exp\left(\frac{4i\pi}{3}\right)$. On constate que les restrictions sur H de la représentation triviale de G et de la signature sont triviales, et que la restriction sur H de π est équivalente à la somme directe de ρ_1 et ρ_2 (car $\pi(c)$ et $\pi(c^2)$ ont les mêmes sous-espaces propres engendrés respectivement par les vecteurs $(1, i)$ et $(1, -i)$). Alors, on a

$$\Lambda_A^B = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

On peut dessiner le diagramme de Bratteli correspondant (il y a évidemment 3 sommets pairs et 3 impairs).

6 Indice.

Définition 6.1. Soient $A \subset B$ une inclusion d'algèbres semi-simples et $\Lambda_A^B = (\lambda_{ij})_{i=1,\dots,l}^{j=1,\dots,r}$ sa matrice d'inclusion. On considère $\Lambda_A^B \in M_{l,r}(\mathbb{N})$ comme une application linéaire continue $\Lambda_A^B : \mathbb{R}^r \to \mathbb{R}^l$ entre deux espaces euclidiens. On définit **l'indice** $[B : A]$ de l'inclusion $A \subset B$ comme $\|\Lambda_A^B\|^2$: le carré de la norme de cette application.

Proposition 6.1. Soient $\Lambda \in M_{r,l}(\mathbb{R})$ et

$$\Sigma = \begin{pmatrix} 0 & \Lambda \\ \Lambda^t & 0 \end{pmatrix} \in M_{r+l}(\mathbb{R}),$$

où Λ^t est la matrice transposée de Λ vue comme une application linéaire continue de $\mathbb{R}^r \to \mathbb{R}^l$. Alors :

$$\|\Lambda\| = \|\Lambda^t\| = \|\Sigma\| = \|\Lambda^t\Lambda\|^{\frac{1}{2}} = \|\Lambda\Lambda^t\|^{\frac{1}{2}}, \quad \text{où} \quad \|\Lambda\| = \max_{\{f\in\mathbb{R}^r : \|f\|\leqslant 1\}} \|\Lambda f\| = \max_{\{f\in\mathbb{R}^r : \|f\|=1\}} \|\Lambda f\|$$

Preuve. Pour tout $f \in \mathbb{R}^r$ on a :

$$\|\Lambda f\|^2 = < \Lambda f, \Lambda f > = < \Lambda^t\Lambda f, f > \leqslant \|\Lambda^t\Lambda\|.\|f\|^2 \leqslant \|\Lambda^t\|.\|\Lambda\|.\|f\|^2,$$

d'où $\|\Lambda\| \leqslant \|\Lambda^t\|$. En échangeant Λ et Λ^t, on obtient l'égalité des normes, d'où $\|\Lambda\|^2 = \|\Lambda^t\|^2 = \|\Lambda^t\Lambda\| = \|\Lambda\Lambda^t\|$. Finalement,

$$\|\Sigma\|^2 = \|\Sigma^t\Sigma\| = \left\| \begin{pmatrix} \Lambda\Lambda^t & 0 \\ 0 & \Lambda^t\Lambda \end{pmatrix} \right\|$$

d'où $\|\Sigma\| = \|\Lambda\|$. ∎

On peut considérer, comme dans [3], Λ comme une application linéaire $\mathbb{C}^r \to \mathbb{C}^l$. On écrit tout vecteur $f \in \mathbb{C}^r$ sous la forme $f = f' + \mathrm{i}f''$, où $f', f'' \in \mathbb{R}^r$ donc $\|f\|^2 = \|f'\|^2 + \|f''\|^2$, et on pose $\Lambda(f' + \mathrm{i}f'') := \Lambda(f') + \mathrm{i}\Lambda(f'')$. On peut vérifier que les deux normes de Λ ainsi définies coïncident, et il est plus facile de traiter d'applications linéaires d'espaces vectoriels complexes. Comme $\Lambda^t\Lambda \in M_l(\mathbb{N})$ est une matrice positive, $\|\Lambda^t\Lambda\|$ est la valeur propre maximale de cette matrice. Alors, d'après la définition, $[B : A]$ est un entier algébrique positif.

Exemples 6.1. -

a) (i) Si B est un facteur, $[B : A] \in \mathbb{N}^*$.

(ii) si $A \subset B$ sont deux sous-facteurs d'un facteur F, on a $[B : A] = [C_F(A) : C_F(B)] \in (\mathbb{N}^*)^2$ (on utilise le lemme 4.2 (iii)).

b) Pour l'inclusion d'algèbres de groupe $k\mathbb{Z}_3 \subset kS_3$, on a calculé la matrice d'inclusion Λ (voir exemple 3.1 et exemple 5.1). On a donc

$$\Lambda\Lambda^t = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix},$$

Par suite, les valeurs propres sont 2 (double) et 0, et on obtient $[kS_3 : k\mathbb{Z}_3] = 2$.

Lemme 6.1. On considère l'inclusion $A \subset B \subset F$ de sous-algèbres semi-simples d'un facteur F. Alors, la matrice $\Lambda_{C_F(B)}^{C_F(A)}$ est la transposée de la matrice Λ_A^B.

Preuve. Si A et $B = F$ sont des facteurs, l'affirmation découle du lemme 4.2 (iii) et de la définition de matrice d'inclusion. En général, on a $B = \oplus_i p_i B$, $A = \oplus_j q_j A$ et $\Lambda_A^B = (\lambda_{ij})$, et on va noter μ_{ji} les coefficients de la matrice de l'inclusion.

$$C_F(B) = \oplus_i p_i C_F(B) \subset C_F(A) = \oplus_j q_j C_F(A).$$

On a, par définition :

$$\mu_{ji} = [q_j p_i C_F(A) q_j p_i : q_j p_i C_F(B) q_j p_i]^{\frac{1}{2}},$$

et par le lemme 4.5 (ii) :

$$\mu_{ji} = [C_{q_j p_i F q_j p_i}(A_{i,j}) : C_{q_j p_i F q_j p_i}(B_{i,j})]^{\frac{1}{2}},$$

où $A_{i,j} := q_j p_i A q_j p_i$ et $B_{i,j} := q_j p_i B q_j p_i$ sont des sous-facteurs de $q_j p_i F q_j p_i$. Donc, $\mu_{ji} = [B_{ij} : A_{ij})]^{\frac{1}{2}}$ par le lemme 4.2 (iii). ∎

Théorème de Kronecker. -

(i) Si $\Lambda \in M_{r,l}(\mathbb{Z})$ $(r, l \in \mathbb{N}^*)$, $\Lambda \neq 0$, alors ou bien $\|\Lambda\| = 2\cos\frac{\pi}{q}$, où $q \geqslant 3$ est un entier naturel, ou bien $\|\Lambda\| \geqslant 2$.

(ii) Si $q \geqslant 3$, il existe $\Lambda \in M_l(\{0,1\})$ avec $\|\Lambda\| = 2\cos\frac{\pi}{q}$, où l est le plus grand entier naturel tel que $l \leqslant \frac{q}{2}$.

Pour prouver ce théorème, on va procéder en plusieurs étapes.

Proposition 6.2. Si toutes les racines ν_i $(i \in \{1, \ldots, l\})$ d'un polynôme normalisé $P_l(X) \in \mathbb{Z}[X]$ sont dans $\{z \in \mathbb{C} : |z| \leqslant 1\}$, alors toute racine $\lambda \neq 0$ est une racine de l'unité.

Preuve. Remarquons tout d'abord qu'il n'y a qu'un nombre fini de tels polynômes. En effet, on a

$$P_l(X) = X^l - a_1X^{l-1} + \ldots + (-1)^l a_l = \prod_{i=1}^{l}(X - \nu_i),$$

d'où

$$|a_1| = |\nu_1 + \ldots + \nu_l| \leqslant l = \binom{1}{l},$$

$$|a_2| = \left|\sum_{1\leqslant i,j\leqslant l} \nu_i\nu_j\right| \leqslant \binom{2}{l},$$

$$\ldots$$

$$|a_l| = |\nu_1\nu_2\ldots\nu_l| \leqslant 1 = \binom{l}{l},$$

et comme tous les a_i sont entiers, l'affirmation est claire.
Pour $k \in \{1, 2, \ldots\}$, on définit maintenant la suite de polynômes

$$P_{l,k}(X) = \prod_{i=1}^{l}(X - \nu_i^k) = X^l + \sum_{n=1}^{l}(-1)^n s_n(\nu_1^k, \ldots, \nu_l^k)X^{l-n}, \quad \text{où} \quad s_n(\nu_1^k, \ldots, \nu_l^k) := \sum_{1\leqslant i_1<i_2<\ldots<i_n\leqslant l} \nu_{i_1}^k \ldots \nu_{i_n}^k$$

En particulier, on a $P_{l,1}(X) = P_l(X)$ et $s_n(\nu_1, \ldots, \nu_l) = a_n$, $\forall n \in \{1, 2, \ldots, l\}$. On va montrer que tous les $s_n(\nu_1^k, \ldots, \nu_l^k)$ sont entiers. Pour cela, on remarque que ce sont des **polynômes symétriques** en les $\nu_1, \ldots, \nu_l$. Plus précisément, tout $s_n(\nu_1^k, \ldots, \nu_l^k)$ est la somme de monômes **distincts** dans la famille des $l!$ monômes de la forme $\sigma(M)$ (où $\sigma \in S_l$ et M est un monôme fixé). On peut appliquer la proposition 3 de [1], Appendice I qui dit qu'on peut exprimer tout $s_n(\nu_1^k, \ldots, \nu_l^k)$ comme polynôme à coefficients entiers en $s_1(\nu_1, \ldots, \nu_l) = a_1, \ldots, s_l(\nu_1, \ldots, \nu_l) = a_l$. Ainsi, ils sont tous entiers donc $P_{l,k}(X) \in \mathbb{Z}[X]$, et la remarque précédente montre qu'il existe $1 \leqslant j < k$ tels que $P_{l,j}(X) = P_{l,k}(X)$. Donc, il existe une permutation σ de $\{1, 2, \ldots, l\}$ telle que $\nu_1^j = \nu_{\sigma(1)}^k, \ldots, \nu_l^j = \nu_{\sigma(l)}^k$. Il est clair qu'il existe $m \in \{1, 2, \ldots, l\}$ tel que $\sigma^m(1) = 1$, et si on choisit $\nu_1 = \lambda$, alors

$$\lambda^{j^m} = \lambda^{jj^{m-1}} = \nu_{\sigma(1)}^{kj^{m-1}} = \nu_{\sigma(\sigma(1))}^{k^2j^{m-2}} = \ldots = \lambda^{k^m}.$$

Cela prouve que λ est une racine de l'unité. ■

Proposition 6.3. Si toutes les racines ν_i $(i \in \{1, \ldots, l\})$ d'un polynôme normalisé $P_l(X) \in \mathbb{Z}[X]$ sont dans $[-2, 2]$, alors toute racine $\lambda \neq 0$ est de la forme $2\cos(2\pi\tau)$, où $\tau \in \mathbb{Q}$.

Preuve. On pose

$$Q(X) := X^l P_l\left(X + \frac{1}{X}\right) \in \mathbb{Z}[X],$$

et soient $\lambda = 2\cos(\theta_1), \ldots, 2\cos(\theta_l)$ les racines de $P_l(X)$. Alors

$$P_l(X) = \prod_{j=1}^{l}(X - 2\cos(\theta_j)) \quad \text{et} \quad Q(X) = \prod_{j=1}^{l}(X^2 - 2X\cos(\theta_j) + 1) = \prod_{j=1}^{l}(X - e^{\mathrm{i}\theta_j})(X - e^{-\mathrm{i}\theta_j})$$

La proposition 6.2 dit que $\lambda = e^{\mathrm{i}\theta_j}$ est une racine de l'unité donc $\frac{\theta_j}{2\pi}$ est rationnel. ■

Corollaire. Si toutes les racines ν_j $(j \in \{1, \dots, l\})$ d'un polynôme normalisé $P_l(X) \in \mathbb{Z}[X]$ sont dans $]-2, 2[$ et si $P_l(X) \neq X^l$, alors
$$\max\{|\nu_j| : 1 \leqslant j \leqslant l\} = 2\cos\frac{\pi}{q}, \quad \text{où} \quad q \in \mathbb{N},\ q \geqslant 3$$

Preuve. La proposition 6.3 dit qu'il existe $p_1, \dots, p_l, q_1, \dots, q_l \in \mathbb{Z}$ avec p_j et q_j premiers entre eux pour tout $j \in \{1, \dots, l\}$, tels que $\nu_j = 2\cos(2\pi\frac{p_j}{q_j})$ (on peut se limiter au cas où $p_j \in \{1, \dots, q_j - 1\}$ car cos est 2π-périodique et si $p_j = 0$, on a $\nu_j = 2$). On va montrer, en utilisant la théorie de Galois des extensions algébriques de corps (cf [7]) que $2\cos(\frac{2\pi}{q_j})$ est aussi une racine de $P_l(X)$. En effet, on remarque que non seulement $2\cos(2\pi\frac{p_j}{q_j})$ et $2\cos(\frac{2\pi}{q_j})$ sont tous les deux dans la même extension algébrique $\mathbb{Q}(\exp(2\pi i\frac{p_j}{q_j})) = \mathbb{Q}(\exp(\frac{2\pi i}{q_j})) = \{\sum_{k=0}^{q_j-1} r_k \exp(\frac{2\pi i k}{q_j}) : r_k \in \mathbb{Q}\}$ du corps $\mathbb{Q}$, mais ils sont aussi conjugués par l'automorphisme $\theta : \sum_{k=0}^{q_j-1} r_k \exp(\frac{2\pi i k}{q_j}) \mapsto \sum_{k=0}^{q_j-1} r_k \exp(\frac{2\pi i k p_j}{q_j})$ de ce corps tel que $\mathbb{Q}$ est stable par θ. Les coefficients de $P_l(X)$ étant entiers, $2\cos(\frac{2\pi}{q_j})$ est aussi une racine de $P_l(X)$. Si q_j est pair, l'argument du cosinus est déjà de la forme nécessaire, et si $q_j = 2k_j + 1$ est impair, $2\cos(\frac{2\pi k_j}{q_j})$ est aussi une racine de $P_l(X)$, et on a : $|2\cos(\frac{2\pi k_j}{q_j})| = |2\cos(\pi - \frac{\pi}{q_j})| = |2\cos(\frac{\pi}{q_j})|$. Alors, $\max\{|\nu_j| : 1 \leqslant j \leqslant l\} = 2\cos\frac{\pi}{q}$, où $q = \max\{q', q''\}$ avec $q' = \max\{|q_j| :\ q_j \text{ est impair}\}$ et $q'' = \frac{1}{2}\max\{|q_j| :\ q_j \text{ est pair}\}$.
Finalement, $q \geqslant 3$ car $2|\cos\pi| = 2$ et $2|\cos\frac{\pi}{2}| = 0$. ∎

Preuve du théorème de Kronecker. (i) Soient $\Lambda \in M_{r,s}(\mathbb{N})$ et Σ comme dans la proposition 6.1. Comme Σ est symétrique, ses valeurs propres ν_j $(j \in \{1, \dots, l = r + s\})$ sont réelles et $\|\Lambda\| = \|\Sigma\| = \max\{|\nu_j| : 1 \leqslant j \leqslant l\}$. Comme les ν_j sont les racines du polynôme caractéristique de Σ, ou bien $\Sigma = 0$, ou bien, par le corollaire précédent, $\|\Sigma\| = 2\cos\frac{\pi}{q}$, où $q \in \mathbb{N},\ q \geqslant 3$.
(ii) **Exemple.** Étant donné un entier $l \geqslant 2$, on considère la matrice
$$\Sigma = \begin{pmatrix} 0 & 1 & 0 & \cdot & 0 & 0 \\ 1 & 0 & 1 & \cdot & 0 & 0 \\ 0 & 1 & 0 & \cdot & 0 & 0 \\ . & . & . & . & . & . \\ 0 & 0 & 0 & \cdot & 0 & 1 \\ 0 & 0 & 0 & \cdot & 1 & 0 \end{pmatrix} \in M_l(\{0, 1\}).$$

Pour $j \in \{1, \dots, l\}$, on vérifie que $\Sigma\zeta_j = \nu_j\zeta_j$, avec
$$\nu_j = 2\cos\left(\frac{\pi j}{l+1}\right) \in \mathbb{R}, \quad \text{et} \quad \zeta_j = \left[\sin\left(\frac{\pi j}{l+1}m\right)\right]_{1 \leqslant m \leqslant l} \in \mathbb{R}^l.$$
Comme Σ est symétrique, on a $\|\Sigma\| = \max\{|\nu_j| :\ j \in \{1, \dots, l\}\} = 2\cos\frac{\pi}{l+1}$.
On récrit les lignes et les colonnes de Σ dans l'ordre : $2, 4, \dots, l, 1, 3, \dots, l-1$ si l est pair, et $2, 4, \dots, l-1, 1, 3, \dots, l$ si l est impair, et on obtient une matrice de la forme
$$\Lambda = \begin{pmatrix} 1 & 1 & 0 & \cdot & 0 & 0 \\ 0 & 1 & 1 & \cdot & 0 & 0 \\ 0 & 0 & 1 & \cdot & 0 & 0 \\ . & . & . & . & . & . \\ 0 & 0 & 0 & \cdot & 1 & 1 \\ 0 & 0 & 0 & \cdot & 0 & 1 \end{pmatrix} \in M_t(\{0, 1\}) \text{ si } l = 2t,$$
$$\Lambda = \begin{pmatrix} 1 & 1 & 0 & \cdot & 0 & 0 & 0 \\ 0 & 1 & 1 & \cdot & 0 & 0 & 0 \\ 0 & 0 & 1 & \cdot & 0 & 0 & 0 \\ . & . & . & . & . & . & . \\ 0 & 0 & 0 & \cdot & 1 & 1 & 0 \\ 0 & 0 & 0 & \cdot & 0 & 1 & 1 \end{pmatrix} \in M_{t,t+1}(\{0, 1\}) \text{ si } l = 2t + 1.$$
Dans les deux cas, on a $\|\Lambda\| = 2\cos\frac{\pi}{l+1}$. ∎

Conclusion. Si $A \subset B$ est une inclusion d'algèbres semi-simples, alors l'entier algébrique $[B : A]$ vérifie
$$[B : A] \in \left\{4\cos^2\left(\frac{\pi}{q}\right) :\ q \in \mathbb{N},\ q \geqslant 3\right\} \cup [4, +\infty[.$$

7 La construction fondamentale. Traces. Espérances conditionnelles.

7.1 La construction fondamentale.

Définition 7.1. La **construction fondamentale** associe à une inclusion $N \subset M$ d'algèbres semi-simples unifères l'inclusion suivante de même type : $M \subset L$, où $L := \mathrm{End}_N^d(M)$ est l'algèbre d'endomorphismes de M vue comme un N-module à droite ; on identifie M à une sous-algèbre de L, tout $x \in M$ étant identifié à l'opérateur de multiplication à gauche : $y \mapsto xy$ $(\forall y \in M)$.

Proposition 7.1. Soient $N \subset M$ une inclusion d'algèbres semi-simples et $M \subset L := \mathrm{End}_N^d(M)$ l'inclusion donnée par la construction fondamentale. Alors :

(i) L est une algèbre semi-simple dont les idempotents centraux minimaux sont de la forme $\rho(q)$, où q sont les idempotents centraux minimaux de N, et $\rho(q)$ est l'opérateur de multiplication à droite par q.

(ii) La matrice d'inclusion de $M \subset L$ est la transposée de Λ_N^M.

Preuve. On pose $F := \mathrm{End}_k(M)$ et on définit les applications $\lambda, \rho : M \to F$ par $\lambda(x)y = xy$, $\rho(x)y = yx$ pour tout $x, y \in M$. L'homomorphisme λ est la composition des inclusions $M \subset L$ et $L \subset F$; l'application ρ est un homomorphisme d'algèbres M^{op} dans F. Comme l'inclusion $N \subset M$ est isomorphe à l'inclusion $N^{op} \subset M^{op}$ par la proposition 5.2, elle est aussi isomorphe à $\rho(N) \subset \rho(M)$. Mais $\mathrm{End}_N^d(M) = C_F(\rho(N))$ et $M = \lambda(M) = C_F(\rho(M))$ donc (i) découle du lemme 4.3 (i) et (ii) du lemme 6.1. ■

Corollaire. $[M : N] = [L : M]$.

Alors, la construction fondamentale associe à une inclusion $N \subset M$ d'algèbres semi-simples unifères par induction la tour d'algèbres semi-simples (**la tour de V. Jones**)

$$N \subset M \subset M_1 \subset \ldots \subset M_n \subset \ldots$$

dont toute matrice d'inclusion est la transposée de la matrice d'inclusion précédente et suivante (périodicité de période 2) et les indices de toutes les inclusions sont les mêmes. Cela veut dire aussi que le diagramme de Bratteli de toute inclusion de cette tour est une réflexion du diagramme de Bratteli précédent et suivant.

Exemple 7.1. On connaît déjà la matrice d'inclusion et le diagramme de Bratteli de l'inclusion d'algèbres semi-simples $k\mathbb{Z}_3 = N \subset kS_3 = M$ (voir exemple 5.1). La proposition 7.1 permet de construire la tour de V. Jones correspondante et en particulier, de montrer que M_1 est isomorphe à $M_2(k) \oplus M_2(k) \oplus M_2(k)$, M_2 est isomorphe à $M_2(k) \oplus M_2(k) \oplus M_4(k)$ etc.

7.2 Trace.

Définitions 7.1. -

- Soient A une k-algèbre et V un espace vectoriel sur k. On dit qu'une application linéaire $\varphi : A \to V$ est **fidèle à droite** (resp., **à gauche**) si, pour tout $x \in A$, $x \neq 0$, il existe $y \in A$ tel que $\varphi(xy) \neq 0$ (resp., $\varphi(yx) \neq 0$).
- Une **trace** sur A est une forme linéaire $\varphi : A \to k$ telle que $\varphi(xy) = \varphi(yx)$, $\forall x, y \in A$.
- On dit qu'une **trace** est **fidèle** si elle est fidèle en tant que forme linéaire (dans le cas d'une trace, les notions de "fidèle à gauche" et de "fidèle à droite" coïncident).

Exemple 7.2. Si $A = M_n(k)$ $(n \in \mathbb{N}^*)$, alors $\mathrm{Tr}\,(a_{ij}) := \sum_i a_{ii}$ est une trace : la trace matricielle usuelle. On va montrer que toute trace $\varphi(\cdot)$ sur $A = M_n(k)$ est de la forme $\lambda \mathrm{Tr}\,(\cdot)$, $\lambda \in k$. En effet, notons e_{ij} $(i, j \in \{1, \ldots, n\})$ les unités matricielles de A. Alors, on a, pour tous $i \neq j$: $\varphi(e_{ij}) = \varphi(e_{ii}e_{ij}) = \varphi(e_{ij}e_{ii}) = 0$ et $\varphi(e_{ii}) = \varphi(e_{ii}(e_{ii} + e_{jj})) = \varphi(e_{ii}(e_{ij} + e_{ji})(e_{ij} + e_{ji})) = \varphi((e_{ij} + e_{ji})e_{ii}(e_{ij} + e_{ji})) = \varphi(e_{jj})$, d'où le résultat. Évidemment, cette trace est fidèle ssi $\lambda \neq 0$.

Conclusion. Une trace $\varphi(\cdot)$ sur l'algèbre $A = M_n(k)$ est parfaitement déterminée par la valeur des $\varphi(e_{ii})$, où e_{ii} $(i \in \{1, \ldots, n\})$ est un idempotent minimal quelconque de A.

Si $M = \oplus_i p_i M$ est une algèbre semi-simple, où $p_i M$ est isomorphe à $M_{n_i}(k)$, alors toute trace $\varphi(\cdot)$ sur M est de la forme $\sum_i \lambda_i Tr(\cdot)$, $\lambda_i \in k$. On va associer à cette trace le vecteur-ligne $\overline{\varphi} := (\varphi(e_1), \ldots, \varphi(e_n))$, où e_i est un idempotent minimal de $p_i M$. Ce vecteur définit la trace φ de manière unique, cette trace est fidèle ssi toutes les composantes de $\overline{\varphi}$ sont non nulles. On dit que la **trace** est **positive** si toutes les composantes de $\overline{\varphi}$ sont positives ; cette **trace** est **strictement fidèle** ssi toutes les composantes de $\overline{\varphi}$ sont strictement positives.

Proposition 7.2. Soit $N \subset M$ une inclusion d'algèbres semi-simples de dimension finie : $N = \oplus_{j=1}^{n} q_j N$, $M = \oplus_{i=1}^{m} p_i M$ avec une matrice d'inclusion Λ_N^M.

(i) Si σ est une trace sur M avec $\overline{\sigma} \in k^m$ et τ est une trace sur N avec $\overline{\tau} \in k^n$, alors σ est une extension de τ ssi $\overline{\tau} = \overline{\sigma}\Lambda_N^M$.

(ii) Il existe une trace fidèle sur M dont la restriction sur N est fidèle.

Preuve.

(i) Si f_j est un idempotent minimal de $q_j N$, alors $f_j p_i$ est la somme de λ_{ij} idempotents minimaux de $p_i M$. Donc la restriction de σ sur N est définie par le vecteur $\overline{\tau}'$ ayant pour composantes

$$\overline{\tau}'_j = \sigma(f_j) = \sum_{i=1}^{m} \sigma(f_j p_i) = \sum_{i=1}^{m} (\overline{\sigma})_i \lambda_{ij} = (\overline{\sigma}\Lambda_N^M)_j.$$

(ii) On définit la trace σ sur M avec les poids (les composantes de $(\overline{\sigma})_i$) toutes égales à 1. Sa restriction sur N, τ, a les poids $\overline{\tau}_j = \sum_{i=1}^{m} \lambda_{ij} \neq 0$ (car Λ_N^M est irredondante par le lemme 5.2 (ii)) donc cette trace est fidèle. ■

7.3 Espérance conditionnelle.

Définition 7.2. Une **espérance conditionnelle** E d'une k-algèbre M sur une sous-algèbre N est une application de N-bimodules dont la restriction sur N est l'identité.

Comme E est une application linéaire, on peut parler d'une espérance conditionnelle **fidèle** à droite ou à gauche. Par exemple, une trace τ sur M telle que $\tau(1_M) = 1$, est une espérance conditionnelle fidèle à gauche et à droite sur la sous-algèbre $k1_M$.
On considère l'ensemble $\mathrm{Hom}_N^d(M, N)$ d'applications de N-modules à droite de M vers N, muni de la structure de N-module à gauche définie par $(x\varphi)(y) := x\varphi(y),\ \forall x \in N,\ \forall y \in M,\ \forall \varphi \in \mathrm{Hom}_N^d(M, N)$.
On associe à une espérance conditionnelle $E : M \to N$ l'application $E^+ : M \to \mathrm{Hom}_N^d(M, N)$ de N-modules à gauche définie par : $E^+(x)(y) := E(xy),\ \forall x, y \in M$. Alors, E est fidèle à droite ssi E^+ est injective. On dit que E est **strictement fidèle** si E^+ est un isomorphisme.

Proposition 7.3. Soit $N \subset M$ une inclusion d'algèbres de dimension finie. Si N possède une forme linéaire τ fidèle à droite, alors toute espérance conditionnelle $E : M \to N$ fidèle à droite est strictement fidèle.

Preuve. On pose $\sigma := \tau \circ E$. Si $x \in M$ est tel que $\sigma(xx') = 0,\ \forall x' \in M$, alors $\sigma(xyz) = \tau(E(xy)z) = 0,\ \forall y \in M,\ \forall z \in N$ donc $E(xy) = 0$ par fidélité de τ et finalement $x = 0$ par fidélité de E. Ainsi, σ est fidèle, et puisque M est de dimension finie, toute forme linéaire sur M est de la forme $x \mapsto \sigma(ax)$ pour un $a \in M$. En effet, la dualité non dégénérée $< x, a > := \sigma(ax)$ définit un isomorphisme entre les espaces vectoriels M et M^*.
Maintenant, on va prouver la surjectivité de E^+. On considère une application de N-modules à droite $\varphi : M \to N$. Il existe $a \in M$ tel que $\tau \circ \varphi(x) = \sigma(ax),\ \forall x \in M$. On définit $\psi : M \to N$ par $\psi := E^+(a)$, c'est-à-dire, $\psi(x) = E(ax)$. Pour montrer que $\psi = \varphi$, il suffit de vérifier que $\lambda \circ \psi = \lambda \circ \varphi$ pour toute forme linéaire λ sur N. Mais comme τ est fidèle, une telle forme linéaire λ est donnée par $y \mapsto \tau(yb)$ pour un $b \in N$. Maintenant, pour tout $x \in M$: $\lambda \circ \psi(x) = \tau(E(ax)b) = \tau \circ E(axb)$ et $\lambda \circ \varphi(x) = \tau(\varphi(x)b) = \tau \circ \varphi(xb) = \sigma(axb) = \tau \circ E(axb)$. ■

Remarques. -
- Toute algèbre semi-simple N possède une forme linéaire fidèle, et même une trace fidèle.
- Si V est un espace vectoriel sur k, on définit sur $A = k \oplus V$ la multiplication suivante : $(\lambda, v)(\lambda', v') := (\lambda\lambda', \lambda v' + \lambda' v)$. On a ainsi une algèbre unifère dont tout sous-espace de $0 \oplus V$ est un idéal bilatère. Si $\dim(V) \geqslant 2$ et $\varphi : A \to k$ est une forme linéaire quelconque, alors $\mathrm{Ker}\,(\varphi) \cap V$ est un idéal bilatère dans $\mathrm{Ker}\,(\varphi)$. Donc A ne possède aucune forme linéaire fidèle. Par contre, si $V = kv$ (et donc $\dim(V) = 1$), alors la forme $(a, bv) \mapsto a + b$ est fidèle sur A.

Maintenant on va discuter l'existence d'espérances conditionnelles fidèles pour une inclusion d'algèbres donnée.

Proposition 7.4. Soient $N \subset M$ une inclusion d'algèbres unifères avec N de dimension finie, $\tau : M \to k$ une trace fidèle dont la restriction sur N est fidèle. Alors, il existe une application linéaire $E : M \to N$ telle que :

(i) $\tau \circ E = \tau$.

(ii) $E|_N = id_N$.

(iii) $E(xy) = E(x)y, \ \forall x \in M, \ \forall y \in N$.

De plus, E est une espérance conditionnelle fidèle, c'est-à-dire :

(iv) $E(yx) = yE(x), \ \forall x \in M, \ \forall y \in N$.

(v) $E(xy) = 0, \ \forall y \in N$ entraîne $x = 0$.

Si M est aussi de dimension finie, alors E est strictement fidèle :

(vi) $E^+ : M \to \mathrm{Hom}_N^d(M, N)$ défini par $a \mapsto (x \mapsto (E(ax))$ est un isomorphisme.

Preuve. (i) On considère l'algèbre M munie de la forme bilinéaire non-dégénérée $(x, z) \mapsto \tau(xz)$ et de la notion d'orthogonalité associée. Comme $\tau|_N$ est fidèle, on a $M = N \oplus N^\perp$. En effet, si $m \in M$, la forme linéaire $n \mapsto \tau(mn)$ est dans N^* donc il existe un unique $a \in N$ tel que $\tau(mn) = \tau(an), \ \forall n \in N$, d'où $(m - a) \in N^\perp$. De plus, $N \cap N^\perp = \{0\}$.
On vérifie d'abord que E, vérifiant (i)-(iii), est unique. Comme sur N on définit E par (ii), il suffit démontrer que $E|_{N^\perp} = 0$. Pour tous $t \in N^\perp$ et $y \in N$, on a par (i) et (iii) : $\tau(E(t)y) = \tau(E(ty)) = \tau(ty) = 0$ donc $E(t) \in N^\perp$. Mais on a aussi $E(t) \in N$ donc $E(t) = 0$.
Pour prouver l'existence, on définit E comme projection orthogonale de M sur N. Il est clair que (ii) est vraie. Pour tout $x \in M$, $E(x) - x$ est orthogonal à N donc à 1_N, donc (i) est vraie.
On va noter que $N^\perp$ est un N-module à droite par la propriété de trace de τ. Notamment, si $y, y' \in N, z \in N^\perp$, on a : $\tau(y'(zy)) = \tau((yy')z) = 0$ donc $zy \in N^\perp$. Maintenant, $xy - E(xy)$ et $x - E(x)$ sont dans $N^\perp$, et donc aussi $xy - E(x)y \in N^\perp$. La différence $(xy - E(xy)) - (xy - E(x)y) = E(x)y - E(xy)$ est dans $N \cap N^\perp = \{0\}$ donc (iii) est vraie. On prouve (iv) de manière similaire.
Comme $\tau \circ E = \tau$, la fidélité de E découle de celle de τ. Finalement, si M est de dimension finie, alors E est strictement fidèle par la proposition 7.3. ∎

Remarque. L'ensemble des conditions (i) à (iii) est équivalent à la seule condition :

$$\tau(E(x)y) = \tau(xy), \ \forall x \in M, \ \forall y \in N.$$

En effet, si on applique τ à l'égalité (iii), les conditions (i) et (ii) donnent la dernière égalité.
Réciproquement, à partir de cette dernière égalité, on obtient (i) si $y = 1_N$, on obtient (ii) si $x \in N$ par fidélité de τ sur N, et on obtient (iii) par : $\tau(E(xy)z) = \tau(xyz) = \tau(E(x)yz), \ \forall x \in M, \ \forall y, z \in N$, et par fidélité de τ sur N.

8 Une caractérisation de la construction fondamentale.

Dans ce cours, on va donner une description de la construction fondamentale en termes de générateurs et relations entre eux. Mais nous commençons d'abord par quelques rappels sur la théorie des modules.

8.1 Dual et bidual d'un module.

Définition 8.1. Pour tout A-module à gauche (resp., à droite) E, le A-module à droite $E^* = \mathrm{Hom}_A(E, {}_gA)$ (resp., le A-module à gauche $E^* = \mathrm{Hom}_A(E, A_d)$) s'appelle le **dual** de E.

Pour un A-module à gauche E et son dual E^*, on définit la **forme bilinéaire canonique** $< x, x^* > := x^*(x) \in A,\ \forall x \in E,\ \forall x^* \in E^*$. On a évidemment les relations

$$< a \cdot x, x^* > = \ a < x, x^* > \quad \text{et} \quad < x, x^* \cdot a > = < x, x^* > a, \quad \forall x \in E,\ \forall x^* \in E^*,\ \forall a \in A.$$

Si E et F sont deux A-modules à gauche et $u \in \mathrm{Hom}_A^g(E, F)$, on appelle **transposée** de u le morphisme $u^t \in \mathrm{Hom}_A^d(F^*, E^*)$ défini par :

$$< u(x), y^* > = < x, u^t(y^*) >, \quad \forall x \in E,\ \forall y^* \in F^*.$$

On peut donner une définition similaire pour des A-modules à droite. On a évidemment que $(u_1 + u_2)^t = u_1^t + u_2^t$, $(\nu \circ u)^t = u^t \circ \nu^t$, $\forall u, u_1, u_2 \in \mathrm{Hom}_A^g(E, F)$, $\forall \nu \in \mathrm{Hom}_A^g(F, G)$, où G est un troisième A-module à gauche, et $(id_E)^t = id_{E^*}$.
On dit que deux éléments $x \in E$ et $x^* \in E^*$, sont **orthogonaux** si $< x, x^* >= 0$. Si $P \subset E$ est une partie, alors on définit la partie de E^* orthogonale à P comme l'ensemble des $x^* \in X^*$ orthogonaux à tous les $x \in P$.
Ces définitions entraînent que :

(i) l'orthogonal de $u(E)$ dans F^* est le noyau de ${}^tu$.

(ii) si u est un isomorphisme d'inverse ν alors u^t est un isomorphisme d'inverse ν^t.

(ii) La transposition est un anti-isomorphisme entre les algèbres $\mathrm{End}_N^g(E)$ et $\mathrm{End}_N^d(E^*)$.

Exemples 8.1. -

a) Si $E = {}_gA$, alors l'application $a \mapsto \rho(a)$ est un isomorphisme entre E^* et A_d.

b) Si $E = \oplus_{i=1}^n E_i$ est une somme finie de A-modules, alors on peut identifier E^* à la somme directe $\oplus_{i=1}^n E_i^*$. En particulier, si E est libre de type fini donc isomorphe à $\oplus_{i=1}^n g_A$, alors on peut identifier E^* à $\oplus_{i=1}^n A_d$. Si $\{e_i\}$ est une base de E, alors les éléments $e_i^* \in E^*$ tels que $< e_i, e_j^* >= \delta_{i,j}$ pour $i, j \in \{1, 2, \ldots, n\}$ forment une **base** de E^* dite **duale** de la base $\{e_i\}$.

c) De manière un peu plus générale, le dual E^* d'un module projectif de type fini E est aussi un module projectif de type fini. En effet, par définition, il existe un autre module F tel que $E \oplus F = \oplus_{i=1}^n A \circ e_i$ pour un ensemble libre fini $e_i,\ i \in \{1, \ldots, n\}$ sur A. D'après b), on a $E^* \oplus F^* = \oplus_{i=1}^n [A \cdot e_i]^*$, d'où le résultat.

Pour le dual E^* d'un A-module à gauche E, on peut aussi définir le dual $E^{**} := (E^*)^*$ comme A-module à gauche ; on dit que c'est le **bidual** de E. Pour tout $x \in E$, l'application qui à x associe $(x^* \mapsto < x, x^* >) \in \mathrm{Hom}_A(E^*, A_d)$ est un morphisme de A-modules à gauche $c_E : E \to E^{**}$ appelé **l'application canonique**.
On note $\tilde{x} := c_E(x),\ \forall x \in E$.

Proposition 8.1. Si E est un A-module libre de base finie $\{e_i\}$, $(i \in \{1, 2, \ldots, n\})$, alors l'application canonique c_E est bijective.

Preuve. Comme $x = \sum_{i=1}^n x_i \cdot e_i,\ \forall x \in E$ avec $x_i \in A$, on peut considérer, pour $i \in \{1, 2, \ldots, n\}$, la famille de morphismes de A-modules à gauche $e_i^* : E \to {}_gA : x \mapsto x_i$. Par définition, si $\tilde{x} = 0$, alors $\forall i \in \{1, 2, \ldots, n\}$, on a $< x, e_i^* >= x_i = 0$ donc $x = 0$ et c_E est injective. On a aussi $< \tilde{e}_i, e_j^* >= \delta_{i,j},\ \forall i, j \in \{1, 2, \ldots, n\}$ donc $\{\tilde{e}_i\}$ est la base de E^{**} duale de $\{e_i^*\}$. Comme c_E transforme une base de E en une base de E^{**}, c_E est bijective (on peut utiliser le raisonnement de la preuve du lemme 2.2). ■

8.2 Produit tensoriel de deux modules.

Soient A une algèbre unifère, E un A-module à droite et F un A-module à gauche. On considère le produit tensoriel de k-espaces vectoriels $E \otimes_k F$ et le sous-espace H de cet espace engendré par les éléments de la forme $(x \cdot a) \otimes y - x \otimes (a \cdot y)$, pour tous $x \in E, y \in F$ et $a \in A$.

Définition 8.2. On appelle **produit tensoriel** des modules E et F, et on note $E \otimes_A F$, l'espace vectoriel quotient $(E \otimes F)/H$. Pour $x \in E$ et $y \in F$, on note $x \otimes_A y$ l'image canonique de l'élément $x \otimes_k y \in E \otimes_k F$.

La méthode utilisée dans la preuve de la proposition 4.1, (voir aussi [2], p. 77) nous donne la preuve de la

Proposition 8.2. -

(i) Soit X un espace vectoriel sur k, et soit $g : E \otimes_A F \to X$ une application linéaire. L'application $(x, y) \mapsto f(x, y) := g(x \otimes_A y)$ est une application bilinéaire de $E \times F$ dans X vérifiant la condition $f(v \cdot a, w) = f(v, a \cdot w)$, $\forall x \in E$, $\forall y \in F$, $\forall a \in A$.

(ii) Réciproquement, soit f une application bilinéaire de $E \times F$ dans X vérifiant la dernière condition. Il existe alors une application linéaire $g : E \otimes_A F \to X$ et une seule telle que $f(x, y) := g(x \otimes_A y)$ pour tous $x \in E$ et $y \in F$.

Soient $\varphi : E \to E'$ et $\psi : F \to F'$ deux morphismes de A-modules à droite, (resp., à gauche). On vérifie que l'application $(x, y) \mapsto \varphi(x) \otimes \psi(y)$ de $E \times F$ dans $E' \otimes_A F'$ vérifie les conditions de la proposition 8.2 donc il existe une application linéaire et une seule $\varphi \otimes \psi : E \otimes_A F \to E' \otimes_A F'$ telle que $(\varphi \otimes \psi)(x \otimes_A y) = \varphi(x) \otimes_A \psi(y)$ $\forall x \in E$, $\forall y \in F$. On l'appelle le **produit tensoriel** des morphismes φ et ψ.
On vérifie, en utilisant de nouveau la proposition 8.2, que si $E = \oplus_i E_i$ (resp., $F = \oplus_j F_j$) sont des sommes directes de A-modules à droite (resp., à gauche), on a un isomorphisme (à préciser !) entre les espaces vectoriels $E \otimes_A F$ et $\oplus_{i,j}(E_i \otimes_A F_j)$.

Proposition 8.3. -

(i) Si M est un A-module à gauche, alors l'application $h : M \to A_d \otimes_A M : \ x \mapsto 1_A \otimes_A x$ est un isomorphisme d'espaces vectoriels dont la réciproque g est définie par $g(a \otimes_A x) = a \cdot x$, $\forall x \in M$, $\forall a \in A$.

(ii) Si E est un A-module à droite projectif et M est un A-module à gauche, alors, pour tout A-module à gauche M' et tout morphisme injectif $\nu : M' \to M$, l'application linéaire $id_E \otimes \nu : E \otimes_A M' \to E \otimes_A M$ est injective.

Preuve.

(i) On vérifie directement que $g \circ h = id_M$ et que l'application linéaire $h \circ g$ est l'application identique sur les éléments de la forme $a \otimes_A x$ qui engendrent l'espace vectoriel $A_d \otimes_A M$.

(ii) Si $E = A_d$, alors le résultat découle de (i) car $id_A \otimes \nu$ est la composition de deux isomorphismes et une application injective. Si $E = \oplus_i A_d$ est la somme directe de copies de A_d, alors l'espace vectoriel $E \otimes_A M$ (resp., $E \otimes_A M'$) est isomorphe à $\oplus_i(A_d \otimes_A M)$ (resp., $\oplus_i(A_d \otimes_A M')$) et l'application linéaire $id_E \otimes \nu$ se transforme en $\oplus_i(id_A \otimes \nu)$ qui est injective car ν est injective. Finalement, si E est projectif alors, par définition, il existe un A-module à droite libre L et un autre A-module à droite F tels que $L = E \oplus F$, et on vient de voir que l'application linéaire $id_L \otimes \nu : L \otimes_A M' \to L \otimes_A M$ est injective. Mais $id_L \otimes \nu$ est la somme directe des applications linéaires $id_E \otimes \nu$ et $id_F \otimes \nu$ qui sont donc injectives (raisonner par l'absurde).

■

Soient E et F deux A-modules à gauche, et $E^* = \mathrm{Hom}_A^g(E, {}_gA)$ le dual de E. On définit l'application linéaire :

$$\theta : E^* \otimes_A F \to \mathrm{Hom}_A^g(E, F) : x^* \otimes_A y \mapsto (x \mapsto < x, x^* > y), \ \forall x \in E, \ \forall y \in F, \ \forall x^* \in E^*.$$

Si E est un A-module à droite, en remplaçant ci-dessus E par E^* et en utilisant l'application canonique $c_E : E \to E^{**}$, on obtient l'application linéaire :

$$\theta' : E \otimes_A F \to \mathrm{Hom}_A^g(E^*, F) : x \otimes_A y \mapsto (x^* \mapsto < x, x^* > y), \ \forall x \in E, \ \forall y \in F, \ \forall x^* \in E^*.$$

On va montrer que, si E est un A-module à droite projectif de type fini, alors θ' est un isomorphisme d'espaces vectoriels. En effet, si d'abord $E = A_d$, alors $A_d \otimes_A F$ est isomorphe à F ainsi qu'à $\mathrm{Hom}_A^g({}_gA, F)$ (le dernier par l'isomorphisme $y \in F \mapsto (a \mapsto a \cdot y)$). Comme $\mathrm{Hom}_A^g(\oplus_{i=1}^n E_i, F) = \oplus_{i=1}^n \mathrm{Hom}_A^g(E_i, F)$ pour toute famille F_i de

A-modules à droite et que $(\oplus_i E_i) \otimes F$ est isomorphe à $\oplus_i (E_i \otimes F)$ (voir ci-dessus), l'affirmation est vraie pour tout E libre. Finalement, si E est projectif de type fini alors il existe un A-module à droite libre de type fini G et un A-module à droite de type fini H tels que $G = E \oplus H$, on a déjà un isomorphisme d'espaces vectoriels $(E \otimes_A F) \oplus (H \otimes_A F)$ et $\mathrm{Hom}_A^g(E^*, F) \oplus \mathrm{Hom}_A^g(H^*, F)$ qui est la somme directe des applications linéaires entre les facteurs correspondants. Alors, ces application linéaires sont nécessairement des isomorphismes.

Théorème 8.1. Soient $N = \oplus_{j=1}^n q_j N \subset M = \oplus_{i=1}^m p_i M$ une inclusion d'algèbres semi-simples de dimension finie, et $L = \oplus_{j=1}^n \rho(q_j) L = \mathrm{End}_N^d(M)$. Par la proposition 7.4, il existe une espérance conditionnelle strictement fidèle $E : M \to N$, et :

(i) Les éléments de la forme $\lambda(x)E\lambda(y)$ engendrent L comme espace vectoriel sur k.

(ii) L'application linéaire $\varphi : N \to ELE$ définie par $\varphi(x) = \lambda(x)E$ est un isomorphisme d'algèbres.

(iii) Si f_j est un idempotent minimal du facteur $q_j N$, alors $\lambda(f_j)E$ est un idempotent minimal du facteur $\rho(q_j)L$.

Preuve.

(i) L'existence d'une espérance conditionnelle strictement fidèle $E : M \to N$ dit que l'application $E^+ : M \to M^* = \mathrm{Hom}_N^d(M, N)$ de N-modules à gauche (voir ci-dessus) est un isomorphisme. Le N-module à droite M est projectif de type fini car tout module sur une algèbre semi-simple de dimension finie est projectif par le lemme 2.2, alors la proposition 8.3 (ii) dit que l'application $id_M \otimes E^+ : M \otimes_N M \to M \otimes_N M^*$ est bijective. Si on remarque que la transposition est un anti-isomorphisme de $L := \mathrm{End}_N^d(M)$ et $\mathrm{End}_N^g(M^*)$, alors le raisonnement utilisé avant le théorème dit que $\theta : M \otimes_N M^* \to L : x \otimes_N x^* \mapsto \lambda(x)x^*$ est un isomorphisme d'espaces vectoriels. Finalement, l'application $\Phi := \theta(id_M \otimes E^+) : M \otimes_N M \to L$ est un isomorphisme d'espaces vectoriels comme application composée de deux isomorphismes, et on calcule directement que $\Phi(x \otimes y) = \lambda(x)E\lambda(y), \ \forall x, y \in M$.

(ii) Comme E est un idempotent de L qui commute à $\lambda(N)$, φ est un morphisme d'algèbres. Si $x \in N$ et $\varphi(x) = 0$, alors $x = E(x1_M) = \varphi(x)1_M = 0$ donc φ est injectif. Finalement, φ est surjectif par (i).

(iii) Pour tout $j \in \{1, 2, \ldots, n\}$, l'idempotent $\rho(q_j)E = \lambda(q_j)E \in \rho(q_j)L$ est non nul. Alors $\rho(q_j)ELE = \rho(q_j)\lambda(N)E$ est un facteur. Comme φ est un isomorphisme d'algèbres, sa restriction φ_j sur $q_j N$ est aussi un isomorphisme d'algèbres sur $\rho(q_j)ELE$. Or, si $e \in L$ est un idempotent non nul dominé par $\lambda(f_j)E$ et donc aussi par $\lambda(q_j)E = \rho(q_j)E$, alors $e = \rho(q_j)Ee\rho(q_j)E \in \rho(q_j)ELE$, d'où $e = \lambda(f_j)E$. Autrement dit, l'idempotent $\lambda(f_j)E$ est aussi minimal dans L.

■

9 Les traces de Markov.

Soient $N \subset M$ une inclusion d'algèbres semi-simples de dimension finie, et $\lambda : M \to L = \mathrm{End}_N^d(M)$ l'inclusion obtenue par la construction fondamentale. Si $E : M \to N$ est une espérance conditionnelle fidèle, le théorème 8.1 indique que L est engendré en tant qu'espace vectoriel par les éléments de la forme $\lambda(x)E\lambda(y),\ \forall x, y \in M$.
Toute trace Tr sur L vérifie les relations :

$$\mathrm{Tr}\,(\lambda(x)E\lambda(y)) = \mathrm{Tr}\,(\lambda(yx)E) = \mathrm{Tr}\,(E\lambda(yx)E) = \mathrm{Tr}\,(\lambda(E(yx))E), \quad \forall x, y \in M,$$

donc la trace Tr est définie de manière unique par ses valeurs sur les éléments de la forme $\lambda(x)E,\ \forall x \in N$.

Définition 9.1. On dit qu'une trace fidèle tr sur M dont la restriction sur N est fidèle, est une **trace de Markov de module** $\beta \in k$ s'il existe une trace Tr sur L tel que :

$$\mathrm{Tr}\,(\lambda(x)) = tr(x) \quad \text{et} \quad \beta\mathrm{Tr}\,(\lambda(x)E) = tr(x), \quad \forall x \in M.$$

La fidélité de tr implique que $\beta \neq 0$. Si une telle trace Tr existe, elle est unique dans le sens suivant :

Lemme 9.1. Soit $N \subset M$ une inclusion d'algèbres semi-simples de dimension finie, soit $\beta \neq 0$ et soient tr et E définis comme précédemment. Il existe alors au plus une trace Tr sur L telle que :

$$\beta\mathrm{Tr}\,(\lambda(y)E) = tr(y),\ \forall y \in N.$$

Si une telle trace Tr existe, alors elle est fidèle et vérifie :

$$\beta Tr(\lambda(x)E) = tr(x),\ \forall x \in M.$$

Si $\overline{\tau} = (\tau_1, \ldots, \tau_n)$ et $\overline{t} = (t_1, \ldots, t_n)$ sont les vecteurs correspondants respectivement à Tr et $tr|_N$, alors $\overline{\tau}\beta = \overline{t}$.

Preuve. Si une telle trace Tr existe, avec les notations du théorème 8.1, on a pour tout $j \in \{1, 2, \ldots, n\}$, $\beta\tau_j = \beta\mathrm{Tr}\,(\lambda(f_j)E)$ qui est égal, par le théorème 8.1 (iii), à $tr(f_j) = t_j$ donc on a bien $\overline{\tau}\beta = \overline{t}$. L'unicité et la fidélité de Tr suivent. Finalement, pour tout $x \in M$:

$$\beta\mathrm{Tr}\,(\lambda(x)E) = \beta\mathrm{Tr}\,(E\lambda(x)E) = \beta\mathrm{Tr}\,(\lambda(E(x))E) = tr(E(x)) = tr(x).$$

■

Théorème 9.1. Soient $N \subset M$ une inclusion d'algèbres semi-simples de dimension finie donnée par matrice d'inclusion Λ et $\lambda : M \to L$ l'inclusion obtenue par la construction fondamentale. Soient les décompositions des algèbres N, M et L en facteurs :

$$N = \bigoplus_{j=1}^{n} q_j N, \quad M = \bigoplus_{i=1}^{m} p_i M, \quad L = \bigoplus_{j=1}^{n} \rho(q_j) L,$$

où $q_j N \simeq M_{\nu_j}(k),\ p_i M \simeq M_{\mu_i}(k),\ \rho(q_j)L \simeq M_{\kappa_j}(k),\ \overline{\nu} = (\nu_1, \ldots, \nu_n), \overline{\mu} = (\mu_1, \ldots, \mu_m)$ et $\overline{\kappa} = (\kappa_1, \ldots, \kappa_n)$.
En particulier, on a $\Lambda\overline{\nu} = \overline{\mu}$ et $\Lambda^t\overline{\mu} = \overline{\kappa}$.
Soient tr une trace fidèle sur M dont la restriction sur N est fidèle, E l'espérance conditionnelle associée, $\overline{s} \in k^m$, $\overline{t} \in k^n$ les vecteurs correspondants donc $\overline{s}\Lambda = \overline{t}$. Soit $\beta \neq 0$. Alors les affirmations suivantes sont équivalentes :

(i) tr est une trace de Markov de module β.

(ii) $\overline{s}(\Lambda\Lambda^t) = \beta\overline{s}$ et $\overline{t}(\Lambda^t\Lambda) = \beta\overline{t}$.

En particulier, si $k = \mathbb{C}$, alors tout module β d'une trace de Markov est un entier algébrique positif.

Preuve. $(i) \Rightarrow (ii)$. Soient Tr une trace de la définition d'une trace de Markov et $\overline{\tau}$ le vecteur correspondant. Alors, $\overline{t} = \overline{\tau}(\Lambda^t\Lambda)$ puisque Tr est une extension de tr, et $\overline{\tau}\beta = \overline{t}$ par le lemme précédent, donc $\overline{t}(\Lambda^t\Lambda) = \beta\overline{t}$. On a aussi $\overline{\tau}\Lambda^t = \overline{s}$, donc $\overline{s}\Lambda\Lambda^t = \tau\Lambda^t\Lambda\Lambda^t = \beta\overline{\tau}\Lambda^t = \beta\overline{s}$.
$(ii) \Rightarrow (i)$. On pose $\overline{\tau} := \beta^{-1}\overline{t}$, et soit Tr la trace correspondante. Alors, Tr est une extension de tr parce que $\overline{\tau}\Lambda^t = \beta^{-1}\overline{t}\Lambda^t = \beta^{-1}\overline{s}\Lambda\Lambda^t = \overline{s}$.
On considère l'application linéaire $\tilde{\tau} : N \to k$ définie par $\tilde{\tau}(y) = \beta\mathrm{Tr}\,(\lambda(y)E)$; c'est une trace parce que E est une application N-linéaire et en même temps un idempotent dans q_jN ; on a $\tilde{\tau}(f_j) = \beta\mathrm{Tr}\,(\lambda(f_j)E) = \beta\tau_j = t_j,\ \forall j \in$

$\{1, 2, \ldots, n\}$ par le théorème 8.1 et par la définition de $\overline{\tau}$, donc $\tau = tr|_N$. Alors, par le lemme précédent, Tr vérifie la condition de Markov $\beta\mathrm{Tr}\,(\lambda(x)E) = tr(x),\ \forall x \in M$.
Finalement, si $k = \mathbb{C}$, alors toute valeur propre d'une matrice de la forme $\Lambda^t\Lambda$ est un entier algébrique positif. ∎

Remarques. -

– Soient $\Lambda = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$, $\overline{s} = (3, 1)$ donc $\overline{t} = (4, 4)$. Alors, $\overline{t}\Lambda^t\Lambda = 4\overline{t}$, mais $\overline{s}\Lambda\Lambda^t$ n'est pas un multiple scalaire de $\overline{s}$. Cela montre qu'on ne peut pas supprimer la première égalité dans la condition (ii).
– Si $k = \mathbb{C}$, on a la condition $\beta > 0$ sans aucune condition de positivité sur tr.
– Soient $k = \mathbb{C},\ \beta \neq 0,\ Z(M) \cap Z(N) = k1_M$. Alors, on peut montrer (voir [4], théorème 2.7.3), qu'une trace de Markov **positive** de module β existe ssi $\beta = [M : N] = \|\Lambda\|^2$ et que cette trace de Markov est unique à un multiplicateur scalaire près. L'élément crucial dans la preuve est (voir [3]) :

Théorème de Perron-Frobenius. Si une matrice carrée réelle a tous ses coefficients strictement positifs, alors son rayon spectral est une valeur propre positive dont l'espace propre associé est de dimension 1. Elle admet un vecteur propre pour cette valeur propre dont tous les coefficients sont strictement positifs.

Maintenant on va montrer que si tr sur une paire d'algèbres $N \subset M$ est une trace de Markov, alors la trace Tr sur la paire $M \subset L$ est aussi une trace de Markov. Plus précisément :

Proposition 9.1. Soient tr une trace de Markov de module β sur une paire d'algèbres semi-simples de dimension finie $N \subset M,\ L = \mathrm{End}_N^d(M)$ et Tr l'extension de tr définie comme dans le lemme 9.1. Soit enfin $D : L \to \lambda(M)$ l'espérance conditionnelle définie par Tr et tr. Alors :
(i) Tr est une trace de Markov de module β par rapport à $\lambda : M \to L$;
(ii) $\beta D(E) = 1_M$;
(iii) $\beta D\overline{\lambda}(E)D = D$, où $\overline{\lambda}$ est la multiplication à gauche sur L ;
(iv) $\beta\overline{\lambda}(E)D\overline{\lambda}(E) = \overline{\lambda}(E)$.

Preuve.
(i) Soient $\overline{s}$ et $\overline{t}$ les vecteurs qui définissent respectivement la trace tr sur M et N. Comme tr est une trace de Markov de module β, on a : $\overline{s}(\Lambda\Lambda^t) = \beta\overline{s}$ et $\overline{t}(\Lambda^t\Lambda) = \beta\overline{t}$ par le théorème 9.1. La preuve du lemme 9.1 dit que Tr est défini par $\overline{\tau} = \beta^{-1}\overline{t}$ donc $\overline{s}(\Lambda\Lambda^t) = \beta\overline{s}$ et $\overline{\tau}(\Lambda^t\Lambda) = \beta\overline{\tau}$ et (i) découle du théorème 9.1.
(ii) La forme bilinéaire $(u, v) \mapsto \mathrm{Tr}\,(uv)$ est non dégénérée sur L ainsi que sa restriction sur $\lambda(M)$. Alors, $L = \lambda(M) \oplus \lambda(M)^\perp$, avec orthogonalité dans le sens de cette forme bilinéaire. Pour tout $x \in M$, on a :

$$\mathrm{Tr}\,(\beta E\lambda(x) - \lambda(x)) = \beta\mathrm{Tr}\,(\lambda(x)E) - \mathrm{Tr}\,(\lambda(x)) = tr(x) - tr(x) = 0,$$

donc $\beta E - 1_M \in \lambda(M)^\perp$. Comme D est la projection orthogonale de L sur $\lambda(M)$, cela implique $D(\beta E) = 1_M$.
(iii) Par M-linéarité de D, on a : $D\overline{\lambda}(E)D = \overline{\lambda}(D(E))D$ donc (iii) découle de (ii).
(iv) On pose $u = \lambda(x)E\lambda(y) \in L$, où $x, y \in M$. Les trois applications suivantes de M dans M sont égales par (N, N)-linéarité de E :

$$E\lambda(x)E\lambda(y) : z \mapsto E(xE(yz))$$

$$E\lambda(E(x))\lambda(y) : z \mapsto E(E(x)yz)$$

$$\lambda(E(x))E\lambda(y) : z \mapsto E(x)E(yz)$$

Par (M, M)-linéarité de D, on a :

$$\overline{\lambda}(E)D\overline{\lambda}(E)u = ED(E\lambda(x)E\lambda(y)) = ED(\lambda(E(x))E\lambda(y)) = E\lambda(E(x))D(E)\lambda(y).$$

Par conséquent, en utilisant (i) :

$$\beta\overline{\lambda}(E)D\overline{\lambda}(E)u = E\lambda(E(x))\lambda(y) = Eu = \overline{\lambda}(E)u,$$

ce que prouve (iv).

∎

10 Tours d'algèbres.

10.1 Généralités.

On considère d'abord une tour **arbitraire** (finie ou infinie) d'algèbres semi-simples de dimension finie :

$$M_0 \subset M_1 \subset \ldots \subset M_k \subset M_{k+1} \subset \ldots,$$

munie des diagrammes de Bratteli de toutes les inclusions.

Proposition 10.1. Soient $M_0 \subset M_1 \subset M_2 \subset \ldots$ et $M_0' \subset M_1' \subset M_2' \subset \ldots$ deux tours d'algèbres semi-simples avec les mêmes ensembles (finis ou non) de diagrammes de Bratteli. On note M_∞ la limite inductive de toutes les algèbres M_k. C'est une k-algèbre unifère qui est la réunion de ses sous-algèbres semi-simples de dimension finie. De même pour M_∞'. Alors, il existe un isomorphisme d'algèbres $\psi : M_\infty := \cup_i M_i \to M_\infty' := \cup_i M_i'$ tel que $\psi(M_i) = M_i'$ pour tout $i \in \{0, 1, \ldots\}$.

Preuve. Il suffit de construire une suite d'isomorphismes $\psi_i : M_i \to M_i'$ tels que $\psi_{i+1}|_{M_i} = \psi_i$. Soit ψ_0 un isomorphisme quelconque, et on suppose qu'on a déjà construit $\psi_0, \ldots, \psi_i$. Alors, on a vu qu'il existe un isomorphisme $\alpha_{i+1} : M_{i+1} \to M_{i+1}'$ tel que $\alpha_{i+1}(M_i) = M_i'$, et d'après la proposition 5.1, il existe un automorphisme intérieur β_{i+1} de M_{i+1}' qui est une extension de $\psi_i \circ \alpha_{i+1}^{-1}|_{M_i'}$. On peut alors poser $\psi_{i+1} := \beta_{i+1} \circ \alpha_{i+1}$. ∎

Maintenant, on analyse le rôle des traces de Markov pour les tours d'algèbres **engendrées par la construction fondamentale**. Plus précisément, on considère une inclusion $M_0 \subset M_1$ d'algèbres semi-simples de dimension finie, la tour d'algèbres $M_k,\ k \geqslant 0$ **engendrée par la construction fondamentale**, et la trace de Markov tr_1 de module β sur la paire $M_0 \subset M_1$. On note tr_2 l'extension de cette trace sur M_2 (notée précédemment Tr), et on désigne par $E_1 = E : M_1 \to M_0,\ E_1 \in M_2,\ E_2 = D : M_2 \to M_1,\ E_2 \in M_3$ les espérances conditionnelles associées. Selon la proposition 9.1, on peut itérer le processus d'extension de trace de Markov, notamment : si $E_k : M_k \to M_{k-1}$ est l'espérance conditionnelle associée aux tr_k et tr_{k-1}, et tr_{k+1} est l'unique extension de tr_k qui vérifie $\beta tr_{k+1}(xE_k) = tr_k(x)\ \forall x \in M_k$ (voir ci-dessus), alors tr_{k+1} est aussi une trace de Markov, et on peut continuer ce processus. On remarque que l'algèbre M_{k+1} est engendrée par M_k et E_k, brièvement $M_{k+1} =< M_k, E_k >$. L'algèbre M_∞ a un centre de dimension finie isomorphe à $Z(M_0) \cap Z(M_1)$. La réunion des tr_k définit une trace non-dégénérée $tr : M_\infty \to k$ (en effet, $tr(xy) = 0,\ \forall y \in M_\infty$ entraîne $x = 0$). Si $k = \mathbb{C}$ et tr_1 est positive, alors tr est aussi positive dans le sens que $tr(\varepsilon) > 0$ pour tout idempotent non nul $\varepsilon \in M_\infty$. Dans ce cas, et si de plus $Z(M_0) \cap Z(M_1) = k1_{M_1}$, alors le théorème de Perron-Frobenius entraîne que tr est l'unique trace positive sur M_∞, à un multiplicateur scalaire près (voir remarques du paragraphe 9).

Théorème 10.1. Soient $M_0 \subset M_1$ une inclusion d'algèbres semi-simples de dimension finie et $tr_1 : M_1 \to k$ la trace de Markov de module β. Avec les notations précédentes, on a :

(i) $\beta E_i E_j E_i = E_i$ si $i \geqslant 1,\ j \geqslant 1$ et $|i - j| = 1$;

(ii) $E_i E_j = E_j E_i$ si $i \geqslant 1,\ j \geqslant 1$ et $|i - j| \geqslant 2$;

(iii) $\beta tr(wE_k) = tr(w)$ pour tout $w \in M_k$.
En particulier, si tr est normalisée par $tr(\mathbf{1}) = 1$, alors $tr(E_k) = \beta^{-1},\ \forall k \geqslant 1$.

Preuve. Les affirmations (i) et (iii) découlent des affirmations (i),(iii) et (iv) de la proposition 9.1. Si $j \geqslant i + 2$, alors $E_i \in M_{j-1}$, et on a (ii) par M_{j-1}-linéarité de l'espérance conditionnelle E_j. ∎

10.2 Exemple : les algèbres de Temperley-Lieb.

Le théorème 10.1 est une motivation pour la définition suivante :

Définition 10.1. Étant donné un $\beta \in k^\times$ et un entier naturel non nul n, on note $\mathcal{A}_{\beta,n}$ l'**algèbre** associative unifère engendrée par les générateurs $\mathbf{1}, e_1, \ldots, e_{n-1}$ vérifiant les relations de **Temperley-Lieb** :

$$\begin{array}{rlll} e_i^2 = e_i & \text{si} & i \geqslant 1 & \\ \beta e_i e_j e_i = e_i & \text{si} & i \geqslant 1,\quad j \geqslant 1 & \text{et} \quad |i-j| = 1 \\ e_i e_j = e_j e_i & \text{si} & i \geqslant 1,\quad j \geqslant 1 & \text{et} \quad |i-j| \geqslant 2 \end{array}$$

Un **monôme** dans $\mathcal{A}_{\beta,n}$ est un produit $e_{i_1} e_{i_2} \ldots e_{i_p}$, où tout e_{i_j} est un des $e_1, \ldots, e_{n-1}$ ou $\mathbf{1}$ (produit vide).

Proposition 10.2. On peut écrire tout monôme $w \in \mathcal{A}_{\beta,n}$ sous forme réduite :

$$\beta^{-r}(e_{i_1}e_{i_1-1}\dots e_{j_1})(e_{i_2}e_{i_2-1}\dots e_{j_2})\dots(e_{i_p}e_{i_p-1}\dots e_{j_p}),$$

où $r \in \mathbb{N}$, $1 \leqslant i_1 < i_2 < \dots < i_p \leqslant n-1$, $1 \leqslant j_1 < j_2 < \dots < j_p \leqslant n-1$, $i_1 \geqslant j_1, i_2 \geqslant j_2, \dots, i_p \geqslant j_p$, $0 \leqslant p \leqslant n-1$. De plus :

$$\dim(\mathcal{A}_{\beta,n}) \leqslant C_n := \frac{1}{n+1}\binom{n}{2n}$$

Preuve. On considère un entier m tel que $0 \leqslant m \leqslant n-1$; on va prouver la 1ère affirmation par récurrence sur m pour un monôme w en $e_1, \dots, e_m$. Comme c'est évident pour les monômes tels que $m \leqslant 1$, on peut supposer que $m \geqslant 2$ et que l'affirmation est vraie pour $m-1$.
Si w est un monôme contenant e_m au moins 2 fois, alors entre les plus proches e_m se trouve un monôme en $e_1, \dots, e_{m-1}$ qui, par l'hypothèse de récurrence, ou bien ne contient pas e_{m-1}, ou bien est de la forme $ae_{m-1}b$, où a, b sont des monômes en $e_1, \dots, e_{m-2}$. Alors w est ou bien de la forme $w = w_1 e_m a e_m w_2$, ou bien de la forme $w = w_1 e_m a e_{m-1} b e_m w_2$, où a, b sont des monômes en $e_1, \dots, e_{m-2}$. Comme ils commutent à e_m, alors w est égal ou bien à $w_1 e_m a w_2$, ou bien à $\beta^{-1} w_1 a e_m b w_2$ donc le nombre de e_m a été réduit. Par conséquent, on peut supposer que w contient exactement un e_m.
Soit $w = w_1 e_m w_2$, où w_1, w_2 sont des monômes en $e_1, \dots, e_{m-1}$. En utilisant l'hypothèse de récurrence pour w_2 et le fait que e_m et tous les e_j pour tout $j \leqslant m-2$ commutent entre eux, on se ramène au cas $w = w_1 e_m e_{m-1} \dots e_s$, où w_1 est un monôme réduit se terminant, disons, par e_l. Si $l \geqslant s$, on a : $e_l e_m e_{m-1} \dots e_s = e_m \dots e_{l+2}(e_l e_{l+1} e_l) e_{l-1} \dots e_s = \beta^{-1} e_l e_{l-1} \dots e_s e_m e_{m-1} \dots e_{l+2}$.
Donc, on peut supposer que $l < s$, c'est-à-dire, que w est de la forme

$$w = \beta e_{i_1} \dots e_{j_1} e_{i_2} \dots e_{j_2} \dots e_{i_p} \dots e_{j_p} \ (i_p = m, j_p = s),$$

ce qui termine la démonstration par récurrence.
Maintenant, on veut calculer le nombre de monômes réduits dans $\mathcal{A}_{\beta,n}$ ou encore le nombre de suites associées de la forme $(i_1, j_1, \dots, i_p, j_p)$. On peut associer à cette suite le chemin entre les points $(0,0)$ et (n,n) dans $\mathbb{Z}^2$ formé de segments horizontaux et verticaux dont les sommets se trouvent aux points

$$(0,0), (i_1, 0), (i_1, j_1), (i_2, j_1), (i_2, j_2), \dots, (i_p, j_p), (n, j_p), (n, n).$$

On remarque que tout chemin entre $(0,0)$ et (n,n) dont les sommets se trouvent sous ou sur la droite passant par ces deux points, est de cette forme avec une suite qui correspond à un des monômes réduits dans $\mathcal{A}_{\beta,n}$. Évidemment, l'ensemble de ces chemins est en bijection avec l'ensemble des chemins entre $(1,0)$ et $(n+1,n)$ qui sont strictement sous la diagonale principale.
D'autre part, tout chemin entre $(1,0)$ et $(n+1,n)$ contient n segments horizontaux et n segments verticaux de longueur 1 donc le nombre total de ces chemins est égal au nombre de combinaisons de n parmi $2n$ possibilités, c'est-à-dire, à $\binom{n}{2n}$. De même, le nombre de chemins entre $(0,1)$ et $(n+1,n)$ est $\binom{n+1}{2n}$. Mais l'ensemble de ces derniers chemins est en bijection avec l'ensemble des chemins entre $(1,0)$ et $(n+1,n)$ touchant la diagonale principale : en effet, si (j,j) appartient à un chemin entre $(1,0)$ et $(n+1,n)$ avec j minimal, on remplace la partie de ce chemin entre $(1,0)$ et (j,j) par sa réflexion, et on ne change pas l'autre partie de ce chemin.
Ainsi, le nombre de chemins entre $(1,0)$ et $(n+1,n)$ qui sont strictement sous la diagonale principale, est

$$\binom{n}{2n} - \binom{n+1}{2n} = \frac{1}{n+1}\binom{n}{2n} := C_n$$

d'où le résultat. ∎

Définition 10.2. - On définit par récurrence la suite de polynômes :

$$\begin{cases} P_0(X) \equiv 1, \\ P_1(X) \equiv 1, \\ \forall n \geqslant 1, \quad P_{n+1}(X) = P_n(X) - X P_{n-1}(X) \end{cases}$$

Ainsi, $P_2(X) = 1 - X,\ P_3(X) = 1 - 2X,\ P_4(X) = 1 - 3X + X^2,\ P_5(X) = 1 - 4X + 3X^2, \dots$
Le polynôme P_n est le n-ème **polynôme de Jones**.

Théorème 10.2. Soient $n \in \mathbb{N}^{\times}$, $\beta \in k^{\times}$ tel que $P_j(\beta^{-1}) \neq 0$, $\forall j \in \{2, 3, \ldots, n-1\}$. Alors :

(i) $\mathcal{A}_{\beta,n}$ est une algèbre semi-simple de dimension $C_n = \dfrac{1}{n+1}\dbinom{n}{2n}$, isomorphe à $\bigoplus_{j=0}^{m} M_{m(n,j)}(k)$, où m est la partie entière de $\dfrac{n}{2}$ et $m(n,j) = \dbinom{j}{n} - \dbinom{j-1}{n}$.

(ii) Il existe une trace normalisée unique $tr_n : \mathcal{A}_{\beta,n} \to k$ telle que $\beta tr_n(we_j) = tr_n(w)$ si $1 \leqslant j \leqslant n-1$ et w est dans la sous-algèbre engendrée par $\mathbf{1}, e_1, \ldots, e_{j-1}$. De plus, tr_n est fidèle si $P_n(\beta^{-1}) \neq 0$.

(iii) L'application naturelle $\mathcal{A}_{\beta,n-1} \to \mathcal{A}_{\beta,n}$ est injective et tr_n est une extension de tr_{n-1}.

Pour la preuve de ce théorème, voir [4], théorèmes 2.1.7 et 2.1.8.

Remarques. -
- Les nombres C_n s'appellent les **nombres de Catalan**. On a $C_1 = 1,\ C_2 = 2,\ C_3 = 5,\ C_4 = 14, \ldots$
- On peut calculer : $\mathcal{A}_{\beta,1} = k,\ \forall \beta \neq 0$, et $\mathcal{A}_{\beta,2} = k \oplus k,\ \forall \beta \neq 0$.
- Étudions la structure de l'algèbre $\mathcal{A}_{\beta,3}$ en fonction de $\beta \neq 0$. Il existe exactement 5 monômes réduits dans ce cas : $\mathbf{1}, e_1, e_2, e_1e_2, e_2e_1$ donc $\dim(\mathcal{A}_{\beta,3}) \leqslant 5$, et cette algèbre n'est pas commutative car il n'y a pas de relation $e_1e_2 = e_2e_1$. Comme $n = 3$, le théorème 10.2 dit que si β^{-1} n'est pas racine de l'équation $P_2(X) = 1 - X = 0$, c'est-à-dire, si $\beta \neq 1$, alors cette algèbre est semi-simple donc nécessairement isomorphe à $k \oplus M_2(k)$. Il est plus difficile d'établir un isomorphisme explicite entre $\mathcal{A}_{\beta,3}, \forall \beta \notin \{0,1\}$ et $k \oplus M_2(k)$.
  On calcule $Z(\mathcal{A}_{\beta,3}) =< \mathbf{1}, r >$, où $r = e_1(\mathbf{1} - e_2) + e_2(\mathbf{1} - e_1)$ vérifie la relation $r^2 = (1 - \beta^{-1})r$. On peut alors conclure que $\mathcal{A}_{1,3}$ n'est pas semi-simple car le seul élément central r de l'algèbre $k \oplus M_2(k)$ tel que $r^2 = 0$, est 0.

Références

[1] N. Bourbaki *Éléments de mathématique, Algèbre, Chapitres 4 et 5*, Hermann (1967).

[2] N. Bourbaki *Éléments de mathématique, Algèbre, Chapitre 2*, Hermann (1962).

[3] F.R. Gantmacher *Théorie des matrices, Tomes 1 et 2*, Dunod (1966).

[4] F. Goodman, P. de la Harpe, V.F.R. Jones *Coxeter Graphs and Towers of Algebras*, Springer-Verlag (1989).

[5] V. Jones, V. S. Sunder *Introduction to Subfactors*, Cambridge University Press (1997).

[6] R.S. Pierce *Associative Algebras (Graduate Texts in Mathematics)*, Springer-Verlag (1982).

[7] B.L. Van der Waerden *Algebra*, Springer-Verlag (1991).

